Cisco Policy Suite 19.3.0 Release Notes (1)

First Published: June 02, 2019

Last Updated: October 08, 2021

Introduction

This Release Note identifies new features and enhancements, limitations and restrictions, and open and resolved CDETS in Cisco Policy Suite (CPS) software version 19.3.0. 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

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 19.3.0 software package (ISO image) from:
https://software.cisco.com/download/home/284883882/type/284979976/release/19.3.0

Md5sum Details

013cb8c14634dff65f0a1b5368243516	CPS_19.3.0.release.iso.tar.gz
84fc7e92a01d6d2842407cad2755a279	CPS_19.3.0_Base.qcow2.release.tar.gz
04b05fa275a1bec28e50f2c1e75f9f0b	CPS_19.3.0_Base.vmdk.release.tar.gz

Component Versions

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

Table 5 Component Versions

Component	Version
ANDSF	19.3.0.release
API Router	19.3.0.release
Audit	19.3.0.release
Balance	19.3.0.release
Cisco API	19.3.0.release
Cisco CPAR	19.3.0.release
Congestion Reference Data	19.3.0.release
Control Center	19.3.0.release
Core	19.3.0.release
CSB	19.3.0.release
Custom Reference Data	19.3.0.release
DHCP	19.3.0.release
Diameter2	19.3.0.release
DRA	19.3.0.release
Entitlement	19.3.0.release
Fault Management	19.3.0.release
IPAM	19.3.0.release
ISG Prepaid	19.3.0.release
LDAP	19.3.0.release
LDAP Server	19.3.0.release
LWR	19.3.0.release
Microservices Enablement	19.3.0.release
Notification	19.3.0.release
NSSF	19.3.0.release
PCF	19.3.0.release
Policy Intel	19.3.0.release
POP-3 Authentication	19.3.0.release
Recharge Wallet	19.3.0.release
SCE	19.3.0.release
Scheduled Events	19.3.0.release
SPR	19.3.0.release

Component	Version
UDC	19.3.0.release
UDSN Interface	19.3.0.release
Unified API	19.3.0.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 19.3.0 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 19.3.0, additional application and platform statistics are enabled. Hence, there can be an increase in the disk space usage at pcrfclient VMs. Once CPS 19.3.0 is deployed, monitor the disk space usage and if required, increase the disk space.

OpenStack Environment

To perform a new installation of CPS 19.3.0 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 19.3.0, additional application and platform statistics are enabled. Hence, there can be an increase in the disk space usage at pcrfclient VMs. Once CPS 19.3.0 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 14.0.0/18.0.0 to CPS 19.3.0.

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 19.3.0, additional application and platform statistics are enabled. Hence, there can be an increase in the disk space usage at pcrfclient VMs. Once CPS 19.3.0 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 18.2.0 to CPS 19.3.0.

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 19.3.0, additional application and platform statistics are enabled. Hence, there can be an increase in the disk space usage at pcrfclient VMs. Once CPS 19.3.0 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 set tings 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

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.

CSCvp86618: LWR processes not getting started after ISSM

Issue: After the LWR VMs were migrated, the LWR process is not getting started automatically.

Condition: Issue occurs during ISSM from CPS 18.2.0 to CPS 19.2.0 and later release.

Workaround:

NOTE: The steps need to be executed per cluster and per set after deploying VM for LWR.

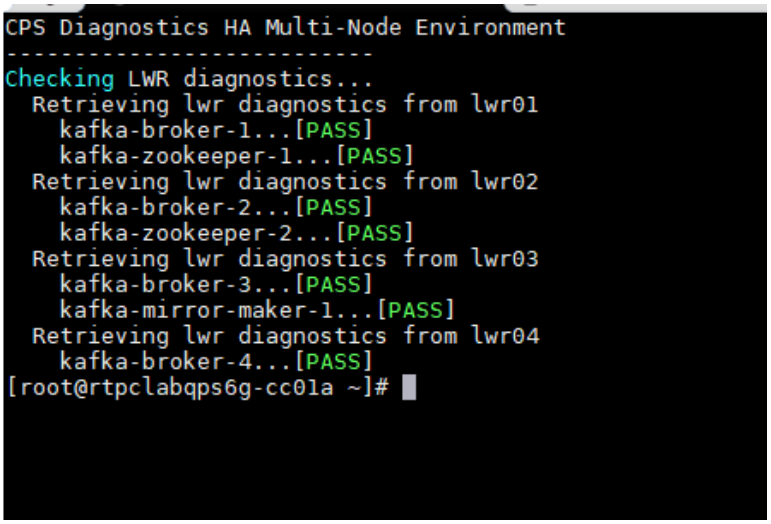
1. Run the following commands on LWR VM:

   ssh root@<LWRHostName>

   build_kafka_server.sh --migrate-vm <Region Name> <Mirror number>

2. Repeat Step 1 for all LWR VMs after deploying.
3. After running above step on all LWR VMs on same cluster, verify zookeeper, broker, mirror-maker are UP by running the following command:

   diagnostics.sh --lwr_diagnostics



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.
- CSCvp73644: diagnostics.sh replica status showing some part of ipv6 address
  diagnostics.sh replica status displays some part of IPv6 address in REPLICA SET STATE field if IPv6 address is more than 23 characters.

Common Vulnerabilities and Exposures (CVE)

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

- CSCvp71683: Evaluation of qps for Intel 2019.1 QSR – MDS
  - CVE-2018-12127, CVE-2018-12126 , CVE-2018-12130, CVE-2019-11091
- CSCvp36644: Unassign Multiple Vulnerabilities in bind
  - CVE-2018-5741, CVE-2017-3141, CVE-2019-6465, CVE-2013-6230, CVE-2014-0591, CVE-2018-5745, CVE-2016-2775, CVE-2013-4854
- 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
- CSCvp36730: Multiple Vulnerabilities in samba
  - CVE-2018-14629, CVE-2018-16853, CVE-2018-16851, CVE-2018-10919, CVE-2018-10918, CVE-2018-1140, CVE-2019-3824, CVE-2019-3880, CVE-2018-16841
- 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

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 6 CPS Open CDETS

CDETS ID	Headline
CSCvh53895	Rx AARs are not routed via secondary when Mongo DB primaries are down.
CSCvh89463	qns process in QNS VM does not recover when backup sessionmgr's are down
CSCvi23619	After ISSU, diag shows list of alarms not cleared, while conn btwn LB & PCEF/CSCF/TDF clients came up
CSCvj29993	vPAS DRA: Region 1 failure cause 1 minute outage on region 2.
CSCvk52072	During longevity run with Redis enable, system response time for CCR-I/T increased upto ~8-9 ms.
CSCvn04062	session replica set going to recovering state on leaving load running on vzw setup
CSCvn70448	call failures with MongoWaitQueueFullException exception in logs with high tps >20K, on 14.0.1drop19
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
CSCvo17404	c.b.policy.impl.RulesPolicyService java.lang.IllegalArgumentException: null
CSCvo17405	RAR Collisions occurring, race condition seen on CPS 18.0 (ASE 3.0)
CSCvo61728	Idel CPU on 2 qns VMs is much higher than remaining qns VMs, on scale setup.
CSCvo76428	Vulnerability observed during HAProxy URL Web Interface Vulnerability Scan
CSCvo77082	mongodb-logs are not getting rotated and growing very huge - 16GB
CSCvo94066	Performance degradation observed with ZING enabled on CPS 19.2.0
CSCvp01393	Sylog Defect POLICY RESULT ERROR: Error saving session
CSCvp01446	burst of ccr-i and ccr-t at 50K / sec - application seems to process but no response received pcef
CSCvp22554	CPS is not sending Rx RAR to MOG with custom dpcc report after ccr-u wait timer expiry
CSCvp22928	REDIS not generating all EDR fields in csv file
CSCvp25193	Whisper service install failing on UDC VMs during 19.1.2 ISSM or Fresh install
CSCvp25862	PATS is delaying send messages, which is causing failures in automation
CSCvp27161	Number of AVPs exceeded documented limit.
CSCvp32982	After disabling zing also, zing-memory status shows as INITIALIZED at LB02
CSCvp36274	Delete quarantined entry only if default pool is defined and IP is available
CSCvp36644	Multiple Vulnerabilities in bind
CSCvp36655	Multiple Vulnerabilities in glibc
CSCvp36730	Multiple Vulnerabilities in samba
CSCvp36735	Multiple Vulnerabilities in sssd
CSCvp36738	Multiple Vulnerabilities in wget

CDETS ID	Headline
CSCvp36930	PCRF does not update the health check timer after CCR-U received for revalidation timer expire
CSCvp38312	WARN message in diagnostics for VMs Post Upgrade to CPS19.3 S1
CSCvp41428	Performance Degradation on Scale setup Post Upgrade to CPS19.3 S1 - Increase in Response Time
CSCvp47247	'E11000 duplicate key error index' error for Np call model on Sol2 VMW GR setup.
CSCvp53290	BEMS946608. Cannot remove replica sets
CSCvp56121	Unable Retrieve Diameter Stats From Graphite Db
CSCvp57877	During Load, only 25% of Sy-STR seen for dynamic Sy-realm evaluation with SingleSy enabled
CSCvp60198	Improper QoS Action handling
CSCvp60541	Optimize current BLANK_PROFILE scenarios to query MIND when message is revalidated after 30min
CSCvp61755	Diagnostics script output Missing Last Sync Time when arbiter is down
CSCvp62630	Execution intermittently failing due to SSH Response not available
CSCvp63161	On CRD import we see diameter request failures
CSCvp63380	Competing replica set priorities
CSCvp64616	Removing subnet from dynamic pool throws error when dynamic free ip list not created for subnet
CSCvp65306	gx and rx timeouts observed once during qns reboot multiple times separated by 10
CSCvp65502	CALEA log filled the disk and VM crashed
CSCvp65752	Script app_monitor fails to restart application in case of large number oif TIME_WAIT connection
CSCvp66657	Increase in response time with 19.3 sprint 3 early drop 2 build
CSCvp69046	Exceptions during broadcast of soap notification from site2 to site1
CSCvp71048	Subscribers of all clusters or locations won't appear in CC in Active-Active GR setup
CSCvp71136	CPS: Blueprint error observed while publishing PB
CSCvp71683	Evaluation of qps for Intel 2019.1 QSR - MDS
CSCvp73644	diagnostics.sh replica status showing some part of ipv6 address
CSCvp74332	Calls Failures during ISSM due to missing lbvip02 after set1 migration (after traffic swap command)
CSCvp75265	Beyond 2500 diameter TPS, all CDRs are not getting written in csv.
CSCvp78205	Sy Pending Policy Counter not working
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
CSCvp79674	Sol-3 call model broken in load condition having high number of timeouts for Rx-AAR,Sy-SNR,CCR-I/U
CSCvp82209	Retry_Attempts_Exhausted is not shown in Grafana even if there are "max retries reached"
CSCvp82251	noisy memory in sm nodes leads to timeouts/error spikes

CDETS ID	Headline
CSCvp83563	NTP Conflict with Chronyd Service on Fresh Install / Upgrade
CSCvp83884	Timeout support required for REST/SOAP response messages
CSCvp83937	Some QNS process are not getting paused during ISSM after traffic swap
CSCvp84217	Rx-ASR observed going out from pcrf while running noisy cpu on sm nodes
CSCvp84261	Observed 20% performance degradation after enabled the SKDB on build CPS 19.3
CSCvp86618	LWR processes not getting started after ISSM
CSCvp86626	Traffic restore script stuck due to SILO command blocked
CSCvp89477	Failed to store featureData as prevFeatureData
CSCvp91055	Flooding of INFO logs after enabling Feature F3526
CSCvp91071	No alarms in either trap file or active alarm (diagnostics.sh) after shard down
CSCvp91141	Timeouts and high response time during issu from 14.0.1 Drop 22 to Drop 23
CSCvp91152	Lb01 Node process qns02 not accepting any connections post ISSU from 14.0.1 Drop 22 to Drop 23
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 F3526 is enabled
CSCvp93314	Issue with API Router while creating the subscriber
CSCvp93435	Failed to store featureData as prevFeatureData- Error Flooding

Resolved CDETS

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

CPS Resolved CDETS

Table 7 CPS Resolved CDETS

CDETS ID	Headline
CSCvk26197	start-db-traps.sh is not finishing with success and report the following error in /var/log/messages
CSCvn06506	Security AppScan Test: Older TLS Version Supported
CSCvn43499	Tacacs configuration on cluman remove when running reinit.sh
CSCvn76709	Stale sessions are not getting removed on a permanent basis
CSCvn94814	19.1 SSL Vulnerabilities
CSCvn95204	active mq exceptions from lb nodes to other nodes
CSCvo12098	java.lang.ClassCastException: java.lang.String cannot be cast to java.util.List
CSCvo14185	LWR Processes Up/Down Traps are needed

CDETS ID	Headline
CSCvo14313	ARP/QCI mirroring failing to take the right ARP/QCI for pending policy evaluation
CSCvo14600	CCA-i response time increase upon disconnecting all UDCs from LWR in a region
CSCvo21016	Issue creating mirror maker process - pid file not created
CSCvo29904	Cache data out of date - max retries reached. retryCounter: 2
CSCvo32990	Subscriber is not getting cleared from SPR on receiving CCR-T.
CSCvo35075	individual session count stats showing old values when total session count is zero
CSCvo36816	Puppet ssh_authorized_key causes failure
CSCvo37141	BEMS899005 - Sessionmgr's boot in recovery state after reboot
CSCvo65930	unreadable/cropped values in PB
CSCvo66313	Haproxy-diameter Execution failed on passive LB
CSCvo76498	puppet should not be successful with wrong node_type in broadhop.profile
CSCvo83578	Grafana old data missing while ISSM 14.0.1 to 19.2 when Prometheus Datastore enabled
CSCvo83593	/mnt/iso/migrate disable set 2 command Failed
CSCvo83636	many call failures with 3004 after "/mnt/iso/migrate.sh traffic restore" cli
CSCvo83658	collision on Sy SLR-I halts Gx session update and doesn't trigger needed RAR
CSCvo84430	java.lang.NullPointerException - DiameterGxTGPPDeviceMgr.getSessionLifecycle
CSCvo85222	ERROR c.b.c.s.mongosk.MongoSkJanitor - Exception while scrubbing sk shard
CSCvo85384	endpoint db populated with wrong ipv6 addresses after ISSM from 14.0.1 to 19.1.3
CSCvo85912	GR SITE tags got removed from rs.conf of session/spr replica sets after ISSM(14.0.1 to 19.1.3)
CSCvo87473	rebalance of shards timing out on full blown gr setup
CSCvo87719	aido unable to bring up arbitervip member in replica sets (Ipv6 address has ::1)
CSCvo90648	Transaction Manager - Ending Balance transaction when it has not been started - Logs Flooding
CSCvo94974	PRA-Identifier AVP Value type wrongly encoded
CSCvo98582	message Timeouts when Message Count Threshold per PD Configured
CSCvo98865	SY-OCS session stale. no next eval set and expiration hours crossed
CSCvp01698	CALEA X1 Alarms not clearing from Diagnostic
CSCvp02737	Syprime Session Termination is not initiated on Gx_CCR-T
CSCvp05377	Full db scan is happening for "userIdenityKey" for Np call model executes with full TSP
CSCvp08582	control center GUI showing duplicate credentials while spr DB doesn't
CSCvp10407	Kafka logs ending in *.out in are not log rotated
CSCvp21054	BEMS928919 : config_br.py --action import --mongo <<file>> procedure is NOT working/failing

CDETS ID	Headline
CSCvp22873	LDAP write generating multiple bind/unbind request and creating multiple tcp connections
CSCvp29459	UDC is not retrying for LDAP modify failure on backoff timer expiry
CSCvp34490	[PCF-SVI] N28 - Nchf_SpendingLimitControl_Unsubscribe service operation timed out
CSCvp34813	gen-failover-traps.sh rasied incorrrect failover traps and .lst files were empty on the setup
CSCvp36745	Monitoring Key Dosage Override option not working with Shared Per User Limit use case
CSCvp37737	For GR deployment memcache misses are incorrectly reported as memcache timeouts in stats
CSCvp38399	Getting"ERROR c.b.spr.impl.PolicyEngineMsgQueue - exception during submit!"after upgrade 19.3sprint1
CSCvp41385	Sync action resubmits message multiple times causing session collision
CSCvp41471	Session growth issue - RxCaleaFeature duplicates added
CSCvp46942	Solution3 Call Model Broken Post CentOS 7.6 Upgrade on Scale Setup
CSCvp47098	Incorrect bill cycle is assigned for subscriber having 2 balance quotas
CSCvp48759	Not able to search subscriber through Control Center.
CSCvp48904	ERROR: "Sk db async max wait time reached: 500" in GR VMW Sol2 lead to Gx-CCR-U/T 5002
CSCvp50427	Seeing POST rules during upgrade/rollback between patch 19 and 25
CSCvp51661	NullPointerException occurred while creating Sy v11 session : {}
CSCvp53381	No package should be updated after executing 'yum update --assumeno'
CSCvp54529	qns is sending 11 digit MSISDN in FETCH_REQ profile refresh retry leading to duplicate UDC sessions
CSCvp58077	Call model with memcache
CSCvp59360	TableDrivenGxMindAttributes does not works on CCR-U
CSCvp59625	pcrfclient qns.log continuously showing Unexpected character ('\' (code 92)): error
CSCvp63834	tempOptions.xmi causing policy corruption
CSCvp64272	LWR diagnostics not working with qns user
CSCvp69802	During 19.3 ISSM , there is no Grafana is showing before recreate set 2 VMs
CSCvp73784	SPR indexes dropped manually, do not get restarted/re-created after qns process restart
CSCvp74212	After completion ISSU full path process "Stale Session" rate is high
CSCvp78198	ifrename.py script throws error when two or more network drivers are used
CSCvp79493	Add Region name in LWR mirror-maker consumer groupId to avoid partial replication
CSCvp83678	msec format not updated in GR.
CSCvp88258	Error in Puppet log on cluman and Non-cluman VMs
CSCvp88331	changes made manually in mongoConfig.cfg is getting overridden on OSP setup

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 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 API Reference*
- *CPS UDC Administration Guide*
- *CPS UDC Installation Guide*
- *CPS UDC Session Migration Guide*
- *CPS UDC SNMP and Alarms Guide*
- *CPS Unified API Reference 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.