Cisco Policy Suite 19.4.0 Release Notes

First Published: July 25, 2019

Last Updated: August 30, 2019

Introduction

This Release Note identifies installation notes, limitations and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 19.4.0. Use this Release Note in combination with the documentation listed in the *Related Documentation* section.

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 *CPS Release Change Reference*.

Installation Notes

Download ISO Image

Download the 19.4.0 software package (ISO image) from:
https://software.cisco.com/download/home/284883882/type/284979976/release/19.4.0

Md5sum Details

PCRF

39c15b3c2f9aa488aab2f9cdc092bc53	CPS_19.4.0_Base.release.qcow2_signed.tar.gz
e083674572aa5fc233680a17ad713127	CPS_19.4.0_Base.release.vmdk_signed.tar.gz
65da94fdf5b843ef7e1d8bf69683cbd6	CPS_19.4.0.release.iso_signed.tar.gz

DRA

6bd8a70973c04952517956211ca5623c	CPS_Microservices_19.4.0_Base.release.qcow2_signed.tar.gz
ca5b0643c424717b2bf2f8c3c8fdadbc	CPS_Microservices_19.4.0_Base.release.vmdk_signed.tar.gz
52ca116bedcb8c716b032f4a7d509832	CPS_Microservices_19.4.0_Deployer.release.qcow2_signed.tar.gz
4783ade568626d473a9c5e893ea362a2	CPS_Microservices_19.4.0_Deployer.release.vmdk_signed.tar.gz
f5f8a945cc14fa94f0ea7ef7cb952461	CPS_Microservices_DRA_19.4.0.release.iso_signed.tar.gz
ea75600b63a4653bc2eeedf6ef067f72	CPS_Microservices_DRA_Binding_19.4.0.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	19.4.0.release
API Router	19.4.0.release
Audit	19.4.0.release
Balance	19.4.0.release
Cisco API	19.4.0.release
Cisco CPAR	19.4.0.release
Congestion Reference Data	19.4.0.release
Control Center	19.4.0.release
Core	19.4.0.release
CSB	19.4.0.release
Custom Reference Data	19.4.0.release
DHCP	19.4.0.release
Diameter2	19.4.0.release
DRA	19.4.0.release
Entitlement	19.4.0.release
Fault Management	19.4.0.release
IPAM	19.4.0.release
ISG Prepaid	19.4.0.release
LDAP	19.4.0.release

Component	Version
LDAP Server	19.4.0.release
LWR	19.4.0.release
Microservices Enablement	19.4.0.release
Notification	19.4.0.release
Policy Intel	19.4.0.release
POP-3 Authentication	19.4.0.release
Recharge Wallet	19.4.0.release
Scheduled Events	19.4.0.release
SPR	19.4.0.release
UDC	19.4.0.release
UDSN Interface	19.4.0.release
Unified API	19.4.0.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 19.4.0 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 an 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.

NOTE: In CPS 19.4.0, additional application and platform statistics are enabled. Hence, there can be an increase in the disk space usage at pcrfclient VMs. Once CPS 19.4.0 is deployed, monitor the disk space usage and if required, increase the disk space.

OpenStack Environment

To perform a new installation of CPS 19.4.0 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 an 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.

NOTE: In CPS 19.4.0, additional application and platform statistics are enabled. Hence, there can be an increase in the disk space usage at pcrfclient VMs. Once CPS 19.4.0 is deployed, monitor the disk space usage and if required, increase the disk space.

Migrate an Existing CPS Installation

To migrate an existing CPS installation, see the *CPS Migration and Upgrade Guide*. CPS migration is supported from CPS 18.0.0/18.2.0 to CPS 19.4.0.

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 an 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: In CPS 19.4.0, additional application and platform statistics are enabled. Hence, there can be an increase in the disk space usage at pcrfclient VMs. Once CPS 19.4.0 is deployed, monitor the disk space usage and if required, increase the disk space.

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

To upgrade an existing CPS installation, see the *CPS Migration and Upgrade Guide*. CPS upgrade is supported from CPS 19.3.0 to CPS 19.4.0.

NOTE: Before upgrade, 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 upgrade. If you fail to add the user, then Grafana will not have an access to Graphite database and you will get continuous prompts for Graphite/Grafana credentials.

All Grafana users configured will be available after upgrade. 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: In CPS 19.4.0, additional application and platform statistics are enabled. Hence, there can be an increase in the disk space usage at pcrfclient VMs. Once CPS 19.4.0 is deployed, monitor the disk space usage and if required, increase the disk space.

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 of 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 to disable 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.

- 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

CSCvi94552: Primary Member is Isolated from all Arbiters

Issue: If the primary database member gets isolated from all the arbiters then diagnostics output displays incorrect states.

Solution: If a member is shown in an unknown state, it is likely that the member is not accessible from one of other members, most likely an arbiter. In that case, you must go to that member and check its connectivity with other members. Also, you can login to mongo on that member and check its actual status.

CSCvn06270: PB publishing time is high in B if compare with A Cluster

Issue: It takes longer time to publish the Policy Builder configuration in HA clusters.

Condition: SVN source and destination repositories are on different hosts/clusters rather than on the same host/cluster.

Solution: This is SNV server behavior and not CPS issue. If you are publishing on same host then use *svn copy* command and if host is different than use *svn import* command. As mentioned in the SVN docs, copy is faster than import.

For example, if you are logged in using http://lbvip02/repos/configuration and publishing to http://lbvip02/repos/run then both the hosts are same (lbvip02) and you can *use svn copy* command.

But if you are logged in using http://lbvip02/repos/configuration and publishing to http://<different_host>/repos/run then you can use *svn import* command.

SVN import takes more time than copy command. So this is expected SVN server behavior.

The recommendation is, if you want to publish on different host or cluster, then open Policy Builder of other cluster and use other Cluster's run repository to publish.

1. Export policy configurations from hostA (clusterA) and push the same on hostB (clusterB) in /repos/configuration using SVN import command.
2. Open Policy Builder with other Cluster's IP address.
3. Login to Policy Builder with http://lbvip02/repos/configuration.
4. Publish to Cluster's to run repository using http://lbvip02/repos/run.

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.

Limitations and Restrictions

This section covers the following topics:

- Limitations
- Common Vulnerabilities and Exposures

Limitations

- The following restriction applies to LWR:
  - In this release, LWR supports read and write of one user attribute to the replication framework specific to the ADTM bearer counting attribute.

    In future releases, UDC and other applications will be enhanced to provide support of new attributes or user profile details that may require replication
- 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.
- The Linux VM message.log files repeatedly report errors similar to the following:

  `vmsvc [warning] [guestinfo] RecordRoutingInfo: Unable to collect IPv4 routing table.`

  This is a known issue affecting ESXi 5.x. Currently, there is no workaround for this. The messages.log file entries are cosmetic and can be safely ignored. For more information, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2094561
- 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.

CSCvq31313: Alarms raised are not getting Cleared even after the shards are brought up

Limitation: When a GR site failover happens and sessionmgr VMs on Site1 are shutdown, the database shards which are primary become secondary post failover. Since these VMs are not reachable, the shards are not reachable alarm is generated.

When the primary becomes reachable, the alarms generated don't get cleared. This is a stale alarm which needs to be ignored until the bug is fixed.

CSCvq63596: Alarm/alert not generated when a single mongo shard db is down while it is configured in admin db

Limitation: No alarm/alert is generated when a single shard database is manually dropped from a MongoDB replica-set, but is still configured in the Admin database. However, CPS *diagnostics.sh, --get_session_shard_health* option does display the affected shard database is in an "err" state. Even though this scenario is unlikely, the user still should be alerted if a single configured shard database is dropped/down.

Common Vulnerabilities and Exposures (CVE)

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

- CSCvp36655: Multiple Vulnerabilities in glibc
  - CVE-2018-19591, CVE-2013-1914, CVE-2018-20796, CVE-2013-4458, CVE-2017-1000409, CVE-2013-4332, CVE-2009-5155, CVE-2013-0242, CVE-2019-9169, CVE-2013-4237, CVE-2019-7309, CVE-2019-6488
- CSCvp36735: Multiple Vulnerabilities in sssd
  - CVE-2019-3811, CVE-2018-16838, CVE-2018-16883
- CSCvp36738: Multiple Vulnerabilities in wget
  - CVE-2016-7098, CVE-2018-20483
- CSCvp71683: Evaluation of qps for Intel 2019.1 QSR – MDS
  - CVE-2018-12127, CVE-2018-12126 , CVE-2018-12130, CVE-2019-11091

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 2 CPS Open CDETS

CDETS ID	Headline
CSCvk52072	During longevity run with Redis enable, system response time for CCR-I/T increased upto ~8-9 ms.
CSCvn73888	Observing Traffic loss during In Service Migration from CPS 13.1 to CPS 18.2
CSCvo09736	LwrStreamer Logs flooding in region 2 and region 3. Brokers are up and running
CSCvo94066	Performance degradation observed with ZING enabled on CPS 19.2.0
CSCvp22928	REDIS not generating all EDR fields in csv file
CSCvp36930	PCRF does not update the health check timer after CCR-U received for revalidation timer expire
CSCvp71683	Evaluation of qps for Intel 2019.1 QSR - MDS
CSCvp93314	Issue with API Router while creating the subscriber with Balance
CSCvp99275	The GUI "import all" features over utilizes CPU resource by 25-30%
CSCvq17980	in install.sh --User input prompt is showing wrong value
CSCvq24369	UDC is sending LDAP messages on already closed connection
CSCvq37340	Sy SLA error not mapped with proper error code
CSCvq40603	LWR processes not getting started after reboot the LWR VM
CSCvq54392	Not able to import SVN using "Import/Export API" url however same works with CPS Central
CSCvq56711	All TPS dropped after a policy rollback
CSCvq58509	LDAP Write CRD tables evaluation result in multiple duplicate operations
CSCvq58639	Request change to DEBUG level of message "POLICY RESULT ERROR: NO_LDAP_ATTRIB-UTE_FOUND 1"
CSCvq58682	PCRF is not sending Charging Rule as per sec 4.4.5 of 29.214 incase flow-description is not present
CSCvq59909	Broken softlink leads to missing of Platform patches

CDETS ID	Headline
CSCvq60066	Inconsistent behavior with next hop routing for Gx RAR retry messages

Microservices Open CDETS

Table 3 Microservices Open CDETS

CDETS ID	Headline
CSCvk39920	DRA - Wrong TPS displayed on Grafana after rebooting DD-1, PR-1 and DW on site1
CSCvp48553	DRA - orchestrator-backup containers not working properly
CSCvp94651	DRA - after control vm power off/power on cycle, some Grafana stats are incorrectly displayed.
CSCvq15669	DRA - jdiameter exception thrown on session count limit threshold
CSCvq18829	DRA - Weave connections issue to all the VNF VMs if Master is redeployed
CSCvq25709	DRA - High CPU spike on all Bind VNF VMs post bringing down 1 DB instance
CSCvq27866	DRA - Distributor VM not distributing connections in perfect round robin fashion
CSCvq33406	Site failover or DD failure takes 2min for VIP to come UP
CSCvq35646	DRA - some intermittent call fails on 3 days longevity
CSCvq39177	DRA - One worker CPU single spike to 100% after rebooting control VM
CSCvq45175	DRA - add Distributor VIP's to IP_NOT_REACHABLE alert.
CSCvq45202	DRA - PGW client connections not balanced post Application upgrade
CSCvq52640	DRA - Unable to route AAR message post bulk relay peers flap
CSCvq61671	DRA - Peer flap observed when distributor VM reboot.

Resolved CDETS

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

CPS Resolved CDETS

Table 4 CPS Resolved CDETS

CDETS ID	Headline
CSCvn94961	VM taking 20 ~ 25 seconds to ssh. Issue with systemd-logind, d-bus packages.
CSCvo74555	vPCRF - Rule Install Retry doesn't work when used with QCI/ARP mirroring
CSCvo76428	Vulnerability observed during HAProxy URL Web Interface Vulnerability Scan

CDETS ID	Headline
CSCvo85402	Nessus Scan Vulnerability: Web Server HTTP Header Internal IP Disclosure
CSCvp22554	CPS is not sending Rx RAR to MOG with custom dpcc report after ccr-u wait timer expiry
CSCvp25193	Whisper service install failing on UDC VMs during 19.1.2 ISSM or Fresh install
CSCvp33006	[PCF-SVI] Unable to open CRD USD table
CSCvp36644	Unassign Multiple Vulnerabilities in bind
CSCvp36672	Multiple Vulnerabilities in Grafana
CSCvp36730	Multiple Vulnerabilities in samba
CSCvp47098	Incorrect bill cycle is assigned for subscriber having 2 balance quotas
CSCvp47247	'E11000 duplicate key error index' error for Np call model on Sol2 VMW GR setup.
CSCvp48904	ERROR: "Sk db async max wait time reached: 500" in GR VMW Sol2 lead to Gx-CCR-U/T 5002
CSCvp51661	NullPointerException occurred while creating Sy v11 session : {}
CSCvp53290	sessionmgr init file residual left after remove replica sets
CSCvp53381	No package should be updated after executing 'yum update --assumeno'
CSCvp56109	Provide passphrase generation for users
CSCvp60198	Improper QoS Action handling
CSCvp60541	Optimize current BLANK_PROFILE scenario, avoid extra unsubscribe on collision & throttle notification
CSCvp61755	Diagnostics script output Missing Last Sync Time when arbiter is down
CSCvp65752	Script app_monitor fails to restart application in case of large number of TIME_WAIT connection
CSCvp71136	CPS: Blueprint error observed while publishing PB
CSCvp73644	diagnostics.sh replica status showing some part of ipv6 address
CSCvp73784	SPR indexes dropped manually, do not get restarted/re-created after qns process restart
CSCvp78198	ifrename.py script throws error when two or more network drivers are used
CSCvp78205	Sy Pending Policy Counter not working
CSCvp78231	Improve PCF Policy Engine Logging
CSCvp78277	local_time_sync script enhancement needed to wait until lb VM comes up
CSCvp78540	No action on Pending-Policy-Counter status of Sy-SUBSCRIBER-STATUS as CANCELED_SUB
CSCvp79115	"NullPointerException: null" during broadcast of soap notification from site2 to site1
CSCvp79493	Add Region name in LWR mirror-maker consumer groupId to avoid partial replication

CDETS ID	Headline
CSCvp82209	Retry_Attempts_Exhausted is not shown in Grafana even if there are "max retries reached"
CSCvp83563	NTP Conflict with Chronyd Service on Fresh Install / Upgrade
CSCvp83678	msec format not updated in GR.
CSCvp83937	Some QNS process are not getting paused during ISSM after traffic swap
CSCvp86618	LWR processes not getting started after ISSM
CSCvp86626	Traffic restore script stuck due to SILO command blocked
CSCvp88331	changes made manually in mongoConfig.cfg is getting overridden on OSP setup
CSCvp91055	Flooding of INFO logs after enabling feature
CSCvp91071	No alarms in either trap file or active alarm (diagnostics.sh) after shard down
CSCvp91903	SILO Support for Multiple LB setup. I do not see qns excluding endpoints to LB03
CSCvp91936	java.lang.OutOfMemoryError: GC overhead limit exceeded when feature is enabled
CSCvp93439	MongoDB Client Resiliency Improvement
CSCvp96770	Issue in Mongo PrimaryDB connectivity
CSCvp97403	Provision to limit number of session loaded on query
CSCvq06394	vm-init script failed when bond interface is configured for internal network
CSCvq07354	Alarm Resync Feature - Fixes
CSCvq21609	[PCF SVI] - Rx & N7 binding don't work on IPV6 address
CSCvq21717	[PCF SVI] - Rx STA 5002 & Rx ASA Time Out issue
CSCvq22061	Request for MIN support in LDAP notification (without IMSI)
CSCvq23097	UDC traps to control center regarding outgoing API timeouts framed incorrectly.
CSCvq23128	Control center process failure represents single point of failure for CPS alerting
CSCvq23939	Add Alarm Resync Feature in add_component_notification_to_db script
CSCvq24335	Incorrectly appending Binding health check counter for AAA with 0 (bindDB_AAA_0), BEMS970074
CSCvq25983	No trap is getting recorded into /var/log/snmp/trap
CSCvq27329	PCRF is throwing NPE while running the call flow as per section 4.4.5 and 4.4.5a on 29.214
CSCvq32280	UDC throwing exception while upgrading from CPS 18.2 to 19.3
CSCvq33317	Peer Monitoring: Filter by All Visible Columns Doesn't Work for Peer IP or Application ID
CSCvq33694	monit is getting stopped on the LB VM after the puppet completion

CDETS ID	Headline
CSCvq34755	Upgrade failed and halted at "waiting puppet to finish" stage on TMO drop2
CSCvq36143	Observing com.mongodb.MongoTimeoutException in qns for skdb configuration after upgrade to CPS 19.3
CSCvq37113	Disabling SET-2 is failed while doing ISSM 18.2 to CPS 19.3 Patch_1, due to lbvip02 not came up
CSCvq41723	Inconsistency in CPS after upgrade to CPS_19.3.3_20190702_055445_79.iso
CSCvq41858	[PCF-SVI] N7 traffic completely stops after configuring engine with skdb config
CSCvq47704	diagnostics.sh --lwr "checking LWR diagnostics" more than 4K times
CSCvq47718	after vm-init in lwr, it is waiting & printing ...not set
CSCvq47968	Null pointer exception encountered when PLF query response is sent by pcf to pcrf.
CSCvq48055	Calls failing on GR setup
CSCvq48539	Some of the mongo services stopped after arbitervip shift
CSCvq49613	qns diagnostics is not printing all required VM's/ports information in output.
CSCvq49823	API support required for OSP installation.
CSCvq51043	If both PCF sites is down, all PLF queries on PCRF time out even when session is present on pcrf.
CSCvq53659	while running diagnostics.sh, cpu load average is increasing & no of diag.. process is more than 120
CSCvq58271	callP stops when feature is enabled (true)

Microservices Resolved CDETS

Table 5 Microservices Resolved CDETS

CDETS ID	Headline
CSCvp11943	DRA - High CPU usage for worker VMs in 96 shards setup
CSCvp18889	DRA - mongo health status check scripts causing High CPU on DB Master VM for 192 shards setup
CSCvp27438	Director uses IPv6 VIP as source for neighbor solicitation
CSCvp45019	vPAS: Error in querying reference data. Max number of threads (maxWaitQueueSize) of 125 has exceeded.
CSCvp48703	Mongo Authentication : Changing password using CLI on DRA VNF not working
CSCvp52899	DRA - DB related errors while running longevity at 70 K TPS with APP based sharding
CSCvp63303	DRA - consul connection exceptions causing database config load issue

CDETS ID	Headline
CSCvp66463	DRA - Worker contributing to DB stats shooting to 100% cpu utilization
CSCvp70574	vPAS: show system diagnostics displays false alarm output.
CSCvp73912	vPAS: weave container crashing on binding db vm and won't restart even after vm reboot
CSCvp74166	vPAS: MongoShardPinger warn logs : 27020 in unreachable mongos
CSCvp75114	vPAS: diameter-endpoint automatically starting after issuing 'docker stop' command.
CSCvp79164	ipv6 interface discovery fails on distributor
CSCvp88400	vPAS: Grafana screen is not updating correct count for IMSI APN and MSISDN APN binding query.
CSCvp88417	vPAS: Static sessions not cleaned up after Stale session expiry count reached.
CSCvp92266	upgrade stuck with mongo auth enabled
CSCvp97629	vPAS: Distributor taking long time to reconnect peers among the active directors
CSCvp99957	vPAS: Peer response time graph is been plotted incorrectly in grafana after 57K TPS traffic
CSCvq03634	orchestrator java process hitting GC overhead limit
CSCvq07169	vPAS: Changing shard-metadata-db-connection config on the fly is not working as expected.
CSCvq10596	supervisorctl stop unexpected behavior when PRIMARY of a shard is stopped
CSCvq10951	DRA - upgrade stuck due to high Master CPU and I/O Wait issue
CSCvq13972	add member or arbiter fails sometimes - need fix in mongo healthcheck
CSCvq13990	vPAS: Peer connections not syncing among distributor clients and servers.
CSCvq15228	vPAS- IMSI/MSISDN APN Binding-static session goes to zero
CSCvq17241	vPAS: RX-_AAR time out
CSCvq20575	DRA - continuous few CCR-I timeouts at the beginning of call model
CSCvq22325	Distributor connections are dropped after changing the configuration
CSCvq22357	vPAS: director spinning at 95% for 24 minutes after cyclic endpoint container restart.
CSCvq24991	vPAS: result FAILED : Unable to set password.com.mongodb.MongoCommandException
CSCvq25373	vPAS: docker engines going in JOINING state after reboot/networking restart.
CSCvq25880	DRA - Timeout observed after PB publish on DRA at load call model of 125K TPS
CSCvq27619	Optimize mongo-auth functionality
CSCvq27990	DRA - CCR and AAR timeouts during initial bring up of Call Model
CSCvq29175	vPAS: WARN logs flooding weighted peer selection total weight 0 <= 0 for relay calls.

CDETS ID	Headline
CSCvq33340	vPAS: WARN level logs seen during longevity - queueCounter removed reason: EXPIRED, key:
CSCvq35538	DRA - Exceptions for IPv4 connections during longevity run
CSCvq37573	vPAS: Rx-AAR errors observed during Longevity run post MongoDB Authentication
CSCvq38881	vPAS: exception - there are no users authenticated is observed after mongo auth set on DRA VNF.
CSCvq41724	vPAS: Grafana shows negative values Query response graph.
CSCvq43281	vPAS: change mongo auth password is not working as expected.
CSCvq43444	vPAS: Mongo Auth password plain text printed in application logs.
CSCvq44867	vPAS: mongo auth change password causes AAR failures on DRA vnf side.
CSCvq44896	vPAS: password visible in mongod process running on vm.
CSCvq48313	Statistics document update for platform Prometheus status
CSCvq51105	vPAS: endpoint error logs : Error sending message java.lang.NullPointerException: null
CSCvq52134	DRA - Issue in Grafana's Planning datasource: Not able to see Application summary stats
CSCvq52655	vDRA Deployer: TLS 1.2 support
CSCvq55731	DRA - Binding config parameter is getting duplicate on modifying the value
CSCvq57526	vPAS: mongo auth sync passwd causing reloading connections and AAR timeouts.
CSCvq57879	DRA - AAR timeouts when trying to test site failover TPS on latest sprint build
CSCvq59364	DRA Migration: Session/Binding count stopped after upgrading to 19.4

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 ANDSF Configuration Guide*
- *CPS ANDSF SNMP and Alarms 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 LWR Guide*
- *CPS LWR Installation Guide - OpenStack*
- *CPS LWR Installation Guide - VMware*
- *CPS Migration and Upgrade Guide*
- *CPS Mobile Configuration Guide*
- *CPS MOG API Reference*
- *CPS MOG Guide*
- *CPS MOG Installation Guide - OpenStack*
- *CPS MOG SNMP, Alarms, and Clearing Procedures Guide*
- *CPS MOG Troubleshooting 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 UDC Administration Guide*
- *CPS UDC API Reference*
- *CPS UDC Installation Guide*
- *CPS UDC Session Migration Guide*
- *CPS UDC SNMP and Alarms 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)