Cisco Policy Suite 20.2.0 Release Notes (1)

First Published: August 27, 2020

Last Updated: December 8, 2020

Introduction

This Release Note identifies installation notes, limitations, and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 20.2.0. Use this Release Note in combination with the documentation listed in the *Related Documentation* section.

NOTE: The PATS/ATS, ANDSF, and MOG products have reached end of life and are not supported in this release. Any references to these products (specific or implied), their components or functions in this document are coincidental and are not supported. Full details on the end of life for these products are available at: https://www.cisco.com/c/en/us/products/wireless/policy-suite-mobile/eos-eol-notice-listing.html.

This Release Note includes the following sections:

- New and Changed Feature Information
- Installation Notes
- Limitations and Restrictions
- Open and Resolved CDETS
- Related Documentation
- Obtaining Documentation and Submitting a Service Request

New and Changed Feature Information

For information about a complete list of features and behavior changes associated with this release, see the *CPS Release Change Reference*.

Installation Notes

Download ISO Image

Download the 20.2.0 software package (ISO image) from:

https://software.cisco.com/download/home/284883882/type/284979976/release/20.2.0

Md5sum Details

PCRF

35a61deed535f5f831c1dc13179cc64c	CPS_20.2.0_Base.release.qcow2_signed.tar.gz
5552a4b0222712e9760277301c09591c	CPS_20.2.0_Base.release.vmdk_signed.tar.gz
70a7d374b5e51a6503e00501292e4eff	CPS_20.2.0.release.iso_signed.tar.gz

DRA

0b7dd85ea47160ed00ca0bf839b35ef2	CPS_Microservices_DRA_20.2.0_Base.release.vmdk_signed.tar.gz
a3b972310f30634b8cf7438264809392	CPS_Microservices_DRA_20.2.0_Deployer.release.vmdk_signed.tar.gz
40165f852d2d32198c6f25ae96853770	CPS_Microservices_DRA_20.2.0.release.iso_signed.tar.gz
d521df12d843ff0094faae5d2be46547	CPS_Microservices_DRA_Binding_20.2.0.release.iso_signed.tar.gz

Component Versions

The following table lists the component version details for this release.

Table 1 Component Versions

Component	Version
ANDSF	20.2.0.release
API Router	20.2.0.release
Audit	20.2.0.release
Balance	20.2.0.release
Cisco API	20.2.0.release
Cisco CPAR	20.2.0.release
Congestion Reference Data	20.2.0.release
Control Center	20.2.0.release
Core	20.2.0.release
CSB	20.2.0.release
Custom Reference Data	20.2.0.release
DHCP	20.2.0.release
Diameter2	20.2.0.release
DRA	20.2.0.release
Entitlement	20.2.0.release
Fault Management	20.2.0.release
IPAM	20.2.0.release
ISG Prepaid	20.2.0.release
LDAP	20.2.0.release
LDAP Server	20.2.0.release
LWR	20.2.0.release
Microservices Enablement	20.2.0.release
Notification	20.2.0.release

Component	Version
NSSF	20.2.0.release
Policy Intel	20.2.0.release
POP-3 Authentication	20.2.0.release
RADIUS	20.2.0.release
Recharge Wallet	20.2.0.release
SCE	20.2.0.release
Scheduled Events	20.2.0.release
SPR	20.2.0.release
UDC	20.2.0.release
UDSN Interface	20.2.0.release
Unified API	20.2.0.release

Additional security has been added in CPS to verify the downloaded images.

Image Signing

Image signing allows for the following:

- Authenticity and Integrity: Image or software has not been modified and originated from a trusted source.
- Content Assurance: Image or software contains code from a trusted source, like Cisco.

Software Integrity Verification

To verify the integrity of the software image you have from Cisco, you can validate the md5sum checksum information against the checksum identified by Cisco for the software.

Image checksum information is available through **cisco.com Software Download Details**. To find the checksum, hover the mouse pointer over the software image on cisco.com.

If md5sum is correct, run *tar -zxvf* command to extract the downloaded file.

The files are extracted to a new directory with the same name as the downloaded file name without extension (.tar.gz).

The extracted directory contains the certificate files (.cer), python file (cisco_x509_verify_release.py), digital certificate file (.der), readme files (*.README), signature files (.signature) and installation files (.iso .vmdk, .qcow2 and .tar.gz).

Certificate Validation

To verify whether the installation files are released by Cisco System Pvt. Ltd and are not tampered/modified or infected by virus, malware, spyware, or ransomware, follow the instruction given in corresponding *.README file.

NOTE: Every installation file has its own signature and README file. Before following the instructions in the README file, make sure that cisco.com is accessible from verification server/host/machine/computer. In every README file, a Python command is provided which when executed connects you to cisco.com to verify that all the installation files are released by cisco.com or not. Python 2.7.4 and OpenSSL is required to execute cisco_x509_verify_release.py script.

New Installations

- VMware Environment
- OpenStack Environment

VMware Environment

To perform a new installation of CPS 20.2.0 in a VMware environment, see the *CPS Installation Guide for VMware*.

NOTE: After installation is complete, you need to configure at least one Graphite/Grafana user. Grafana supports Graphite data source credential configuration capability. Graphite data source requires common data source credential to be configured using Grafana for Grafana user. Data source credential must be configured after fresh installation. If you fail to add the user, then Grafana will not have access to Graphite database and you will get continuous prompts for Graphite/Grafana credentials.

All Grafana users configured will be available after fresh installation. However, you need to configure the graphite data source in Grafana UI.

For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in CPS Operations Guide.

OpenStack Environment

To perform a new installation of CPS 20.2.0 in an OpenStack environment, see the *CPS Installation Guide for OpenStack*.

NOTE: After installation is complete, you need to configure at least one Graphite/Grafana user. Grafana supports Graphite data source credential configuration capability. Graphite data source requires common data source credential to be configured using Grafana for Grafana user. Data source credential must be configured after fresh installation. If you fail to add the user, then Grafana will not have access to Graphite database and you will get continuous prompts for Graphite/Grafana credentials.

All Grafana users configured will be available after fresh installation. However, you need to configure the graphite data source in Grafana UI.

For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in CPS Operations Guide.

Migrate an Existing CPS Installation

To migrate an existing CPS installation, see the *CPS Migration and Upgrade Guide*. CPS migration is supported from CPS 19.4.0 to CPS 20.2.0.

NOTE: Before migration, you need to configure at least one Graphite/Grafana user. Grafana supports Graphite data source credential configuration capability. Graphite data source requires common data source credential to be configured using Grafana for Grafana user. Data source credential must be configured before migration. If you fail to add the user, then Grafana will not have access to Graphite database and you will get continuous prompts for Graphite/Grafana credentials.

All Grafana users configured will be available after migration. However, you need to configure the graphite data source in Grafana UI.

For more information on updating graphite data source, see *Configuring Graphite User Credentials in Grafana* in CPS Operations Guide.

NOTE: As CPS 20.2.0 is built on a newer version of CentOS 8.1 which supports ESXi 6.7, make sure OVF tool version 4.3.0 is installed in CPS 19.4.0 from where you are migrating.

Version 4.3.0 for VMware 6.5/6.7: VMware-ovftool-4.3.0-13981069-lin.x86_64.bundle

You can download the OVF tool version 4.3.0 from https://code.vmware.com/web/tool/4.3.0/ovf.

NOTE: In CPS 20.2.0, puppet is upgraded from 3.6.2-3 to 5.5.19 version. Puppet code has been modified to adapt to this change. Previous release puppet code is not compatible with the current puppet version (5.5.19). Customer specific puppet code must be adapted to current release puppet version (5.5.19) before applying it to CPS 20.2.0.

IMPORTANT: Customers using Prometheus datastore must store data manually and recover it after the migration is complete. For more information, contact your Cisco Account representative.

Upgrade an Existing CPS Installation

As CPS 20.2.0 is built on a newer version of CentOS 8.1, so an in-service software upgrade (ISSU) is not supported.

Post Migration/Upgrade Steps

Re-Apply Configuration Changes

After the migration/upgrade is complete, compare your modified configuration files that you backed up earlier with the newly installed versions. Re-apply any modifications to the configuration files.

Verify Configuration Settings

After the migration/upgrade is finished, verify the following configuration settings.

NOTE: Use the default values listed below unless otherwise instructed by your Cisco Account representative.

NOTE: During the migration/upgrade process, these configuration files are not overwritten. Only during a new install will these settings be applied.

- `/etc/broadhop/qns.conf`
    - `-Dmongo.client.thread.maxWaitTime.balance=1200`
    - `-Dmongo.connections.per.host.balance=10`
    - `-Dmongo.threads.allowed.to.wait.for.connection.balance=10`
    - `-Dmongo.client.thread.maxWaitTime=1200`
    - `-Dmongo.connections.per.host=5`
    - `-Dmongo.threads.allowed.to.wait.for.connection=10`
    - `-Dcom.mongodb.updaterIntervalMS=400`
    - `-Dcom.mongodb.updaterConnectTimeoutMS=600`
    - `-Dcom.mongodb.updaterSocketTimeoutMS=600`
    - `-DdbSocketTimeout.balance=1000`
    - `-DdbSocketTimeout=1000`
    - `-DdbConnectTimeout.balance=1200`
    - `-DdbConnectTimeout=1200`
    - `-Dcontrolcenter.disableAndsf=true`
    - `-DnodeHeartBeatInterval=9000`
    - `-DdbConnectTimeout.balance=1200`
    - `-Dstatistics.step.interval=1`
    - `-DshardPingLoopLength=3`
    - `-DshardPingCycle=200`

  - `-DshardPingerTimeoutMs=75`
  - `-Ddiameter.default.timeout.ms=2000`
  - `-DmaxLockAttempts=3`
  - `-DretryMs=3`
  - `-DmessageSlaMs=1500`
  - `-DmemcacheClientTimeout=200`
  - `-Dlocking.disable=true`

NOTE: The following setting should be present only for GR (multi-cluster) CPS deployments:

```
-DclusterFailureDetectionMS=1000
```

NOTE: In an HA or GR deployment with local chassis redundancy, the following setting should be set to true. By default, it is set to false.

```
-Dremote.locking.off
```

- `/etc/broadhop/diameter_endpoint/qns.conf`
  - `-Dzmq.send.hwm=1000`
  - `-Dzmq.recv.hwm=1000`

Reconfigure Service Option

After upgrading from previous release to the current CPS release, Service option configured with Subscriber-Id becomes invalid and you need to reconfigure multiple Subscriber Id in SpendingLimitReport under Service Configurations.

Verify logback.xml Configuration

Make sure the following line exists in the logback.xml file being used. If not, then add the line:

<property scope="context" name="HOSTNAME" value="${HOSTNAME}" />

To ensure logback.xml file changes are reflected at runtime, the scanPeriod must be explicitly specified:

<configuration scan="true" scanPeriod="1 minute">

NOTE: In case scanPeriod is missing from already deployed logback.xml file, the application needs to be restarted for the updated scanPeriod configuration to be applicable.

After completing the updates in logback.xml, execute the following command to copy the file to all the VMs:

SSHUSER_PREFERROOT=true copytoall.sh /etc/broadhop/logback.xml /etc/broadhop/logback.xml

Additional Notes

This section provides additional notes necessary for proper installation/working of CPS.

- Session Manager Configuration: After a new deployment, session managers are not automatically configured.

  a. Edit the */etc/broadhop/mongoConfig.cfg* file to ensure all the data paths are set to /var/data and not /data.

  b. Then execute the following command from pcrfclient01 to configure all the replication sets:

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

- Default gateway in lb01/lb02: After the installation, the default gateway might not be set to the management LAN. If this is the case, change the default gateway to the management LAN gateway
- By default, pending transaction feature is enabled. If you are not using it, Cisco recommends disabling pending transaction feature post deployment.

  To disable pending transaction, the following parameter can be configured in */etc/broadhop/qns.conf* file:

  com.broadhop.diameter.gx.pending_txn.attempts=0

  After adding the parameter in qns.conf file, restart all VMs using *stopall.sh*/*startall.sh* or *restartall.sh* command.

- Add support to disable syncing carbon database and bulk stats files (ISSM)

  Add the following flags in */var/install.cfg* file:

  SKIP_BLKSTATS

  SKIP_CARBONDB

  Example to disable synching:

  SKIP_BLKSTATS=1

  SKIP_CARBONDB=1

- Add the following parameters in */var/install.cfg* file to skip installation type selection and initialization steps during ISSU/ISSM:

  INSTALL_TYPE

  INITIALIZE_ENVIRONMENT

  Example:

  INSTALL_TYPE=mobile

  INITIALIZE_ENVIRONMENT=yes

- Inconsistency in DPR sent by CPS on executing `monit stop` command

  Issue: When `monit stop all` is executed on Policy Director (LB) VMs with active VIP, DPR is not sent to all the diameter peers.

  Conditions: `monit stop all` executed on Policy Director (LB) VMs with active VIP

  Cause: DPR is sent to all the connected diameter peers. However, since `monit stop all` is executed , all the processes on the Policy Director (LB) go down including corosync/haproxy. As a result, some of the DPR messages go out and some are not delivered based on the order of the services going down.

  Workaround: Instead of `monit stop all`, you can stop all the qns process on Policy Director (LB) VMs by executing `monit stop qns-2/3/4` and then issue a `monit stop all` comand.

  With this workaround, processes such as, haproxy/coronsync are up when DPR messages are generated, CPS makes sure that all DPR messages generated by the Policy Directors are delivered.

CSCvq51622: AAA-5065 due to missing RemoteGeoSiteName in /etc/broadhop/qns.conf

This is known issue due to missing RemoteGeoSiteName parameter configuration in qns.conf file or parameter is available but is not added in the SK database shards for the remote sites. You will observe the Null Pointer exception.

If the parameter is configured and remote SK database shards are available, you will not observe the Null Pointer exception.

This CDET is to avoid Null Pointer exception issue which is mentioned above.

CSCvq27866: DRA - Distributor VM not distributing connections in perfect round robin fashion

As vDRA does not support connection rebalancing, sometimes due to improper distribution, a single Policy Director (lb) having more connections than other Policy Directors crosses its rated capacity and results in a call failure.

CSCvr34614: Prometheus Containers stuck in started state after recovering from site failover

Prometheus is the third-party code, used in DRA and Binding VNFs.

For more information related to the issue, see https://github.com/prometheus/prometheus/issues/4058

Issue: Prometheus database blocks contain corrupted data and does not have *meta.json* file to initialize the database when Prometheus comes up.

Solution: Prometheus doesn't have enough capability to repair the corrupted database blocks. Currently, the solution is to manually delete the corrupted block and start the Prometheus process manually.

NOTE: If the Prometheus containers having issue are from Master VM, then some data will not be available and Grafana displays some gap in the data. It is expected behavior as corrupted folders have been deleted. One can access the missing data by adding the data source with another Prometheus container present on control-0 and control-1 VMs (HA for master Prometheus).

The following steps must be performed to delete the corrupted block and start the Prometheus process manually:

NOTE: If there are more than one failed Prometheus containers, the steps need to be repeated for each corrupted block.

1. Connect to the container which has failed to come up.

   ```
   docker connect prometheus-hi-res-s101
   ```

2. From container, check whether Prometheus process is in FATAL state or not.

   ```
   supervisorctl status prometheus
   ```

3. If the process is in "FATAL" state, remove the data folder from container.

   ```
   rm -rf /data-2/*
   ```

   NOTE: The command deletes the data folder. As Prometheus data is available between master/control-0/control-1 VMs, data can be restored.

4. Inside container, start the Prometheus process again.

   ```
   supervisorctl start prometheus
   ```

5. From inside container, check again whether Prometheus process is in RUNNING state or not.

   ```
   supervisorctl status Prometheus
   ```

CSCvr21943: After site resiliency the consul gets struck in STARTED state

Issue: Consul containers remain in STARTED state when a site failure scenario is executed. After the failure scenario is executed, the system does not come up again in the expected state.

Condition: After multiple VM (or) site power off/on cycle, consul containers are stuck in STARTED/STARTING (non-HEALTHY) state.

```
admin@orchestrator[an-master]# show scheduling status | tab | include consul

consul      1     50    infrastructure  SCHEDULING  false

admin@orchestrator[an-master]# show docker service | tab | include consul
```

```
consul  1  consul-1   19.4.5-2019-10-01.8115.4fb2b4a  an-master    consul-1   STARTED  true   Pending health check
consul  1  consul-2   19.4.5-2019-10-01.8115.4fb2b4a  an-control-0 consul-2   STARTED  true   Pending health check
consul  1  consul-3   19.4.5-2019-10-01.8115.4fb2b4a  an-control-1 consul-3   STARTED  true   Pending health check
```

Solution:

- Prepare **peers.json** file: Connect to the consul-1 container.

  ```
  root@consul-1:/# consul info
  ```

  Get the "latest_configuration" value under **raft**:

  Sample output of consul info:

  ```
  ....
  raft:
    ...
      last_snapshot_term = 1083
      latest_configuration = [{Suffrage:Voter ID:bb7e19b5-e709-3c8c-686f-e839e941773f Address:10.42.0.1:8300}
  {Suffrage:Voter ID:66a6756f-49ac-b2a7-74c6-07922e8c2f81 Address:10.40.0.3:8300} {Suffrage:Voter ID:7b62389e-af67-d0f3-
  79d9-95bb356ea52c Address:10.47.128.3:8300} {Suffrage:Voter ID:b753a43f-4278-6f45-27f1-d2f88081b6d3
  Address:10.38.0.30:8300} {Suffrage:Voter ID:ad423368-98bd-d87a-4d73-99520091321b Address:10.45.0.26:8300}
  {Suffrage:Voter ID:b916b8d1-b2dd-4799-db95-09a1e1144380 Address:10.37.0.11:8300} {Suffrage:Voter ID:543ba9f7-110a-
  7559-3607-ea6d5d1ef83b Address:10.37.192.2:8300}]
      latest_configuration_index = 2503803
      num_peers = 6
    ...
  ...
  ```

- **latest_configuration:** This is a list of dictionaries. The number of dictionaries is equal to the **num_peers** field. Each dictionary has 2 keys, which are **Voter ID** and **Address**.

  In the sample output above, the number of dictionaries is 7 (num_peers + self) corresponding to num_peers=6.

  Each dictionary represents the **Voter ID** and **Address** corresponding to each Consul Node (consul-1, consul-2, consul-3, and so on) not in any particular order.

  So, fetch the **Voter ID**/**Address** corresponding to consul-1, consul-2 and consul-3 from the latest_configuration as mentioned below.

  ```
  root@consul-1:/# ifconfig
  ```

  Get the inet addr: value (IP adress) corresponding to ethwe: interface.

  Compare this IP address from ifconfig command against the **Address** field in **latest_configuration**. Make a note of the corresponding **Voter ID** field of the matching **Address** field.

  Identify the values of **Voter ID** and **Address** fields corresponding to consul-1 that need to be populated into peers.json file

  NOTE: Mapping between latest_configuration and peers.json.

  Table 2 - Mapping Table

latest_configuration	peers.json
Address (should be same as IP address got from Consul container's ifconfig command)	address
Voter ID	id

  Similarly, connect to consul-2 and consul-3 containers and get the **Voter ID** for the matching **Address**.

Identify the details of **Address** and **Voter ID** corresponding to consul-2 and consul-3 containers, they must be populated into peers.json file.

Now peers.json file should be populated with details corresponding to consul-1, consul-2 and consul-3 containers as identified above.

- Create peers.json file on Master VM.

  NOTE: The sample peers.json file should not be used. The file is for reference purposes only. Add “id” and “address” fields based on your deployment.

  Sample peers.json

  ```
  -----------------
  [
   {
    "id": "bb7e19b5-e709-3c8c-686f-e839e941773f",
    "address": "10.42.0.1:8300",
    "non_voter": false
   },
   {
    "id": "66a6756f-49ac-b2a7-74c6-07922e8c2f81",
    "address": "10.40.0.3:8300",
    "non_voter": false
   },
   {
    "id": "7b62389e-af67-d0f3-79d9-95bb356ea52c",
    "address": "10.47.128.3:8300",
    "non_voter": false
   }
  ]
  ```

- Restart the service after copying peers.json file:

  peers.json is created on the Master VM.

  Copy peers.json file from Master VM to the Control VM's.

- Stop the services:

  Stop all the services on all the consul containers of Master and Control VM's.

  From Orchestrator CLI:

  ```
  admin@orchestrator[an-master]#  docker connect consul-1
  root@consul-1:/#  supervisorctl stop all
  admin@orchestrator[an-master]#  docker connect consul-2
  root@consul-2:/#  supervisorctl stop all
  admin@orchestrator[an-master]#  docker connect consul-3
  root@consul-3:/#  supervisorctl stop all
  ```

- Copy peers.json file:

  On Master VM, copy peers.json file onto "/data/raft" of the consul-1 container.

  ```
  sudo cp peers.json /data/consul-1/data/raft/
  ```

  On Control-0 VM, copy peers.json file onto "/data/raft" of the consul-2 container.

  ```
  sudo cp peers.json /data/consul-2/data/raft/
  ```

  On Control-1 VM, copy peers.json file onto "/data/raft" of the consu-3 container.

  ```
  sudo cp peers.json /data/consul-3/data/raft/
  ```

- Start the services:

  Start all the services on all the consul containers of Master and Control VM's.

  From Orchestrator CLI:

  ```
  admin@orchestrator[an-master]#  docker connect consul-1
  root@consul-1:/#  supervisorctl start all
  admin@orchestrator[an-master]#  docker connect consul-2
  root@consul-2:/#  supervisorctl start all
  admin@orchestrator[an-master]#  docker connect consul-3
  root@consul-3:/#  supervisorctl start all
  ```

All the consul containers will be restored to HEALTHY state.

```
admin@orchestrator[an-master]# show docker service | tab | include consul
consul  1  consul-1   19.4.5-2019-10-01.8115.4fb2b4a  an-master     consul-1   HEALTHY  false   -
consul  1  consul-2   19.4.5-2019-10-01.8115.4fb2b4a  an-control-0  consul-2   HEALTHY  false   -
consul  1  consul-3   19.4.5-2019-10-01.8115.4fb2b4a  an-control-1  consul-3   HEALTHY  false   -
admin@orchestrator[an-master]# show scheduling status | tab | include consul
consul  1     50    infrastructure  RUNNING     false
```

CSCvv46487: snmpwalk alternatives for CPS 20.2 running on Centos 8

As CPS 20.2.0 is built on CentOS 8.1, *snmpwalk* command has limitations and hence cannot perform a direct snmpwalk on the OID such as .1.3.6.1.4.1.26878.200.3.2.70. Instead of *snmpwalk*, you need to use *snmpget* command along with the complete OID such as .1.3.6.1.4.1.26878.200.3.2.70.1.1. The list of OIDs for the individual machines are available in /etc/snmp/snmpd.conf file. The OIDs are part of the line containing the word proxy.

Here is an example:

```
proxy -e 0x0102030405060708 -v 3 -u cisco_snmpv3 -a SHA -m 0x71d8d544a7447e377fa5fc355d8f08f81f1a901c -x AES -m 0x71d8d544a7447e377fa5fc355d8f08f8 -l authPriv localhost .1.3.6.1.4.1.26878.200.3.2.70.1.1.0  .1.3.6.1.4.1.2021.11.9.0
```

Here **.1.3.6.1.4.1.26878.200.3.2.70.1.1.0** is the OID and hence the snmpget must be triggered as follows:

```
snmpget -e 0x0102030405060708 -v 3 -u cisco_snmpv3 -a SHA -A cisco_12345 -x AES -l authNoPriv -m +/etc/snmp/mibs/BROADHOP-MIB.txt:/etc/snmp/mibs/CISCO-QNS-MIB.txt lb01 ".1.3.6.1.4.1.26878.200.3.3.70.11.2.0" CISCO-QNS-MIB::kpiLBPCRFProxyInternalCurrentSessions.0 = STRING: 0
```

For more information, see *Configuration for SNMP Gets and Walks* section in the *CPS SNMP, Alarms, and Clearing Procedures Guide*.

Limitations and Restrictions

This section covers the following topics:

- Limitations
- Common Vulnerabilities and Exposures

Limitations

- Solicited Application Reporting

  The following are some restrictions on configuration for the new service options:

  - The pre-configured ADC rule generated by CRD lookup has ADC-Rule-Install AVP definition with support for only three AVPs ADC-Rule-Name, TDF-Application-Identifier, Mute-Notification.
  - For AVPs that are multi-valued, CRD tables are expected to have multiple records - each giving the same output.
  - Comma(,) is not a valid character to be used in values for referenced CRD column in SdToggleConfiguration.
  - AVP Table currently only supports OctetStringAvp value for AVP Data-type.
- During performance testing, it has been found that defining a large number of QoS Group of Rule Definitions for a single session results in degraded CPU performance. Testing with 50 QoS Group of Rule Definitions resulted in a 2x increase in CPU consumption. The relationship appears to be a linear relationship to the number of defined QoS Group of Rule Definitions on a service.
- Hour Boundary Enhancement

  Change in cell congestion level when look-ahead rule is already installed:

  If a cell congestion value changes for current hour or any of the look-ahead hours, there will be no change in rule sent for the rules that are already installed.

  No applicability to QoS Rules:

  The look-ahead works for PCC rules only where we have rule activation/deactivation capabilities and can install upcoming changes in advance. However, if the RAN Congestion use case is changed to use the QoS-Info AVP instead of using PCC rules, we need to fall back to the current RAR on the hour boundary implementation for that use case since the standard do not let us install QoS-info changes ahead of time like we can with PCC rules.
- The Cluster Manager's internal (private) network IP address must be assigned to the host name "installer" in the `/etc/hosts` file. If not, backup/restore scripts (`env_import.sh`, `env_export.sh`) will have access issues to OAM (pcrfclient01/pcrfclient02) VMs.
- CSCva02957: Redis instances continue to run, even after Redis is disabled using the parameter `-DenableQueueSystem=false` in qns.conf (`/etc/broadhop/`) file and `/etc/broadhop/redisTopology.ini` file.
- CSCva16388: A split-brain scenario (that is, VIPs are up on both nodes) can still occur when there is connectivity loss between lb01 and lb02 and not with other hosts.

Common Vulnerabilities and Exposures (CVE)

The following is the list of CVEs open in this release:

- CSCvv23847: Evaluation of qps for Grub2-Aug20 vulnerability
  - CVE-2020-10713
- CSCvv29333: CIAM: curl d-bus glibc gnutls libvirt linux-kernel
  - CVE-2016-10739, CVE-2019-10166, CVE-2019-10167, CVE-2019-10168, CVE-2019-10639, CVE-2019-18282, CVE-2019-3016, CVE-2019-3882, CVE-2019-3887, CVE-2019-5481, CVE-2020-10757, CVE-2020-11501, CVE-2020-12049, CVE-2020-13777

Open and Resolved CDETS

The following sections list open and resolved CDETS for this release. For your convenience in location CDETS in Cisco's Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation might be necessary to provide the most complete and concise description.

NOTE: If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

https://tools.cisco.com/bugsearch

To become a registered cisco.com user, go to the following website:

https://tools.cisco.com/RPF/register/register.do?exit_url=

Open CDETS

The following table lists the open CDETS in this release.

CPS Open CDETS

Table 3 CPS Open CDETS

CDETS ID	Headline
CSCvs82943	CWE-176 Improper Handling of Unicode Encoding issue seen during web application http suite
CSCvu29050	All Primary Session db SMs hit 100% CPU upon burst and traffic did not recover.
CSCvu48624	stale values of lwr attribute lwrwps in corner cases
CSCvu62671	Performance Impact - High response time for Gy with SK_DB - 20.2 CentOS 8 SVI Sanity Private Image
CSCvu78157	Rx-AAR-5065 errors observed during Rx-STR burst while same was not the case during Rx-AAR-5065.
CSCvu82089	Increasing trend of Rx-AAR timeouts observed during longevity.
CSCvu98512	CPS Security Testing- VulScan Result-JQuery 1.2 < 3.5.0 Multiple XSS Issue on 20.2
CSCvv07102	Observed errors and timeouts and rx-5065 errors, during the in-service mongo auth enable process
CSCvv21665	Change password in mongodb is not in-service in 20.2 release
CSCvv23847	Evaluation of qps for Grub2-Aug20 vulnerability

CDETS ID	Headline
CSCvv29333	CIAM: curl d-bus glibc gnutls libvirt linux-kernel CVE-2019-5481 and ...
CSCvv30162	Issue in diagnostics.sh options
CSCvv33838	Rx-AAR not rejected if AF-Application ID AVP is missing
CSCvv34543	Continuous Exceptions in logs with patch-10
CSCvv34846	Observed top_qps showing lot of UdcUnSubscribeRequestMessage errors on sp10 and sp11
CSCvv36679	SNMP walk command not getting the qps component OID from MIB
CSCvv37708	Grafana shows incorrect data for RestAPI
CSCvv38709	PCRF is not sending SUCCESS for PCI to MOG in Rx RAR
CSCvv39971	enable_tacacs+ is not working when tacacs_secret is having $ in it
CSCvv42814	Performance Impact seen after enabling real time notification
CSCvv43602	Tags are not padded when tag length configures is less than one of actual tag
CSCvv43623	AAR is getting rejected with IP-CAN_SESSION_NOT_AVAILABLE when SK not found, and FTS is enabled
CSCvv43629	Null Pointer Exception while testing Feature F5031
CSCvv44692	During mongo auth enable or disable observed traffic loss in HA/GR setups

vDRA Open CDETS

Table 4 vDRA Open CDETS

CDETS ID	Headline
CSCvr50904	Security Issues reported in App Scan for vPAS DRA
CSCvu01157	vPAS: Errors-Thread pool reject, queue full after 18Hrs of 190K TPS run, error range- 0-5
CSCvu92283	[vDRA] diameter endpoint is going into unhealthy state after few docker stop and docker restart
CSCvv05278	vPAS: db-vnf not in good state after blade reboot
CSCvv19293	GTAC login is not working for DRA API documentation & API's
CSCvv28443	[vDRA]: MOP steps required to recover some shards in database cluster
CSCvv33250	CIAM: jackson-databind mongodb nurses open source vulnerabilities
CSCvv33257	CIAM: Ubuntu system libraries vulnerabilities
CSCvv34569	[vDRA] DB VM went into joining state when we executed a longevity test in stormy scenario
CSCvv35110	[vDRA] When changing config for stormy scenario, PRIMARY shard display is visible after 15 min

Resolved CDETS

This section lists the resolved/verified CDETS in this release.

CPS Resolved CDETS

Table 5 CPS Resolved CDETS

CDETS ID	Headline
CSCvn24592	During ISSM from CPS 13.1 to CPS 18.2 qns VMs are sending request to disabled udc
CSCvn41655	Quota is not getting updated sometimes by CPS
CSCvo17413	qns node fails to connect to remote sessionmgr during startup
CSCvo76428	Vulnerability observed during HAProxy URL Web Interface Vulnerability Scan
CSCvq61775	Unable to access Control Center GUI when Grafana and CC opened on the same browser
CSCvq83038	The 404 (session not found) is not captured in statistics / bulkstats / Grafana.
CSCvr13820	Delay in CEA/DWR processing causing connection reset by peer
CSCvr54441	Evaluation of qps for Intel 2019.2 IPU
CSCvr76128	validating the configured host configs in noSSH deployment
CSCvr82473	CPS 19.4 Upon entering service after restart, Policy Server causes errors and timeouts
CSCvs02725	Single SH disabled - but SPR delete and query happening still to the SPR DB
CSCvs03948	SK DB sharding "rebuildskdb" and "rebuildAllSkRings" cmd show in running/pending state
CSCvs14226	CPS 19.4.x Performance Numbers not hit
CSCvs39940	Upgrade failing due to whisper status retrieval
CSCvs46255	Differential rating peers are catering SySLR traffic of remote cluster when cluster1 goes down.
CSCvs49188	CPS 19.3 - SK DB sharding: Seeing CCR-I timeouts and Nullpointer exception
CSCvs63645	Incorrect CDRs produced when multiple services configured
CSCvs66497	Need support to disable policy reporting in systems.json
CSCvs81256	Observing that lwr processes did not come up on lwr01 post ISSM
CSCvs81879	Session manager services getting hanged during ISSU
CSCvs89358	show_subs.py not working in pcrfclient
CSCvs93851	Warning message "Realm is registered but all end points are down - for realm" flooded in logs
CSCvs94495	Not able Set Secure Cookies Attributes in CC
CSCvs98673	install.sh fails as it could not backup /opt/whisper/whisper-agent.jar
CSCvt00798	Timeouts seen during ISSM due to QNS process paused early
CSCvt01005	Failure of Rx messages with 5065 after removing of sk.db.skip* paramater from qns.conf
CSCvt01476	ISSM 19.3 to 19.5: lb01 and lb02 /etc/hosts pointing to wrong installer ip
CSCvt07971	vm-init failed on UDC VM conflicting with cloud-init service
CSCvt09682	BEMS01048711: Urgent, Gx+ is not working

CDETS ID	Headline
CSCvt10295	During cluster A upgrade on one of the sessionmgr VM SPR i.e. 27720 mongo process did not come up.
CSCvt10939	sudo cache fails for users authenticated through tacacs
CSCvt12292	Crontab/cronjob execution of update-uaf.sh is running for every minute
CSCvt12422	aido_server- Re-adding replica members in case of GR- Site isolation process
CSCvt14788	Both timeout and error code counters are incremented in case of response with error code
CSCvt15621	Rx-AAR 5065 seen when there are cross site messages of Gx and Rx
CSCvt17261	Default logback has duplicate entry for com.broadhop.diameter2.registry.impl.EndpointRegistry
CSCvt17766	Error while refreshing Custom AVP's {} java.lang.ClassCastException: null
CSCvt20558	sk_search_scan_full stats are not showing correct values as per different values of Ddb.full.scan.tps
CSCvt21013	Next eval time is not getting set properly when 2 Pending Policy counter Info is present in Sy_SLA
CSCvt22348	WPS feature is not removing stale attribute
CSCvt23729	High Mongo response time experienced after enabling the feature
CSCvt28843	migrate.sh rollback option failed to connect to pcrfclient VMs due to ssh hostkey mismatch error.
CSCvt31002	check in the changes to qps statistics in git
CSCvt32636	Mongo processes not coming up when arbitervip moves to another cluster (during 19.5 ISSM)
CSCvt38089	Thick Disk VM Creation not working
CSCvt39990	Stale session does not get cleaned due to timer incremented by subscriber profile refresh
CSCvt41454	inflight messages are not processed after sending DPR even though tcp.hold.timer.after.dpr configured
CSCvt44881	PCRF flooding LDAP Server with Bind Requests in the event of Invalid Credentials Bind Response
CSCvt46606	[PCRF: NAP] : NullPointerException: null while submitting message to QNS from LB on CSP20.1
CSCvt46984	DiameterPeerDown trap being generated continuously every 5 minutes
CSCvt49648	Missing LWR Rx WPS related Stats in QPS_statistics file
CSCvt50154	check in the changes to qps statistics in git
CSCvt51797	http port 80 on cluman listen on all interface after fresh deployment
CSCvt56990	PCRF: NAP states LdapChangeMessage/LdapResponseMessage not seen in grafana states even successful API
CSCvt59599	CDR balanceUsed and balanceRemaining fields are incorrect
CSCvt59637	Deploy all with nossh option is failing with SSL Cert error
CSCvt60973	PCRF is not doing graceful rejection in case of malformed User-Location-Info AVP
CSCvt61349	After upgrade HA setup with CPS PCRF 20.2 Sprint2 ISO Getting ERROR
CSCvt61604	Failed to add a member to replica set with error id field value of 256 is out of range
CSCvt62335	Support for API (PCRF IPV6 Session Key Query) execution on rx/Gx interface

CDETS ID	Headline
CSCvt64183	Gx+: PCRF is not removing ADTM R1 rules when acwentitlement changes mid-session
CSCvt64318	Memcache Timeout Exceptions flooding the QNS logs and repeated traps
CSCvt64799	gen-gx-drop-trap.sh - Provide different threshold values for CCR-I/U/T response times
CSCvt64805	Memory available in Grafana is incorrect for Centos 7
CSCvt65314	Empty error message is coming while import CRD data
CSCvt66202	rebalance fails with java exception
CSCvt67416	Upgrade CentOS to latest stable version 8.1 on CPS and fix security vulnerabilities.
CSCvt70167	Charging Rules not getting installed as of Tariff Times config while DST changes on diameter message
CSCvt73304	Multiple alarms generated with the message 'LDAP Query Result dropped to 0'
CSCvt73511	No UPDATE_REQ from UDC to QNS when the counter list is empty/5015 in SLA-Intermediate
CSCvt76740	Day-Rule does not get installed with TimeZone 4200
CSCvt80130	Change SKDB Scrubbing/Auditing TPS rate default value to 100 TPS rather than 200 TPS
CSCvt80841	Total Bytes field is empty in CCR-T CDR
CSCvt88032	Wrong number of tags shown in generated sessions
CSCvt92439	gen-ldap-trap.sh - enable threshold values to be configurable from yaml/csv
CSCvt96039	Rx-AAR - 5065 observed due to secondary key missing
CSCvt98058	Unable to change password if user forgets the current password
CSCvu03544	During ISSU After upgraded SET-1 it prompted wrong set
CSCvu06707	CPS Stats mismatch
CSCvu07384	UDC is not deleting the session after hold timer expiry in case of Gx RAA-5002
CSCvu14958	UDC - ENT ID is not sent to udc from pcrf for assurance event
CSCvu21234	20.x new KPIs are missing in QPS_Statistics.xlsx
CSCvu26104	PCRF is not setting GBR value same as MBR value for IMS video bearer in case of throttling
CSCvu28307	Diameter All peer down alarm is not getting generated
CSCvu29054	Unable to add new backup sk_shards when already shards backup shards exist.
CSCvu29557	mongo process on sessionmgr VM doesn't t come up when pid and port number collision take place.
CSCvu29607	CPS 19.4, billCycle info not available in GetSubscriber API Resp for subscriber created with balance
CSCvu31713	Subscriber not able to use last chunk of quota when using AmountRemainingWithoutReservation(ARWOR)
CSCvu31769	balanceUsed field is reflecting wrongly as "0" in CDR for CCR-U when TOD is being used.
CSCvu31812	stale-session-cleaner is in 'Not-monitored' state in both pcrfclient VMs
CSCvu33385	some test cases failed due to no SSH response received from CPS server for curl command

CDETS ID	Headline
CSCvu35369	Eliminate dependency on configuring 'StaleSession.SupportedErrorCodes=7000' from qns.conf
CSCvu40692	ErrorCode:15 - Error Searching for Object with key: networkId - did not retrieve a subscriber
CSCvu40709	Error Code 9: Duplicate Value for Unique Data Constraint for ChangeCredentialUsername Request
CSCvu44342	CPS throws NullPointerException on next event post a Rx AAR with blank MCPTT-Id AVP
CSCvu46051	PCRF Diameter Call Fails when Kafka link is down
CSCvu46583	CPS Central - Embedded PB issue
CSCvu52323	diagnostics.sh --get_session_shard_health not showing udc shard information
CSCvu54405	kafka producer not sending enterprise id in CCR-T
CSCvu59273	NTP is deprecated from CentOS 8 onward and chrony is alternative for ntp
CSCvu61656	FTS seen on Sh PNR messages
CSCvu64547	False 3002 Up/Down traps are generated every 5mins
CSCvu67535	Optimize the temporary object creation when SK-DB Janitor scrub runs
CSCvu69917	gen-db-traps.sh - Log the error while generating alarm
CSCvu70426	Command Execution Getting Timedout post Upgrade to CentOS8
CSCvu70971	Subscription ID AVP not sent in Sy-STR
CSCvu90139	cluman is not showing cps version, CM is not listening at port 80.
CSCvu90493	Different qns load for the same two services
CSCvu90935	Quota on breach does not send Real Time Notification
CSCvu91929	Incorrect Logging on upgrade status even though upgrade was not successful
CSCvu92274	After upgrade ISO Error coming during doing 'rebalance'
CSCvu93920	Improper peer down status reported by show_peers.py
CSCvu94718	Observed Continuous Sd-CCR-T message Timeouts, after ISSM from 19.5
CSCvu96554	Arbitervip and Resource Group is not Moving to C-B side on post Centos 8 upgrade HA setup
CSCvu97554	Exception - An error occurred while processing a Sync Policy Action
CSCvu99761	Traffic loss is observed during the disabling mongo auth process in HA and GR
CSCvv02947	Unable to Migrate Arbiter VM via ISSM
CSCvv04009	list_installed_features.sh throws errors when run by non-root user
CSCvv07671	PCRF sending 5002 errors for Rx AAR
CSCvv07821	rsyslog service bouncing because port value is missing in /etc/rsyslog.conf
CSCvv11955	diagnostics.sh --policy_revision_status failing for VMs with space separated hostname in /etc/hosts
CSCvv15086	iproute-tc package not available with CentOS8 - Unable to add or remove latency for GR Regression

CDETS ID	Headline
CSCvv15386	Errors during PATS installation on Centos8
CSCvv16000	Mongo replica sets in arbitervip vm are not moving to transitionToAuth state, after ISSM
CSCvv16634	PCRF is terminating Rx session on receiving RAA-3004 but not on RAA-3002
CSCvv17197	Service 'mon_qns_lb' not found on lb after migration
CSCvv18901	SAR report not showing /var/log/sa
CSCvv20105	AN Trusted AVP should be sent in Rx_AAR and Rx_RAR message for IP_CAN_CHANGE notification
CSCvv20128	Configuration Option to set RAT TYPE as VIRTUAL when the IP_CAN_TYPE is NON_3GPP_EPS(6)
CSCvv23316	No TPS_COUNT nor SESSION_COUNT data in consolidated-sessions.log
CSCvv31342	puppet, monit summary is not running on lb02 after set-1 deployed_during ISSM
CSCvv34725	CPS_PSB_Tyw52036c_SEC-PWD-LIMOLD: Limit old password reuse _ PSB linux job is failed
CSCvv40333	SNMPV3 snmptrap not sent to NMS server (PATS VM)
CSCvv41559	CPS does not match Balance Code returned in the Result of STG/CRDT for Quota Reservation

vDRA Resolved CDETS

Table 6 vDRA Resolved CDETS

CDETS ID	Headline
CSCvr75104	DRA - DB VMs in joining state and mongo containers are missing from the VM
CSCvs09998	vPAS: continuous Rx AAR timeouts when mongo auth disable steps followed.
CSCvs22514	State_13 for Shard members after Mongo-auth Enable
CSCvs83154	vDRA Memory depletion on persistent DB VM on site DB down over a period
CSCvs87885	vDRA - Shard-10 not showing PRIMARY in database status, in actual it has PRIMARY assigned
CSCvs97592	[VDRA] System upgrade gets stuck at 6.25% for one of the db vnf
CSCvs97709	vDRA - Downgrade from Latest Vers is not supported when setup is not on latest VMDK
CSCvt07846	IPv6 bindings not getting deleted after PCRF query
CSCvt15192	Routing to remote site fails if last peer group of the peer route is inactive
CSCvt17532	Diameter health check script not checking for whole IP address match - upgrade stuck
CSCvt28271	vDRA 19.4: Security test point to the /etc/passwd cps-app user
CSCvt29907	High CCR-I/CCR-T burst, without rate limiting enabled, causes bindings with incorrect SRK
CSCvt34974	vDRA - RAM Depletion for DB VMs while running 170K TPS traffic, Mongo exception observed in logs
CSCvt38698	API is unable to fetch imsi-apn binding in mongo-sharded setup
CSCvt38840	Local site Arbiter member stuck in STATE_13 intermittently when remote sites are down

CDETS ID	Headline
CSCvt43273	With active control plane, messages are routing to a remote site even there is no active relay link
CSCvt44901	Rx messages with MPS-identifier AVP failing onPeer limit is reach, message is not prioritized as P0
CSCvt50192	vPAS: Resp Time surge observed form DDs & for differ Message type too during Control & Master- OFF/ON
CSCvt53950	vDRA: Minor Memory depletion on persistent DB VM on site DB down/UP over a period
CSCvt56963	fPAS_19.4_patch6: Static DB rate limit is not being imposed in mongo based sharding environment
CSCvt64188	missing zone sharding clear zoneinfo script in orchestrator
CSCvt70649	VIP not failing over to drd02 after resiliency test done at ESXi host level
CSCvt83200	vDRA: Post ISO upgrade of DRA-APPVNF,two containers of Control VMs-going into STARTED/ABORTED state
CSCvt87293	Audit RAR messages are breaching configured rate limit
CSCvt96988	ConfD rollback data getting wiped out after an ISO upgrade
CSCvu09539	Unable to find route: DiameterRoute log enhancement
CSCvu29122	[vDRA-SVI]: Issues seen when using docker start command for diameter-endpoint
CSCvu29462	HopbyHop Identifier greater than 32 bits
CSCvu31502	other VMs local host name is wrongly mapped to installer (master) internal ip
CSCvu32748	Deletion of agg-stats.0.csv leading to disk space issues
CSCvu35071	build fix in cps_microservices_base_image/cps_microservices_deployer repositories
CSCvu37568	[vDRA]: DRA DP2: show network IPs not showing all the VIPs and other IPs
CSCvu38654	Enhancing Err Response in CCA for generalized error timeout 3002.
CSCvu41543	Preventive fix for binding deletion for out of sequence CCR-I and CCR-T calls
CSCvu51431	build fix in cps_microservices_base_image/cps_microservices_deployer repositories
CSCvu58014	vDRA - Alert Create Time gets updated intermittently when alerts are in firing state
CSCvu94380	[vDRA]: Medium severity vulnerability reported for DRA during nessus scan
CSCvv17186	vPAS: 20.2- Removal of mongo-auth passkey is getting timed-out
CSCvv19279	DB VNF cli debug get-shardindb-output output text needs to be changed
CSCvv19488	vPAS: State_93 and mongo-monitor in STARTED state after lab outage
CSCvv27691	Remove weak ciphers (SHA) from 10443 (zvision) port
CSCvv28188	[vDRA]: Tmpfs distribution is showing wrong in mongo-s*** containers
CSCvv39810	[vDRA]: Ubuntu 16.04 LTS / 18.04 LTS / 20.04: software-properties vulnerability (USN-4457-1)

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 Cisco Policy Suite.

- *CPS Advanced Tuning Guide*
- *CPS Backup and Restore Guide*
- *CPS CCI Guide for Full Privilege Administrators*
- *CPS CCI Guide for View Only Administrators*
- *CPS Central Administration Guide*
- *CPS Documentation Map*
- *CPS Geographic Redundancy Guide*
- *CPS Installation Guide - OpenStack*
- *CPS Installation Guide – VMware*
- *CPS Migration and Upgrade Guide*
- *CPS Mobile Configuration Guide*
- *CPS Operations Guide*
- *CPS Policy Reporting Guide*
- *CPS Release Change Reference*
- *CPS Release Notes*
- *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *CPS Troubleshooting Guide*
- *CPS Unified API Reference Guide*
- *CPS vDRA Administration Guide*
- *CPS vDRA Configuration Guide*
- *CPS vDRA Installation Guide for VMware*
- *CPS vDRA Operations Guide*
- *CPS vDRA SNMP and Alarms Guide*
- *CPS vDRA Troubleshooting Guide*

These documents can be downloaded from https://www.cisco.com/c/en/us/support/wireless/policy-suite-mobile/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 deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

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)