Release Notes for *Cisco Policy Suite* for Release 6.1.1

First Published: July 10, 2014
Last Updated: July 10, 2014
Release: 6.1.1

Contents

This document describes the new features, feature versions and limitations for Cisco Policy Suite. Use this document in combination with documents listed in the "Related Documentation" section on page 13.

This document includes the following sections:

- Introduction, page 1
- New and Changed Information, page 2
- Installation Notes, page 4
- Limitations and Restrictions, page 10
- Caveats, page 11
- Related Documentation, page 13

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:

- Cisco Policy Server (PS)
- Cisco Charging Server (CS)
- Cisco Application Gateway (AGW)

Cisco Systems, Inc.
www.cisco.com

- Cisco Unified Subscriber Manager (USuM)
- Cisco 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 6.1.1.

New Software Features in Release *6.1.1*

The following features have been added in Release 6.1.1:

- Bulk Statistics, page 3
- Charging Characteristics AVP in Diameter Gy CDR's, page 3
- Framed IP based Service Classification, page 3
- Gy EDR Enhancement, page 3
- Graphite Grafana Tool, page 3
- Handling Write Failures during Balance DB Failover, page 3
- IPv6 Diameter Endpoints, page 3
- Quota Enhancements, page 4
- Rx Proxy Support, page 4
- SNMP Enhancements, page 4
- Software Development Kit (SDK), page 4
- SOS e911 Processing Priority by APN, page 4

- Traffic Steering and DSCP, page 4

Bulk Statistics

Bulk Statistics are the statistics that are gathered over a given time period and written to a set of files. This statistics can be used by external analytic processes and/or network management systems. With this release we have extended our support for new statistics based on our customer(s) requirement.

Charging Characteristics AVP in Diameter Gy CDR’s

Cisco Policy Suite (CPS) provides the ability to produce reports on Gy Charging Characteristics AVP in Call Data Records (EDR/CDRs). Diameter2 is the existing component in CPS that supports the processing of records on the Gy interface.

Framed IP based Service Classification

CPS supports dual stack sessions for Gx and Rx interfaces. With this feature the service grant can be based on the type of Framed-IP-Address AVP (IPv4 or IPv6 or Both).

Gy EDR Enhancement

Cisco Policy Suite (CPS) provides the ability to produce reports on Gy Charging Characteristics AVP in Event Data Records (EDR/CDRs). Diameter2 is the existing component in CPS that supports the Processing of records on the Gy interface.

Graphite Grafana Tool

Grafana tool provides a graphical or text-based representation of statistics and counter, collected in its database. Graphite database is used to collect the statistics and counter information. The graphite database is in addition to the Collectd Mongo database.

Going forward Zabbix will be phased out. The required information for graphical representation is fetched by querying the Graphite database.

Handling Write Failures during Balance DB Failover

Prior to CPS 6.1.1 release, whenever primary balance DB used to go down, one of the secondary balance DBs used to become primary but CPS was not able to handle these write failure during failover time from primary to secondary balance DB.

Now, CPS supports enabling of Handling Write Failures During Balance DB Failover. Based on the input from the user, database is created while starting up the bundle i.e., in init() method and also by publishing the configuration done in Policy Builder under Balance Configuration.

IPv6 Diameter Endpoints

CPS now supports IPv6 for control plane and send/receive diameter messages using IPv6 interface endpoints. With this feature, flexibility to add IPv6 on interfaces and on virtual IP's is introduced.

Quota Enhancements

CPS already supported Shared Quota among a group of subscribers. With this Enhancement each subscriber can have a configurable, limited (capped) share from the total Shared Quota.

Rx Proxy Support

When an Rx session is initiated from a P-CSCF to CPS, it checks for a linked IP-CAN session (Gx session). If no linked IP-CAN session is found, the Rx request is rejected with the error IP-CAN Session Not found.

In the case of a P-CSCF failure in one region, traffic from that region is routed to the P-CSCF in the opposite region.

In this feature, an Rx Proxy is configured on the CPS for both sites, replacing the external DRA agent. In order to achieve this, the CPS of both the North Site and South Site are connected to each other. If there is failure to process the Rx request from either of the sites, the CPS proxies (forwarded) the Rx request to find a linked IP-CAN session.

SNMP Enhancements

CPS generate alarms when diameter connection(s) is/are disconnected. The service provider's administrator is alerted so that appropriate action can be taken to restore services. The alarms Severity depends on the number of “down” connections within a realm. If all the connections within a realm are down then Critical Alarm is raised or else one Major alarm for each disconnected peer is raised.

Software Development Kit (SDK)

CPS 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 core policy engine.

SOS e911 Processing Priority by APN

Currently, e911 sessions are fast tracked through the CPS platform by by-passing authorization logic. The CPS platform is now enabled to prioritize these emergency sessions based on APN. Numerical Priority is configured for the desired “Called-Station-Id” AVP, to determine the internal processing priority by the QNS(s).

Traffic Steering and DSCP

CPS is now enabled to steer the flows installed from Rx by implementing Flow-Direction (release 10 and onwards). CPS also supports ToS-Traffic-Class AVP over Gx.

Installation Notes

This section describes the installation notes in Release 6.1.1.

Note Currently, direct upgrading of CPS from version 5.3.5 to 6.1.1 is not supported. Customer first needs to upgrade CPS to 5.5 and then can upgrade the system to 6.1.1.

Note Customer must download the latest software package available from the link http://software.cisco.com/download/type.html?mdfid=284883882&catid=null.

Feature Versions

The following table mentions the component version for CPS 6.1.1 Release:

Component	Version
Core	6.1.1
Audit	1.3.1
Balance	3.3.1
Control Center	3.3.1
Congestion Reference Data	1.1.1
Customer Reference Data	2.3.1
DHCP	1.3.1
Diameter2	3.3.1
ISG Prepaid	1.7.1
LDAP	1.4.1
Notifications	5.7.1
Policy Intel	2.1.1
POP-3 Authentication	1.3.1
Radius	3.2.1
SCE	2.0.9
Scheduled Events	1.2.1
SPR	2.2.1
Unified API	2.2.1
Web Services	1.4.1
Recharge Wallet	1.1.1
Installer	6.1.1
RPMS	6.1.1

Removing MySQL JDBC Connectors from Standard Load Line-up

Step 1 Add the following entry to `qns.conf` file on all the CPS boxes.

-DmysqlDriver=file:///var/broadhop/jdbc/jdbc_5_1_6.jar

Step 2 Download MySQL jdbc 5.1.6 binary jar from http://ebr.springsource.com (search for com.springsource.com.mysql.jdbc and download version 5.1.6 from the link).

Step 3 Rename the downloaded jar file to `jdbc_5_1_6.jar` and copy the jar file to `/var/broadhop/jdbc/` directory on all CPS boxes.

Step 4 Synchronize all the boxes and then restart CPS.

Deployment Management Console

Deployment Management Console feature is released as patch over 6.1.1 release build. Patch release covers instructions to install the feature in the setup environment.

Step 1 Download `qps_mgmt_console.zip` to `/tmp` directory.

Step 2 Unzip `qps_mgmt_console.zip` to `/tmp` directory.

Step 3 Run `update_console.sh` from `/tmp` directory.

Step 4 Execute the command `qps_management_console` to check management console is installed or not.

RAR Fix for GR Setup

The following configuration changes need to be done:

Step 1 Add SiteId and RemoteSiteId VM arguments in all `qns.conf` files mentioned below, so that all outbound messages get processed by RemoteSite when GGSN link failure occurs on Site.

-DSiteId=Site1

-DRemoteSiteId=Site2

Files that need to be updated:

/etc/broadhop/diameter_endpoint/qns.conf, /etc/broadhop/diameter_endpoint_stby/qns.conf,

/etc/broadhop/iomanager01/qns.conf,

/etc/broadhop/iomanager02/qns.conf,

/etc/broadhop/iomanager_stby_01/qns.conf,

/etc/broadhop/iomanager_stby_02/qns.conf,

/etc/broadhop/pcrf/qns.conf,

/etc/broadhop/pcrf_stby/qns.conf,

/etc/broadhop/qns.conf,

Step 2 Similarly, the user needs to configure the following VM arguments in the above mentioned files in other sites.

```
-DSiteId=Site2 (should be same as SiteId of other site)
```

```
-DRemoteSiteId=Site1 (should be same as RemoteSiteId of other site)
```

Note -DSiteId and -DRemoteSiteId values can be custom names. The purpose of the naming conversion is useful in finding out from which site CPS is sending outbound messages.

Upgrade Portal DB Arbiter from pcrfclient01 to sessionmgr01

Step 1 Login to pcrfclient01.

Step 2 Stop portal DB arbiter on pcrfclient01.

```
[root@pcrfclient01 ~]# /etc/init.d/portalDB-27749 stop
```

```
[root@pcrfclient01 ~]# chkconfig --del portalDB-27749
```

Step 3 Start portal DB arbiter on sessionmgr01.

```
[root@sessionmgr01 ~]# /etc/init.d/portalDB-27749 start
```

If it fails to start, then create a directory called `portal.1` in `/data` on sessionmgr01 and start it.

```
[root@sessionmgr01 ~]# chkconfig --add portalDB-27749
```

Step 4 On pcrfclient01, execute the command.

```
scp /etc/init.d/portalDB-27749 sessionmgr01://etc/init.d/
```

Step 5 Modify portal replication set (add sessionmgr01 arbiter and remove pcrfclient01 arbiter).

```
[root@pcrfclient01 ~]# mongo portal01:27749
```

```
portal01:PRIMARY> rs.addArb("sessionmgr01:27749") output is:
```

```
{ "down" : [ "sessionmgr01:27749" ], "ok" : 1 }
```

```
portal01:PRIMARY> rs.remove("pcrfclient01:27749")
```

output is:

```
Wed Apr  2 03:33:16.371 DBClientCursor::init call() failed Wed Apr  2 03:33:16.372 Error: error
    doing query: failed at src/mongo/shell/query.js:78 Wed Apr  2 03:33:16.373 trying reconnect to
    portal01:27749 Wed Apr  2 03:33:16.374 reconnect portal01:27749 ok
```

Step 6 Verify portal replica set.

```
[root@pcrfclient01 ~]# diagnostics.sh --get_replica_status
```

Peer Connection with GGSN not Coming UP on new OVF for AIO Setup

Problem In Policy builder we observe that Diameter stack definition is given at two places i.e. under system-1 as well as under cluster. Hence the configuration defined under System is not being applied and so the peer connection with GGSN is not established.

Configuration: It comes as default when we deploy OVF for AIO.

Explanation CER/CEA is not exchanged. Hence the configuration defined under System is not being applied and so the peer connection with GGSN is not established.

Recommended Action Remove the Diameter Stack configuration from Cluster.

Generate Certificate for SSL and CA

Generate a key and a certificate using openssl and concatenate them in a file, the certificate first, then the key.

Step 1 Go to directory `/etc/pki/tls/certs`.

Step 2 Create the following directories under certs directory as follows:

1. mkdir Certificates
2. mkdir Keys
3. mkdir CSR

Step 3 Create file index.txt under certs directory:

```
touch index.txt
```

Step 4 Create file serial under certs directory:

```
cat “01” > serial
```

Step 5 Create a private key of CA.

```
openssl genrsa -des3 -out Keys/RootCA.key 2048.
```

Step 6 Create self-signed certificate of CA.

```
openssl req -config /etc/pki/tls/openssl.cnf -new -x509 -days 360 -key Keys/RootCA.key -out
    Certificates/RootCA.crt
```

Step 7 Create private key for the server.

```
openssl genrsa -des3 -out Keys/server.key 2048
```

Step 8 Create CSR for the server.

```
openssl req -config /etc/pki/tls/openssl.cnf -new -key Keys/server.key -out CSR/server.csr
```

Step 9 Create server certificate.

```
openssl ca -config /etc/pki/tls/openssl.cnf -days 360 -in CSR/server.csr -out Certificates/server.crt
    -keyfile Keys/RootCA.key -cert Certificates/RootCA.crt -policy policy_anything
```

Step 10 Remove passphrase from private key so that while starting/restarting the HA proxy it won't ask for passphrase.

```
cp RootCA.key RootCA.key.orig

openssl rsa -in RootCA.key.orig -out RootCA.key

cp server.key server.key.orig

openssl rsa -in server.key.orig -out server.key
```

Step 11 Copy and paste the RootCA and server certificate and key as certificate first and then the key to a file; For example

```
vi /etc/pki/tls/certs/haproxy.pem
```

```
-----BEGIN CERTIFICATE-----
MIIBrzCCARgCCQCfMsCGwq31yzANBgkqhkiG9w0BAQUFADAcMRowGAYDVQQDExF3
d3cuZXhjZWxpYW5jZS5mcjAeFw0xMjA5MDQwODU3MzNaFw0xMzA5MDQwODU3MzNa
MBwxGjAYBgNVBAMTEXd3dy5leGNlbGlhbmNlLmZyMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDFxSTUwX5RD4AL2Ya5t5PAaNjcwPa3Km40uaPKSHlU8AMydxC1
wB4L0k3Ms9uh98R+kIJS+TxdfDaYxk/GdDYI1CMm4TM+BLHGAVA2DeNf2hBhBRKb
TAgxCxXwORJQSB/B+1r0/ZiQ2ig5Jzr8xGHz+tBsHYZ+t+RmjZPQFjnlewIDAQAB
MA0GCSqGSIb3DQEBBQUAA4GBABqVuloGWHReSGLY1yAs20uhJ3j/9SvtoueyFBag
z5jX4BNO/4yhpKEpCGmzYtjr7us3v/s0mKoIVvAgah778rCZW3kF1Y6xR6TYqZna
1ryKB50/MJg9PC4LNL+sAu+WSslOf6+6Ru5N3JjhIZST8edJsGDi6/5HTKoqyvkp
wOMn
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDFxSTUwX5RD4AL2Ya5t5PAaNjcwPa3Km40uaPKSHlU8AMydxC1
wB4L0k3Ms9uh98R+kIJS+TxdfDaYxk/GdDYI1CMm4TM+BLHGAVA2DeNf2hBhBRKb
TAgxCxXwORJQSB/B+1r0/ZiQ2ig5Jzr8xGHz+tBsHYZ+t+RmjZPQFjnlewIDAQAB
AoGBALUeVhuuVLOB4X94qGSe1eZpXunUol2esy0AMhtIAi4iXJsz5Y69sgabg/qL
YQJVOZO7Xk8EyB7JaerB+z9BIFWbZwS9HirqR/sKjjbhu/rAQDgjVWw2Y9sjPhEr
CEAvqmQskT4mY+RW4qz2k8pe4HKq8NAFwbe8iNP7AySP3K4BAkEA4ZPBagtlJzrU
7Tw4BvQJhBmvNYEFviMScipHBlpwzfW+79xvZhTxtsSBHAM9KLbqO33VmJ3C/L/t
xukW8SO6ewJBAOBxU0TfS0EzcRQJ4sn78G6hTjjLwJM2q4xuSwLQDVaWwtXDI6HE
jb7HePaGBGnOrlXxEOFQZCVdDaLhX0zcEQECQQDHcvc+phioGRKPOAFp1HhdfsA2
FIBZX3U90DfAXFMFKFXMiyFMJxSZPyHQ/OQkjaaJN3eWW1c+Vw0MJKgOSkLlAkEA
h8xpqoFEgkXCxHIa00VpuzZEIt89PJVWhJhzMFd7yolbh4UTeRx4+xasHNUHtJFG
MF+0a+99OJIt3wBn7hQ1AQJACScT3p6zJ4llm59xTPeOYpSXyllR4GMilsGIRNzT
RGYxcvqR775RkAgE+5DHmAkswX7TBaxcO6+C1+LJEwFRxw==
-----END RSA PRIVATE KEY-----
```

Step 12 Save and close the file haproxy.pem and edit the configuration file `/etc/haproxy/haproxy.cfg`.

Step 13 Go to section listen controlcenter_proxy and add the following lines:

listen andsf_proxy

bind *:8071 ssl crt /etc/pki/tls/certs/haproxy.pem ca-file /etc/pki/tls/certs/Certificates/RootCA.crt verify optional

default_backend andsf_server

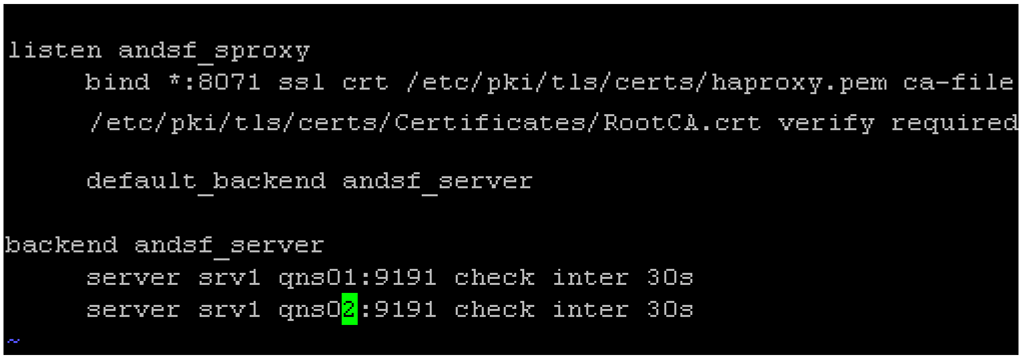
backend andsf_server

option httpchk GET /Security.html

server srv1 qns01:9091 check inter 30s

server srv2 qns02:9092 check inter 30s

A sample configuration section of haproxy.cfg for ssl looks as follows;



```
listen andsf_sproxy
     bind *:8071 ssl crt /etc/pki/tls/certs/haproxy.pem ca-file
      /etc/pki/tls/certs/Certificates/RootCA.crt verify required

     default_backend andsf_server

backend andsf_server
     server srv1 qns01:9191 check inter 30s
     server srv1 qns02:9191 check inter 30s
~
```

Limitations and Restrictions

The Cisco Policy Suite has the following limitations and restrictions:

- After database role change for multiple sessionMgrs, CPS is unable to stabilize the calls and timeouts happen constantly.
- On receiving Accounting Stop message, the Radius call is not disconnected and the session is also present in mongo database.
- As graphite-db and grafana setup on pcrfclient01 and pcrfclient02 is independent. Whatever dashboard configuration is saved on pcrfclient01's, grafana will not be available on pcrfclient02.

  The easiest way to configure dashboards on pcrfclient02 (if not configured earlier) is to import pre-configured dashboard templates from working pcrfclient01's grafana setup.
- For current release, graphite grafana tool is supported for mobile customers only.
- To support repairing of heartbeat resources like haproxy and memcached in IPv6 scenario, you need to update script `/etc/repair_hb_resources.sh` on all lb VMs.

  Modify `/etc/repair_hb_resources.sh` to handle IPv6 and IPv4 addresses:

  #Comment below two lines (line no: 60, 61)

```
#vip=$(echo $line | /bin/cut -d':' -f1)
#port=$(echo $line | /bin/cut -d':' -f2)
 #Add below two lines
vip=$(echo $line | rev | /bin/cut -d':' -f2- | rev)
port=$(echo $line | rev | /bin/cut -d':' -f1 |rev)
```

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=

Open Caveats

Table 1 lists the open caveats in the CPS 6.1.1 release.

Table 1 Open Caveats

CDET ID	Status	Headline
CSCup75836	A	[Sys Test] : Unable to send RAR

A - Assigned

N - New

O - Opened

Resolved/Verified Caveats

Table 2 lists the resolved/verified caveats in the CPS 6.1.1 release.

Table 2 Resolved/Verified Caveats

CDET ID	Status	Headline
CSCum68136	C	Deployment Management Console has display issues
CSCun71902	R	UnifiedAPI GetSubscriber - Threshold breach status missing for 2nd quota
CSCup38812	R	QNS:Subscriber is not moving to individQuota if sharedquota is depleted.
CSCuo63312	R	QPS Policy Intel Batch Report (Jasper) differs from Reporting

Table 2 Resolved/Verified Caveats

CDET ID	Status	Headline
CSCuo96323	R	QPS Rx and Gx session binding failure for IPv6
CSCuo36305	R	Update PAX-WEB
CSCuo95860	R	On startup the system may timeout msgs due to Java hotspot compilation
CSCup24446	R	QPS 6.0 to 6.1 upgrade issues
CSCup27638	R	Additional support of ARP and Media Type in RxAppQosInfo
CSCup14278	R	QPS builds incorrect Partial Rule Name for VOLTE call
CSCuo52091	R	Discard Duplicate Gy CCR Message
CSCup47478	R	Configuring Diameter outbound queue in PB causing issue for stats.
CSCup59672	R	Recharge Wallet / Session Wallet Enhancement for 6.1.1
CSCup32332	R	QNS: Notifications not installed across the board.
CSCup39578	R	Gy Messages not coming in Taileng logs
CSCup63086	R	[Sys.Test] HAProxy over IPv6
CSCup63368	R	[sys-test]6.1.1:Emergency calls dropped when per Instance TPS configured
CSCup65430	R	Change Openet vendor specific AVPs to Cisco AVPs
CSCup70260	R	[Sys Test] : Bin Upgrade on GR
CSCup47494	R	Memcached configuration need to be set at least 1Gb on session managers.
CSCup53235	V	Enforcement-free license message should be log on warning level.
CSCup53230	V	Enforcement-free license fucntiionality not working
CSCup49547	V	Sys Test: Trouble accessing pcrfclient01 after upgrade
CSCup47496	V	MAX_UPDATES_PER_SECOND in the /etc/carbon/carbon.conf to 100
CSCup47480	V	incorrectly classifying some calls as timeouts when they are 3002.
CSCup39691	V	Upgrade issue from 6.1.1 to 6.1.1 progressive builds.
CSCup35295	V	Too many Rx binding keys having impact on system performance
CSCup27047	V	QNS: Subscriber is able to use more than his/her limit.
CSCuo91267	V	QPS processing node does not disconnect cleanly from diameter endpoint
CSCuo63445	V	Policy Builder: Does not work in Firefox 29+/ Chrome 33+
CSCup62529	V	Graphite not installed on pcrfclient02 so it's not HA enabled.
CSCup62546	V	Missing Active sessions stats
CSCup57723	V	Feature com.broadhop.diameter2.policy.endpoint is unable to start
CSCup55146	V	Balance module not starting
CSCup36472	V	6.1.1- upgrd fail from 6.1.1_72 to *_81 due to collectd rpm Failed depe
CSCun86794	V	Suspending or deleting a sub-account does not prevent logins
CSCuo31259	V	AVP Substitution for Sub Account in 5.5.3
CSCuo44344	V	All SubAccount Credentials being changed when using Auto Reg. MAC Creds.
CSCuo65409	V	No Counter List in Counter Name Column in PB GUI

Table 2 Resolved/Verified Caveats

CDET ID	Status	Headline
CSCuo67791	V	fix Jetty bundler upgrade of 7.0
CSCuo70382	V	Cell Congestion provision tool issue due to QPS 6.0.1 patch
CSCuo89129	V	GetSubscriber fails for retrieval of quota with rollover quota defined
CSCuo68179	V	QPS does not send AAA to IMS behind DRA
CSCup42502	V	6.1.1-All memcached of smgr are off after upgrde to 6.1.1_122 in HAsetup
CSCup43026	V	upgrade failed because not able to ping sessionmgr.
CSCup47471	V	Some stats was missing in release-train-6.1.1_124.bin
CSCup47475	V	Ldap search stats are missing
CSCup67348	V	6.1.1_US2701:No Gx sessi, Rx_AAA should be sent no IP can sess code 5065
CSCup70266	V	6.1.1_US2701:In response to STR getting 3 differnt STA messages in Rx

R - Resolved
V - Verified
C - Closed

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 6.1.1 Alarming and SNMP Guide*
- *Cisco Policy Suite 6.1.1 Backup and Restore Guide*
- *Cisco Policy Suite 6.1.1 Installation Guide*
- *Cisco Policy Suite 6.1.1 Mobile Configuration Guide*
- *Cisco Policy Suite 6.1.1 Operations Guide*
- *Cisco Policy Suite 6.1.1 Policy Reporting Guide*
- *Cisco Policy Suite 6.1.1 Troubleshooting Guide*
- *Cisco Policy Suite 6.1.1 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/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.

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.