Cisco Policy Suite 21.1.0 Release Notes

First Published: February 25, 2021

Last Updated: October 7, 2021

Introduction

This Release Note identifies installation notes, limitations, and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 21.1.0. 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 21.1.0 software package (ISO image) from:

https://software.cisco.com/download/home/284883882/type/284979976/release/21.1.0

Md5sum Details

PCRF

adc7f45a2112224ca564f5472121da98	CPS_21.1.0.release.iso_signed.tar.gz
7254f3ffa67ef289105531a0fc0969d9	CPS_21.1.0_Base.release.qcow2_signed.tar.gz
f2aaa163bf474b23e69746f33508ff5a	CPS_21.1.0_Base.release.vmdk_signed.tar.gz

DRA

f35515615fac2ec968155ffb3dd212fe	CPS_Microservices_DRA_21.1.0.release.iso_signed.tar.gz
bd708fd84645b684e9f94532835da753	CPS_Microservices_DRA_21.1.0_Base.release.vmdk_signed.tar.gz
41717fb273074bba9aa13d6b3c6dff5c	CPS_Microservices_DRA_21.1.0_Deployer.release.vmdk_signed.tar.gz
cdc4eec48aca4b1c982a2168c551e627	CPS_Microservices_DRA_Binding_21.1.0.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	21.1.0.release
API Router	21.1.0.release
Audit	21.1.0.release
Balance	21.1.0.release
Cisco API	21.1.0.release
Cisco CPAR	21.1.0.release
Congestion Reference Data	21.1.0.release
Control Center	21.1.0.release
Core	21.1.0.release
CSB	21.1.0.release
Custom Reference Data	21.1.0.release
DHCP	21.1.0.release
Diameter2	21.1.0.release
DRA	21.1.0.release
Fault Management	21.1.0.release
IPAM	21.1.0.release
ISG Prepaid	21.1.0.release
LDAP	21.1.0.release
LDAP Server	21.1.0.release
LWR	21.1.0.release
Microservices Enablement	21.1.0.release
Notification	21.1.0.release

Component	**Version**
Policy Intel	21.1.0.release
POP-3 Authentication	21.1.0.release
Recharge Wallet	21.1.0.release
SCE	21.1.0.release
Scheduled Events	21.1.0.release
SPR	21.1.0.release
UDC	21.1.0.release
UDSN Interface	21.1.0.release
Unified API	21.1.0.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 viru s, 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 21.1.0 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 sou rce 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 21.1.0 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 sour ce credential configuration capability. Graphite data source requires common data source credential to be configured using Grafa na 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/CPS 19.5.0 to CPS 21.1.0.

NOTE: CPS 19.5.0 was a Limited Availability release with user restrictions.

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 Gr afana 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: CPS 21.1.0 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/CPS19.5.0 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: CPS 21.1.0 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 21.1.0.

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

In-Service Software Upgrade (ISSU) is not needed when migrating from CPS 19.4.0/CPS 19.5.0 to CPS21.1.0 .

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`
  - o `-Dmongo.client.thread.maxWaitTime.balance=1200`
  - o `-Dmongo.connections.per.host.balance=10`
  - o `-Dmongo.threads.allowed.to.wait.for.connection.balance=10`
  - o `-Dmongo.client.thread.maxWaitTime=1200`
  - o `-Dmongo.connections.per.host=5`
  - o `-Dmongo.threads.allowed.to.wait.for.connection=10`
  - o `-Dcom.mongodb.updaterIntervalMS=400`
  - o `-Dcom.mongodb.updaterConnectTimeoutMS=600`
  - o `-Dcom.mongodb.updaterSocketTimeoutMS=600`
  - o `-DdbSocketTimeout.balance=1000`
  - o `-DdbSocketTimeout=1000`
  - o `-DdbConnectTimeout.balance=1200`
  - o `-DdbConnectTimeout=1200`
  - o `-Dcontrolcenter.disableAndsf=true`
  - o `-DnodeHeartBeatInterval=9000`
  - o `-DdbConnectTimeout.balance=1200`
  - o `-Dstatistics.step.interval=1`
  - o `-DshardPingLoopLength=3`
  - o `-DshardPingCycle=200`
  - o `-DshardPingerTimeoutMs=75`
  - o `-Ddiameter.default.timeout.ms=2000`
  - o `-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 21.1.0 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 SdToggleCon figuration.
  - AVP Table currently only supports OctetStringAvp value for AVP Data-type.
- During performance testing, it has been found that defining many 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 DRA CVEs open in this release:

- CSCvx05836 - CIAM: Ubuntu system library vulnerabilities

  — CVE-2019-18276,CVE-2019-5481,CVE-2019-5443,CVE-2019-19646,CVE-2019-9923,CVE-2019-3855,CVE-2019-13115, CVE-2020-1747,CVE-2019-19246,CVE-2019-9070,CVE-2019-9075,CVE-2020-11655,CVE-2020-11656
- CSCvw73327 - CIAM: mongodb, zookeeper, ncurses, sqlite, go

  - CVE-2019-13734,CVE-2019-20838,CVE-2019-15043,CVE-2020-13379,CVE-2019-2390,CVE-2019-20925,CVE-2019-17221, CVE-2018-21035,CVE-2020-26160,CVE-2019-10192,CVE-2020-14147,CVE-2020-28362,CVE-2020-7919,CVE-2020-28367

- CSCvx05887 - CIAM: Zing libraries vulnerabilities.
  - CVE-2020-2803,CVE-2020-2816,CVE-2020-2805,CVE-2020-2604,CVE-2020-8492,CVE-2019-20907,CVE-2019-9948,CVE-2019-16056

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 t o 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
CSCvw84771	PCRF is not mirroring PCI value from MOG AAR when sending Gx RAR
CSCvx14463	diagnostics.sh script is taking indefinite time to display health check results in some scenarios
CSCvx30637	Exception thrown when Session Id Handling configuration is enabled with an invalid regex.

vDRA Open CDETS

Table 4 - vDRA Open CDETS

CDETS ID	Headline
CSCvw73327	CIAM: mongodb zookeeper ncurses sqlite go
CSCvx05836	CIAM: Ubuntu system Library Vulnerabilities.
CSCvx05887	CIAM: Zing library Vulnerabilities.
CSCvx08040	Grafana displaying contradictory logs for different panel width and duration
CSCvx14701	Gx / Rx Timeout dashboard shows incorrect message processing time
CSCvx42930	Some CRD table do not allow rows to edit which has null/blank fields.

CDETS ID	Headline
CSCvx45818	Some database CLIs execution fails with permission denied error

Resolved CDETS

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

CPS Resolved CDETS

Table 5 - CPS Resolved CDETS

CDETS ID	Headline
CSCvv05099	SVN error is observed in ClusterA while fetching policy audit once ISSM is completed on both Cluster
CSCvv30162	BEMS01129718 issue in diagnostics.sh options
CSCvv36679	snmpwalk command not getting the qps component OID from MIB
CSCvv46496	The config_br.py backups the sessionDB data which is contradicting to the product document.
CSCvv61026	Realtime -Notification is not getting triggered for all types of Threshold type defined in CRD table
CSCvv62029	Diameter Successful TPS is reduced after installing latest Patch
CSCvv67042	Attempting to enable smart licensing generates error
CSCvv76377	OSGI access to JMX on eth1 of both PCRF clients
CSCvv82797	LWR SubscriberUpdate with "last_change_feid":null
CSCvv84066	ServiceType amount in SubscriberType
CSCvv97117	Mongo password visible in ps output in SessionMgr VM (CT1937: SEC-SCR-CONFLEAK-3)
CSCvv97885	removal of shard from balance db is not working
CSCvv98825	qns logs indicate an "errmsg" : "auth failed" when connecting to binding db sessionmgr and port
CSCvv99613	broadhop alarm/traps are incorrect when send Realtime Notification
CSCvw03326	UDC trying to retrieve subscriber LWR record from UDC that is down and gives error
CSCvw12529	/etc/sudoers changes getting overwritten by reinit.sh when F528 is enabled
CSCvw17568	CPS PCRF 19.4, LB not clearing the alerts of peer down after the peers are connected
CSCvw40253	Deletion / Deactivation of balance service is not deleting mon key while uninstalling the rules
CSCvw43384	Delayed incomplete response to Rx STR with Required-Access-Info=0 for VoLTE to VoWiFi handover
CSCvw46277	Gx 3GPP-User-Location-Info evaluation in policy condition in case of RAT_CHANGE
CSCvw53947	On start of engine_id service, it's giving error intermittently
CSCvw58470	cannot modify subscriber on 20.2 AIO
CSCvw58976	TACACS support for UDC VMs

CDETS ID	Headline
CSCvw61996	CDR does not support multiple quota code, balance used and balance remaining values
CSCvw69818	CDR info incomplete when Usage report is sent for inactivated service.
CSCvw70079	Move auth.info logs to /var/log/secure instead of /var/log/messages
CSCvw73519	PCRF 20.2 on CVIM 3.4.6 - TACACS not authenticating properly
CSCvw74003	UDC is sending multiple SUBSCRIPTION_ID AVPs in SLR-Intermediate instead of one
CSCvw77206	CPS 20.2 : Cluster Manager boot up time is quite high post Centos 8
CSCvw77530	diagnostics.sh and about.sh is broken with non-root user
CSCvw89974	hidden parameter not set to true for arbiter members after fresh install
CSCvx00228	Restrict ARP Normalization in Rx-AAR PRELIM and FINAL message when there is only one Rx Session
CSCvx01216	Performance degrades of createSubscriberRequst
CSCvx07745	CPS is dropping CCR-I & CCR-T messages intermittently
CSCvx10817	diagnostics.sh reporting "all peers are down" alarms which is not accurate
CSCvx14116	Enable TACACS script showing line 39: TMPFILES: unbound variable
CSCvx36059	show_subs.py script is working for LDAP auth but failing for Sh/No auth

vDRA Resolved CDETS

Table 6 - vDRA Resolved CDETS

CDETS ID	Headline
CSCvv08594	Application Troubleshooting Enhancement (KPI and Grafana)
CSCvv19293	GTAC login is not working for DRA API documentation & API's
CSCvv25132	Grafana KPI Expression query - Peer Response time
CSCvv33250	CIAM: jackson-databind open-source vulnerabilities
CSCvv33257	CIAM: Ubuntu system libraries vulnerabilities for linux-kernel
CSCvv74233	[vDRA]: Ubuntu16.04LTS/18.04LTS/20.04:nss vulnerability, Ubuntu16.04LTS/18.04LTS:Samba vulnerability
CSCvv83241	Multiple Vulnerabilities in dnsmasq DNS Forwarder Affecting Cisco Products: January 2021
CSCvv98119	Grafana takes long time to load when number of peers is high
CSCvw05903	CRD table displays wrong value (Peer Group SRK Mapping- Destination Host Routing Rule)
CSCvw06416	NTPD warning because of a stale NTP process
CSCvw08636	Mediation failed (Add/remove postfix) without mandatory AVP dictionary configured
CSCvw18745	HSTS not being enforced for DRA Master, Controller and CentralGUI on port 10443,
CSCvw22612	Home directory not created for GTAC users.

CDETS ID	Headline
CSCvw25120	vDRA, logger level check failed when run from remote VM
CSCvw25340	vDRA, Need orchestrator cli for - admin database status
CSCvw38652	vDRA, Error processing control plane message null pointer exception
CSCvw47378	vDRA: Security-Intel Microcode vulnerabilities(USN-4628-1) & Linux kernel vulnerability(USN-4627-1)
CSCvw47383	[vDRA]: Ubuntu 16.04 LTS/18.04 LTS/20.04 LTS/20.10 : python-cryptography vulnerability (USN-4613-1)
CSCvw47397	vDRA: AccountsService vulnerabilities, OpenLDAP vulnerability, Samba vulnerabilities & MongoDB Auth
CSCvw68751	DRA: Enhancement Req: Docker logging improvement
CSCvw70123	DRA: improve orchestrator container for health check visibility
CSCvw72083	DRA: Directors Validate fields/IPv6 Binding / Detect Improper CRD table
CSCvw73385	ISO Upgrade takes more time for Bind-VNF as mongo-monitor-s* takes high time
CSCvw75803	During Resiliency of VIP Interface LINK_DOWN Test. VIP not going back to Primary directly
CSCvw83714	[vDRA]:Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10 : OpenSSL vulnerability (USN-4662-1)
CSCvw85221	NO_PEER_GROUP_MEMBER_AVAILABLE alert message doesn't mention if the peer group is local or remote
CSCvw99464	GTAC access to perform GUI queries/post actions, to check API, Docs, bulk-stats, is not working
CSCvw99846	[vDRA]:Ubuntu 16.04 LTS : Linux kernel vulnerabilities (USN-4681-1)
CSCvx18130	ntp-relay not started, failed after few tries due to stale NTP process
CSCvx18595	Validation of blank or white spaces in CRD for the Key/Required fields.
CSCvx20131	Sudo Privilege Escalation Vulnerability Affecting Cisco Products: January 2021
CSCvx31461	Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 20.10 : OpenLDAP vulnerabilities (USN-4724-1)

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 Advanced Tuning 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 se rvice.

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.