Release Notes for *Cisco Policy Suite* for Release 7.0.1

First Published: January 28, 2015
Last Updated: July 10, 2015
Release 7.0.1

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 "Related Documentation" section on page 37.

This document includes the following sections:

- Introduction, page 1
- New and Changed Information, page 2
- Installation Notes, page 12
- Limitations and Restrictions, page 19
- CDETS, page 27
- Related Documentation, page 37
- Obtaining Documentation and Submitting a Service Request, page 38

Introduction

The Cisco Policy Suite (CPS) is a comprehensive policy, charging, and subscriber data management solution that allows service providers to control and monetize their networks and to profit from personalized services. The Cisco Policy Suite has the following components:

- Policy Server (PS)
- Charging Server (CS)

Cisco Systems, Inc.
www.cisco.com

- Unified Subscriber Manager (USuM)
- Subscriber Analytics

The Cisco Policy Suite provides an intelligent control plane solution, including southbound interfaces to various policy control enforcement functions (PCEFs) in the network, and northbound interfaces to OSS/BSS and subscriber applications, IMSs, and web applications. The Cisco Policy Suite modules are enabled individually or deployed as an integrated end-to-end policy, charging, and service creation solution.

Competitive Benefits

The new Cisco Policy Suite solution provides these benefits over competitive solutions.

- Cisco Policy Suite architecture allows simultaneous sessions and transactions per second (TPS) capacity to be independently scaled (For more information, refer to *CPS 7.0.1 Mobile Configuration Guide* and *CPS 7.0.1 Installation Guide*). This allows Cisco Policy Suite to be efficiently sized for both high simultaneous sessions with low TPS or low sessions with high TPS, resulting in lower total cost of ownership when compared to traditional PCRF models. As soon as sessions are bound to a given processing node, the ability to handle traffic spikes is reduced.
- Cisco Policy Suite virtual architecture supports flexible and cost-effective carrier grade strategies. Virtual instances are spread across multiple blade serves for full hardware and software redundancy within a Cisco Policy Suite cluster.
- The flexible nature of the Cisco Policy Suite lets a service provider go beyond standard policy definition to add new, customized functionality. It provides unified APIs which allows provisioning. Customized or vendor scripting is not needed, which allows service providers to create plug-ins within the existing policy server and automatically exposes the new services to the policy engine.

New and Changed Information

This section describes the new and changed features for the Cisco Policy Suite Release 7.0.1.

New Software Features in 7.0.1

The following features have been added in Release 7.0.1:

- AF Application-ID Validation
- Application Driven default Bearer QoS
- Best Match Table Logic (Ancient Trees)
- Diameter Retries
- Hour Boundary RAR Enhancement
- PBJ API
- CPS Recovery Control
- Quota Based Services
- Rsyslog Log Processing
- Rx PCC Rule Flow Direction Behavior
- Secondary Key Ring Feature
- Security Enhanced Linux

- SPR Revalidation
- SNMPD Configuration for Memory
- Table Driven Rules

AF Application-ID Validation

Old behavior:

On the Rx interface, CPS accepts all valid AARs irrespective of whether the Af-App-Id is recognized by CPS or not. There was no configuration to provide allowed AF-App-Ids.

New behavior:

A new configuration is introduced in the Rx Profile configuration which allows operator to define allowed Af-App-Id/Apn/Media-Type combinations. When CPS receives a new AAR, it validates the AAR against this configuration. If validated, the AAR is accepted and processing is done as earlier. If validation fails, the AAR is rejected with REQUESTED_SERVICE_NOT_AUTHORIZED (5063) experimental code.

By default, the AF Application-ID is not configured and hence all AAR's are accepted.

Impact on Customer:

Customers who do not need validation can skip configuration of valid Af-App-Ids.

Application Driven default Bearer QoS

On receipt of an Application-Start trigger on Sd Interface, CPS informs the PCEF via an RAR having a Charging rule containing Default Bearer QoS that is appropriately derived.

Best Match Table Logic (Ancient Trees)

The custom reference data tables support a capability labeled “best match”. If a table is marked as “best match” then all operators are ignored and a table search is executed using the following algorithm:

1. Search Key Columns recursively from top to bottom as defined in the table definition.
2. Retrieve the value of a column as a string. If no value is found then set the value to “*”.
3. Return the first result set that matches using the following search rules:
   a. Search for an exact match.
   b. Search for a regular expression match. A regular expression match is defined as a cell with a value that starts with “match=”. After the match “match=” string the regular expression is defined. The system uses the regular expression pattern rules defined in http://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html.
   c. Search for a value of “*”.
4. If a value is found, then continue searching to the next key level OR if all keys are searched return the result set for that row.

Diameter Retries

For CPS application originated traffic such as RAR's, CPS supports a customer configurable parameter to enable retries and enable a configurable number of retries.

For example, when CPS initiates a RAR request to the PCEF and no response is received from the PCEF within the timeout period configured (default timeout is 3 seconds), then CPS resends the RAR request (default number of retries are 1).

CPS supports the following:

- User is able to configure retry count and timeout.
- User can disable diameter retry feature.
- By default, CPS supports diameter retry feature with retry count as one.

Diameter retry feature is for those requests which are initiated by CPS. To support diameter retry requirements, CPS resends the request again when there is no response within configured timeout.

Hour Boundary RAR Enhancement

Old Behavior

Previously, when RAN congestion was configured, at the hour boundary there was a check for congestion level change. If the congestion level changed, then an RAR was sent in which new rules corresponding to changed congestion level were applied.

The next evaluation time for session was set to the time when the congestion level changes next. At that hour boundary again the session was evaluated, and new rules applicable to changed level were applied.

Since all the sessions were getting re-evaluated at applicable hour boundaries where the congestion level changes, there was a possibility of a large amount of RARs being generated by CPS. In cases where a combination of RAN congestion and HTTP optimization use cases were both present, this could lead to a condition of RARs being generated towards both the SAE-GW(NSN) and the F5 gateway.

CPS can generate this load of RARs without any issues as it is distributed among the CPS VMs. But there seems to be a limit on number of RARs which can be supported by other network elements.

New Behavior

To prevent RAR burst at the hour boundary, CPS can evaluate configured services for next hour based on the appropriate congestion levels for next hour and pre-install the rules specifying activation/de-activation times.

PBJ API

The Policy Builder with JSON (PBJ) API provides an alternate method of accessing and updating Policy Builder configurations using JSON. This API can be used to Create, Read, Update, and Delete (CRUD) CPS Customer Reference Data Tables and columns and fields within a table.

The PBJ API components are now installed by default in the 7.0.1 release.

For more information about this API, refer to the *PBJ API* chapter of the *CPS Operations Guide*.

CPS Recovery Control

CPS includes new functionality to allow the system to gracefully recover from unexpected outages. Due to the operational inter-dependencies within the solution, it is necessary for some software components to become active before others.

CPS can now inspect the state of the system from the pcrfclient VMs and, if necessary, inhibit the start of certain processes if the appropriate state has not been detected. By default, this functionality is disabled.

This functionality can be enabled by setting the **cluster_state_monitor** option to **true** in the CPS Deployment Template (Excel spreadsheet).

The monitoring system reports the state of the system as an integer value as follows:

Cluster State	Description
0	unknown state/pre-inspection state
1	lbvip02 is alive and all DBs in /etc/broadhop/mongoConfig.cfg have an accessible primary
2	lbvip02 port 61616 is accepting TCP connections
3	at least 50% of backend QNS processes are alive

In addition to the monitoring functionality, there is new functionality which inhibits the startup of some of the CPS solution pending the appropriate state. This behavior is optional on a per-VM basis, but it requires that the cluster monitoring be enabled to function at all.

To enable this behavior on a given VM, create a /etc/broadhop/cluster_state file. This can be done by issuing the following command:

```
# touch /etc/broadhop/cluster_state
```

To apply this functionality across the entire deployment, execute the above command on the Cluster Manager VM and use the **syncconfig.sh** script to push those changes out to the other VMs.

To view the current cluster state, refer to the **/var/run/broadhop.cluster_state** file.

Quota Based Services

CPS supports remaining quota to be generated in Event Data Record (EDR) at session start and stop. This works with both time and volume quotas.

To support the amount remaining, CPS uses the existing amount field from the MSBMCreditStatus class. This amount field indicates the volume (bytes) remaining in case of volume quota and time (seconds) remaining in case of time quotas.

A new parameter *quotaExpirationTimeRemaining* has been added to provide information on the time left for the balance to expire. This field is added in **MSBMCreditStatus** class.

By default, *quotaExpirationTimeRemaining* is configured to -1, which means the quota never expires or does not have any end date. In other cases, it can configured to the **quota credit end date minus the current time**. The value must be in seconds.

quotaExpirationTimeRemaining must be configured whenever it is necessary to query the subscriber account for balance.

Rsyslog Log Processing

Rsyslog Overview

Enhanced log processing is provided in this release using Rsyslog.

Rsyslog logs Operating System (OS) data locally (`/var/log/messages` etc.) using the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*conf` configuration files.

On all nodes, Rsyslog forwards the OS system log data to lbvip02 via UDP over the port defined in the `logback_syslog_daemon_port` variable as set in the CPS Deployment Template (Excel spreadsheet).

To download the most current CPS Deployment Template, refer to the Additional Notes section.

Refer to http://www.rsyslog.com/doc/ for more details and Rsyslog documentation.

Rsyslog-proxy

A second instance of Rsyslog called Rsyslog-proxy is installed only on AIO and LB nodes. Rsyslog-proxy is only installed if the `syslog_managers_list` variable is set in the CPS Deployment Template.

Rsyslog-proxy is the main log forwarding process as set up by the `/etc/rsyslog-proxy.conf` file.

- It receives OS system log data from all the nodes via UDP over the PORT defined in the logback_syslog_daemon_port variable. The default port number is 6514.
- It receives all CPS log data via UDP over the PORT defined in the logback_syslog_daemon_port variable. The default port number is 6514.

  The `/etc/broadhop/controlcenter/logback.xml` file on pcrfclients or `/etc/broadhop/logback.xml` file on AIO is configured to send logs to rsyslog-proxy via UDP using the logback SyslogAppender. See Configuration of Logback.xml for more information.
- Rsyslog-proxy forwards the OS system log data and CPS log data to logstash via TCP on PORT 6513 with a UDP backup.
- Rsyslog-proxy does not log any data to local files because the rsyslog instance is already doing that.
- It receives CPS JSON formatted log data via TCP on PORT 5544. rsyslog-proxy forwards that to logstash via TCP on PORT 5543 with a UDP backup.
- It receives SNMP events via TCP on PORT 7546. rsyslog-proxy forwards that to logstash via TCP on PORT 7545 with a UDP backup.
- rsyslog-proxy sends all OS system log data and CPS log data to any number of remote servers via UDP. (Of course, the remote servers must be setup to receive traffic but that is not a part of the scope of this document.)

Configuration for HA Environments

Configuration of Rsyslog for High Availability CPS environments is performed using the CPS Deployment Template.

Refer to the following information available in the template tabs.

Configuration Variables

The following variables can now be set in the CPS Deployment Template:

- **syslog_managers_list** — space separated list of remote logging servers (tuple protocol:hostname:port). Only UDP is currently supported.
- **syslog_managers_ports** — comma separated list of the remote logging server ports (must match the ports in the syslog_managers_list).
- **logback_syslog_daemon_addr** — hostname of the internal UDP server that rsyslog-proxy runs to receive incoming logs from CPS and OS (defaults to lbvip02)
- **logback_syslog_daemon_port** — incoming port for rsyslog-proxy (defaults to 6514).

Note If the syslog_managers_list variable is empty, the rsyslog-proxy instance is not installed or configured.

Additional Hosts Tab

The following parameter can be configured in the Additional Hosts tab of the CPS Deployment Template file:

corporate_syslog_ip	syslog_manager	<IP ADDR>

Configuration Tab

The following parameters can be configured in the Configuration tab of the CPS Deployment Template file:

syslog_managers_list	udp:corporate_syslog_ip:<PORT>
syslog_managers_ports	<PORT>
logback_syslog_daemon_addr	lbvip02
logback_syslog_daemon_port	6514

- lbvip02 is the default address for logback to send data
- 6514 is the default port for logback to send data

Configuration for AIO

The Rsyslog-proxy configuration for AIO environment uses a custom “facts” file: `/etc/facter/facts.d/rsyslog.txt`

The same variables are used as in the CPS Deployment Template.

For example,

syslog_managers_list=udp:corporate_syslog_ip:514

syslog_managers_ports=514

logback_syslog_daemon_addr=lbvip02

logback_syslog_daemon_port=6514

On AIOs, you must add aliases to `/etc/hosts` for the remote servers as defined in the syslog_managers_list.

Configuration of Logback.xml

The `/etc/broadhop/controlcenter/logback.xml` file on pcrfclients or `/etc/broadhop/logback.xml` file on AIO is configured to send logs to rsyslog-proxy via UDP using the logback SyslogAppender.

Refer to http://logback.qos.ch/manual/appenders.html#SyslogAppender for the Syslog Appender documentation.

The following appender forwards all CPS logs to a remote server.

```
<appender name='SYSLOG' class='ch.qos.logback.classic.net.SyslogAppender'>
  <syslogHost>lbvip02</syslogHost><!--#SAP#-->
  <port>6514</port><!--#SAP#-->
  <suffixPattern>[qps] [%d{yyyy-mm-dd'T'HH:mm:ss.SSSZ}] %msg</suffixPattern>
  <facility>LOCAL0</facility>
</appender>
```

Rx PCC Rule Flow Direction Behavior

Old Behavior:

CPS derived the Flow-Direction AVP and included it in all Gx Rel10 or higher RARs under Flow-Information for Rx dynamic rules.

New Behavior:

A new configuration is added under Gx Client that enables operator to choose how flow-direction should be handled for Rx dynamic rules.

Three options are available:

1. Exclude flow-direction: The flow-direction AVP is always skipped.
2. Derive flow-direction: CPS derives the Flow-Direction AVP and includes it in all Gx Rel10 or higher RARs under Flow-Information for Rx dynamic rules. This is the default option.
3. 3GPP Gx Rel11 compliant: Flow-direction and flow-description are handled as per the 3GPP Gx 29.212 Rel11 specification.

Impact on Customer:

Customers requiring flow-direction behavior different from what CPS currently provides should select the proper option under GxClient in Policy Builder.

Secondary Key Ring Feature

In this release, CPS provides a high availability solution for secondary key to primary key mappings. These mapping entries are stored in memcached servers which accelerate access to entries when secondary key lookups are required. Examples of secondary key lookups include: framed ip, rx session id, imsi, msisdn.

Architecturally the solution is divided into the following components:

- Secondary Key Ring — A secondary key ring is a set of nodes that have a complete set of secondary key to primary key mappings. The secondary keys are partitioned using consistent hashing across the nodes within the ring to ensure an even distribution of the keys.

- Ring Set — Each node on a secondary key ring is called a ring set. A ring set can have 1 to many physical servers. Each server has an exact copy of the data stored for that node. Each additional server within a ring set increases the high availability capability of the system.

Using these component pieces, the system supports parallel searching of key mappings across the physical servers to find a specific entry. If a physical server is shutdown or becomes unavailable, the system automatically rebuilds the rings and remap the secondary keys to the primary keys when the server comes back online.

The system does not support the following scenario:

- Detecting if a ring is need of a rebuild due to issuing a flush_all command.

Key Ring Commands

The following commands are provided to support this new functionality.

Note Before implementing any of these commands, contact the Cisco AS team to discuss the optimal architecture for your CPS deployment.

All commands must be issued from a qns server.

Telnet to any qns machine on port 9091 to enter the OSGI console.

Creating a New Ring

To create a new secondary key (sk) ring with a given id:

createSkRing *ringid*

Note: This id must be numeric and the ring must initially be empty with no ring sets defined.

Example:

createSkRing 2

Adding a New Endpoint

This command assigns a set of servers to act as node on the cache ring. Each server will have an exact copy of the data. If a node exists in the ring with that id then it is replaced and the ring is automatically rebuilt.

setSkRingSet ringid setid cacheserver1:port[,cacheserver2:port,cacherverN:port]

Example:

setSkRingSet 1 1 sessionmgr01:11211,sessionmgr02:11211

Removing an Endpoint

This command removes a ring set from a ring. This triggers an automatic rebuild of the ring.

removeSkRingSet ringid setid

Example:

removeSkRingSet 1 2

Removing a Ring

This command removes a ring. Note: You cannot remove the last ring from the system.

removeSkRing *ringid*

Example:

removeSkRing 2

Triggering a Ring Rebuild

To trigger a rebuild of a secondary key ring with a given id:

rebuildSkRing *ringid*

Ring ids are numeric.

Example:

rebuildSkRing 1

To track the progress of a ring rebuild, refer to the following statistic:

skcache_ring[ring id]_entry_rebalance

Security Enhanced Linux

This release provides support for Security Enhanced Linux (SELinux).

Note You must use htpasswd based authentication instead of PAM based authentication for SElinux.

To enable SElinux:

Step 1 Update **/var/qps/config/deploy/csv/Configuration.csv** with the following information:

```
selinux,true,
selinux_state,enforcing,
selinux_type,targeted,
```

The following configuration shows SELinux disabled:

```
selinux,false,
selinux_state,disabled,
selinux_type,targeted,
```

Step 2 Import the new configuration using the following command:

/var/qps/install/current/scripts/import/import_deploy.sh

Step 3 Verify that the proper paths are available for custom puppet configuration:

mkdir -p /etc/puppet/env_config/nodes

Step 4 If **/etc/puppet/env_config/nodes/pcrfclient.yaml** does not exist, copy the existing pcrfclient node definition into the env_config nodes, using the following command:

cp /etc/puppet/modules/qps/nodes/pcrfclient.yaml /etc/puppet/env_config/nodes

Step 5 Create your new custom manifest '/etc/puppet/env_config/modules/custom/manifests/selinux_httpd_config.pp' for SELinux settings using below content:

```
cat modules/custom/manifests/selinux_httpd_config.pp
# == Class: custom::selinux_httpd_config
class custom::selinux_httpd_config (
) {

  if ('vmware' == $virtual and $::selinux == 'true' and $::selinux_state != 'disabled') {
    selboolean { "allow_httpd_mod_auth_pam":
      persistent => true,
      value => 'on',
    }
    selboolean { "httpd_setrlimit":
      persistent => true,
      value => 'on',
    }
    selboolean { "allow_httpd_anon_write":
      persistent => true,
      value => 'on',
    }
    selboolean { "httpd_can_network_connect":
      persistent => true,
      value => 'on',
    }

  exec { "chcon_var_log_graphite_web":
    command   => "/usr/bin/chcon -R -h -t httpd_sys_content_t /var/log/graphite-web",
    logoutput => 'on_failure',
    require => Package['graphite-web'],
  }

  }
}
```

Step 6 Validate the syntax of your newly created puppet script:

puppet parser validate /etc/puppet/env_config/modules/custom/manifests/selinux_httpd_config.pp

Step 7 Add a reference to your custom Puppet class 'custom::selinux_httpd_config' in **/etc/puppet/env_config/nodes/pcrfclient.yaml**

Step 8 Rebuild your Environment Configuration using the following command:

/var/qps/install/current/scripts/build/build_env_config.sh

Step 9 For new installations which enable SELinux, after the deployment of all VMs, you must restart the VM for the changes to take effect.

Step 10 For an existing deployed VM, after changing selinux_state (like disabled to enforcing, enforcing to disabled), you need to re-initialize setup using `reinit.sh` and restart the VM for the changes to take effect.

SPR Revalidation

This release now supports the ability to provision the interval when CPS should trigger an LDAP search query to fetch the most recent subscriber's profile. This ensures the most up to date policies are applied.

A new field (Profile Refresh Interval) is provided on the Additional Profile Data tab under Generic LDAP in Domain configuration. This value defines the interval after which CPS triggers an LDAP search request to retrieve the subscriber's profile for a particular network session.

This value must be entered in minutes. By default, this functionality is disabled (Profile Refresh Interval = 0).

SNMPD Configuration for Memory

SNMPD is an SNMP agent which binds to a port and awaits requests from SNMP management software. Upon receiving a request, it processes the request(s), collects the requested information and/or performs the requested operation(s) and returns the information to the sender.

Table Driven Rules

ASR5K supports handling of Service Group QoS and defines new Gx AVPs which are exchanged between PCEF and PCRF. Additionally CPS (PCRF) already supports various use cases related to PCC. Rules provisioning and usage monitoring control as defined in 3gpp specification 29.212. Also the new AVPs related to CISCO Service Group QoS are already supported in CPS.

This feature uses capabilities of Customer Reference Data tables and Search Table Group functionality of CPS.

CPS supports defining a Customer Reference Data table where in all sub-elements of Cisco QoS Group rules are possible to be configured with different values for each element. Also it is possible to group these rules under a logical group. The application at run time supports queries based on this configured logical group, and Search Table group, and is able to retrieve all applicable CISCO Service QoS Group rules and its sub-elements.

Installation Notes

Download Software

Download the latest software package available from:

http://software.cisco.com/download/release.html?i=!y&mdfid=284883910&softwareid=284979976&release=7.0.1&os=

Md5sum Details: e31a87854b472fdb79d1c10a0f14aa87 QPS_7.0.1.release.iso

This image can be used to perform a new installation as well as for upgrading an existing CPS system.

Feature Versions

The following table lists the component versions for the CPS 7.0.1 Release:

Component	Version
Core	7.0.1.release
Audit	1.4.1.release
Balance	3.4.1.release
Cisco API	1.0.0.release
Cisco CPAR	1.0.0.release
Control Center	3.4.1.release
Congestion Reference Data	1.2.1.release
Customer Reference Data	2.4.1.release
DHCP	1.4.1.release
Diameter2	3.4.1.release
Fault Management	1.0.1.release
ISG Prepaid	1.8.1.release
LDAP	1.5.1.release
Notifications	5.8.1.release
Policy Intel	2.2.1.release
POP-3 Authentication	1.4.1.release
RADIUS	3.3.1.release
Recharge Wallet	1.2.1.release
Scheduled Events	1.3.1.release
SCE	2.1.1.release
SPR	2.3.1.release
Unified API	2.3.1.release
Web Services	1.5.1.release

New Installations

To perform a new installation of CPS 7.0.1, follow these steps:

Step 1 Mount the ISO image to the Cluster Manager as described in the *CPS 7.0.1 Installation Guide*.

Step 2 Execute `install.sh` script from the `/mnt/iso` directory.

Step 3 Select the new installation option as described in the *CPS 7.0.1 Installation Guide*.

Upgrading an Existing CPS Installation

To upgrade from 7.x, refer to Chapter 4 of the *CPS Installation Guide*.

To migrate from 6.x, refer to Chapter 5 of the *CPS Installation Guide*.

Additional Notes

The following section contains some additional notes which are necessary for proper installation of CPS:

- User can download the CPS Deployment Template file from http://173.36.208.90/customers/template/7.0.1/Deployer-templates-MR-7.0.1.xlsm.

  User Name: template701

  Password: TemQps4Deoply#701

  This file is used to configure the deployment parameters.
- **CSCur86459**: A new retriever has been added that pulls the IPv6 Prefix value off the subscriber network session.
- As a result of the introduction of the Cluster Manager VM in the CPS 7.0 release, and associated changes to the installation and deployment process, support for the Deployment Management Console has been discontinued, and it is no longer part of the software distribution.
- Session Manager Configuration: After a new deployment, session managers are not automatically configured. `build_set.sh` needs to be executed to configure all the replication sets:

  From pcrfclient01, execute:

  /var/qps/bin/support/mongo/build_set.sh --*sessionmgrVM* --create**.

  Edit /etc/broadhop/mongoConfig.cfg file. Make sure all of your data paths are `/var/data` and not `/data`.
- By default, CPS is installed without the password being set for `qns` user. User needs to set it manually for the system, `change_passwd.sh` script can be used to set the password.
- If lb01 VM, confirm that the `/etc/broadhop/diameter_endpoint/jvm.conf` file has the following content:

```
JVM_OPTS="
-server
-verbose:gc
-XX:+PrintGCTimeStamps
-XX:+PrintGCDetails
-XX:+UnlockDiagnosticVMOptions
-XX:+UnsyncloadClass
-XX:+TieredCompilation
-XX:ReservedCodeCacheSize=256m
-XX:MaxPermSize=256m
-XX:PermSize=256m
-Xms512m
-Xmx512m
-XX:+AggressiveOpts
-XX:+UseLargePages
-XX:+UseCompressedOops
-XX:+UseParallelOldGC
-XX:-DisableExplicitGC
"
```

- Default gateway in lb01/lb02: After the installation, the default gateway might not be set to the management LAN, in that 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.

- Datastore name in the ESX server should not contain spaces. This fails the `jvalidate.py` test and so the user is not able to deploy VMs.
- **CSCur37107**: The POODLE issue (CVE-2014-3566) has been addressed by completely disabling SSLv3 in HAProxy.
- **CSCur77002**: When creating the Cluster Manager, instead of using the default E1000 adapter, select the VMXNET 3 driver from the **Adapter** drop-down list on **Create Network Connections** window. To improve network throughput for CPS. apply the same change to all other VMs in the cluster.
- **CSCus68676**: If a user selects the upgrade option when running install.sh, a new prompt is added for the user to pick the repository (in this example, configuration or run). If the user does not pick anything, the default is configuration.

```
read existing deployment data if exists...
collecting SM data...
collecting GEO data...
Please select the type of installation to complete:
1) New Deployment
2) Migration from pre 7.0 system
3) Upgrade from existing 7.x system
3
Upgrading...
Please pick a svn repository to backup the policy files [configuration]:
configuration/ run/
:configuration
```

Updating Customer Reference Data AVPs

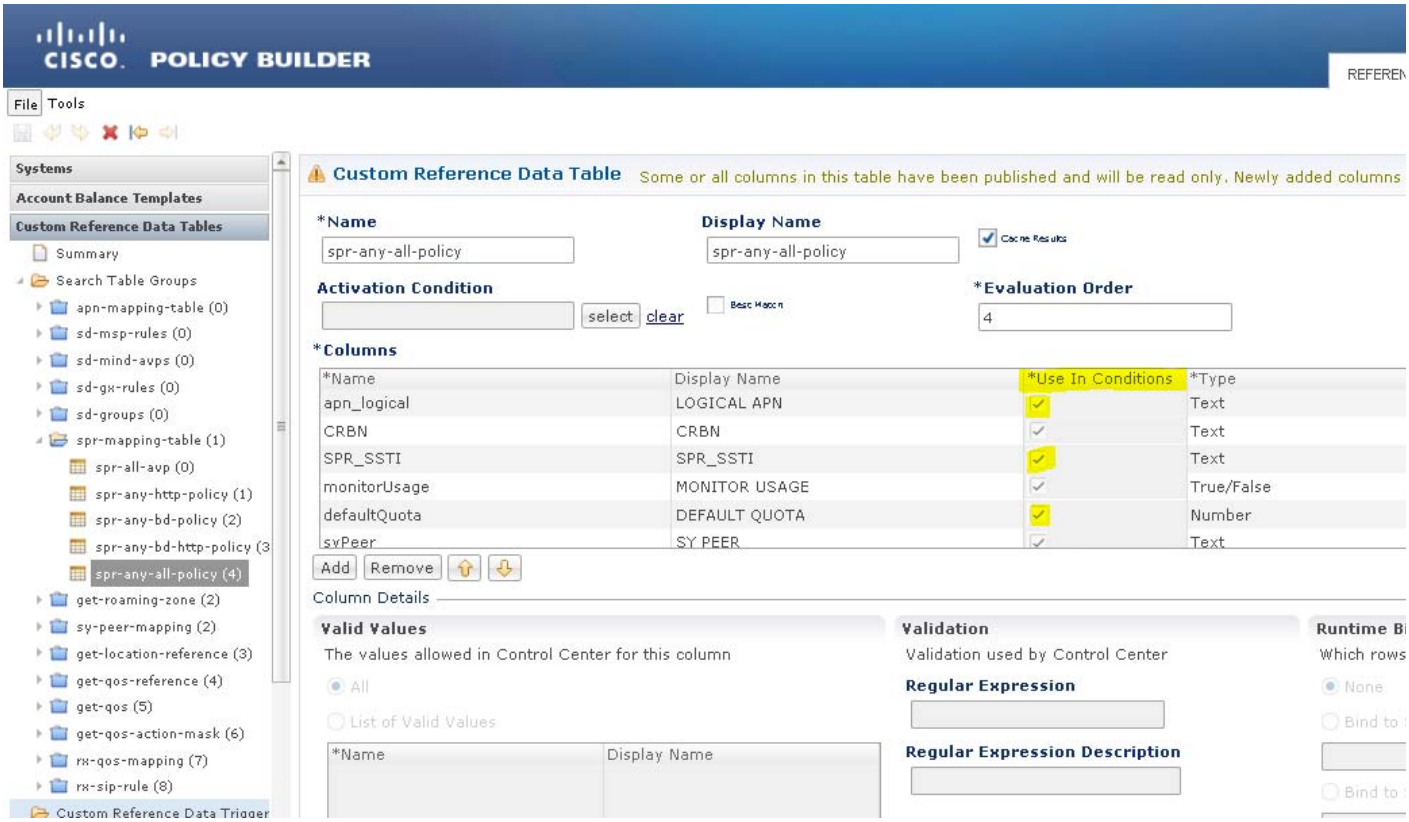
In the 7.0.1 release, existing Search Table Groups (STG) and Customer Reference Data (CRD) tables have been updated with a new ***Use in Conditions** option for CRD AVPs. This option is provided to maintain backward compatibility.

By default, this option is enabled for all AVPs in existing STGs and CRD tables.

For new deployments, the ***Use in Conditions** option is disabled by default.

To improve system performance, it is recommended to set this value to false (disabled) for all AVPs except those which are used as **Initiator conditions for STG evaluation** or **Initiator conditions in Use-Case Templates**.

The following screen shows the new ***Use in Conditions** option enabled in a CRD table:



CSCur08021 — Custom scripts are lost in the upgrade procedure

CPS has a mechanism to create custom puppet scripts that can be used during deployment. To create `backup_custom.sh` (example) and cron entry, perform the following steps on the Cluster Manager:

Step 1 Make sure that the proper paths are available:

```
mkdir -p /etc/puppet/env_config/nodes
```

Step 2 Install the necessary Puppet module if required:

```
$ puppet module install \
--modulepath=/etc/puppet/env_config/modules:/etc/puppet/modules \
example42-network
Notice: Preparing to install into /etc/puppet/env_config/modules ...
Notice: Downloading from https://forge.puppetlabs.com ...
Notice: Installing -- do not interrupt ...
/etc/puppet/env_config/modules
```

example42-network (v3.1.13)

For more information on installing and updating Puppet modules, refer to https://docs.puppetlabs.com/puppet/latest/reference/modules_installing.html.

Step 3 Create pcrfclient01 node definition. Here pcrfclient01 is an example. You can create other CPS node definitions also.

cat /var/qps/env_config/nodes/pcrfclient01.yaml

classes:

qps::roles::pcrfclient01:

custom::backup_custom:

Step 4 Create the `/var/qps/env_config/modules/custom/manifests/backup_custom.pp` file manifest.

For example, the manifest below creates a script in `/var/broadhop/scripts/backup_custom.sh` and sets up a cronjob to execute it every two hours:

```
class custom::backup_custom {
   file {'/var/broadhop/scripts/backup_custom.sh':
     ensure => file,
     owner => 'root',
     group => 'root',
     mode => '0744',
     content => '
#!/bin/sh -x
#Add your script logic content
',
     require => File['/var/broadhop/scripts'],
   }

   cron {'cron backup_custom':
     command => '/var/broadhop/scripts/backup_custom.sh > /var/tmp/backup_custom.log
2>&1',
     user => root,
     hour => x, # Where 'x' is a variable defining your network
                # requirements. For example, if you wan to take
                # the backup every 2 hours, then x should be 2.
     require => File['/var/broadhop/scripts/backup_custom.sh'],
   }
}
```

Step 5 Validate the syntax of your newly created puppet script(s):

$ puppet parser validate

/etc/puppet/env_config/modules/custom/manifests/backup_custom.pp

Step 6 Rebuild your Environment Config:

$ /var/qps/install/current/scripts/build/build_env_config.sh

Step 7 Reinitialize your environment:

$ /var/qps/install/current/scripts/updater/reinit.sh

At this point your new manifest (custom script) is applied across the deployment. For more details, refer to the Cluster Manager image in the `/etc/puppet/env_config/README`.

CSCur48114 — Publishing Policy Builder Takes Too Long

By default, CPS uses Pluggable Authentication module (PAM) based authentication for Subversion. PAM checks for every single file causing slow response for Subversion operations.To improve performance of Subversion operations (like publish from Policy Builder) use htpasswd based authentication instead of PAM based authentication.

To disable PAM based authentication and use htpasswd authentication for Subversion, perform the following steps:

Step 1 Make a backup of the **subversion.conf** file

```
cp /etc/puppet/modules/qps/templates/etc/httpd/conf.d/subversion.conf
    /etc/puppet/modules/qps/templates/etc/httpd/conf.d/subversion.conf.backup
```

Step 2 Modify **subversion.conf** to support htpasswd instead of PAM (update on installer VM):

```
# cat /etc/puppet/modules/qps/templates/etc/httpd/conf.d/subversion.conf
# Needed to do Subversion Apache server.
LoadModule dav_svn_module modules/mod_dav_svn.so
# Only needed if you decide to do "per-directory" access control.
LoadModule authz_svn_module modules/mod_authz_svn.so

<Location <%= @reposUrlPath %>>
    DAV svn
    SVNPath <%= @svnReposPath %>
    AuthName "SVN Repos"
    AuthType Basic
    AuthBasicProvider file
    AuthUserFile <%= @authFile %>
    Require valid-user
    AuthzSVNAccessFile <%= @userAccessFile %>
</Location>

<Location <%= @slaveUrlPath %>>
    DAV svn
    SVNPath <%= @svnReposPath%>
    Order deny,allow
    Deny from all
    Allow from ::1 127.0.0.1 <%= @masterSvnHost%>
</Location>
```

Step 3 Add SVN users in **.htpasswd** by executing the following commands and provide password (run on installer VM):

```
sudo htpasswd -m /etc/puppet/modules/qps/templates/var/www/svn/.htpasswd qns-svn
```

```
sudo htpasswd -m /etc/puppet/modules/qps/templates/var/www/svn/.htpasswd qns-ro
```

Step 4 Build puppet image by executing the following command (run on installer VM):

```
/var/qps/install/current/scripts/build/build_puppet.sh
```

Step 5 Re-initialize pcrfclient01/02 VM and restart httpd by executing the following commands:

```
ssh pcrfclient01 and run /etc/init.d/vm-init and service httpd restart
```

ssh pcrfclient02 and run /etc/init.d/vm-init and service httpd restart

Step 6 Restart CPS applications from installer VM.

Step 7 Verify setup by executing **diagnostics.sh** command from installer VM.

How to Apply the license to pcrfclient02

Currently, the license file for pcrfclient02 has to be manually copied. To copy the license file to pcrfclient02, perform the following steps:

Step 1 To generate the license file for pcrfclient02, repeat the steps used to generate the license file for pcrfclient01. For more information on generating license for pcrfclient02, refer to the section *License Generation and Installation* in *CPS 7.0.1 Installation Guide*.

Step 2 After pcrfclient02 is deployed, ssh into pcrfclient02.

Step 3 In pcrfclient02, modify the MAC address of the pcrfclient02 by editing the `/etc/sysconfig/network-scripts/ifcfg-eth0` file with the following line:

MACADDR=xxxxxx

where, MACADDR must be same as the MAC address in the license file but this MAC address must be different from the one from pcrfclient01.

Step 4 Restart the network service.

service network restart

Step 5 After restarting the network service, execute the following commands:

service lmgrd start

Limitations and Restrictions

This section covers the following topics:

- Limitations
- Common Vulnerabilities and Exposures (CVE)

Limitations

- If you have a system with 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 7.0.1 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 to cell congestion level when look-ahead rule is already installed:

  If a cell value changes for current hour or any of the look-ahead hours, there will be no change in rule for the rules which rules 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.
- Make sure the Cluster Manager's internal (private) network IP address can only be assigned to the host name “installer” in the `/etc/hosts` file. If this is not the case, backup/restore (`env_import.sh`, `env_export.sh`) can have access issues to pcrfclient01/pcrfclient02.
- In case of Geographical Redundancy solution where balance replication is configured, but session replication is not configured, quotas outstanding at time of failure event will be lost as usage information has not been reported from the PCEF for those grants which are pending at the time of the failure event. Outstanding reservations for impacted sessions are released (not debited from the balance).
- Balance EDR generation using the OSGi command line interface is not supported.

CSCur61904 –After VM is deployed, sometimes the memory is not reserved

Root Cause Analysis (RCA)

During the deployment of VMs (deploy_all.py and deploy.sh), make sure that vCenter is not managing the ESX servers that hosts the VMs. If vCenter is managing, the VM deployed will not have memory reserved.

Fix

During the deployment of VMs (deploy_all.py and deploy.sh), make sure that vCenter is not managing the ESX servers that host the VMs.

Result if not followed: For VMs with large memory size, if the memory is more than 100 GB, VM would not boot.

CSCus15225 – PBJ fails to initialize

Symptoms

A known issue occurs where the PBJ API does not fully initialize and errors are seen in the /var/log/puppet.log on pcrfclient01 and pcrfclient02.

Examples

```
[2014-12-11 16:29:54] Notice: /Stage[main]/Qps::Pbj/File[/etc/broadhop/pbj]/ensure:
created
[2014-12-11 16:29:54] Notice: /Stage[main]/Qps::Qps_java/Exec[Initialize
/etc/broadhop]/returns: executed successfully
[2014-12-11 16:30:02] Info: /Stage[main]/Qps::Qps_java/Exec[Initialize /etc/broadhop]:
Scheduling refresh of Exec[build_images.sh]
...
[2014-12-11 16:30:02] Notice:
/Stage[main]/Qps::Pbj/Qps::Pbj::Init_pbj_config_file[database.php]/Exec[initialize_pbj_con
fig_file database.php]/returns: cp: cannot create regular file
`/etc/broadhop/pbj/database.php': No such file or directory
[2014-12-11 16:30:02] Error: cp -f /var/www/html/pbj/app/Config/database.php
/etc/broadhop/pbj/database.php returned 1 instead of one of [0]
```

Workaround

Run **pupdate** on pcrfclient01/02 until no errors are seen (1-2 times).

CSCus50941 — qns startup script: /opt/broadhop/qns-1/plugins missing files

Symptoms

After upgrade (install.sh with upgrade option) finishes, when restartall.sh is run, some CPS nodes do not start the CPS process. This occurs if startall.sh is run right after reinit.sh or install.sh finishes.

Workaround

After install.sh or reinit.sh is finished, wait for 10 minutes before running restartall.sh. If the above error is still seen in a VM after waiting 10 minutes:

1. Run **diagnostics.sh** to identify which VM has the issue.
2. ssh to the VM.
3. Run **/etc/init.d/vm-init**

CSCus54189 — restartall.sh failed to start qns service sometimes

Symptoms

After running restartall.sh, the qns service on some VMs does not start. diagnostics.sh shows the qns service on the VM is not running.

Workaround

1. Run **diagnostic.sh** to determine which VM has errors.
2. ssh into the VM.
3. Run **service qns start**.
4. Run **service qns status** to make sure qns service is up.

5. Repeat steps 3 and 4 multiple times until the qns service is up.

CSCuo08815 — Gx TCP sessions take > 90s to re-establish upon lb switchover

Symptoms

Upon lb switchover by means of executing "shutdown -r now" at the active one, TCP sessions take over 90 seconds to re-establish on the standby.

Conditions

Default heartbeat/corosync send_arp fails to update ARP table of PCEF when gateway is not defined between PCEF and PCRF (i.e. lb01/02) and there are on same subnet. For example:

```
# /usr/libexec/heartbeat/send_arp -i 200 -r 5 -p
/var/run/resource-agents/send_arp-20.20.20.10 eth2 20.20.20.10 auto not_used not_used
ARPING 20.20.20.10 from 20.20.20.10 eth2
Sent 5 probes (5 broadcast(s))
Received 0 response(s)
```

Workaround

1. Add the following custom script **/etc/init.d/gxarp** on lb01 and lb02.

```
#!/bin/bash
#Replace eth2 to your Gx interface
#Replace 20.20.20.202 to your Gx VIP
#Replace 20.20.20.31 to your Gx client IP
arping -I eth2 -s 20.20.20.202 20.20.20.31 -c 3
```

2. Give execute permission to custom script.

```
chmod +x /etc/init.d/gxarp
```

3. Add gxarp (highlighted text) script as heartbeat resource (/etc/ha.d/haresources) on lb01 and lb02, which execute after gx VIP come up (when lb switchover occurs):

```
lb01 IPaddr2::20.20.20.202/255.255.255.0/eth2:0 haproxy gxarp
```

Common Vulnerabilities and Exposures (CVE)

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

Vulnerability	CVE Number	Summary	Technical Details
Pacemaker 1.1.10	CVE-2013-028	Pacemaker contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service condition on a targeted system. Updates are available.	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.
subversion-1 .6.11	CVE-2011-1752	Apple has released a security advisory and updated software to address the Apache Subversion Server mod_dav_svn denial of service vulnerability.	The vulnerability exists because the mod_dav_svn module fails to handle exceptional conditions when it processes the WebDAV and DeltaV protocols. An unauthenticated, remote attacker could exploit this vulnerability by transmitting crafted HTTP requests to the affected software. When the requests are processed, the mod_dav_svn module could dereference a NULL pointer, which may cause the affected software to terminate unexpectedly. Exploitation could result in a DoS condition.
	CVE-2010-3315	Apple has released a security update and updated software to address the Apache subversion server SVNPathAuthz security bypass vulnerability.	The vulnerability is due to an implementation error in the affected software's WebDAV module, mod_dav_svn, that is used to grant access to portions of a repository. As a result, when the value for the SVNPathAuthz directive in the mod_dav_svn module is set to short_circuit, the affected software does not honor access rules that contain a repository name prefix in the statement. his flaw could allow a user to bypass the access rules and access restricted repository content. An unauthenticated, remote attacker could exploit this vulnerability by submitting crafted requests to the targeted server. Exploitation could allow the attacker to read or write to certain restricted portions of the repository.
	CVE-2013-1968	Red Hat has released a security advisory and updated packages to address the Apache Subversion FSFS repositories newline characters corruption vulnerability. CentOS has also released updated packages to address the vulnerability.	The vulnerability exists because the affected software fails to validate the user-supplied filename while handling repository commits. An authenticated, remote attacker could exploit the vulnerability by using a filename that contains a newline character (0x0a) and is committed to a repository using the FSFS format. This could cause the files system to corrupt and may cause unresponsive service to subversion users.

Vulnerability	CVE Number	Summary	Technical Details
	CVE-2013-1849	Red Hat has released a security advisory and updated packages to address the Apache Subversion PROPFIND requests against activity URLs denial of service vulnerability. CentOS has also released updated packages to address this vulnerability.	The vulnerability is in the mod_dav_svn/liveprops.c source file due to insufficient validation of user-supplied request. The affected software may not properly process the PROPFIND requests on activity URLs on a targeted system, which could cause a memory corruption error when a request maps to an invalid URL. An authenticated, remote attacker could exploit the vulnerability by transmitting crafted LOCK requests to the targeted system. Successful exploitation could allow the attacker to cause a DoS condition.
	CVE-2013-1847	Red Hat has released an additional security advisory and updated software to address the Apache Subversion mod_dav_svn LOCK request against nonexistent URLs denial of service vulnerability. CentOS has also released updated packages to address this vulnerability.	The vulnerability is in the mod_dav_svn/lock.c source file of the SVN server module and is due to insufficient validation of user-supplied LOCK requests. The affected software could incorrectly execute a LOCK request against a URL for a nonexistent path or an invalid activity URL for the repository. This could lead to a memory corruption error, triggering the affected software to stop responding to legitimate requests. An authenticated, remote attacker could exploit the vulnerability by transmitting crafted LOCK requests to the targeted system. Successful exploitation could allow the attacker to cause a DoS condition.
	CVE-2013-1846	Red Hat has released an additional security advisory and updated software to address the Apache Subversion mod_dav_svn LOCK on requests denial of service vulnerability. CentOS has also released updated packages to address this vulnerability.	The vulnerability is in the mod_dav_svn/lock.c source file of the SVN server module and is due to insufficient validation of user-supplied LOCK requests. The module incorrectly processes LOCK requests on activity URLs to map commits to the repository, which could allocate invalid memory to activity URLs even though they should be rejected with the LOCK method. This could lead to a memory corruption error that may result in an unresponsive module process. An authenticated, remote attacker could exploit the vulnerability by transmitting crafted LOCK requests to the targeted system. Successful exploitation could allow the attacker to cause a DoS condition.
	CVE-2011-1783	Apple has released a security advisory and updated software to address the Apache Subversion SVNPathAuthz denial of service vulnerability.	The vulnerability exists because the mod_dav_svn module fails to properly process the SVNPathAuthz directive defined in the httpd.conf file when processing HTTP requests. If this directive is set to a value of short_circuit, the module erroneously enters into an infinite loop when querying for path-based authorization and consumes an overly large amount of memory resources. This behavior could be leveraged to prevent access to a Subversion server by using crafted HTTP requests. An unauthenticated, remote attacker could exploit this vulnerability by sending crafted HTTP requests to the targeted system. Processing such requests could consume excessive amounts of system memory, leading to a DoS condition on the server.

Vulnerability	CVE Number	Summary	Technical Details
	CVE-2011-0715	Apple has released a security update and updated software to address the Apache Subversion Server mod_dav_svn denial of service vulnerability.	The vulnerability is due to improper handling of lock token HTTP requests by the mod_dav_svn module used by the affected software. A lock token is a unique identifier that consists of long strings for each lock that grants exclusive access to one user to change a file. An unauthenticated, remote attacker could exploit this vulnerability by sending an HTTP request that contains a lock token to the affected software. When the request is processed, the mod_dav_svn module may dereference a NULL pointer, causing the affected software to terminate unexpectedly, resulting in a DoS condition.
	CVE-2013-2088	Apache Subversion contains a vulnerability that could allow an authenticated, remote attacker to execute arbitrary code on the targeted system. Updates are available.	The vulnerability exists in the contrib/hook-scripts/check-mime-type.pl script used in the affected software. The script fails to escape argv arguments starting with a hyphen to the svnlook utility and could cause an error in the script. Later, a different script, contrib/hook-scripts/svn-keyword-check.pl script is used to parse filenames from the output of the command, svnlook changed, and passes the output to a shell command. An authenticated, remote attacker could exploit this vulnerability by making crafted requests to the vulnerable scripts. If successful, it could allow the attacker to execute arbitrary shell commands on the targeted system.
	CVE-2013-2112	Red Hat has released a security advisory and updated packages to address the Apache Subversion svnserve remote denial of service vulnerability. CentOS has also released updated packages to address the vulnerability.	The vulnerability is in the accept() function call of the main.c source file of the affected software. While handling the TCP connection request, the affected function call performs insufficient checks on aborted connections and will treat them as critical errors, print an error message, and exit. This error could cause the affected process to stop responding to legitimate requests. An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted TCP requests to the targeted system. When a request is processed, it could cause the affected system to stop responding to legitimate users and cause a DoS condition on the targeted system.
	CVE-2011-1921	Apple has released a security advisory and updated software to address the Apache Subversion Server mod_dav_svn information disclosure vulnerability	The vulnerability is due to incorrect authorization of path-based file access subrequests by the affected software. The Apache authorization subsystem partially processes a subrequest, indicating whether a request was successful or unsuccessful with a status code. When processing certain crafted URLs, Apache could respond with a status code that could be incorrectly processed by the mod_dav_svn module to allow unauthorized access to protected resources. An unauthenticated, remote attacker could exploit this vulnerability by transmitting certain crafted HTTP requests to the system. If successful, the attacker could gain unauthorized access to sensitive information on the system.

Vulnerability	CVE Number	Summary	Technical Details
	CVE-2010-4644	CentOS has released updated packages to address the Apache Subversion svn commands remote denial of service vulnerability.	The vulnerability exists because the affected software improperly handles svn commands in specific repository files. The commands could cause a memory leak error when displaying the additional merge history of the repository files. An unauthenticated, remote attacker could exploit the vulnerability by executing the svn blame or svn log commands on the targeted system via the svn clients. An exploit could cause the application to consume available memory resources, which could cause the affected software to become unresponsive, resulting in a DoS condition.
	CVE-2013-1845	Red Hat has released a security advisory and updated packages to address the Apache Subversion mod_dav_svn excessive memory vulnerability. CentOS has also released updated packages to address this vulnerability.	The vulnerability exists within the mod_dav_svn/deadprops.c source file of the SVN server module due to insufficient validation of user-supplied request. Due to this flaw, the affected module could assign uncontrolled memory resources to module processes, while setting or deleting a large number of properties on a node (file or directory) in the SVN repository. This could lead to exhaustion of memory available to other module processes. An authenticated, remote attacker could exploit the vulnerability by transmitting crafted node modification requests such as PROPPATCH to the targeted system. A successful exploit could allow the attacker to cause the affected server to stop responding to legitimate users.
	CVE-2010-4539	CentOS has released updated packages to address the Apache Subversion Server SVNListParentPath denial of service vulnerability.	The vulnerability exists due to improper handling of user requests for displaying the Subversion repositories on an affected system. An unauthenticated, remote attacker could exploit this vulnerability by making crafted requests to display the Subversion repositories on the affected system. If successful, it could cause the affected system to stop responding to user requests, resulting in a DoS condition.
	CVE-2013-4505	Apache Subversion contains an issue that could allow an unauthenticated, remote attacker to cause a denial of service condition. Updates are available.	An issue in the mod_dontdothat component of Apache Subversion could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The issue exists because the mod_dontdothat component of the affected software fails to restrict REPORT requests from serf-based clients. An unauthenticated, remote attacker could exploit this issue to cause a targeted device to consume excessive amounts of system resources, resulting in a DoS condition. Apache has confirmed the vulnerability and released software updates

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=

This section covers the following topics:

- Open CDETS
- Resolved/Verified CDETS

Open CDETS

The following table lists the open CDETS in the CPS 7.0.1 release.

CDETS ID	Status	Headline
CSCup88212	A	Need to avoid overwriting Diagonistic.ini during upgrade
CSCuq05123	A	Missing Configuration for QPS Multi-node affecting auto launch of VM's
CSCuq22563	A	Enhance Diameter plugin logging
CSCuq53544	A	RAN Congestion use case RAR issue: one more EDR was generated.
CSCuq78140	A	Window Sizing parameters for Optimum Network Bandwidth
CSCuq79550	A	Portal admin does not load
CSCuq92782	A	release train archive is double-compressed
CSCur02781	A	Separate configuration export.
CSCur12843	A	too many APIs for the same account creates a RAR Issue
CSCur19570	A	Slow Policy calculator causing Performance degradation.
CSCur22765	A	Patch script inside of .tgz file does not have execute permission
CSCur48643	A	Missing: AWK to version 3.1.8 and Orchestration post install upgrade
CSCur49903	A	QNS: session* files are not present on pcrfclient01 after manual deploy.
CSCur50414	A	Kill behavior not set for QPS High Availability
CSCur59445	A	NPE observed in consolidated log on QPS request timeout
CSCur60705	A	GR: Authorization Failure Event on both sites
CSCur62128	A	/var filesystem is filled up after longevity test
CSCur68164	A	Call Model not shifted to other site all spr/session cache brought down
CSCur72536	A	init.log in OCTL VM not showing complete logs
CSCur73042	A	Errors in Diagnostic.sh and qns VM's when the system comes up

CDETS ID	Status	Headline
CSCus15225	A	PBJ fails to initialize
CSCus18168	A	Need to set cluster info in db during configuration of GR setup.
CSCus24935	A	\"Data store is not available\" error is observed during plain longevity
CSCus33071	A	send_diameter stat names: bulkstats uses dot, whisper uses underscore.
CSCus35531	A	observing continuous timeouts at PCEF after SPR failover to site2
CSCus37444	A	QPS sending wrong QCI value when VoLTE call is followed by MSRP session
CSCus37968	A	qps recovery control
CSCus38876	A	QPS re-sending IPME MESSAGE Charging Rule
CSCus50897	A	IPME 4G to 2G HO-Getting exception and error processing policy request
CSCus50941	A	qns startup script: /opt/broadhop/qns-1/plug-ins missing files
CSCus53093	A	Session removal issue during longevity
CSCus51416	A	While making a VoLTE call, QPS does not respond back for Rx-AAR message.
CSCur85551	O	Policy Intel Feature has issues writing CDRs
CSCus53821	O	QPS sending wrong QCI and no ARP during Multiple IPME MSRP

A - Assigned
N - New
O - Open

Resolved/Verified CDETS

The following table lists the resolved/verified CDETS in the CPS 7.0.1 release.

CDETS ID	Status	Headline
CSCur21116	C	US136 Shared Quota Not behaving as expected
CSCur26383	C	QPS sends Abort session request after receiving CCR-U
CSCur61162	C	SPR DB query taking longer
CSCus21117	C	GR: Unnecessary switches at PCEF
CSCus32646	C	QNS sends correct radius request - getting bad response (from phys IP).
CSCus53257	M	RAR processing from all VM take more time to process all shards
CSCuq95735	M	High Number of LDAP connections on Lb
CSCur08058	M	PCRF crashing PAS connection during continuous traffic
CSCur10821	M	PCRF Fails to start PAS peer connection
CSCur11946	M	CRD enhancement to support SGSNIP with subnet
CSCur30766	M	QPS overwrites the SY SSTI value with the one from the SPR table
CSCur37767	M	Sy-Prime - Threshold Breach Scenario not working as expected
CSCur44183	M	message null check in DiameterGyV8DeviceMgr.sendResponse.
CSCur44883	M	Sy-Prime Balance Template - Initiator Condition (Requirements)
CSCur58930	M	qps stops responding to updates during capacity test

CDETS ID	Status	Headline
CSCur64909	M	Unable to exclude Flow-Information AVP in CCAi message
CSCur75835	M	Custom AVP dictionary - Gx
CSCur77566	M	Sy Granted Service Unit (GSU) needs to be exposed as Session Retriever
CSCur79637	M	2 digit MNC support in QPS
CSCur81500	M	Support for input files for importing policy configuration
CSCus24027	M	MSRP handover from UTRAN to EUTRAN is not working
CSCus26038	M	FRD-Count of dedicated bearer setup requests sent by PCRF/per QCI
CSCus26045	M	FRD-Count of failed dedicated bearer setup received at PCRF per QCI
CSCus26051	M	FRD-Count of dedicated bearer requests at PCRF from P-CSCF per QCI
CSCus26064	M	FRD-Count of failed dedicated bearer sent by PCRF to P-CSCF per QCI
CSCus44945	M	QPS needs to use Service-URN as AF-Application-Id for E911 call
CSCup84467	R	QPS should send Disconnect-Cause: Rebooting in DPR when restarting
CSCup95322	R	Document setup for porting AIO PB config to HA PB
CSCuq15893	R	System group and user to allow limited and read-only ssh access
CSCuq16999	R	QPS: SNMP trap LicenseUsageThresholdExceeded not sent from any QNS VMs
CSCuq45638	R	Policy Execution Flow Analyzer feature docs
CSCuq50585	R	Add Logging to examine replication performance
CSCuq54942	R	CRD REST API _update creates multiple fields in existing key field
CSCuq56485	R	In Puppet syncconfig.sh takes more time
CSCuq56997	R	PB does not show correct data after restore svn data using env_import.sh
CSCuq57193	R	QPS not sending TSR with DRA
CSCuq60272	R	about.sh script Core Versions is not getting output
CSCuq63711	R	document how to configure: TACAC, build_set.sh
CSCuq67978	R	Optimistic Locking error observed for Wrapper API in GR Testing
CSCuq68974	R	slave PCEF CCR-I ignored by QPS when master session not created
CSCuq69001	R	By default Diagnostics should check VIP and Replica status
CSCuq72845	R	Diameter not installed by default in AIO when choosing \“mobile\” type
CSCuq73960	R	Schedule Detail empty fields in Control Center
CSCuq79536	R	Access Request Guard Timer not working
CSCuq85386	R	false mongo replica set alarm generated
CSCuq86942	R	Incorrect hostnames are listed in bulk stats
CSCuq87195	R	Gx.CCA-I not sent to PGW
CSCuq88720	R	Installing vPCRF on VLAN Based model of OpenStack is not supported
CSCuq90869	R	vminstaller upgrade should be non service interrupt
CSCuq94824	R	BHN - PMIPv4 TALs failing with duplicate constraint error
CSCuq94984	R	Publish to runtime \“run\” svn dir missing from AIO
CSCuq95395	R	No ARP for Rx dedicated bearer (no GBR)
CSCuq95596	R	Not able to disable iptables after import_deploy.sh
CSCuq98239	R	Feature com.broadhop.snmp is unable to start on GR Active-Standby setup

CDETS ID	Status	Headline
CSCuq98959	R	Redhook migration requires design decision on where to store the mgmt VM
CSCuq99330	R	Repository user credential is showed in the system process
CSCur02768	R	Compliance document for Gy (32.299) for R11
CSCur02776	R	QPS Rolling Restart
CSCur02785	R	Diameter retries.
CSCur02792	R	US3095 - SPR Revalidation (Time based events)
CSCur03960	R	Multiple issues in new QPS VM installer- fresh deployment
CSCur05661	R	QPS / evaluation for CVE-2014-6271 and CVE-2014-7169
CSCur07874	R	add a macro to create csv files for the excel template
CSCur08021	R	Custom scripts are lost in the upgrade procedure.
CSCur08395	R	An error occurred while creating a session, session may already exist
CSCur09263	R	NSCD cache not getting cleared in configure time-to-live
CSCur11614	R	TACACS+ technical specification for QPS 7.0
CSCur11620	R	Reboot of PRIMARY Sessionmgr cause QPS not to process incoming calls
CSCur12060	R	Sy SLR INTERMEDIATE_REQUEST not sent when no policy counter on service
CSCur12548	R	Haproxy Diameter config is not correct for stats
CSCur13421	R	On 7.0.0.4 AIO, session_count.sh is using wrong port to connect to mongo
CSCur14206	R	4 Diameter Outgoing connections to OCS instead of 1.
CSCur14440	R	Support for retrieving \“Network Requested Support\” AVP
CSCur17982	R	QPS is not sending LDAP Request to MIND (Intermittent Issue)
CSCur18079	R	Support for Redirect-Information AVP
CSCur18700	R	Invalid LDAP credentials, results in flood of authentication attempts
CSCur20411	R	QPS incorrectly encoding the Cisco Monitoring Key AVP(1066)
CSCur21715	R	support env_import, env_output
CSCur22589	R	With 580K subscribers the memory usage is 99% on the session manager
CSCur23442	R	Publish repository missing after applying new patch on HA setup
CSCur23661	R	service qns restart required after adding use case option-AIO
CSCur23701	R	DRA_Sy-Session failed if Next Hop Routing Table has entry for it.
CSCur25548	R	QPS SoC 29.212 needs updates - misleading information.
CSCur25793	R	SVN Synchronization between pcrfclient01 and pcrfclient02
CSCur28226	R	SN1-APN-Name AVP with Incorrect ID in QPS
CSCur28423	R	Documentation errors License Installation steps of Install Guide.
CSCur28522	R	QPS 7.0 (FCS) Does not send CCA-I to PGW
CSCur29540	R	Flow-Direction incorrectly calculated by the QPS-Gx R10
CSCur29797	R	QPS-7.0BackupandRestoreGuide.pdf need to be update
CSCur30135	R	Issue with PVI/PCI in QPS
CSCur30192	R	Session ID for Gx transactions and Sy transactions are different.
CSCur30295	R	Control Center using Secondary Reporting Database

CDETS ID	Status	Headline
CSCur30793	R	GR- if all qns are down,lb01/lb02 should be made down by qns
CSCur32170	R	TACAC - Timeout doesn't work and in turn keeps root user from logging in
CSCur32271	R	qns-su user not getting created on pcrfclient01/pcrfclient02
CSCur32503	R	PRIMARY Session Manager Failure
CSCur33330	R	Admin Db primary not shifting to Standby site post both prim lb failover
CSCur34104	R	QPS is not sending error when it gets incorrect AF_ID
CSCur34157	R	QPS Comprehensive Back-Up and Recovery Procedure
CSCur34935	R	lmgrd not automatically starting up on pcrfclient0X nodes.
CSCur35412	R	Flow-Status: 'Removed' in Gx message
CSCur35611	R	Comprehensive Alarm and KPI Documentation
CSCur36445	R	SNMP alarms don't work when networks are not reachable (ssh hangs)
CSCur37107	R	POODLE vulnerability fix for QPS platform
CSCur37387	R	QPS GUI Authentication
CSCur38384	R	7.0.0.5 Patch Broke the snmptrapd.conf on LB01 and LB02
CSCur38461	R	QPS doesn't support deployments that don't start with sessionmgr01
CSCur38711	R	Bulkstats documentation does not specify how multi pcrfclients work
CSCur38901	R	QPS - snmpd and snmptrapd do not start automatically.
CSCur40234	R	QPS Control Center cannot read cust_ref_data collections
CSCur40724	R	Enhancement for multiple Subscriber AVP code bindings on QPS
CSCur43692	R	update geo_mongoconfig_template
CSCur43841	R	RAR sent instead of ASR when removing the last installed Media component
CSCur43906	R	QPS is sending two ASR when Dedicated bearer is released by PGW.
CSCur43934	R	QPS is not supporting UNSUCCESSFUL_QOS_VALIDATION error
CSCur44195	R	MBR is sent lower than GBR
CSCur44716	R	Support for multiple LDAP values for an LDAP attribute on QPS
CSCur46310	R	build_shard.sh broken
CSCur47501	R	summaryall.sh having issue
CSCur47943	R	In-service patch installation is not possible in QPS
CSCur48114	R	QPS 7.0.0.5: Publishing Policy Builder Takes Too Long
CSCur48369	R	QPS fails to refresh BGAN FAP balance with 0
CSCur49102	R	QPS inot able to use the SdToggleConfiguration use-case
CSCur49128	R	Control Center SGSN IP table showing error
CSCur50980	R	HO sending charging_rule in RAR after enabling 2nd USUM load
CSCur53647	R	High rate of RAR in EDR
CSCur54022	R	QPS 7.0 Cluster-Manager /etc/broadhop/logback-debug.xml need correction
CSCur55889	R	sync_times.sh is broken due to sudoers configuration
CSCur55944	R	RxQoSDerivation is not correct if RxAppQoS and RxQoS both in service
CSCur56321	R	Stopall.sh leaves residue processes which needs to be cleaned manually
CSCur56347	R	QPS Incorrectly creates PreConfiguredRule

CDETS ID	Status	Headline
CSCur57536	R	LDAP Attributes Regex matching not working as expected
CSCur57565	R	QPS - Alarm for memory consumption > 80%
CSCur57660	R	clear, count and list_mongo_session scripts are not working properly
CSCur57841	R	Error sending message null reported by LB server
CSCur60023	R	Missing qns-admin and qns-su account when upgrading to 7.0.0.6
CSCur60796	R	GR: Stale session not cleared from the QPS after GR failover
CSCur61444	R	QPS sending Route-Record in all answers
CSCur61872	R	QPS includes Flow-Direction for pre-defined rules
CSCur61971	R	cloud init file sym link got removed
CSCur63468	R	CCR-U RAT-Type is not updating in session without Rat-type event
CSCur64529	R	seeing \"lb01 snmpd[4407]: error on subcontainer 'ia_addr' insert (-1)\"
CSCur64613	R	SNMP alarms not expected on QPS
CSCur66553	R	Add Support for Sy-Gx related AVP in session retrievers
CSCur66666	R	QPS did not generate any SNMP alarms when expected
CSCur66866	R	puppet fails to download and apply updated files
CSCur68154	R	Unable to reach performance targets for AT&T
CSCur70117	R	Installation of ISO is broken on HA setup
CSCur70510	R	SNMP traps dir should be moved out of /etc/broadhop
CSCur71105	R	The logic for ARP AVP is wrong for BOUND_ALL
CSCur72156	R	GR:PB configuration not accessible when active site is down
CSCur72882	R	Rx-RAR for successful resource allocation not sent
CSCur73213	R	QPS timing out valid LDAP search responses
CSCur75028	R	sudoers file clean up
CSCur75327	R	Unexpected VM Down/VM Up SNMP traps
CSCur75344	R	Undocumented SNMP Alert Raised: \“InvalidLicense\”
CSCur76876	R	Incomplete set of alarms raised for recovery of mongo replica
CSCur76919	R	Incomplete set of alarms raised when mongo arbiter is lost/recovered
CSCur77002	R	Change default interface driver in installer
CSCur77244	R	No trap for loss of sessionmgr
CSCur77299	R	Undocumented Alert Raised: \“ApplicationEvent\”
CSCur77413	R	Table Driven Rules
CSCur77416	R	Best Match Table Logic (Ancient Trees)
CSCur77419	R	US3521 - Document all QPS admin interfaces
CSCur77428	R	US4165 - API to CRUD tables, columns and fields in a QPS CRDT
CSCur78975	R	Custom AVP dictionary - Sy OSP grouping
CSCur79053	R	SNMP:- Restoring IP link does not clear link down trap
CSCur79957	R	Customer scripts were lost after upgrading to 7.0.0.6
CSCur80989	R	No hard limit to protect total session to go over DB limitation
CSCur81640	R	logstash causes high load averages on pcrfclient01/02

CDETS ID	Status	Headline
CSCur81649	R	SY PRIME RAR (with OSP change) does not trigger session update
CSCur82130	R	synchosts not working on 7.0.0.7 build
CSCur82802	R	Remote SPR Lookup based on IMSI/MSISDN prefix
CSCur82806	R	SPR Query from standby restricted to local site only (Geo aware query)
CSCur83380	R	CC does not search sub-account Names
CSCur83504	R	Flow direction AVP in Gx-RAR for VoLTE call
CSCur83718	R	No QPS backup and restore solution
CSCur84769	R	RAR processing from ALL VMs.
CSCur85933	R	haproxy is resetting the TCP connection continuously with pcrfclient01
CSCur85963	R	Grafana Timezone Mismatch Issue
CSCur86307	R	Customer Reference Data: Column bindings fail
CSCur86734	R	Internal user account need be be set as never expired
CSCur87623	R	reboot of one of QNS VM out of the two about 5% of the calls are failing
CSCur87688	R	Gy Use case Initiator APN input variable is not working
CSCur89670	R	run management scripts other than root account
CSCur90101	R	Deployment scripts doest not quote list varialbes
CSCur90145	R	Deployment script does not quote list variable
CSCur94791	R	QPS sends corrupt SY prime diameter packets under stress
CSCur94842	R	Remote Balance Lookup/Provisioning based on IMSI/MSISDN prefix
CSCur95130	R	Use in conditions on CRD columns should default to 'true'
CSCur95285	R	QPS - Alarm for memory consumption > 80%
CSCur95414	R	incorrect port numbers listed in v7.0.0.8
CSCur95482	R	Statistics not consistent across all QPS VM's
CSCur97458	R	Request to forward system and application logs to IT SMLS server
CSCur97851	R	QPS - CCR-T timeout statistic not reported, throws error
CSCur99247	R	Enhancements to Monitoring
CSCus00110	R	Sd CCA-u sent in response to Gx CCR-t in Sd scenario with Sy timeout
CSCus00120	R	Framed IP addr and IPv6 prefix not correctly encoded in Sd CCA message
CSCus00742	R	MTS QPS 5.5.2 Timeout template issue
CSCus03609	R	LDAP Statistics List and Description
CSCus04104	R	Wrong Access-Network-Charging-Identifier Openet Service Parameter
CSCus05757	R	statistics generated do not match documentation
CSCus06595	R	Policy Builder: When 'publish' is clicked 'null' exception is shown.
CSCus06871	R	Statistics counters for different session counts (Rx, Sy Prime, Sp, Sd)
CSCus06893	R	QPS sends RAR (via SPR validation) even when there is no change in LDAP
CSCus07448	R	Initiator Conditions not working for newly created templates and CRDs
CSCus08933	R	Clean-Up of Orphaned Sessions - QPS should notify peers of the cleanup
CSCus08954	R	Sy statistics have diameter cmd code in name instead interface name
CSCus09223	R	selinux_state set to enforcing but pcrfclient01 shows it as Permissive

CDETS ID	Status	Headline
CSCus13225	R	Call failed due to NullPointerException wiht patch r068113
CSCus13482	R	DIAMETER_UNABLE_TO_COMPLY when upgrading to Video call
CSCus14818	R	Update/Add/Delete/SwitchService APIs Optimistic Lock issue
CSCus14942	R	httpd service is not started on deploy.sh
CSCus15255	R	Graphite doesn't initialize on pcrfclient01/02 race condition
CSCus15328	R	session_coiunt.sh broken
CSCus15447	R	Two LBs have the same VIPs during migration
CSCus15494	R	cloud-init instance symlink missing on lb01 - system doesn't initialize
CSCus15502	R	syncconfig.sh should not overwrite /etc/broadhop/servers
CSCus15554	R	Gx retries counters are not available
CSCus15556	R	Sp retry counters are not available
CSCus16083	R	7.0.1 GR : Error processing policy request: key.cpp:433 and
CSCus17283	R	top_qps.sh should display date
CSCus17642	R	SVN repository does not exist after migrating pcrfclients
CSCus17651	R	Migrated sessionmgrs execute mongo scripts before mongo is installed
CSCus18842	R	Add support of SE-Linux
CSCus19527	R	RAR not sent after revalidation timer expires
CSCus19941	R	migrate_qps_6 tells users to stop corosync after migration
CSCus20496	R	qns user not able to login without password on the QPS components
CSCus21308	R	mongo_stat.sh script is causing lots of extraneous stats
CSCus22544	R	Migration does not properly support features/repos
CSCus23414	R	Memory Reservation when using vSphere client
CSCus24100	R	In Selinux Enforcing mode Grafana is not able to access the dashboards.
CSCus25173	R	QPS network MAC address mismatch
CSCus26696	R	We need to set Flow-Usage AVP to default value if not present
CSCus26937	R	GR: Incorrect diameter endpoints in haproxy config.
CSCus27735	R	QPS not able to delete session (java.util.HashMap) 5012 in engine logs
CSCus28708	R	Script needs to be enhanced to handle diameter proxies for lbs
CSCus32118	R	session sharding related information not there in the documentation
CSCus33990	R	QPS does not send rule changes in RAR message
CSCus33997	R	TACACS not working after 7.0.1 upgrade
CSCus34001	R	Initiators that check a policy derived AVP to be missing doesn't work.
CSCus37511	R	session_count.sh creating too many processes
CSCus37515	R	pcrfclient running above 80% CPU
CSCus40329	R	Script for active session count
CSCus41451	R	Failure of Memcached Servers Results in High Query TPS
CSCus41590	R	Rx-RAR is not sent to the AF for resource allocation failure
CSCus42366	R	Table driven attributes are not included in Sy STR messages
CSCus44300	R	QPS not sending ARP parameters during MSRP bearer establishment

CDETS ID	Status	Headline
CSCus47086	R	Unable to update Mongo Exprion on mongodb MongoExpirationQuery
CSCus54189	R	restartall.sh failed to start qns service sometimes
CSCus68676	R	Installer is trying to backup hardcoded SVN folder "repos/configuration"
CSCus15523	V	No SNMP traps generated when L3 LDAP connections are lost
CSCun29725	V	Basic GR Site outage GR failure trigger is failing
CSCuo95569	V	Insecure HTTP Method TRACE Enabled for Jetty Server
CSCuo95578	V	Missing Http Only Attribute in Session Cookie
CSCuo95601	V	Cross Site Scripting for the Credential field
CSCup92693	V	Operations documentation should describe shutting down each VM type
CSCuq03699	V	Primary sessionmgr shutdown result into instable Call Model no CCA
CSCuq09541	V	No login required to access Policy Builder and publish policies
CSCuq24743	V	LMGRD stop/restart doesn't work
CSCuq46505	V	built_set.sh script does not support more than 7 RS members addition
CSCuq47779	V	Incorrect flag values for APN-Aggregate-Max-Bitrate-UL/DL
CSCuq50564	V	deploy_all.py throws la license error
CSCuq50700	V	LDAP Search user Password should be encrypted
CSCuq53049	V	Policy Builder Rule Base Corruption
CSCuq55352	V	Mongo Session db reboots into STARTUP mode
CSCuq60309	V	pb gui access need authentication; default broadhop user be configurable
CSCuq60476	V	zip_debug_info.sh is not working as expected
CSCuq63299	V	Portal mongorestore errors out
CSCuq73883	V	get_replica_status shows incorrect LAG information
CSCuq75907	V	build_set.sh: monit shows Execution failed for mongod/'sessionmgr-portno
CSCuq76561	V	Diameter Gx is peer is not coming up between GGSN and 7.0 puppet QPS
CSCuq76656	V	ssh putty of 7.0 puppet installed VMs is not happen until iptables stop
CSCuq79312	V	PCRF sending 3002 with PAS peering
CSCuq86133	V	For Gx call, CCA-I is not sending back to GGSN after lb VMs reboot
CSCuq86932	V	bulk-stats.sh creating files with incorrect filenames in QPS7
CSCuq87593	V	Empty QoS information in CCA-I
CSCuq87988	V	QPS US3025 user story mirror functionality not working for Vulnerability
CSCuq88871	V	jhosts.py needs to handle empty entries in the json file.
CSCuq88934	V	QPS is not mapping Rx specific action 8 to Gx event trigger
CSCuq90892	V	LDAP connection up but no user query
CSCuq95424	V	Remove ApnAggMaxBitrate UL/DL from the RxSTGConfiguration object
CSCuq95593	V	reinit.sh is not working on all qps components (VMs)
CSCuq95998	V	set_priority.sh not setting DB priority for non voting SPR members
CSCuq97140	V	Unexpected behavior from syncconfig.sh
CSCur02309	V	RxProfile:support for reporting level and precedence
CSCur03181	V	TACACS configuration not successful in Cluster A

CDETS ID	Status	Headline
CSCur03355	V	CCA-U not sending QOS values whereas system calculates correct values
CSCur03804	V	Rx Dedicated Bearer QoS, Mirroring and Bounding -Additional Requirements
CSCur03949	V	Sy Prime additional Requirements
CSCur04958	V	Sessionmgr not monitored by Monit in PCRFCLIENT
CSCur04964	V	QNS Restart fails to start QNS Processes
CSCur05506	V	Unable to publish repository after upgrade to 7.0.0.4
CSCur07147	V	Unable to deploy VM's with Long name, File Too Long
CSCur07212	V	Puppet deploy not happening if the name of Arbiter is like sessionmgr09
CSCur08978	V	Arbiter details in Template
CSCur09239	V	TACACS user unable to login from console
CSCur10365	V	reinit and diagnostics should not use sessionmgrxx from Additional hosts
CSCur10828	V	PCRF Fails to start QNS features after patch apply due to Database Issue
CSCur10863	V	QNS processes fails to start on LB Servers
CSCur10915	V	Database Timer issue causing 3xxx error
CSCur11284	V	TACACS superuser privilege group not implemented
CSCur11292	V	No provision for TACACS user \"shared home directories\"
CSCur11893	V	TACACS uid definition deviates from AT&T requirement
CSCur11897	V	TACACS gid definition deviates from AT&T requirement
CSCur11957	V	TACACS admin user unable to run qns group commands
CSCur11985	V	AnGwAddress is not sent on SY prime AAR
CSCur12618	V	pcrfclient need load average threshold of 6
CSCur12822	V	Patching for platform changes
CSCur16079	V	Disable monitoring tab in Policy Builder
CSCur18048	V	Access Network Charging Address AVP is not decoded correctly by QPS
CSCur19783	V	LDAP health check not working
CSCur19840	V	LDAP connections established with LDAP server1 and 2 both
CSCur21573	V	Need to set sysctl parameters for data replication
CSCur21716	V	build_set.sh enhancement needed
CSCur26144	V	IPME Support for QPS.
CSCur26540	V	2 connection with Sy when 2 different policy published one after another
CSCur27855	V	\“Replica\” is spelled wrong in build_set.sh
CSCur28389	V	7.0.0.5 - all service start failed
CSCur29751	V	Support Configuration of multiple SNMP NMS configuration
CSCur29760	V	need cron job to restart collectd
CSCur29986	V	Incorrect output file in qps_users.pp
CSCur30812	V	Policy Directors Not getting started properly with qns restarts
CSCur37715	V	Sy-Prime - Rule Level Monitoring(1) support on QPS with Balance Mgr
CSCur44913	V	restartall.sh script is broken
CSCur46280	V	Sy-Prime Attribute retrievers in Policy Builder

CDETS ID	Status	Headline
CSCur48831	V	pystache isn't installed in upgrade from 7.0.0.4 to 7.0.0.6
CSCur49355	V	patch is not applied on lb01 while upgrading to patch build87
CSCur50169	V	QNS: \“/root/.ssh/known_hosts\” entry should automatically get updated.
CSCur50399	V	Call model not stable after SPR DB failover
CSCur50745	V	Diagnostics.sh looks for hosts in the QPS_OTHER_HOSTS section
CSCur56311	V	sync_times.sh summaryall.sh giving errors for uid on execution.
CSCur56987	V	Redirect URL and Sy Transaction ID is conveyed in STA message
CSCur57283	V	restartall.sh restarts services on diam-int*-lb* interfaces on active LB
CSCur57604	V	No traps generated when qns process goes down on qns VMs
CSCur58340	V	restartQpsServices.sh not starting haproxy-diameter service on lbs
CSCur62108	V	Unexpected AVP in Sy prime AAR
CSCur66665	V	Support for Multiple \“Subscriber-ID\” in Sy Template
CSCur70742	V	QPS should not remove rule before reinstalling.
CSCur72363	V	CCA-U not sent when the QCI from service option is null
CSCur74179	V	runonall.sh doesn't execute commands on sessionmgrs & portal hosts
CSCur76259	V	QPS doesn't include QCI & ARP for Sd Toggle dynamic rules
CSCur76662	V	QNS.conf GeoTagging should take precedence over PB Read preference
CSCur76679	V	Remote SPR provisioning should work from Site2 for failed Gr site1
CSCur78879	V	Disable mongo admin page display as it reveals version numbers
CSCur79834	V	Redirect URL not initialized with Default URL specified in Sy Template
CSCur80353	V	QNS: Puppet based QPS installation Guide needs update for migration
CSCur83376	V	CC search for sub account credential - No Subscriber Found
CSCur86459	V	Support for FRAMED_IPV6_ADDRESS retriever to send OSP in AAR on Sy'
CSCus01756	V	Add Support for GSU_STATUS retriever
CSCus01770	V	QPS should not send Usage-Monitoring-Info (GSU) in RAR to GW if Sy-GSU=0
CSCus15568	V	Result-Code: DIAMETER_APPLICATION_UNSUPPORTED (3007) in Sy RAA
CSCus26160	V	Remove cust specific information from congestion ref bulk load utility
CSCus33456	V	Wrapper API failing on site 1 and site 2 during longevity GR Option 0

M - More (The resolution is present in this patch release, but not yet included in the main branch.)

R - Resolved

V - Verified

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.

- *Cisco Policy Suite 7.0.1 Alarming and SNMP Guide*
- *Cisco Policy Suite 7.0.1 Backup and Restore Guide*
- *Cisco Policy Suite 7.0.1 Installation Guide*
- *Cisco Policy Suite 7.0.1 Mobile Configuration Guide*
- *Cisco Policy Suite 7.0.1 Operations Guide*
- *Cisco Policy Suite 7.0.1 Policy Reporting Guide*
- *Cisco Policy Suite7.0.1 Release Notes*
- *Cisco Policy Suite 7.0.1 Troubleshooting Guide*
- *Cisco Policy Suite 7.0.1 Wi-Fi/BNG Configuration Guide*

The documents can be downloaded from the following links:

- Common Guides: http://www.cisco.com/c/en/us/support/wireless/quantum-policy-suite-bng/products-installation-and-configuration-guides-list.html
- Mobile Configuration Guide + Common Guides: http://www.cisco.com/c/en/us/support/wireless/quantum-policy-suite-mobile/products-installation-and-configuration-guides-list.html
- Wi-Fi Configuration Guide + Common Guides: 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* at: http://www.cisco.com/en/US/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.

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