Release Notes for *Cisco Policy Suite* for Release 7.0

First Published: September 26, 2014
Last Updated: July 10, 2015
Release: 7.0

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 33.

This document includes the following sections:

Introduction

The Cisco Policy Suite 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)
- Application Gateway (AGW)

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. 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 a comprehensive open policy software development kit (SDK) using industry-standard languages and frameworks. 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.

New Software Features in Release *7.0*

The following features have been added in Release 7.0:

- Access Network Information
- Change Password Script
- CRD Enhancement
- Dedicated Bearer QoS Enhancements
- Grouping and Wildcarding for Realm based Routing Tables
- Message Session Relay Protocol (MSRP)
- Multiple Concurrent User Session Limit
- New Installer Cluster Manager (Shiprock)
- PCC Rule Switching based on Calendar Schedule
- Puppet - Introduction
- REST Technology between CPAR and CPS with JSON Interface
- Runtime Repository Password Encryption

- Scheduled Usage Monitoring
- Sd - Sponsored Data (Solicited Application Reporting)
- SPR Cleanup for Inactive Subscribers
- Subnet-based RADIUS clients
- Sy Prime Diameter Interface
- Corosync
- haproxy-diameter.cfg

Access Network Information

Cisco Policy Suite (CPS) provides Access Network Information (for example, User Location, User Timezone information and so on) Reporting over Gx and Rx Interfaces. In this feature, CPS supports ACCESS_NETWORK_INFO_REPORT Event-Trigger and specific-action on Gx and Rx interface respectively to provide the necessary Access Network Information.

When AF requests the PCRF for access network information, the PCRF (CPS) provides the requested Access Network Information to the PCEF within the Required-Access-Info AVP, which is included in the Charging-Rule-Definition AVP.

When the Access Network Information is available, the PCEF provides the required Access Network Information to the PCRF within the 3GPP-User-Location-Info AVP or 3GPP-MS-TimeZone AVP or both, as requested by the PCRF.

The PCEF provides the following information during an ACCESS_NETWORK_INFO_REPORT event trigger within the Event-Trigger AVP.

- 3GPP-User-Location-Info AVP (If available),
- User-Location-Info-Time AVP (If available),
- 3GPP-SGSN-MCC-MNC AVP (If the location information is not available)
- or 3GPP-MS-TimeZone AVP or both.

Change Password Script

By default, the password for the `qns` user in a multi-server environment is not set. To change the password a new script `change_passwd.sh` (`/var/qps/bin/support/`) has been added to set a password. The script changes the `qns` user password on all nodes: `pcrfclient`, `lb`, `qns`, and `sessionmgr`.

CRD Enhancement

CPS supports grouping of CRD tables, so look up can take place within that group based on the evaluation order. The already existing Customer Reference Data CPS feature is enhanced in order to support wildcarding. With the grouping of CRD support, CPS can:

- Bind the result from a table group.
- Set evaluation priority for tables within the group.
- Set evaluation priority between groups.
- Define default values for the groups.
- Restrict the use of table group based on initiator. (For example, use group A when = "IMS").

Dedicated Bearer QoS Enhancements

CPS supports the management of Default Bearer QoS attribute values for IP-CAN sessions by applying QoS-Bounding, QoS-Mirroring and QoS-Enforced on Default Bearer QoS.

- QoS-Bounding is the ability for the PCRF to calculate the minimum QoS between the Requested QoS (from the P-GW) and the Authorized QoS (based on internal computation of the Logic in the PCRF) and assign that in the response message back to the P-GW.
- QoS-Mirroring is the ability for the PCRF to mirror the same QoS values back that were being requested by the P-GW in the Request Message.
- QoS-Enforcement is the ability for the PCRF to enforce the Authorized QoS computed based on its internal logic back to the P-GW in the response message.

Grouping and Wildcarding for Realm based Routing Tables

CPS supports grouping of realms and application identifiers using wildcarding and assign to a group of next hop peers. CPS while trying to route a message should always select the peer with highest priority.

Message Session Relay Protocol (MSRP)

This feature provides support for the specialized UE clients for Instant Messaging (IM) like session and associated bearer modifications. This new feature supports the following:

- Modification of Rx Interface to support Vendor (CISCO) specific Media-Type AVP value of MESSAGE for creation of dedicated bearer for MSRP Traffic.
- PCRF to derive QCI and ARP values for dedicated bearer in accordance with AAR Request from AF with Media-Type MESSAGE and Gx-RAT Type as per configurations in Policy Builder.
- PCRF to support multiple MSRP sessions.
- PCRF provides support to provision MSRP Rx dynamic rules without MBR Attributes.
- MSRP Functionality is triggered using configuration option.

Multiple Concurrent User Session Limit

CPS control center supports displaying of error message if number of session for the 'x' user exceeds session limit. It also displays notification to the user when another user has logged-in with the same username as the previous user.

New Installer Cluster Manager (Shiprock)

The Cluster Manager is a server that maintains the system and application artifacts such as software and configuration for the CPS cluster. It is also responsible for deploying, installing/upgrading the software for the Virtual Machines in the CPS cluster.

The install.sh script that is shipped with the CPS ISO can be run to kick-off the new install or a software upgrade.

- Cluster Manager file system layout after install
  - All artifacts for a release: `/var/qps/install/current` changed to `/var/qps/install/7.0.0`
  - Tools: `/var/qps/bin` changed to `/var/qps/install/current/scripts/bin`

a. Deployment scripts

b. Build scripts

c. Control scripts

– Application Configuration: This includes the features file, like, `qns.conf` and `qvm.conf` files that are run time configuration files for the software.

`/var/qps/current_config` changed to `/var/qps/config/mobile`

`/etc/broadhop changed` to `/var/qps/current_config/etc/broadhop`

– Deployment Configuration: This includes configurations needed for the deployment and platform level configurations.

`/var/qps/config/deploy`: includes the csv files from the configuration template.

– Build Images: Based on the features files, images are built from the configurations and artifacts installed on the cluster manager to `/var/www/html/images`, and used later by deploying the CPS VMs.

The images in `/var/www/html/images` are downloaded to the VMs and again applied to the VMs using puppet.

PCC Rule Switching based on Calendar Schedule

CPS supports PCC rule provisioning feature over Gx interface. This feature is enhanced to incorporate schedules so that network operator can install specific rules on time-of-day basis. The current Charging-rule service-configurations (Pre-defined/Pre-Configured) in gx-session are added with Time-of-day schedules. CPS can look up the schedules on these rules and install those rules which have schedules matching current time. CPS can also perform a look-ahead and installs the rules that have schedules immediately after the current rule's schedule ends.

CPS supports the following features:

- Rule activation/deactivation time AVP must be added to scheduled PCC rules/rule bases/preconfigured rules.
- Switching rules/rulebases/preconfigured rules based on time.
- Look ahead one interval in schedule when provisioning rules/rulebases/preconfigured rules with schedules. If CPS doesn't receive any CCRu during the look ahead interval, trigger RAR at a random time in the look ahead interval to update rules.
- UE Time-zone (3GPP-MS-TimeZone) if available, takes precedence over PCRF time-zone.

Restrictions:

- The time value should be entered in hh:mm format.
- Charging schedule should be complete for 24 hours.
- First charging schedule should start at mid-night with start-time value as 00:00 and last schedule should end on next mid-night with end-time value as 23:59.
- Time entry with 23:59 is rounded-up to complete the 24 hour schedule.

Puppet - Introduction

In cluster manager, after the images are built, the VMs are deployed to the target ESX servers using the deployment scripts. After the VMs are deployed with base Linux image, the VMs are powered ON automatically.

After a VM is powered ON, it downloads the images files from the cluster manager. One of the downloaded images contains puppet scripts that are triggered to configure the VM.

Puppet is a tool designed to manage the configuration of systems declaratively. The puppet scripts for CPS can be found in the `/etc/puppet` directory in the target VM. An alias `pupdate` is defined in the VM, which is called in use cases such as new VM deployment, software upgrade, patching, etc. The scripts figures out the type of VM the target is running and applies different configurations to the VMs.

The puppet scripts in `/etc/puppet` configures system level settings such as haproxy, corosync (heardbeat), pacemaker (virtual IP addresses), IP tables, license directory, grafana, logstash, NTP, linux limits. Since puppet is a scripting language, it can be modified in the field. CPS provides a mechanism so Advanced Service can create custom puppet scripts. For more information, refer to https://docs.puppetlabs.com/guides/introduction.html.

REST Technology between CPAR and CPS with JSON Interface

Cisco Policy Suite (CPS) provides support to handle multiple Cisco Prime Access Registrar (CPAR) sessions over the REST interface. The Representational state transfer (REST) interface provides the endpoints for both the subscriber and the session having the capability to perform create, read, update and delete operations. CPS exposes the REST endpoints to perform CRUD operations on the session and the subscriber database as requested by CPAR server.

The session and subscriber databases are configurable in the Policy Builder. We use the HTTP methods to distinguish whether the request is for CREATE, READ, UPDATE or DELETE. The following table shows a mapping of the HTTP methods to the type of request and the operation received.

Runtime Repository Password Encryption

CPS supports encryption of the runtime repository password in `qns.conf`. You can use `genpassword` utility in `osgi` command to generate encrypted passwords.

By default the runtime repository password encryption feature is disabled. Password encryption can be enabled by setting the `-Dcom.broadhop.repository.credentials.isEncrypted` flag to true.

Scheduled Usage Monitoring

CPS supports Usage-Monitoring over Diameter Gx interface based on time-of-day schedules with different Balance Code, Dosage and rate across the schedules. To support scheduling, CPS uses Monitoring-Time AVP in Monitoring information. To use Monitoring-Time AVP, CPS supports Usage Monitoring Congestion Handling (UMCH) feature on Gx.

The current Usage-Monitoring information in the Gx session is added with monitoring schedules to grant and track the usage for the PCEF, based on current and adjacent schedules. It also provides support to bind different balance code to each schedule. CPS grants, reserves and charges the respective balance as per the usage monitoring schedule defined.

CPS defines dosage on each schedule and accordingly grant single units to PCEF in Granted-Service-Units AVP. It also defines charging rate on each schedule. The default charging rate is 1. This feature also provides support to configure multiple schedules in monitoring-key service configuration.

Sd - Sponsored Data (Solicited Application Reporting)

CPS supports following two flows for Solicited Application Reporting:

- Report Usage of 3/5-Tuple rule.
- Suppress Usage of 3/5-Tuple Rule

CPS has customized support for Sponsored Data over Sd interface with TDF. Using this customization, CPS receives Sponsor details over Sd interface and either monitors or suppresses Usage over Gx interface. The usage monitoring key is provided as an independent service option that has to be supplied with appropriate conditions within Use case initiators to either suppress or to be sent to the PCEF.

SPR Cleanup for Inactive Subscribers

When a subscriber is found to be idle for a period of time due to expiration of services or insufficient account balances and so on, CPS marks the subscriber as inactive and removes it from the database. Cisco Policy Suite (CPS) provides an automated mechanism to cleanup inactive subscribers from the database eliminating the manual process.

CPS provides the SubscriberInactivity AVP to handle the mechanism.

Subnet-based RADIUS clients

CPS provides the capability to enter the Radius Client IP Address in CIDR (Classless Inter Domain Routing) notation instead of a single IP address. The same shared secret is used for all devices with IP Addresses lying within the IP range specified by the subnet defined. All Policy Enforcement Points such as WLC, ISG, ASR5K, ASR9K, MAG, IWAG, etc. are provided with the ability to define Subnet based RADIUS clients sharing the same secret.

To implement the Subnet based RADIUS client mechanism, the Policy Enforcement Point is configured in the Policy Builder.

Sy Prime Diameter Interface

Cisco Policy Suite (CPS) defines quota control policy over the Sy Prime Interface. The PCRF communicates with the Balance Manager over the Sy Prime Interface to fetch the quota details for a subscriber.

Balance Manager: The Balance Manager is an entity, which holds the account balance information of a subscriber.

The Sy Prime Interface is provided with suitable AVP's to process the communication between the PCRF and Balance Manager. The Sy Prime Interface supports the following scenarios between the PCRF and the Balance Manager during an incoming Gx call:

- Volume Threshold Breached
- SBP Session Pass Expiry
- SBP New Session Pass Purchase
- Mid-session Roaming
- Up-to-date Service Pass Usage for Subscriber
- Terminate Session on Demand

Corosync

In 7.0, corosync replaces heartbeat as the clustering daemon to handshake between lb01 and lb02 for arbitration. `/etc/corosync/conrosync.conf` file is generated by puppet scripts, which defines lb01/lb02 as the nodes in the cluster. Corosync uses pacemaker as the subprocess to assign lbvip01 and lbvip02 to lb01 and lb02. The puppet script `./modules/qps/manifests/vip.pp` determines the VIPs defined in the `/etc/hosts` file and calls pacemaker commands to assign the VIPs to lb01 and lb02 in `qps/var/broadhop/init_pacemaker_res.sh`. For more information, refer to `/usr/bin/pcs` for trouble shooting of the VIP assignment.

haproxy-diameter.cfg

In 7.0, the haproxy is still used in similar way as 6.1, but the `haproxy-diameter.cfg` is dynamically created by the puppet script when `pupdate` is run. The scripts that creates the haproxy configuration is `haproxy_diameter.pp`. If the deployment does not use VIP and haproxy to balance diameter traffic through LB, this is not required.

`haproxy_diameter.pp` assumes that the /etc/hosts file in the VM has hosts in the following format: diam-int1-xxx--yy, where xxx is lb01 or lb02 and yy is the port number. For each address found in the /etc/hosts file, it creates a entry in the haproxy-diameter.cfg file for the backend diameter endpoints. There are a few scenarios:

- Single Endpoint — This is defined by adding an entry to `AdditionalHosts` tab of the Excel spreadsheet. The HA Proxy binds to port 3868 on the defined IP for each host. Format of the hostname is *diam-int1-{hostname}*.

Hostname	IP Address
diam-int1-lb01	XXX.XXX.XXX.108
diam-int1-lb02	XXX.XXX.XXX.109

- Multiple Endpoint/Multiple Interfaces — This is defined by adding multiple entries to `AdditionalHosts` tab of the Excel spreadsheet. The HA Proxy binds to port 3868 on the defined IP for each host. Format of the hostname is *diam-int[1-4]-{hostname}*.

Hostname	IP Address
diam-int1-lb01	XXX.XXX.XXX.108
diam-int1-lb02	XXX.XXX.XXX.109
diam-int2-lb01	XXX.XXX.XXX.110
diam-int2-lb02	XXX.XXX.XXX.111

- Multiple Endpoint/Single Interface/Multiple Ports — This is defined by adding multiple entries to `AdditionalHosts` tab of the Excel spreadsheet. The HA Proxy binds to port 3868 through 3871 on the defined IP for each host. Format of the hostname is *diam-int1-{hostname}* for port 3868 and *iam-int1-{hostname}-[69|70|71]* for ports 3869, 3870 and 3871.

Hostname	IP Address
diam-int1-lb01	XXX.XXX.XXX.108
diam-int1-lb01-69	XXX.XXX.XXX.108
diam-int1-lb01-70	XXX.XXX.XXX.108
diam-int1-lb01-71	XXX.XXX.XXX.108
diam-int1-lb02	XXX.XXX.XXX.109
diam-int1-lb02-69	XXX.XXX.XXX.109
diam-int1-lb02-70	XXX.XXX.XXX.109
diam-int1-lb02-71	XXX.XXX.XXX.109

Additional Notes:

The haproxy configuration that is generated routes the requests to local endpoints where the diameter endpoints are anchored. In order to utilize this, the policy builder settings for diameter ports must be: to 3868 for haproxy server 1, 3878 for haproxy server 2, 3888 for haproxy server 3 and 3898 for haproxy server 4. For example, setting up two stacks on separate VIPs would require setting the two hosts settings: stack 1 to port 3868 and stack 2 to 3878.

```
diam-int1-lb01(3868) - base port defined in stack as 3868, 3869, 3870
diam-int2-lb01 (3868)- base port defined in stack as 3878, 3879, 3880
diam-int3-lb01(3868) - base port defined in stack as 3888, 3889, 3890
diam-int4-lb01(3868) - base port defined in stack as 3898, 3899, 3900
diam-int1-lb01-69(3869) - base port defined in stack as 3878, 3879, 3880
diam-int1-lb01-70(3870) - base port defined in stack as 3888, 3889, 3890
diam-int1-lb01-71(3871)- base port defined in stack as 3898, 3899, 3900
```

haproxy is used to perform least connection load balancing within a VM and does not load balance across a VM.

Installation Notes

This section describes the installation notes in Release 7.0.

Note Customer must download the latest software package available from the link http://software.cisco.com/download/release.html?i=!y&mdfid=284883882&softwareid=284979976&release=7.0&os=.

Feature Versions

The following table mentions the component version for CPS 7.0 Release:

Component	Version
Core	7.0.0
Audit	1.4.0
Balance	3.4.0
Cisco API	1.0.0
Cisco CPAR	1.0.0
Control Center	3.4.0
Congestion Reference Data	1.2.0
Customer Reference Data	2.4.0
DHCP	3.4.0
Diameter2	1.4.0
Fault Management	1.0.0
ISG Prepaid	1.8.0
LDAP	1.5.0
Notifications	5.8.0
Policy Intel	2.2.0
POP-3 Authentication	1.4.0
Radius	3.3.0
Recharge Wallet	1.2.0
Scheduled Events	2.1.0
SCE	1.3.0
SPR	2.3.0
Unified API	2.3.0
Web Services	1.5.0

Additional Notes

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

- Session Manager Configuration. After deployment of all VMs, session managers are not automatically configured. `built_set.sh` needs to executed to configure all the replication sets:

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

  edit /etc/broadhop/mongoConfig.cfg

  Make sure all of your data paths are `/var/data` and not `/data`. Stop all of the mongo services on the sessionmgrs and pcrfclient01 and delete /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 was not assigned with 24 GB memory, then `/etc/broadhop/diameter_endpoint/jvm.conf` in VM installer must be set to the following:

  JVM_OPTS="

  -server

  -verbose:gc

  -XX:+UnlockDiagnosticVMOptions

  -XX:+UnsyncloadClass

  -XX:+TieredCompilation

  -XX:ReservedCodeCacheSize=256m

  -XX:MaxPermSize=256m

  -XX:PermSize=256m

  -Xms1g

  -Xmx1g

  -XX:ParallelGCThreads=5

  -XX:+UseGCTaskAffinity

  -XX:+BindGCTaskThreadsToCPUs

  -XX:ParGCCardsPerStrideChunk=32768

  -XX:+AggressiveOpts

  -XX:+UseLargePages

  -XX:+UseCompressedOops

  -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.
- CSCuq55288: feature changed did not get updated by puppet. Updated only after few tries.
  - Update features in `/var/qps/current_config/etc_aio/broadhop/*/features`
  - Rebuild everything:

    $ /var/qps/install/current/scripts/build_all.sh

  - Touch the release-train package:

    $ touch /var/qps/install/current/release-train-*

  - Apply the updates using puppet:

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

- CSCuq79575:TACAC. If TACAC is enabled, by default all users will have to go through TACAC server. in order to use local PAM for certain users if they were not in TACAC server:
  - In `/etc/puppet/modules/qps/templates/etc/pam.d/tacacs`, make the following changes:

    -auth [success=done new_authtok_reqd=1 default=ignore] /usr/local/lib/security/pam_tacplus.so server=<%= scope::lookupvar('::tacacs_server') -%> secret=<%= scope.lookupvar('::tacacs_secret') -%> login=pap

    -auth requisite pam_deny.so

    -auth required pam_permit.so

    +auth sufficient /usr/local/lib/security/pam_tacplus.so server=<%= scope::lookupvar('::tacacs_server') -%> secret=<%= scope.lookupvar('::tacacs_secret') -%> login=pap

    +#auth requisite pam_deny.so

    +#auth required pam_permit.so

  - Run build_puppet.sh in installer.
  - From each VM, run /etc/init.d/vm-init
- When following the process to install license, user need to manually restart lmgrd.
- 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 traffics should be on different VLANs in VLAN.csv file at the time of deployment.
- CSCuq53049: Partial fix done to only allow generation of drool based code on PB change. However, original issue is still not reproducible in two different longevity setups.

  We also did multiple publishings but not able to reproduce the issue. CPS is able to read from the updated published files from PB.
- In 6.1, various OS were used in different VMs. In 7.0, all VMs are running on CentOS 6.5 and JDK 1.8.
- After Upgrade or patch, some VMs are not configured correctly. This only happens in large cluster environment.

  Fix:

  a. Modify the `reinit.sh` script so make the sleep to sleep(60)

  b. Run `reinit.sh`.

  c. Wait for VMs to be configured. (on average, give each VM 5 minutes)

  d. restartall.sh
- Datastore name in the ESX server should not contain spaces. This will fail the `jvalidate.py` test and not able to deploy VMs.

CSCuq83755 — Policy builder is losing repositories

Root Cause Analysis (RCA)

We have hapoxy load balancer which forwards request to Policy Builder server on pcrfclient01. If it is not available, then it forwards the request to backup server on pcrfclient02.

Consider pcrfclient01 is up and we added new repository from PB GUI. This repository gets saved on pcrfclient01 (on file at `/etc/broadhop/pb/policyRepositories.xml`, `/etc/broadhop/pb/publishRepositories.xml`).

After sometime if because of some reason pcrfclient01 is not accessible, haproxy sends request to pcrfclient02 where it does not find the above mentioned two files (`publishRepositories.xml`, `policyRepositories.xml`) and does not display any repository on PB GUI.

Fix

Currently, we are not supporting automatic synchronization of the two repository files (`/etc/broadhop/pb/policyRepositories.xml`, `/etc/broadhop/pb/publishRepositories.xml`).

Manually copy the two files from pcrfclient01 to pcrfclient02 or vice versa.

CSCuq02899 — create_policy_builder_user.sh does not add read-only user

In 7.0 puppet based installation, we are not supporting `create_policy_builder_user.sh` script. Also user authentication is happening by linux pam.

Fix

To create a new user, perform the following steps:

Step 1 Create linux user by executing the following command:

- useradd -M admina

Step 2 Change password for newly created user:

- passwd admina

Step 3 To provide access to the user, edit the file `/var/www/svn/users-access-file` and enter username against admins for read/write access or enter against nonadmins to provide read only access.

Sample file:

```
[groups]
admins = broadhop, admina
nonadmins = read-only, test,
[/]
@admins = rw
@nonadmins = r
```

CSCuq92634 — Subversion synchronization not working

Fix

To fix this issue, perform the following steps:

Step 1 Delete the svn repository on pcrfclient02:

$ rm -rf /var/www/svn/repos

Step 2 Create a blank repository on pcrfclient02:

$ svnadmin create /var/www/svn/repos

Step 3 Copy the attached file to pcrfclient02:/var/www/svn/repos/hooks and give it execute permission:

$ chmod +x /var/www/svn/repos/hooks/pre-revprop-change

Step 4 Give apache permissions to the new repo on pcrfclient02:

$ chown -R apache:apache /var/www/svn/repos

Step 5 Configure the new repository for synchronization by running this from pcrfclient01:

$ svnsync init http://pcrfclient02/repos-proxy-sync http://pcrfclient01/repos

Step 6 Perform the initial sync by running this from pcrfclient01:

$ /usr/bin/svnsync sync http://pcrfclient02/repos-proxy-sync

CSCuq79550 — Portal admin does not load

Fix

Execute the following commands:

chown apache:apache /etc/broadhop/portal/broadhop.php

chmod 2770 /etc/broadhop/portal/broadhop.php

CSCuq93367 — default sessionmgr deployment should not create the set0 init.d scripts

Root Cause Analysis (RCA)

During an upgrade, the seessionmgr (`/etc/inti.d/sessionmgrxxx`) scripts are always replaced by default set0 and 27717 scripts.

Fix

Manually change the `/etc/init.d/sessionmgrxx` scripts with the set names and port numbers as specified in `/etc/mongoCfg` file.

Limitations and Restrictions

This section covers the following topics:

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 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 multivalued (e.g. Mind attribute acwentitlement), 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.
  - Mind AVP Table currently only supports OctetStringAvp value for AVP Data-type.
- about.sh does not report the correct URL for configured diameter ports.
- CSCuq17957: Datastore name in the ESX server should not contain spaces. This results in `jvalidate.py` test failure and you cannot deploy VMs.
- Balance EDR generation using the OSGi command line interface is not supported.

Common Vulnerabilities and Exposures (CVE)

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.

Vulnerability	CVE Number	Summary	Technical Details
	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 filesystem to corrupt and may cause unresponsive service to subversion users.
	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.

Vulnerability	CVE Number	Summary	Technical Details
	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.

Vulnerability	CVE Number	Summary	Technical Details
	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.
	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.

Vulnerability	CVE Number	Summary	Technical Details
	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.

Vulnerability	CVE Number	Summary	Technical Details
	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.
	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.

Vulnerability	CVE Number	Summary	Technical Details
	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

Caveats

The following sections lists Open Caveats and Resolved Caveats for Cisco Policy Suite. For your convenience in locating caveats 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 Caveats

Table 1 lists the caveats in the CPS 7.0 release.

Table 1 Open Caveats

CDET ID	Status	Headline
CSCuo30008	A	Usage monitoring disables bandwidth monitoring when quota is depleted
CSCuo46183	A	QNS: SNMP trap exception is observed in QNS log in HA setup .
CSCup66866	A	QNS: QNS does not send CCA with Result-Code: 5003
CSCup88212	A	Need to avoid overwriting Diagonistic.ini during upgrade
CSCup97303	A	.bin installer replace collectd types.db with incorrect types.db conts.
CSCuq14732	A	[Tenmile] High latency observed during performance testing.
CSCuq17078	A	QNS: If both GyProxy and RechargeWallet are configured, GyProxy not work
CSCuq17957	A	Puppet deployer won't deploy on datastores with spaces
CSCuq20981	A	SITE: SMS cases failing
CSCuq32146	A	[System-test] - QPS doesn't send all the rules in CCA-U
CSCuq36223	A	Mobile configuration binds all interfaces to lbvip01
CSCuq50720	A	URLs in about.sh are incorrect for AIOs
CSCuq53049	A	VFI 5.5.1 Patch2 longevity failed due to policy builder publish
CSCuq56997	A	PB does not show correct data after restore svn data using env_import.sh
CSCuq59300	A	refactor diagnostics.sh to help maintainability
CSCuq60476	A	zip_debug_info.sh is not working as expected
CSCuq63656	A	Puppet deployment causing issue due to build image failure(CSCuq63655)

Table 1 Open Caveats

CDET ID	Status	Headline
CSCuq63711	A	document how to configure: TACAC, build_set.sh
CSCuq63720	A	update installer guide on how to disable firewall/iptables
CSCuq67941	A	Config. files gets modified after reboot
CSCuq67978	A	Optimistic Locking error observed for Wrapper API in CLAB GR Testing
CSCuq68940	A	Session repository running out of space
CSCuq70967	A	approx 100% CPU utilization by java process on qns10 in MAS PROD .
CSCuq75907	A	build_set.sh: monit shows Execution failed for mongod/'sessionmgr-portno
CSCuq75916	A	build_set.sh: sessionmgr-portno should start/stop through monit
CSCuq76773	A	install.sh exits if an invalid option is selected
CSCuq77188	A	Fix issue in haproxy-diameter
CSCuq78140	A	Window Sizing parameters for Optimum Network Bandwidth
CSCuq79550	A	Portal admin does not load
CSCuq79588	A	If a user is authenticated against TACACS+ and not in local, create one
CSCuq79787	A	Loacl user allowed to login with auth fail from tacacs
CSCuq80659	A	Portal SDK is not available in 7.0 (VM Installer) puppet
CSCuq83478	A	IPV6 diameter peer
CSCuq86932	A	bulk-stats.sh creating files with incorrect filenames in QPS7
CSCuq92634	A	Subversion synchronization is not working
CSCuq93149	A	Errors in initializing portal VMs
CSCuq95708	A	Observed monitored processes in waiting state
CSCuq96759	A	Converting shiprock installer to AIO fails
CSCuq97140	A	Unexpected behavior from syncconfig.sh
CSCuq99332	A	diagnostics.sh not clean in an AIO
CSCuq55352	A	Mongo Session db reboots into STARTUP mode
CSCuq16039	N	Non HTTPS requests do not redirect for applications
CSCuq18210	N	Base VM corrupted
CSCuq24743	N	LMGRD stop/restart doesn't work
CSCuq27145	N	Puppet: new VMs have wrong installer IP in .ssh/known_hosts
CSCuq34020	N	Portal Configuration for AIO is on mongo port 27749
CSCuq48912	N	Unconfigured plugins in PB causing diagnostic errors
CSCuq50564	N	deploy_all.py throws la license error
CSCuq50709	N	QPS release/interim Patch Upgrade overwriting Authorized keys
CSCuq52648	N	HAProxy warnings in diagnostics.sh
CSCuq55292	N	default AIO features should include diameter
CSCuq56485	N	In Puppet syncconfig.sh takes more time
CSCuq63299	N	Portal mongorestore errors out
CSCuq63655	N	\"./initialize_qps.sh\" should remove image_map before get
CSCuq63716	N	need to document how to apply custom plugin in vminstaller

Table 1 Open Caveats

CDET ID	Status	Headline
CSCuq64691	N	Incorrect information regarding import_deploy.sh
CSCuq64974	N	build_set.sh errors
CSCuq65481	N	During releasetrain upgrade pupdate logs shows OS as REDHAT
CSCuq66027	N	PB hosted documentation not updated by binary installer
CSCuq67956	N	In QPS template nmon tool should be available.
CSCuq69001	N	By default Diagnostics should check VIP and Replica status
CSCuq72214	N	Few HA VMs are not pingable from installer VM after 7.0 puppet deployed
CSCuq72841	N	radclient not included in 7.0 AIO
CSCuq72845	N	Diameter not installed by default in AIO when choosing \"mobile\" type
CSCuq76656	N	ssh putty of 7.0 puppet installed VMs is not happen until iptables stop
CSCuq78717	N	After pupdate Publish Repository is missing.
CSCuq79343	N	sessionmgr VMs not getting reinitialized
CSCuq79923	N	puppet not updating all the VMs
CSCuq82126	N	Installer spreadsheet cannot store ESXi host password in clear text
CSCuq86133	N	For Gx call, CCA-I is not sending back to GGSN after lb VMs reboot
CSCuq86543	N	AIO Needs PHP Library for Mongo to Work with PB&J
CSCuq86759	N	shiprock-base not appropriate hostname
CSCuq88871	N	jhosts.py needs to handle empty entries in the json file.
CSCuq90455	N	Portal Install on AIO does not add portal alias to /etc/hosts
CSCuq90863	N	build_set.sh should create the sessionmgrxxx. init script to use syslog
CSCuq90869	N	vminstaller upgrade should be non service interrupt
CSCuq92553	N	puppet upgrade to EFT-3 qns05/06 servers file is not creating
CSCuq92782	N	release train archive is double-compressed
CSCuq94707	N	AIO not properly setup with diameter when selecting \"mobile\" type
CSCuq95049	N	Add screen utility to the vm image
CSCuq95641	N	QPS stats script fail to start - \" is not a Registered Bean \" feedback
CSCuq97043	N	AIO install/deploy does not use excel configuration template
CSCuq98959	N	Redhook migration requires design decision on where to store the mgmt VM
CSCuq99548	N	Plain text pasword string in Configuration.csv file
CSCur03181	N	Tacas configuration not successful in Cluster A
CSCur03320	N	install.sh should not terminate when it receives invalid responses
CSCup90138	O	IO Manager returned error processing RemoteAction Unknown action on QMOG
CSCuq64391	O	Liscense Test Cases Can not be executed For 7.0.0 Current Release.

A - Assigned
N - New
O - Opened

Resolved/Verified Caveats

Table 2 lists the resolved/verified caveats in the CPS 7.0 release.

Table 2 Resolved/Verified Caveats

CDET ID	Status	Headline
CSCuo56475	C	QPS upgrade: CCA does not come after upgrade
CSCup84480	C	5.5.3: High RAR TPS
CSCup97902	C	QPS 7.0 deployments are missing /opt/broadhop/installer scirpts
CSCup97905	C	Diagnostics output has failures in 6.x - > 7.0 migrations
CSCuq06127	C	puppet ISO 174 AIO setup, https based PB,CC, api URL are not working.
CSCuq48945	C	Average response time Doubled post 12hrs longevity for QOS rule group
CSCuq52186	C	QPS: RechargeWallet feature is not sending Gy CCR-I to OCS
CSCuq52204	C	QPS: debiting entire balance after 1st Gy CCR-U
CSCuq56077	C	QNS: Three same CDR value is adding for a single ACR call
CSCuq56096	C	'US1881_eMPS_001' failing with 'QoS-Class-Identifier is not valid'
CSCuq56158	C	QPS: Getting API response code 0 for incorrect version in request
CSCuq56982	C	env_import.sh scripts does not work correctly
CSCuq58253	C	US2010 automated scripts failing at QCI value mismatch
CSCuq63999	C	QNS: Memcached service gets stopped on release train update
CSCuq64028	C	QNS: Other VMs are not password-less from the Installer VM
CSCun43000	R	QPS_6.1_SPRINT3 SNMP: JMSConnectionError traps not being sent
CSCun64063	R	Charge against reservation does not work with 2 Gy sessions.
CSCuo22017	R	On Debit No RAR for Quota depletion,balance amount as Use Case Initiator
CSCuo29155	R	QPS: Multiple duplicate messages.
CSCuo48615	R	QNS: For wrong session ID QNS does not send diameter result code 5002
CSCuo55264	R	QPS_6.1_SPRINT7 SNMP: wrong load average thresholds
CSCuo63003	R	QPS: Gx RAR not triggered when balance added by adding new quota
CSCuo92422	R	Issue with RAR for Rx emergency over Gx emergency for unknown subscriber
CSCuo99796	R	QPS is not taking the decision based on the time-out cause
CSCup54391	R	QNS: Getting exception error when CCR-U contains only EventTrigger=27/28
CSCup56093	R	Diameter Client connections does not use rating for peers
CSCup63373	R	QPS calculates MBR-DL,MBR-UL for a VoLTE GBR bearer wrong
CSCup70440	R	Multiple Gy RARs send by QPS when Recurrence Quota refreshes
CSCup73104	R	CDR Staging size Mb is not working
CSCup76383	R	QPS assigns wrong QCI and GBR is not calculated
CSCup82226	R	PORTAL is not accessible.
CSCup83397	R	Generic LDAP Search should only query for explicitly defined fields

Table 2 Resolved/Verified Caveats

CDET ID	Status	Headline
CSCup84436	R	Issue while adding video to an ongoing VoLTE(audio) call
CSCup87749	R	REST API for CRD Returns Exception
CSCup91142	R	PB defect after adding diameter nodes require a RestartAll
CSCup97915	R	SPWIFI configuration is missing QPS 7.0 deployments
CSCuq03699	R	Primary sessionmgr shutdown result into instable Call Model no CCA
CSCuq05342	R	Realm Table is not in synch with the active peers
CSCuq05536	R	QPS 7.0:get_replica_status does not report replica set statuses properly
CSCuq10975	R	Critical Alarm is not getting generated..
CSCuq11362	R	QPS sends RAR on different GGSN endpoint
CSCuq15893	R	System group and user to allow limited and read-only ssh access
CSCuq16469	R	QPS is not resending the ldap search request on no response
CSCuq20418	R	Increase in session size due to EDR records
CSCuq31734	R	libjvm.so puppet errors when adding features
CSCuq37794	R	jvalidate.py issues
CSCuq38328	R	QPS 6.1.2 High Risk Vulnerability on pcrfclient for Apache Server.
CSCuq38350	R	count_mongo_sessions.sh script is counting the session twice
CSCuq39928	R	update wifi configuration with changes in the mobile
CSCuq41164	R	Default gateway needs to be set for eth1
CSCuq45931	R	Missing/incorrect packages in latest portal VM.
CSCuq48443	R	Add configuration option for TACACS+ to Excel
CSCuq49281	R	CCA-U Qos issues
CSCuq52223	R	asynchronous ldap search
CSCuq55086	R	VM backup and restore to remote storage
CSCuq55288	R	feature changed did not get updated by puppet, only after a few tries.
CSCuq56629	R	Puppet : Policy Builder process not starting with latest release train
CSCuq59559	R	top_qps.sh does not work in 7.0
CSCuq60030	R	QoS testing result observed for CCA_U QOS issue
CSCuq60573	R	'Diameter related configuration' section move before Transport the CSV
CSCuq61723	R	Filter out warnings, etc from about.sh
CSCuq67041	R	LDAP retires not working
CSCuq68937	R	ulimit errors reported by qns servers
CSCuq70509	R	Install Perl modules for migration scripts
CSCuq70881	R	The 'servers' file doesn't get populated correctly
CSCuq77401	R	Grafana doesn't work on AIO
CSCuq78818	R	After rebooting lb VM haproxy is not coming up dead but subsys locked
CSCuq79795	R	Tacacs+ No authorization sent after authentication

Table 2 Resolved/Verified Caveats

CDET ID	Status	Headline
CSCuq79812	R	qns-svn user requests login to tacacs along with other users
CSCuq81743	R	AT&T CLAB | Not able to configure multiple tacacs+ server in qps
CSCuq84296	R	Bad defaults in QPS_deployment_config_template.xlsx
CSCuq84569	R	slow ldap response from internal qps nodes
CSCuq85866	R	Puppet Fresh deployment: subversion user 'qns-svn' does not work in EFT-3
CSCuq86049	R	NPE observed in the log
CSCuq87988	R	QPS user story mirror functionality not working for Vulnerability
CSCuq95091	R	Puppet fails to initialize sessionmgrs
CSCuq95593	R	reinit.sh is not working on all qps components (VMs)
CSCuq97151	R	Permissions on /etc/tacplus.conf are incorrect for QPS and LB VMs
CSCuh88737	V	QNS:Traps are not being generated for invalid license.
CSCun69972	V	Duplicate EDR Data
CSCuo11955	V	QPS returning 'Diameter_too_busy' error with Createbalance API
CSCup43827	V	Grafana stats are notavailable for pcrfclient02
CSCup51499	V	High Message Processing - Response Time time for Gx message
CSCup53735	V	Inbound Message Overload handling option in PB not working
CSCup56060	V	Load Balancers throwing ERROR
CSCup77919	V	SNMPwalk is not showing correct value for lb.
CSCup83727	V	EDR generated for RAR has wrong diameter command code and request type
CSCup89230	V	Outbound Message Overload handling for Message Drop not working
CSCup91165	V	Large scale QPS greenfield installation take too long
CSCup96786	V	Query responses is very slow from some VMs .
CSCup97910	V	After QPS 7.0 install, sessionmgrs have incorrect host names
CSCuq03619	V	Flow-Direction: DOWNLINK (1) AVP observed in Dyanmic Rule.
CSCuq04775	V	Endpoint refresh issue on peer flap
CSCuq05513	V	Some features are missing in 6.0/6.1 to 7.0 migrations
CSCuq05518	V	Puppet Installer: Excel File needs validation
CSCuq05523	V	Puppet Deployment: Duplicate entries for installer in /etc/hosts
CSCuq05528	V	Restarting qns services sometimes results in \"dead but pid file exists\"
CSCuq05534	V	Puppet Deployment: syncconfig.sh fails with permissions issues
CSCuq05549	V	PAM default configuration needed for qns.conf
CSCuq07569	V	QPS 7.0 portal: set allow_url_include = On
CSCuq07857	V	Puppet installation: SELinux is enabled in the base VMDK
CSCuq08969	V	After fresh puppet deployment, PB is not loading into browser -
CSCuq09640	V	VIPs only can be deployed on physical interfaces within the subnet
CSCuq11929	V	Puppet: Historical analysis is not available in puppet HA ISO

Table 2 Resolved/Verified Caveats

CDET ID	Status	Headline
CSCuq12628	V	Puppet: AIO deployment requires a valid name server in /etc/resolv.conf
CSCuq13665	V	Puppet VMInstaller: Portal does not get deployed in AIO
CSCuq15880	V	QPS Puppet Installer - deployed VMs are missing puppet classes
CSCuq16507	V	Defaults in excel sheet are incorrect
CSCuq16513	V	Memcached on LB01/02 needs 1GB of memory
CSCuq16519	V	Puppet 7-29 build can't deploy portals
CSCuq16524	V	Puppet: /etc/broadhop/license directory contains 5.3.X license file
CSCuq17706	V	QPS revalidates and try to install failed rules from PCEF with new one
CSCuq17903	V	Puppet 7-30 build can't deploy all VMs correctly
CSCuq17929	V	Puppet: build QPS_7.0.0_20140729_1754.iso - PB no longer works
CSCuq17964	V	Documentation is unclear about etc/hosts migration requirements
CSCuq17966	V	Documentation needs to be corrected for new excel template
CSCuq18120	V	puppet: pcrfclient01 won't pupdate
CSCuq18361	V	Diagnostics fails because no /opt/broadhop/control/hosts.sh
CSCuq18369	V	Can't sync times because no /opt/broadhop/control
CSCuq18563	V	Puppet 7.0 to 7.0 migration fails with warnings and errors
CSCuq18684	V	QPS puppet installer AIO - portal does not work
CSCuq18747	V	RADIUS fails to install on AIO
CSCuq20140	V	Puppet: new portal01 doesn't have /etc/hosts
CSCuq20346	V	LBVIP01 defaults to lb02 while the other VIPs stay on LB01
CSCuq20509	V	default configuration have demo.mode enabled
CSCuq20703	V	Puppet Deployment: failure to upgrade with new .iso
CSCuq22952	V	install should point to the latest VMDK after upgrade
CSCuq25374	V	QPS 7.0 HA portals and AIOs missing PHP packages
CSCuq25374	V	QPS 7.0 HA portals and AIOs missing PHP packages
CSCuq26907	V	Puppet sanity test is failing with QPS_7.0.0_20140804_1807.iso
CSCuq27019	V	New Install: QPS_7.0.0_20140805_1822.iso will not deploy
CSCuq27529	V	Diagnostics failed on build 0805_1822
CSCuq29634	V	Adding features to an AIO fails... (AIO:10.94.251.108)
CSCuq30524	V	Puppet HA: PB is NOT able to load for higher no. of config
CSCuq30785	V	about.sh shows wrong port for https
CSCuq31577	V	Slow SSH to sessionmgrs and pcrfclient01 after deploying
CSCuq31615	V	build_set.sh is broken
CSCuq34738	V	Puppet HA:Unable to run installer script from ISO dir 7.0.0_20140811_120
CSCuq35803	V	Grafana doesnt work in 7.0 fresh puppet install
CSCuq35842	V	Iptables/HAProxy issues in new Puppet environments

Table 2 Resolved/Verified Caveats

CDET ID	Status	Headline
CSCuq36059	V	Diameter service installed on iomanager01/02 features files
CSCuq36759	V	Puppet HA:Sanity Test is failing with 7.0.0_20140812_0956
CSCuq37924	V	DIAMETER_PENDING_TRANSACTION (4198) Result Code even though no Collision
CSCuq38278	V	VMInstaller: issues with diagnostics.sh
CSCuq38405	V	Control scripts are not in PATH on the installer VM
CSCuq38758	V	No consolidated Engine Logs are generated on 7.0 install or upgrade
CSCuq39858	V	Installer and Control directory is missing puppet AIO fresh installation
CSCuq40378	V	Incorrect mongo PHP driver installed on portals
CSCuq41452	V	Need documentation on installing portal on AIO
CSCuq41690	V	Puppet AIO deployment SVN checkouts are not working
CSCuq45933	V	Incorrect config in latest portal VM.
CSCuq47150	V	Customized feature update is not working with puppet AIO ISO 174
CSCuq48639	V	diagnostics.sh output differs between installer and pcrfclient01
CSCuq48652	V	Issues with two interfaces on the same subnet
CSCuq48693	V	sync_times.sh fails on installer and pcrfclient01
CSCuq48743	V	Portals don't have ntpd on installed
CSCuq48747	V	restartall.sh does not work
CSCuq52827	V	startall.sh does not work due to a typo
CSCuq53854	V	Puppet QPS not able to establish peer conenction with GGSN -timeout 60s
CSCuq55209	V	logback.xml in build 185 only contains a date
CSCuq55403	V	Firewall blocking PB access
CSCuq55883	V	Command alias / shortcuts not working in VM Installer
CSCuq55912	V	Corosync.conf on lb01 showing wrong IP (default IP)
CSCuq56141	V	update.sh in puppet exits while upgrading HA setup
CSCuq56287	V	QPS: QPS unable to send all Usage Monitoring keys through RAR
CSCuq56470	V	PB and CC stops working
CSCuq56834	V	Publish repository missing after pupdate
CSCuq57606	V	Portal replica set missing from default mongoConfig.cfg
CSCuq58536	V	PolicyBuilder.sh script missing after upgrading to 193 puppet build
CSCuq59823	V	mongoConfig.cfg points to /data instead of /var/data
CSCuq60583	V	'location_query_device_type' set to 'isg' in broadhop.php config
CSCuq61524	V	qns.conf not containing proper information
CSCuq61699	V	about.sh does not report QPS versions on an AIO
CSCuq62292	V	VIPs are not coming up
CSCuq63263	V	initialize_qps.sh shows errors during upgrades

Table 2 Resolved/Verified Caveats

CDET ID	Status	Headline
CSCuq63653	V	vm-init should not be in /etc/init.d by default
CSCuq63712	V	reinit.sh should call vm-init instead of pupate
CSCuq63713	V	vminstaller configuration update
CSCuq63717	V	need to reserve memory when vm is deployed
CSCuq64013	V	QNS:Duplicate entry gets added in haproxy config on release train update
CSCuq64652	V	After reboot qns process doesn't come up
CSCuq65347	V	Diameter call not working after one of the qns process stop
CSCuq66008	V	Unable to run build_set.sh
CSCuq67236	V	unable to process CCR as lb01 need 24gb ram as per deployed jvm.conf
CSCuq70931	V	Latest ISO fails to initialize if /var/www/html/vm-init exists
CSCuq70966	V	diagnostics.sh hangs while trying to connect to diam-int*-lb* hosts
CSCuq71778	V	mongodb log should go into logfile instead of syslog
CSCuq72510	V	Base installer does not have any public keys in /root/.ssh
CSCuq72987	V	about.sh should have more relevant information about URLs
CSCuq73139	V	ntp.conf file is not updated with correct ntp server ip address
CSCuq74645	V	fail to restore portal default DB
CSCuq74683	V	build_image.sh to support custom patch file in the repositories file
CSCuq77940	V	getting Error processing and deserializing incoming message exception
CSCuq79228	V	Portal and sessionmgr VMs not getting reinitialized
CSCuq79428	V	Excessive I/O causes
CSCuq79575	V	qps needs to use local pam if not in TACACS+
CSCuq83145	V	No CDR is getting inserted in balanceReconcile db.
CSCuq83831	V	Build_set.sh needs to open firewall ports for the sessionmgrs
CSCuq93296	V	upgrade should preserve qns.conf file
CSCuq93367	V	default sessionmgr deployment should not create the set0 init.d scripts
CSCuq95215	V	/var/log/sudosh needs to exist for TACACS+ logins
CSCuq95216	V	nscd is not running on some VMs after initial deployment
CSCuq97065	V	Sessionmgr VMs have tmpfs in the wrong location
CSCuq97157	V	statusall, stopall, startall, and restartall.sh scripts are not working
CSCuq97169	V	TACACS+ configuration: server not in /etc/tacplus.conf
CSCuq97750	V	TACACS+ server is not in /etc/pam.d/tacacs

C - Closed

R - Resolved

V - Verified

Additional CDETs

Table 3 lists the additional CDETs in the CPS 7.0 release.

Table 3 Additional CDETs

CDET ID	Status	Headline
CSCuq14300	D	QPS 7.0 HA deployment: portal /other VMs not config -nt find qps::users
CSCuq15754	D	Portal takes a long time to load
CSCuq27098	D	No default route for the signalling/mgmt traffic interface
CSCuq29057	D	License not getting applied
CSCuq51066	D	Observed Exceptions for Notification Manager post 12 hours Longevity
CSCuq60309	D	pb gui access need authentication; default broadhop user be configurable
CSCuq63418	D	reinit.sh should call vm-init
CSCuq63443	D	build_set.sh problem
CSCuq66820	D	grafana not accessible
CSCuq70623	D	nitialize_qps.sh does not recreate servers file if image_map exists
CSCuq79231	D	PB Publish is slow due to I/O issues
CSCuq79243	D	Publish on PB is very slow due to I/O issues
CSCuq83903	D	sessionmgr mongo port rules of iptables flush after reboot or reinit.sh
CSCuq86196	D	Puppet Upgrade: faced the svn errors for upgrading EFt-1 to EFT-3
CSCuq91551	D	Roles in servers file messed up after 7.0.0.3 patch upgrade
CSCuq91584	D	Multiple qns failures after 7.0.0.3 upgrade
CSCup37520	I	Radius Access Request message is corrupted at QPS, with new WLC Release
CSCuq72876	I	QPS Shiprock Installer VM Management Requirements
CSCuq76561	I	Diameter Gx is peer is not coming up between GGSN and 7.0 puppet QPS
CSCuq83755	I	Policy builder is losing repositories
CSCuq86003	I	QNS: Emergency calls are getting failed with 2000 tps.
CSCuq86942	I	Incorrect hostnames are listed in bulk stats
CSCup37407	J	Configurable AVP Dictionary: AVP mapping not happening in SLR
CSCup47327	J	No consolidated Engine Logs are generated after 7.0 Upgrade
CSCup63389	J	QNS:Subscriber is able to use shared bucket after useSharedBucket=false
CSCup67144	J	6.1.1 Performance degrade almost after 8 Hours
CSCup89996	J	Wrong cause-code send in Rx RAR when a bearer is deleted
CSCup91137	J	Non standard QNS internal routing required to reach signaling IP on LBs
CSCuq19677	J	Emergency Anonymous Subscriber call is getting rejected
CSCuq30692	J	QNS:Not updating the value of SN-Trans-DATA coming in CCR-U and CCR-T.
CSCuq31269	J	pcrfclient01 slowness
CSCuq31620	J	monit is missing snmp config
CSCuq50690	J	QPS ldap search request is missing o=cingular

Table 3 Additional CDETs

CDET ID	Status	Headline
CSCuq56457	J	Missing config in haproxy-diameter
CSCuq57015	J	CC page does not show correct configuration after restore data
CSCuq59518	J	QPS 7.0.0 - Install script reports to wrong version to upgrade
CSCuq64019	J	QNS: Diameter proxy configurations gets deleted on release train update
CSCuq79296	J	About.sh giving incorrect IP addresses output in QPS 7.0
CSCuq90872	J	Need a script to copy the config files to other nodes
CSCuq57193	M	QPS not sending TSR with DRA
CSCuq67112	M	Next Hop Routing for Secondary DRA (PAS) not working
CSCur04920	M	BASH Security Vulnerability - CVE-2014-6271 shellshock
CSCuo90519	U	QPS: Diameter unable to start on backup Loadbalancer
CSCup05281	U	Balance Error on AAR with Sponsored-Connectivity-Data
CSCup35356	U	Subscriber Credential could not be computed error in qns log on Sy calls
CSCup91147	U	RestartAll prevents PB from starting. Requires subsequent restart on PB
CSCup92443	U	6.1.1[sys-test]:FSM overloaded exception observed on IPV6 diameter endpt
CSCuq08117	U	Inconsistent Session Count warning in Diagnostics
CSCuq09979	U	Puppet Install: Portal takes a long time to load
CSCuq24765	U	QPS binds to IPv6 address on diameter endpoints
CSCuq59263	U	AIO hostname in /etc/broadhop/servers after upgrade

D - Duplicate
I - Info_Req
J - Junked
M - More
U - Unreproducible

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 Alarming and SNMP Guide*
- *Cisco Policy Suite 7.0 Backup and Restore Guide*
- *Cisco Policy Suite 7.0 Installation Guide*
- *Cisco Policy Suite 7.0 Mobile Configuration Guide*
- *Cisco Policy Suite 7.0 Operations Guide*
- *Cisco Policy Suite 7.0 Policy Reporting Guide*

- *Cisco Policy Suite7.0 Release Notes*
- *Cisco Policy Suite 7.0 Troubleshooting Guide*
- *Cisco Policy Suite 7.0 Wi-Fi/BNG Configuration Guide*
- *Cisco Policy Suite Control Center 3.4 Interface Guide for Full Privilege Administrators*
- *Cisco Policy Suite Control Center 3.4 Interface Guide for View Only Administrators*
- *Cisco Subscriber Services Portal 7.0 Interface Guide for Administrators*
- *Cisco Subscriber Services Portal 7.0 Interface Guide for Managers*
- *Cisco Subscriber Services Portal 7.0 Interface Guide for Front Desk Personnel*

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/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers 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 "Related Documentation" section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.