Cisco Policy Suite 19.2.0 Release Notes (1)

First Published: April 3, 2019

Last Updated: October 8, 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 19.2.0. 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

This section identifies features that are new or modified in this release.

ANDSF

No new features or changes were introduced in this release.

ATS

For more information on ATS features, contact your Cisco Account representative.

Kubernetes Artifact Collection

ATS now supports artifact collection of kubernetes platform using kubetail command. To support the artifact collection, following parameters have been introduced:

- QPS.setupType = K8S (New setup type for Kubernetes platform)
- <Logger_Name>.EnableShell = <true/false> (Feature to select shell or channel for artifact collection)

Prometheus JSON Output Validation

ATS now supports verification of Prometheus metrics. You can now:

- Collect Prometheus Metrics
- Validate Prometheus Metrics
- Save Prometheus Metrics

Support for Advanced Control Structure

ATS now supports an advanced control structure as follows:

- Supports nested if-else using conditional expression
- Supports nested if-else on next grammar execution result
- Supports and/or conditional expression to any nested layer
- Supports numeric comparison and string comparison with in same conditional expression.
- Supports nested loops of up to 16 layers
- Supports advanced cucumber reporting for loop execution
- Supports execution of complete loop execution at outer most loop end grammar
- Supports multiple load message bundle in a feature file.
- Supports message bundle loading of all PATS driver present in the POM irrespective of whether the driver is mentioned in the initialized grammar.
- Supports Message Bundle loading depending on some condition (if/else block).
- Supports loading Message Bundle within a loop.
- Supports loading Message Bundle inside the custom teardown block.
- Supports reference or included feature file while loading of single/multiple message bundle.
- Supports usage of data of the message bundle loaded in the parent file in the included or reference file.

Support for Asynchronous Web Service Server Auto Response

ATS now provides support of asynchronous auto response from web service server.

Support for Controlled Step Execute in Reference Feature File

Previous Behavior: All the steps of a reference feature file were executed from another file.

New Behavior: ATS now supports controlled step execution in reference feature file. The steps can be executed based on step number(s) or step label(s).

Support for Dynamic WebService Client

ATS now provides support of dynamic web service client start and validation of request received in any SITE WS Server.

Support for Handling Dynamic SOAP header

ATS now provides support to override the SOAP header using the feature file while sending a generic soap call.

Support for InfluxDB Grammars

ATS now provides support for InfluxDB driver:

- To execute any native query on a remote InfluxDB system and validate the response data.
- To perform tool specific statistics validation and save the output in a single grammar.

Support for NASREQ Grammars

ATS now provides support for NASREQ grammars.

Support for Tag Based Feature Life Cycle Control

When any test execution fails, the default behavior of ATS is to skip remaining feature file steps. ATS now provides support to continue the test case execution until the end of the feature file for some selective test case. The framework provides an option to continue test case execution even after any step failure by providing a special tag.

Support for WaitForMessage and HandleMessage

ATS now provides support for WaitForMessage and HandleMessage in LFS APIs and it validates by using separate grammars.

Support for Wildcard Characters in LFS

ATS now supports wildcard characters which can be used while using an attribute for fetching a specific data in a LFS response message. The following operations can be performed:

- Fetching data based on wildcards in key.
- Applying wildcard on the condition of a specific key. In the condition both criteria and the value can have the wildcard support.

Wildcards have the following limitations:

- They are not supported for the matching value.
- Wildcard support is currently for validating the data. Data overriding grammar does not support wildcard.

Behavior Changes

Bulk Statistics Display Issue

Previous Behavior: In previous release, the bulkstats was displayed with gauge value without decimal point value.

Old format is:

G,udc02,tcpconns.all.tcp_connections.TIME_WAIT,9

New Behavior: In this release, the bulkstats are displayed with gauge values up to one point precision.

New format is:

G,sav-sessionmgr02,tcpconns.all.tcp_connections.TIME_WAIT,130.0

CSCvn38710 - Need to optimize mongo_stats.sh execution

Previous Behavior: In previous releases, mongo_stats.sh used to run on pcrfclient via collectd and fetch mongostat/mongotop of all members defined in *mongoConfig.cfg* from pcrfclient.

New Behavior: In this release, individual sessionmgr VMs will collect the statistics of the replica members present on them and send it to local pcrfclient/collectd. With this approach, only local site members statistics is displayed in Grafana.

You also need to change the Grafana query to collect the statistics from sessionmgr VMs.

Impact on Customer: Grafana query change which collects MongoDB statistics. With this change, MongoDB statistics only from the local site are visible.

CSCvo64649 - session limit overload protection should have a default value

Previous Behavior: Session hard limit parameters were used.

New Behavior: A new mandatory field for **Session Limit Overload Protection** is added. For the deployments using JSON files for Policy Builder configuration, the newly introduced field should be added in JSON file and its value should be set to recommended value (2 * license count) or maximum number of sessions that are supported by the hardware, whichever is less, so that the upgrade is seamless.

In a GR setup, the value for **Session Limit Overload Protection** must be set to session count of all session replica sets (from both sites).

Impact on Customer: If the parameter is not added in JSON file, upgrade fails.

Even if you add a default value of zero in JSON file, you will not be able to publish the Policy Builder. You need to configure 1 or above as **Session Limit Overload Protection**. Hence, default value 0 which means infinite number of sessions will not work.

For GUI-based configuration, the field introduced is validated to check if the value is not 0. During the ISSU upgrade, '0' will be added as default and alarm will be triggered to change the value. You must change this value after upgrade.

Enhance Session Hard Limit Parameter to Accept Absolute Value

- sendErrorOnSessionCreateNotAllowed

  Previous Behavior: After hard limit percentage threshold is breached and the parameter is set to true, error messages were sent back to PCEF instead of dropping the message.

  New Behavior: Sends error messages to PCEF when session count exceeds Session Limit overload protection value.

  If **allow.sessioncreation.license.periodic.check=false**, same error messages are sent during license validation failure.

  If **allow.sessioncreation.license.periodic.check=true**, same error messages are sent during QNS start/restart and license validation failure. Once QNS is started and license validation fails in between (user error – removing entry from database, removing license file or corrupt license file), QNS will process traffic successfully.

- diameter.resultCodeOnSessionCreationNotAllowed=5012(default).

  Previous Behavior: When the parameter is explicitly set to some value, the configured error code is sent on Diameter response after session hard limit percentage has exceeded.

  New Behavior: Same error code can be configured when session count exceeds session limit overload protection. This is combined with parameter **sendErrorOnSessionCreateNotAllowed=true**.

Geographic Redundancy

Support Secondary Key Database for In-Memory Lookup

CPS now supports SK database (MongoDB based SK lookup) in Geo-HA deployments. For SK database, new OSGi commands have been added.

qns.conf file parameter **diameter.dropOnSaveFailure** has been renamed to **diameter.dropOnSaveFailure** in this release.

The default value of **sk.db.asyncMaxWaitInMs** in *qns.conf* file has been changed from 2000 milliseconds to 500 milliseconds.

The following *qns.conf* file parameters have been added:

- sk.db.skipRemote
- sk.db.skipRemotePrimary

For more information on *qns.conf* file parameters, contact your Cisco Account representative.

For more information, see the following sections:

- *OSGi Console* in the *CPS Operations Guide*
- *session_cache_ops.sh* in the *CPS Operations Guide*

LWR

Support to Add Zookeepers

LWR now supports the option to add zookeepers instance (must be a follower and not a leader) to an existing region through a method of procedure outlined in the following guides:

- CPS LWR Installation Guide for OpenStack
- CPS LWR Installation Guide for VMware

For more information, see *Adding New Zookeepers* section in the *CPS LWR Installation Guide for OpenStack* and *CPS LWR Installation Guide for VMware*.

Upgrade Kafka

LWR now supports Kafka 2.0.0 release. This has been done to accommodate bug fixes on Apache Kafka distribution.

NOTE: There is no impact on the features which were using earlier release (1.0.0) of Kafka.

With the new Kafka release, there is no impact on ISSU. During ISSU, when *vm-init/reinit* is called by the upgrade scripts on the LWR VMs, the new package will be propagated to the LWR VMs.

/var/qps/bin/support/lwr/build_kafka_server.sh has been enhanced with **--lwr-rolling-restart** option (*/var/qps/bin/support/lwr/build_kafka_server.sh --lwr-rolling-restart <region-name>*). You can run the enhanced script after upgrading to CPS 19.2.0 release to restart all LWR process in the region.

Upgrade LWR for Nice

LWR now enables LWR processes to run with Nice. For applications which are user level and not scheduled with real time priority, their CPU priority can be managed using Nice value. Its valid range is -20 to 19. -20 means highest CPU priority.

For more information, see the following section:

- *Enabling Nice Value Change on LWR VMs* in the *CPS LWR Installation Guide for OpenStack*
- *Enabling Nice Value Change on LWR VMs* in the *CPS LWR Installation Guide for VMware*

Mobile

Accurate Trigger Policy Timers

CPS is enhanced to provide an enhanced trigger policy to process Sy pending counters events.

Disable Policies Tab

In this release, Policy Builder **Preferences** dialog box has been modified to have a checkbox for Policies tab. When the checkbox is selected, the Policies tab is available in Policy Builder. Also, the Blueprint behavior depends on the Policies checkbox state.

You will be warned in case the policy/blueprint checkboxes are selected and only on accepting that message, will you be able to see the Policies/Blueprint tabs.

NOTE: By default, the Policies and Blueprint tabs are disabled.

For more information, see *Policies* section in *CPS Mobile Configuration Guide*.

Enhanced Diameter Overload Protection on Policy Director

The following new parameters are added under Diameter Messages Action on Threshold in LB in Policy Builder:

- Max TPS per PD: Defines maximum TPS supported per PD process. Default value is 0.
- Default Discard Behavior: Describes the action to be taken when a Diameter request message is received in LB and rate limiter acquire fails. Possible values include **MESSAGE_DROP** and **DIAMETER_TOO_BUSY**. Default value is **MESSAGE_DROP**.

For more information, see *Diameter Messages Action on Threshold in LB* section in *CPS Mobile Configuration Guide*.

Enhance Session Hard Limit Parameter to Accept Absolute Value

In this release, session hard limit parameters have been removed and new session limit overload protection has been added to take a positive integer as the session database capacity limit. For the same purpose, a new parameter, **Session Limit Overload Protection** is added under System configuration in Policy Builder.

In a GR setup, the value for **Session Limit Overload Protection** must be set to session count of all session replica sets (from both sites).

The purpose of the parameter is to protect the system and quickly recover in case of network-wide events triggered by data path or control signal storm.

The following parameters have been removed from **qns.conf** file:

- com.cisco.apply.session.hardlimit
- com.cisco.session.hardlimit.percent

A new **qns.conf** parameter *allow.sessioncreation.license.periodic.check* has been added. The value must be set to true so that the license is validated periodically but session creation will not be impacted. Only during the start/restart of Policy Server (QNS) process, licenses validation failure impacts the traffic and sessions creations are not allowed. Contact your Cisco Account representative for information on **qns.conf** file parameters.

The following new alarms have been added:

- SessionLimitOverloadProtectionNotSet
- SessionLimitOverloadProtectionExceeded

For more information, see the following sections:

- *Adding a System* section in the *CPS Mobile Configuration Guide*
- *Application Notifications* table in the *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *Clearing Procedures* chapter in the *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *Testing Traps Generated by CPS* in the *CPS Troubleshooting Guide*

NOTE: For the deployments using JSON files for Policy Builder configuration, the newly introduced field should be added in JSON file and its value should be set to recommended value (2 * license count) or maximum number of sessions supported by the hardware, whichever is less, so that the upgrade is seamless.

Even if you add a default value of zero in JSON file, you will not be able to publish the Policy Builder. You need to configure Session Limit Overload Protection value ≥ 1. You need to identify the session database capacity and add the absolute value. Hence, default value 0, which means infinite number of sessions will not work.

NOTE: Session Database Capacity > Session Limit overload Protection > License limit (soft limit from license file)

For GUI-based configuration, the field introduced is validated to check if the value is not 0. During the ISSU upgrade, '0' will be added as default and alarm will be triggered to change the value. You must change this value after upgrade which also clears the alarm.

Ingress and Egress Rate Limiting on the API interface (PCRF)

CPS now supports to protect itself from incoming API traffic when acting as a server by rate limiting the incoming traffic on API interface. To support this, two new parameters, **Max API TPS Threshold** and **HTTP Error Code on Threshold Reached** have been added under Unified API Configuration.

For more information, see *Unified API Configuration* section in the *CPS Mobile Configuration Guide*.

Single Sh Enhancement

Single Sh enhancement is fully qualified for deployment in this release.

For more information, see *Setting Up Additional Profile Data* section in *CPS Mobile Configuration Guide*.

Support for Entitlement Attribute Variable

In CPS 19.2.0, a new entitlement variable that cascades/concatenates all the entitlement values of a subscriber's HSS into on e searchable string has been added. It allows efficient use of entitlement attribute in the HSS profile and limit the modification of the CRD table when a new entitlement is introduced.

Currently, this is supported only for Entitlement external code in Profile Mappings under Additional Profile Data tab for Sh Profile.

For more information, see *Setting Up Additional Profile Data* section in the *CPS Mobile Configuration Guide*.

Support to Clean Stale Sessions

CPS now supports cleaning of stale sessions in PCRF. You can run a Stale Session Cleaner application on the pcrfclient VMs on an HA setup.

For more information, see *Cleaning Stale Sessions* in the *CPS Mobile Configuration Guide*.

Support for Robust In-Memory Lookup

CPS now supports a robust in-memory lookup and uses MongoDB replica-sets to store secondary key to primary key mapping.

- In both upgrade and fresh installations, SK DB is disabled by default.
- To enable SK DB, see *Configuring SK DB* section in *CPS Installation Guide for VMware*.
- If secondary key or session database writes fails for Gx or Rx message, diameter request is rejected with failure result code.
- Secondary key audit functionality is added, which deletes the orphan secondary keys in background thread.
- Hot standby and scale up/down support is added for SK DB.

NOTE:

- To prevent confusion between fields, the old field "Min Key Cache Time Min" has been deleted which was not being used.
- This feature is applicable for HA and dual cluster only.
- No GA support is provided for the current release.

For more information, see *Adding an HA Cluster* section in *CPS Mobile Configuration Guide*.

New parameters for SK DB can be configured.

For more information, contact your Cisco Account representative.

Support for QCI Normalization

In addition to ARP normalization, CPS now supports normalization of QCI across multiple simultaneous Rx sessions for IMS services based on 3GPP:

- TS 29.214 R13.6 clause 4.4.8 and 5.3.47
- TS 29.212 R13.6 clause 4.5.27 and 4.5.19.1.1

To support normalization of QCI, **Disable Downgrade of Normalised ARP** checkbox has been renamed to **Disable Downgrade of Normalised ARP and QCI** under Rx Profile.

For more information, see *Rx Profile* section in the *CPS Mobile Configuration Guide*.

Support to Update Subscriber Address

CPS now supports subscriber IP address update on ONT reboot with dual stack. In dual stack scenario, the order in which IPv4 or IPv6 sessions comes up in BNG is based on the sequence of packets received from ONT. Subscriber session is created for first addre ss family and same is sent in the accounting start message to CPS. Whenever the second address family comes up, the same address is sent in interim accounting record to CPS with an CISCO-EVENT-TRIGGER of value 6 (ACCT-TRIGGER-NEW-INFO). CPS collects this information and updates the session context to address any dynamic address change scenario during the life time of the subscriber.

Support to Eliminate Stale Sy Sessions

CPS now supports elimination of stale Sy Sessions on the OCS, due to race conditions within or outside of PCRF.

CPS initiates an Sy SLR towards OCS and terminates the same only when the session is established with OCS. However, this new feature attempts to send an Sy STR when the OCS does not respond on time or a CCR-T is received prematurely from the PGW before an Sy session is established, which might otherwise lead to stale sessions on the OCS.

Along with this feature, Single Sy Soft delete functionality is introduced, which reuses the same soft delete timer configured in system configuration. The purpose is to retain the Single Sy session when Single Sy feature is enabled so we do not purge the Sin gle session immediately and hold it for a period configured in soft delete timer. This helps to process the delayed Sy SLA received from OCS to ensure that an Sy STR is sent in certain race conditions/retries from PCRF.

NOTE: The backward compatibility specification compliant feature terminates Sy sessions only when the Sy session established is still maintained. This is not recommended for customers who do not want this change from the legacy spec ification compliant behavior.

MOG

No new features or changes were introduced in this release.

Operations

No new features or changes were introduced in this release.

API Additions or Changes

No changes were introduced in this release.

MIB Additions or Changes

No changes were introduced in this release.

KPI Additions or Changes

Critical Resources Monitoring in CPS using KPIs

In this release, the following KPIs have been added to monitor critical CPS resources:

- node[x].gauges.inboundMessageQsize.qns_gauge: The size of the inbound message queue. The source of the statistics is Policy Server (QNS) VM.
- node[x].counters.skcache_ring<1|2>_cache_timedout.qns_count: Total count of timed out failed lookup for primary key using the secondary key in cache ring. The source of the statistics is Policy Server (QNS) VM.

Log Additions or Changes

No changes were introduced in this release.

SNMP Alarm Additions or Changes

Support for Heap Threshold Exceed Alarm for JVM

In this release, the following alarms have been added:

- GC State alarms for each Policy Server (QNS) instance running on Policy Director (LB), Policy Server (QNS) or UDC VMs if GC occurs for configurable gc_alarm_trigger_count (default: 3) times within gc_alarm_trigger_interval (default: 10 mins).
- GC clear notification if there are no GCs in last gc_clear_trigger_interval (default: 15 mins).
- OldGen State alarms if two consecutive GC has Oldgen with more than alert threshold (default: 50%).
- OldGen State clear notification if post GC oldgen is below clear threshold (default: 40%)

Currently, the above-mentioned alarms are only supported for VMware environment. By default, the alarms are disabled.

For more information, see the following sections:

- *General Configuration* in the *CPS Installation Guide for VMware*
- *Component Notifications* table in the *CPS SNMP, Alarms, and Clearing Procedures Guide*

Enhance Session Hard Limit Parameter to Accept Absolute Value

The following new alarms have been added:

- SessionLimitOverloadProtectionNotSet
- SessionLimitOverloadProtectionExceeded

For more information, see the following sections:

- *Application Notifications* table in the *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *Clearing Procedures* chapter in the *CPS SNMP, Alarms, and Clearing Procedures Guide*
- *Testing Traps Generated by CPS* in the *CPS Troubleshooting Guide*

Statistics Additions or Changes

CSCvn44955 - Throttle Full DB Scan

Previous Behavior: When secondary key lookup fails from memcache, then *node1.counters.skcache_ring<1|2>_cache_miss.qns_count* gets incremented.

New Behavior: When secondary key lookup fails due to memcache timeout, then *node1.counters.skcache_ring<1|2>_cache_timedout.qns_count* is incremented.

If lookup fails due because data is not present in memcache, then *node1.counters.skcache_ring<1|2>_cache_miss.qns_count* is incremented.

CSCvo46672 - disable tcpconnections listening port statistics

In CPS 19.2.0, statistics related to TCP connection listening port have been removed.

Ingress and Egress Rate Limiting on the API interface (PCRF)

The following statistics have been added:

- com.broadhop.unifiedapi.statistics.<api_type>.<request_type>.request: Total count of API Request (SOAP/REST) received at Policy Server (QNS).

  api_type : SOAP/REST

  request_type : GET/POST

  The source of the statistics is Policy Server (QNS) VM.

- com.broadhop.unifiedapi.statistics.<api_type>.<request_type>.response.<error_code>: Number of ingress API request responded with HTTP error code (configured in PB) when API TPS of incoming request crossed the limit configured in Max API TPS Threshold in Unified API Configuration.

  api_type : SOAP/REST

  request_type : GET/POST

  The source of the statistics is Policy Server (QNS) VM.

- node[x].unifiedapi_<api_type>_<request_type>.success: Success message count of given <api_type> and <request_type>. The source of the statistics is Policy Server (QNS) VM.
- node[x].unifiedapi_<api_type>_<request_type>.error: Erred message count of given <api_type> and <request_type>. The source of the statistics is Policy Server (QNS) VM.
- node[x].unifiedapi_<api_type>_<request_type>.avg: Rolling 5 minute average of successful API request processed by qns vm of given <api_type> and <request_type>. The source of the statistics is Policy Server (QNS) VM.
- node[x].unifiedapi_<api_type>_<request_type>.total_time_in_ms: Total milliseconds of successful API request processed by qns vm of given <api_type> and <request_type>. The source of the statistics is Policy Server (QNS) VM.

SK Database Statistics

The following SK database statistics have been added:

- skdb_entries_scanned_shard_<skshardid>: Increments for each SK entry scanned from SK database.
- skdb_entries_cleaned_up_shard_<skshardid>: Increments for each stale SK entry cleaned from SK database.

- skdb_audit_task: Increments when audit task is performed on SK database.
- skdb_audit_exception: Increments when there is exception while performing audit on SK database.
- skdb_shard_entry_rebuild: Increments for each SK entry inserted into SK database from session database.
- skdb_shard_rebuild_shard_<shard id>: Increments for each time SK rebuild is completed successfully on the shard.
- skdb_mongo_get_found_record: Increments for each SK database record found.
- skdb_mongo_get_no_record: Increments for each SK database record not found.
- skdb_mongo_get_success: Increments for each SK database get query success from secondary.
- skdb_mongo_get_failure: Increments for each SK database get query failure from secondary.
- skdb_mongo_get_success_pri: Increments for each SK database get query success from primary.
- skdb_mongo_get_failure_pri: Increments for each SK database get query failure from primary.
- skdb_mongo_set_success: Increments for each SK database record set success.
- skdb_mongo_set_failure: Increments for each SK database record set failure.
- skdb_mongo_delete_success: Increments for each SK database record delete success.
- skdb_mongo_delete_failure: Increments for each SK database record delete failure.
- skdb_janitor_scrub: Provides average time taken by janitor to scrub/audit shards.
- skdb_janitor_scrub_shard_<shard id>: Increments for each SK database scrub for each shard.
- skdb_failback_remove_success: Increments when SK record marked deleted in SK backup database gets deleted from SK database.
- skdb_failback_move_insert: Increments when SK record migrated from SK backup database and inserted in to SK database.
- skdb_failback_move_update: Increments when SK record migrated from SK backup database and updated into SK database.
- skdb_failback_move_outofdate: Increments when SK record being migrated from SK backup database to SK database is of older version.
- skdb_failback_unable_to_migrate: Increments when SK record unable to migrate from SK backup database to SK database.
- skdb_session_migrated: Increments when SK record is migrated from SK backup database to SK database.
- skdb_transition_update_insert_success: Increments when SK record is inserted to SK database, while SK record migration from SK backup database to SK database is in progress.
- skdb_transition_update_success: Increments when SK record is updated to SK database, while SK record migration fr om SK backup database to SK database is in progress.
- skdb_transition_update_fail: Increments when SK record update to SK database is failed, while SK record migration from SK backup database to SK database is in progress.
- skdb_transition_remove_success: Increments when SK record is deleted from SK database, while SK record migration from SK backup database to SK database is in progress.
- skdb_transition_insert_success: Increments when SK record is inserted to SK database, while SK record migration from SK backup database to SK database is in progress.
- skdb_failover_update_insert_success: Increments when SK record is inserted to SK backup database, while SK database primary is not available.
- skdb_failover_update_success: Increments when SK record is updated to SK backup database, while SK database primary is not available.

- skdb_failover_update_fail: Increments when SK record update to SK backup database is failed, while SK database primary is not available.
- skdb_failover_remove_success: Increments when SK record is deleted from SK backup database, while SK database primary is not available.
- skdb_failover_remove_fail: Increments when SK record is failed to delete from SK backup database, while SK database primary is not available.
- skdb_failover_insert_success: Increments when SK record is inserted to SK backup database, while SK database primary is not available.

Support for CPS System Monitoring

The following statistics are monitored for a running process:

- children: Number of children in a given process. Normally this value is 0. Only for processes such as, httpd which creates a child process, the value is more than 1.
- cpu_percent: Provides information about CPU percent over 1 second of the interval when statistics are collected. For example, if a script is executed at time X then CPU usage percentage is calculated for a period of X & X+1 seconds and sent to collectd. Typically, it is similar to the top output of a process though not exact.
- cpu_time_system: Provides information about kernel mode jiffies. Period of time that this process has been scheduled in kernel mode, measured in clock ticks. Value watches with one from /proc/<pid>/stat.
- cpu_time_user: Period of time that this process has been scheduled in user mode, measured in clock ticks. Value watches with one from /proc/<pid>/stat.
- cpu_time_system_children: Period of time that these processes waited-for children have been scheduled in kernel mode, measured in clock ticks.
- cpu_time_user_children: Period of time that these processes waited-for children have been scheduled in user mode, measured in clock ticks.
- num_fds: Number of file descriptors opened by a process. This value typically matches with lsof -p <pid> output. It considers only files for which fd is opened. Lsof has other output files types of “mem” and so on which is a constant number but is not included in this output.
- memory_percent: Gives memory usage in percentage. Matches with top/ps output for a process.
- memory_rss: Gives rss memory usage of a process. Matches with ps/top output. You need to multiply top output with 1024 to match these values.
- memory_vms: Gives virtual memory usage of a process. Matches with ps/top output. You need to multiply top output with 1024 to match these values.
- Pid: Gives pid for which monitoring is being done.
- running_status: Denotes running status of a process when status is captured. The following are the valid values:

  Table 1: Valid Values

Status	Value
Dead	1
disk-sleep	2
Idle	3
Locked	4
Running	5
Sleeping	6
Stopped	7
tracing-stop	8
waiting	9
waking	10
zombie	11

In this release, a new cron script has been added which dumps top CPU and memory consuming processes to the files, */var/log/top_cpu_consuming_processes* and */var/log/top_memory_consuming_processes*

The script is enabled as a cron which runs every minute on all VMs. The files are rotated every day and 10 days of data is stored.

The following statistics have been added for the tcpconn plug-in:

- tcpconns-all/tcp_connections-CLOSED: Number of TCP connections in closed state.
- tcpconns-all/ tcp_connections-ESTABLISHED: Number of TCP connections in established state.
- tcpconns-all/ tcp_connections-LAST_ACK: Number of TCP connections in last_ack state.
- tcpconns-all/ tcp_connections-SYN_SENT: Number of TCP connections in syn_sent state.
- tcpconns-all/ tcp_connections-CLOSE_WAIT: Number of TCP connections in close_wait state.
- tcpconns-all/ tcp_connections-FIN_WAIT1: Number of TCP connections in fin_wait1 state.
- tcpconns-all/ tcp_connections-LISTEN: Number of TCP connections in listen state on a VM.
- tcpconns-all/ tcp_connections-TIME_WAIT: Number of TCP connections in time_wait state.
- tcpconns-all/ tcp_connections-CLOSING: Number of TCP connections in closing state.
- tcpconns-all/ tcp_connections-FIN_WAIT2: Number of TCP connections in fin_wait2 state.
- tcpconns-all/ tcp_connections-SYN_RECV: Number of TCP connections in syn_recv state.

Similarly, for every listening port on a VM, the following statistics are collected:

- tcpconns-<port>-local/tcp_connections-CLOSED: Number of TCP connections which are in closed state for local listening port.
- tcpconns-<port>-local/ tcp_connections-ESTABLISHED: Number of TCP connections in established state to local port.
- tcpconns-all/ tcp_connections-LAST_ACK: Number of TCP connections in last_ack state for local port.
- tcpconns-<port>-local/ tcp_connections-SYN_SENT: Number of TCP connections in syn_sent state.
- tcpconns-all/ tcp_connections-CLOSE_WAIT: Number of TCP connections in close_wait state.
- tcpconns-<port>-local/ tcp_connections-FIN_WAIT1: Number of TCP connections in fin_wait1 state.
- tcpconns-all/ tcp_connections-LISTEN: Number of TCP connections in listen state on a VM.

- tcpconns-<port>-local/tcp_connections-TIME_WAIT: Number of TCP connections in time_wait state.
- tcpconns-<port>-local/tcp_connections-CLOSING: Number of TCP connections in closing state.
- tcpconns-<port>-local/tcp_connections-FIN_WAIT2: Number of TCP connections in fin_wait2 state.
- tcpconns-<port>-local/tcp_connections-SYN_RECV: Number of TCP connections in syn_recv state.

The following statistics have been added for Fhcount plug-in:

- fhcount/file_handles-max: Maximum number of file handles (i.e., the same value as /proc/sys/fs/file-max).
- fhcount/file_handles-unused: Several free file handles. This value is always 0 from Linux 2.6.
- fhcount/file_handles-used: Several allocated file handles.

The following statics have been added for swap:

- io-in: Reports number swap I/O in.
- io-out: Reports number swap I/O out.
- swap-cached: Reports number swap cached.
- swap-free: Reports number swap free.
- swap-used: Reports number swap used.

Support Secondary Key Database for In-Memory Lookup

The following SK database statistics have been added:

- skdb_cache_get: Increments for each SK DB record found.
- skdb_cache_get_failure: Increments for each SK DB record not found.
- skdb_cache_get_pri: Increments for each SK DB get query success from primary.
- skdb_cache_get_pri_failure: Increments for each SK DB get query failure from primary.
- skdb_cache_miss: Increments for each SK DB failed to get the record.
- skdb_cache_set: Increments for each SK DB record set success.
- skdb_cache_set_failure: Increments for each SK DB record set failure.
- skdb_cache_set_timeout: Increments for each SK DB record set timeout.
- skdb_cache_remove: Increments for each SK DB record delete success.
- skdb_cache_remove_failure: Increments for each SK DB record delete failure.
- skdb_cache_remove_timeout: Increments for each SK DB record delete timeout.
- skdb_cache_get.error: Count of failed to get the skdb cache entry.
- skdb_cache_get.success: Count of successful to get the skdb cache entry.
- skdb_cache_get.avg: Rolling 5 minute average of successful get skdb cache entry.
- skdb_cache_get.total_time_in_ms: Total milliseconds of successful get skdb cache entry.
- skdb_cache_remove.error: Count of failed to remove the skdb cache entry.
- skdb_cache_remove.success: Count of successful to remove the skdb cache entry.
- skdb_cache_remove.avg: Rolling 5 minute average of successful remove skdb cache entry.
- skdb_cache_remove.total_time_in_ms: Total milliseconds of successful remove skdb cache entry.
- skdb_cache_set.error: Count of failed to set the skdb cache entry.

- skdb_cache_set.success: Count of successful to set the skdb cache entry.
- skdb_cache_set.avg: Rolling 5 minute average of successful set skdb cache entry.
- skdb_cache_set.total_time_in_ms: Total milliseconds of successful set skdb cache entry.
- skdb_janitor_scrub.error: Count of failed to scrub the skdb shards.
- skdb_janitor_scrub.success: Count of successfully scrub the skdb shards.
- skdb_janitor_scrub.avg: Rolling 5 minute average of successfully scrub skdb shards.
- skdb_janitor_scrub.total_time_in_ms: Total milliseconds of successfully scrub skdb shards.

The following statistics have been removed:

- skdb_shard_entry_rebuild
- skdb_mongo_get_found_record
- skdb_mongo_get_no_record

Performance Improvement

No new features or changes were introduced in this release.

Platform

Ciphers Removed from CPS

The following three ciphers are not mandatory after scanning is done by PSB TLS Compliance tool. Hence, they have been removed from CPS 19.2.0 release onwards:

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA - strong
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - strong
- TLS_RSA_WITH_AES_256_CBC_SHA - strong

Enhanced Performance of Graphite Framework

The existing Graphite framework has been enhanced to add additional carbon-relay process. collectd connects to the carbon-relay processes and in turn sends statistics to two carbon aggregator instances, which then sends the statistics to three carbon-cache instances.

The Graphite-web framework then fetches the statistics from these three carbon-cache instances.

Also, memcache has been enabled for Graphite-web.

The following additional processes are enabled:

- carbon-cache, carbon-cache@b, carbon-cache@c
- carbon-aggregator, carbon-aggregator@b
- carbon-relay

To start/stop the process using systemd, standard systemd commands can be used.

For example:

systemctl status carbon-cache@b

systemctl start carbon-cache@b

systemctl stop carbon-cache@b

Also, the following are the monit names for carbon processes:

- carbon-cache, carbon-cache-b, carbon-cache-c
- carbon-aggregator, carbon-aggregator-b
- carbon-relay

To start/stop processes using monit, standard monit commands can be used.

For example:

monit stop carbon-cache-b

monit start carbon-cache-b

monit status carbon-cache-b

You can also check the status of carbon processes using monit summary command from pcrfclient01/02.

monit summary

Service Name	Status	Type
carbon-relay	OK	Process
carbon-cache-c	OK	Process
carbon-cache-b	OK	Process
carbon-cache	OK	Process
carbon-aggregator-b	OK	Process
carbon-aggregator	OK	Process

Prioritize Message Threads on Policy Director/Policy Server/UDC/Session Manager/LWR

In this release, CPU priority support is added for Diameter processing threads on Policy Director (LB), Policy Server (QNS), Session Manager, UDC, OAM (pcrfclient), and LWR VMs so that application gets priority for CPU and I/O operations. CPS applications which processes diameter messages are given higher priority over other processes on a VM.

CPU priority support is present for fresh installation/upgrade on all VMs except LWR VMs.

- For Policy Director (LB)/OAM (pcrfclient)/Policy Server (QNS)/UDC VMs, qns-java applications are prioritized.
- For SM/arbiter VMs, MongoDB members are prioritized.
- For LWR processes, support is present only for fresh installation. For LWR VMs, LWR processes are prioritized.

service_qns.log on Policy Director moved to tmps

In this release, the Garbage Collector (GC) log file (i.e., /var/log/broadhop/service-qns-1.log) has been moved to a separate tmpfs instead of disk.

After enabling/disabling this feature, *restartall.sh* command must be run to load the updated configuration.

By default, this feature is disabled. You can enable it by configuring *service_log_tmpfs_enabled* to **true** in Configuration.csv file for VMware environment and *serviceLogTmpfsEnabled* to **true** in YAML file for OpenStack environment.

For example:

- In VMware Environment, configure service_log_tmpfs_enabled to true.

- In OpenStack Environment,

  config:

  # Do not change. See install documentation for details.

  # default: sys_user_0

  qpsUser: "sys_user_0"

  # default: disabled

  selinuxState: "disabled"

  # REQUIRED

  serviceLogTmpfsEnabled: "true"

After enabling this feature, you will see the service log file at the same location i.e., /var/log/broadhop/service-qns-1.log. In this release, it is a soft link of /var/service_log/service-qns-1.log which is created on tmpfs.

Currently, this is supported for Policy Director (LB), Policy Server (QNS) and UDC VMs.

For Policy Server (QNS)/UDC only one java process runs on that VM, so 50 MB tmpfs folder is created.

On Policy Director (LB) VM tmpfs folder size is based on a number of java processes. By default, four java processes run on Policy Director (LB) VM, so 200 MB tmpfs folder is created for Policy Director (LB).

For more information, see the following sections:

- *General Configuration Parameters* table in *CPS Installation Guide for VMware*
- *Configuration Parameters - HA System* table in *CPS Installation Guide for OpenStack*
- *Sample YAML Configuration File - HA Setup* in *CPS Installation Guide for OpenStack*
- *Service Log on tmpfs* in *CPS Installation Guide for OpenStack*

Support for CPS Process Monitoring

In this release, process-level monitoring support is added in CPS.

For every VM type, by default important processes are monitored. If any additional processes need to be monitored then it can be done using configurations for both VMware and OpenStack based installations.

Multiple processes can be mentioned in a list separated by semicolon in a VMware environment and as an array (list) in an OpenStack environment.

Process name must match with its corresponding systemd service name.

For more information, see the following sections:

- *General Configuration Parameters* table in the *CPS Installation Guide for VMware*
- *Configuration Parameters - HA System* table in the *CPS Installation Guide for OpenStack*
- *Sample YAML Configuration File - HA Setup* in the *CPS Installation Guide for OpenStack*

Support for Session Shards Health Status

In this release, *--get_session_shard_health* option has been added to check session shard health status on HA and GR setups.

For more information, see *diagnostics.sh* section in *CPS Operations Guide*.

Support for SVN Revision Status

In this release, *--policy_revision_status* option has been added to check the SVN revisions (head and local) available at different Policy Server (QNS)/Policy Director (LB)/UDC VMs.

For more information, see *diagnostics.sh* section in *CPS Operations Guide*.

NOTE: The *--policy_revision_status* option is not applicable for third site arbiter, SITE, and AIO.

ZVM Support on Policy Director/Policy Server/UDC/LWR Node

In this release, option has been added to enable Zing to minimize application impact due to Garbage Collection time. Policy Director (LB)/Policy Server (QNS)/UDC/LWR VMs can be configured to use ZVM.

Default options/configuration:

- Zulu is enabled on all the VMs.
- Kafka process is run on LWR VMs and 8 GB is allocated for Kafka processes (This option is added only for fresh installations).

For more information, see the following sections:

- *General Configuration Parameters* table in the *CPS Installation Guide for VMware*
- *Configuration Parameters - HA System* table in the *CPS Installation Guide for OpenStack*
- *Sample YAML Configuration File - HA Setup* in the *CPS Installation Guide for OpenStack*
- *Performance Mode* in the *CPS Installation Guide for OpenStack*
- *Start Kafka Processes on LWR VM* in the *CPS LWR Installation Guide for VMware*
- *Zing/Zulu Customization for LWR* in the *CPS LWR Installation Guide for OpenStack*

NOTE: In this release, Zulu (enabled by default) and Zing (optional) JVMs are available for pauseless garbage collection. Note that , with Zing, approximately 20% performance degradation is seen. Changes to improve the performance with Zing are planned for a subsequent release. For more information, contact your Cisco Account representative.

Policy Reporting

No new features or changes were introduced in this release.

Product Security

CentOS 7.5 Security Enhancements/Kernel Upgrade

In this release, the kernel has been upgraded to 3.10.0-957.5.1.el7. Also, all the packages have been upgraded to be compatible with CentOS 7.5.
For service related issues, you can use *journactl* to get systemctl logs.

The following tables list the vulnerabilities that have been fixed as a part of this release:

Table 2 CVEs

CVE	Name
CVE-2016-7067	Tildeslash Monit Cross-Site Request Forgery Vulnerability
CVE-2018-1050	CentOS 7 : samba (CESA-2018:3056)

CVE	Name
CVE-2018-10844	CentOS 7 : gnutls (CESA-2018:3050)
CVE-2018-10845	CentOS 7 : gnutls (CESA-2018:3050)
CVE-2018-10846	CentOS 7 : gnutls (CESA-2018:3050)
CVE-2018-10858	CentOS 7 : samba (CESA-2018:3056)
CVE-2018-1139	CentOS 7 : samba (CESA-2018:3056)
CVE-2018-14646	CentOS 7 : kernel (CESA-2018:3651)
CVE-2018-15688	CentOS 7 : NetworkManager (CESA-2018:3665)
CVE-2018-15688	CentOS 7 : systemd (CESA-2019:0049)
CVE-2018-16395	CentOS 7 : ruby (CESA-2018:3738)
CVE-2018-16864	CentOS 7 : systemd (CESA-2019:0049)
CVE-2018-16865	CentOS 7 : systemd (CESA-2019:0049)
CVE-2018-18311	CentOS 7 : perl (CESA-2019:0109)
CVE-2018-18397	CentOS 7 : kernel (CESA-2019:0163)
CVE-2018-18559	CentOS 7 : kernel (CESA-2019:0163)
CVE-2018-20102	HAProxy dns_validate_dns_response Out-of-Bounds Read Vulnerability
CVE-2018-5742	CentOS 7 : bind (CESA-2019:0194)
CVE-2019-3815	CentOS 7 : systemd (CESA-2019:0201)
CVE-2018-1000007	CentOS 7: curl / nss-pem (CESA-2018:3157)
CVE-2018-1000120	CentOS 7: curl / nss-pem (CESA-2018:3157)
CVE-2018-1000122	CentOS 7: curl / nss-pem (CESA-2018:3157)
CVE-2018-1000301	CentOS 7: curl / nss-pem (CESA-2018:3157)
CVE-2018-1000121	CentOS 7: curl / nss-pem (CESA-2018:3157)
CVE-2015-926	CentOS 7: freeglut / libX11 / libXcursor / libXfont / libXfont2 / libXres / libdrm / libepoxy
CVE-2018-17456	CentOS 7: git (CESA-2018:3408)
CVE-2017-16997	CentOS 7: glibc (CESA-2018:3092)
CVE-2018-6485	CentOS 7: glibc (CESA-2018:3092)
CVE-2018-11236	CentOS 7: glibc (CESA-2018:3092)
CVE-2018-11237	CentOS 7: glibc (CESA-2018:3092)

CVE	Name
CVE-2018-5391	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2017-18344	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-8781	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-10902	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-13405	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17

CVE	Name
CVE-2015-8830	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2017-0861	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2017-10661	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2017-17805	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2017-18208	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17

CVE	Name
CVE-2018-1120	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-1130	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-5344	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-5803	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-5848	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17

CVE	Name
CVE-2018-10878	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-1000026	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2016-4913	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2017-18232	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-1092	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17

CVE	Name
CVE-2018-1094	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-1118	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-7740	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-7757	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-10322	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17

CVE	Name
CVE-2018-10879	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-10881	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-10883	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-10940	CentOS 7: kernel (CESA-2018:3083) NEW KERNEL VERSION: kernel-3.10.0-957.e17 kernel-tools-libs-3.10.0-957.e17 kernel-tools-3.10.0-957.e17 kernel-headers-3.10.0-957.e17 python-perf-3.10.0-957.e17
CVE-2018-12910	CentOS 7: PackageKit / accountsservice / adwaita-icon-theme / appstream-data / at-spi2-atk
CVE-2017-18267	CentOS 7: PackageKit / accountsservice / adwaita-icon-theme / appstream-data / at-spi2-atk
CVE-2018-10733	CentOS 7: PackageKit / accountsservice / adwaita-icon-theme / appstream-data / at-spi2-atk
CVE-2018-10767	CentOS 7: PackageKit / accountsservice / adwaita-icon-theme / appstream-data / at-spi2-atk
CVE-2018-10768	CentOS 7: PackageKit / accountsservice / adwaita-icon-theme / appstream-data / at-spi2-atk
CVE-2018-13988	CentOS 7: PackageKit / accountsservice / adwaita-icon-theme / appstream-data / at-spi2-atk
CVE-2018-1000805	CentOS 7: python-paramiko (CESA-2018:3347)

CVE	Name
CVE-2018-7208	CentOS 7: binutils (CESA-2018:3032)
CVE-2018-7568	CentOS 7: binutils (CESA-2018:3032)
CVE-2018-7569	CentOS 7: binutils (CESA-2018:3032)
CVE-2018-7642	CentOS 7: binutils (CESA-2018:3032)
CVE-2018-7643	CentOS 7: binutils (CESA-2018:3032)
CVE-2018-8945	CentOS 7: binutils (CESA-2018:3032)
CVE-2018-10372	CentOS 7: binutils (CESA-2018:3032)
CVE-2018-10373	CentOS 7: binutils (CESA-2018:3032)
CVE-2018-10534	CentOS 7: binutils (CESA-2018:3032)
CVE-2018-10535	CentOS 7: binutils (CESA-2018:3032)
CVE-2018-13033	CentOS 7: binutils (CESA-2018:3032)
CVE-2018-10906	CentOS 7: fuse (CESA-2018:3324)
CVE-2018-10904	CentOS 7: glusterfs (CESA-2018:2607)
CVE-2018-10907	CentOS 7: glusterfs (CESA-2018:2607)
CVE-2018-10911	CentOS 7: glusterfs (CESA-2018:2607)
CVE-2018-10913	CentOS 7: glusterfs (CESA-2018:2607)
CVE-2018-10914	CentOS 7: glusterfs (CESA-2018:2607)
CVE-2018-10923	CentOS 7: glusterfs (CESA-2018:2607)
CVE-2018-10926	CentOS 7: glusterfs (CESA-2018:2607)
CVE-2018-10927	CentOS 7: glusterfs (CESA-2018:2607)
CVE-2018-10928	CentOS 7: glusterfs (CESA-2018:2607)
CVE-2018-10929	CentOS 7: glusterfs (CESA-2018:2607)
CVE-2018-10930	CentOS 7: glusterfs (CESA-2018:2607)
CVE-2018-5729	CentOS 7: krb5 (CESA-2018:3071)
CVE-2018-5730	CentOS 7: krb5 (CESA-2018:3071)
CVE-2018-14679	CentOS 7: libmspack (CESA-2018:3327)
CVE-2018-14680	CentOS 7: libmspack (CESA-2018:3327)
CVE-2018-14681	CentOS 7: libmspack (CESA-2018:3327)
CVE-2018-14682	CentOS 7: libmspack (CESA-2018:3327)
CVE-2017-3735	CentOS 7: openssl (CESA-2018:3221)
CVE-2018-0495	CentOS 7: openssl (CESA-2018:3221)

CVE	Name
CVE-2018-0732	CentOS 7: openssl (CESA-2018:3221)
CVE-2018-0737	CentOS 7: openssl (CESA-2018:3221)
CVE-2018-0739	CentOS 7: openssl (CESA-2018:3221)
CVE-2018-1000119	CentOS 7: pcs (CESA-2018:1060)
CVE-2018-1079	CentOS 7: pcs (CESA-2018:1060)
CVE-2018-1086	CentOS 7: pcs (CESA-2018:1060)
CVE-2018-1060	CentOS 7: python (CESA-2018:3041)
CVE-2018-1061	CentOS 7: python (CESA-2018:3041)
CVE-2018-1113	CentOS 7: setup (CESA-2018:3249)
CVE-2018-0494	CentOS 7: wget (CESA-2018:3052)
CVE-2018-10852	CentOS 7: sssd (CESA-2018:3158)
CVE-2018-14526	CentOS 7: wpa_supplicant (CESA-2018:3107)

NOTE: With the HAProxy version 1.8.17, there is a syntax change in its configuration. Use the "bind" keyword for listening addresses.

Example:

listen http_proxy

bind lbvip02:80

Security Enhancements

This section lists enhancements introduced to support Cisco Product Security Requirements and the Product Security Baseline (PSB). For more information about Cisco Product Security Requirements, refer to: https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle/sdl-process.html

Product Security Baseline Enhancements for CPS Web GUIs

CPS now supports the following PSB requirements:

- Include identifying information in all log entries
- Log unrestricted access to controlled space
- Log sessions and authentication. The following information is displayed:
  - Session creation or attempted session creation.

    For example, if user logs in the following message is displayed:

    User logged in successfully to Policy Builder
  - Session termination by user logout.

    For example, if user logs out the following message is displayed:

    User logged out successfully from Policy Builder.
  - Session termination because of timeout, excessive user sessions, or other resource management.

For example, if session is terminated the following message is displayed:

Exception caught while fetching the last accessed time of PB session. Removing session for user user_Id invalidating session when user user_Id exceeds the number of sessions allowed to login.

- Session termination caused by error.

  For example, if session is terminated due to error the following message is displayed:

  Invalidating session when user exits PB.

  Invalidating session after cancel button is pressed in repository selection dialog.

- Administrative session termination or session locking.
- Successful or unsuccessful resumption of administratively locked or suspended sessions.

- Limit credential tries per source per unit time. After five failed attempts of entering invalid credentials your username is blocked and you are not allowed to log in to the application even if you enter the right credentials. CPS supports five invalid login attempts for this requirement. The blocked user expiry time (locked.user.expiry.time), user login attempts expiry time (user.login.attempts.expiry.time) and number of invalid attempts (number.of.wrong.attempts.allowed) after which user is blocked and configurable. As per the requirement, user can configure these parameters in /etc/broadhop/pb/pb.conf file and all three parameters are optional. Configure the variables in pb.conf file for PB and PB2 applications and in qns.conf for CC application. The default values for the three variables include:

  -Dnumber.of.wrong.attempts.allowed=5

  -Dlocked.user.expiry.time=10 (in mins)

  -Duser.login.attempts.expiry.time=60 (in mins)

UDC

NOTE: When you upgrade/migrate or performing a fresh install for UDC setup, if required, you need to add the cluster ID in */etc/broadhop/iomanager/qns_other.conf* file.

For example, -Dcom.broadhop.run.clusterId=cluster-A

UI Enhancements

CSCvo61912 - P-bit is not set in Binding Db Check Rxb AAR and Dest-Host AVP omission in Rxb AAR

Pre-19.2.0, AAR initiated by CPS for PAS health-check did not have P-Bit set and Destination-Host AVP is set.

In CPS 19.2.0, a new checkbox (**Enable Proxy**) has been added under **PolicyDRA Health Check** in Policy Builder. When checked, P-Bit is set and Destination-Host AVP is not set for the outgoing AAR messages for PAS Health check.

Support for QCI Normalization

To support normalization of QCI, **Disable Downgrade of Normalised ARP** checkbox has been renamed to **Disable Downgrade of Normalised ARP and QCI** under Rx Profile.

vDRA

In this release, vDRA is not supported. For more information, contact your Cisco Account representative.

Installation Notes

Download ISO Image

Download the 19.2.0 software package (ISO image) from:
https://software.cisco.com/download/redirect?i=!y&mdfid=284883882&softwareid=284979976&release=19.2.0&os=

Md5sum Details

81822ba9562ec7e009404a35c0e85b3f	CPS_19.2.0_Base.qcow2.release.tar.gz
e47154b1dd67855dc1b1fd2e56c3abaf	CPS_19.2.0_Base.vmdk.release.tar.gz
e83cb68a40bffde25ad340a24bf5c0d4	CPS_19.2.0.release.iso.tar.gz

Component Versions

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

Table 3 Component Versions

Component	Version
ANDSF	19.2.0.release
API Router	19.2.0.release
Audit	19.2.0.release
Balance	19.2.0.release
CALEA	19.2.0.release
Cisco API	19.2.0.release
Cisco CPAR	19.2.0.release
Congestion Reference Data	19.2.0.release
Control Center	19.2.0.release
Core	19.2.0.release
CSB	19.2.0.release
Custom Reference Data	19.2.0.release
DHCP	19.2.0.release
Diameter2	19.2.0.release
DRA	19.2.0.release
Entitlement	19.2.0.release
Fault Management	19.2.0.release
IPAM	19.2.0.release

Component	Version
ISG Prepaid	19.2.0.release
LDAP	19.2.0.release
LDAP Server	19.2.0.release
LWR	19.2.0.release
Microservices Enablement	19.2.0.release
Notification	19.2.0.release
NSSF	19.2.0.release
PCF	19.2.0.release
Policy Intel	19.2.0.release
POP-3 Authentication	19.2.0.release
Recharge Wallet	19.2.0.release
SCE	19.2.0.release
SCEF	19.2.0.release
Scheduled Events	19.2.0.release
SPR	19.2.0.release
TIM AVP	19.2.0.release
UDC	19.2.0.release
UDSN Interface	19.2.0.release
Unified API	19.2.0.release

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

Image Signing

Image signing allows for the following:

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

Software Integrity Verification

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

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

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

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

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

Certificate Validation

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

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

New Installations

- VMware Environment
- OpenStack Environment

VMware Environment

To perform a new installation of CPS 19.2.0 in a VMware environment, see the *CPS Installation Guide for VMware*.

NOTE: After installation is complete, you need to configure at least one Graphite/Grafana user. Grafana supports Graphite data source credential configuration capability. Graphite data source requires common data source credential to be configured using Grafana for Grafana user. Data source credential must be configured after fresh installation. If you fail to add the user, then Grafana will not have 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 19.2.0, additional application and platform statistics are enabled. Hence, there can be an increase in the disk space usage at pcrfclient VMs. Once CPS 19.2.0 is deployed, monitor the disk space usage and if required, increase the disk space.

OpenStack Environment

To perform a new installation of CPS 19.2.0 in an OpenStack environment, see the *CPS Installation Guide for OpenStack*.

NOTE: After installation is complete, you need to configure at least one Graphite/Grafana user. Grafana supports Graphite data source credential configuration capability. Graphite data source requires common data source credential to be configured using Grafana for Grafana user. Data source credential must be configured after fresh installation. If you fail to add the user, then Grafana will not have 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 19.2.0, additional application and platform statistics are enabled. Hence, there can be an increase in the disk space usage at pcrfclient VMs. Once CPS 19.2.0 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 to CPS 19.2.0.

NOTE: Before migration, you need to configure at least one Graphite/Grafana user. Grafana supports Graphite data source credential configuration capability. Graphite data source requires common data source credential to be configured using Grafana for Grafana user. Data source credential must be configured before migration. If you fail to add the user, then Grafana will not have 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 19.2.0, additional application and platform statistics are enabled. Hence, there can be an increase in the disk space usage at pcrfclient VMs. Once CPS 19.2.0 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 19.2.0.

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 usi ng 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 19.2.0, additional application and platform statistics are enabled. Hence, there can be an increase in the disk space usage at pcrfclient VMs. Once CPS 19.2.0 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 t o 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.

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.

Common Vulnerabilities and Exposures (CVE)

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

- CSCvn86353: HAProxy dns_validate_dns_response Out-of-Bounds Read Vulnerability
  - CVE-2018-20102

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 4 CPS Open CDETS

CDETS ID	Headline
CSCvh30904	Security Issues Identified in CPS 18.0 PB, CC, UnifiedAPI and Import/Export URLs
CSCvh55279	Counters not described in QPS_STATISTICS file
CSCvi23619	After ISSU, diag shows list of alarms not cleared, while conn btwn LB & PCEF/CSCF/TDF clients came up
CSCvj88208	Bulk terminate command not working/getting exception in logs
CSCvk52072	During longevity run with Redis enable, system response time for CCR-I/T increased upto ~8-9 ms.
CSCvm39065	ISSU 13.1 to 18.0 - Found mongotimeout exception, while moving back primary member of replica sets
CSCvm49609	High response time observed during running Sol-3 call model on 18.4-FCV-drop-3
CSCvn04062	session replicaset going to recovering state on leaving load running on vzw setup
CSCvn06280	mongoConfig.cfg format not documented
CSCvn65409	Memcache Exception in qns logs
CSCvn66030	Peers are not connecting after Killing qns process couple of time(10 or more) continuously.
CSCvn70448	call failures with MongoWaitQueueFullException exception in logs with high tps >20K, on 14.0.1
CSCvn73888	Observing Traffic loss during In Service Migration from CPS 13.1 to CPS 18.2
CSCvn94814	19.1 SSL Vulnerabilities
CSCvo03443	After ISSU from CPS18.2 to CPS 19.1, observed memcached server errors on all qns nodes
CSCvo05006	memcache rebalance on cps even when skdb is enabled and memcache is disabled.
CSCvo09736	LwrStreamer Logs flooding in region 2 and region 3. Brokers are up and running
CSCvo11228	Swap Memory Usage on udc VM

CDETS ID	Headline
CSCvo14313	ARP/QCI mirroring failing to take the right ARP/QCI for pending policy evaluation
CSCvo14600	increased in response time and installing post rule when all UDC are disconnected from LWR in Region
CSCvo17404	c.b.policy.impl.RulesPolicyService java.lang.IllegalArgumentException: null
CSCvo17405	RAR Collisions occuring, race condition seen on CPS 18.0 (ASE 3.0)
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
CSCvo55244	out of date collision is causing spr_linked_sessions_key value to be inaccurate - singleSh
CSCvo61728	Idle CPU on 2 qns VMs is much higher than remaining qns VMs, on scale setup.
CSCvo64183	script output is not formatted /var/qps/bin/support/redis/encrypt_passwd.sh
CSCvo64309	systemctl is corrupting the redis configuration file, hence failing to restart redis
CSCvo68142	Alarm "core license has exceeded the allowed parame...."is getting cleared automatically in few sec.
CSCvo70222	Total session count reached 0 for a few seconds during the upgrade the set 2
CSCvo76428	Vulnerability observed during HAProxy URL Web Interface Vulnerability Scan
CSCvo76800	build_set.sh --admin --create --force : failing due to network manager restarted on members
CSCvo83578	Grafana old data missing while ISSM 14.0.1 to 19.1.3
CSCvo83593	"/mnt/iso/migrate disable set 2" command Failed
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)
CSCvo86777	sh cache validity timer not getting updated for multiple APN
CSCvo87216	Mail to mailer list is not being send on job completion
CSCvo87473	rebalance of shards timing out on full blown gr setup
CSCvo89569	MongoExpirationQuery - Exception - Timeout while receiving message
CSCvo89982	14.0.1 Dashboards are not working in 19.x setup
CSCvo90648	TransactionManager - Ending Balance transaction when it has not been started - Logs Flooding
CSCvo93778	Some mongo process running in Other state. Replica Set is showing as UNKNOWN
CSCvo94066	Observed performance degradation with ZING enabled on CPS_19.2.0 FCV drop1
CSCvo94348	CCR-I high response time while session replica set fail-over scenario
CSCvo94974	PRA-Identifier AVP Value type wrongly encoded
CSCvp01332	overload- dummy rx-aar message overload, qns taking too long to process and lb timing out
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

CDETS ID	Headline
CSCvp01698	Alarms not clearing from Diagnostic

Resolved CDETS

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

CPS Resolved CDETS

Table 5 CPS Resolved CDETS

CDETS ID	Headline
CSCvf59237	Missing CNS notification response in policy trace. Add stats for notification.
CSCvk26197	start-db-traps.sh is not finishing with success and report the following error in /var/log/messages
CSCvm43513	/var/tmp/monitor-qns not documented, and in place that can be easily removed
CSCvm73932	config_br.py -a import --users overwrites required CentOS user accounts
CSCvm88058	CPS shows a 10 to 60 secs offset for rule-retry attempts for configured rule-retry profile
CSCvm95474	stale single Sy session persists after Gx session expiration (non RAA 5002 scenario)
CSCvn17263	BEMS884374 - Arbiter VM is not joining replica set
CSCvn17334	svn out-of-sync between pcrfclient01 & pcrfclient02 after policy publish
CSCvn21833	After shutdown/init 0 monit processes goes into not monitored after vm comes up.
CSCvn24532	Restartall.sh should not restart udc qns process in sequence
CSCvn25648	PATS upgrade not showing the upgraded version
CSCvn32856	Process "stale-session-cleaner-helper" status " Execution failed" post upgrade on CPS18.5 FCV drop2
CSCvn60594	monit fails to detect Inactive/Stopped processes active at Kernel-Level
CSCvn61917	Grafana stale session counters are getting pegged before we are due for a stale session RAR
CSCvn64768	CPS 18.x: Missing bulkstats in QPS_statistics sheet
CSCvn69639	Adding additional users fails because generate user group ID conflicts with puppet-installed user
CSCvn75164	With balance call-model getting "java.lang.NullPointerException".
CSCvn76810	httpd.conf (apache config) changes whenever cluman is rebooted
CSCvn77679	CPS 18.5 to CPS 19.1 upgrade indecisive and lbvip didn't came up
CSCvn78288	ERROR DiameterMessageDealer - java.util.ConcurrentModificationException: null
CSCvn79570	Discrepancy In Parallel Queries For All The Clusters
CSCvn80847	Location Constraint doesn't update after enabling avoid split brain feature on CPS 19.1
CSCvn82975	arbiter process in Other state. mongo showing as UNKNOWN

CDETS ID	Headline
CSCvn83621	Gx session deletion on policy error does not clean up single Sy session
CSCvn83718	Build kafka server -- start region input options are not validated correctly
CSCvn83859	add-members REGION is not validating lwr.cfg before add members
CSCvn85412	High response time observed in Rx_ASR, after upgrade to 19.1 build.
CSCvn92129	Np interface: Unexpected SNR triggered after NRR for unknown user
CSCvn92458	Sh : Multiple svcPlan attribute evaluation using Virtual Service is not working
CSCvn95204	active mq exceptions from lb nodes to other nodes
CSCvn97025	can't export policy config
CSCvn98015	Session migration should not happen on Gx RAA if Gx RAR/RAA is processed on the other site
CSCvo00025	DRA - FN - Peer Rate Limit CRD GUI - Not able to unselect "Rate Limit Profile"
CSCvo00626	qns.conf.erb for iomanager blank line error
CSCvo01411	Np_NRA 5030 errors observed.
CSCvo01413	TaskMigratedException found in Log after UDC qns process restart
CSCvo02072	UDC error in diagnostics and LWR call model stopped
CSCvo02490	Issue with bulk-stats.sh removing files in /var/broadhop/stats
CSCvo03171	High response time observed for skdb_janitor_scrub process in top_qps
CSCvo03343	mongod process not running on both pcrfclient after fresh install
CSCvo04485	Monit fails to restart LWR processes
CSCvo04519	With load running, CPS is rejecting a small amount of AARs with 5065
CSCvo04621	Rx rule install stats are broken
CSCvo04637	Stats not showing up for UDC endpoints. LWR stats not broken down per-topic
CSCvo05137	LWR VMs running out of disk space in performance and longevity
CSCvo05407	PCRF is not stopping STA hold timer even on receiving NetLoc CCR-U
CSCvo07972	about.sh is not showing correct ipv6 in CPS URLs
CSCvo08259	ERROR c.broadhop.cache.mongodb.MongoCache - Exception inserting: {}
CSCvo09338	Rx-AAR-5065 Error seen after resiliency event in GR OSP system
CSCvo11295	CPS not including Diameter Result Code in SNA when getting malformed SNR
CSCvo12098	java.lang.ClassCastException: java.lang.String cannot be cast to java.util.List
CSCvo12870	LWR VM is allowing us to run diagnostics.sh command. Ideally it should not.
CSCvo13498	High CPU, memory usage on pcrfclient01 while accessing multiple Grafana instances.
CSCvo13773	Observed performance impact due to QNS CPU utilization after enabled all the CPS19.1 features.

CDETS ID	Headline
CSCvo13952	QPS_statistics.xls does not have PNR/PNA stats
CSCvo14185	LWR Processes Up/Down Traps are needed
CSCvo14931	Observed Intermittent CCRT timeouts after enabled all the CPS19.1 features.
CSCvo15555	CCRT Timeouts observed
CSCvo15690	CPS: Build upgrade failed with No such file or directory error
CSCvo18225	restartall.sh is not restarting all the end points in lb's
CSCvo18619	Error : "java.lang.NullPointerException:" for balance call model going errored Gy 5003 in GR.
CSCvo21658	All process are stopped/not running - after reboot the lwr VM
CSCvo22602	c.b.c.s.mongosk.SkRebuildExecutor - Unable to rebuild sk db java.lang.NullPointerException: null
CSCvo23015	vPCRF Large amount of stale sessions on OCS
CSCvo23056	Incoming VoLTE call CCR-U SRA Timeout
CSCvo25046	SNMP traps are not being cleared by same VM
CSCvo25130	UDC is not sending update message on unsubscribe
CSCvo25597	component trap generated from cluman contain hostname of active LB VM
CSCvo29904	Cache data out of date - max retries reached. retryCounter: 2
CSCvo36126	removing DRemoteGeoSiteName is causing timeout for session failovers failbacks
CSCvo37033	ISSM 19.1.1 - lb VMs in set 1 did not run vm-init after deploy
CSCvo37052	ISSM 19.1.1 - Unable to initialize deletedRxSessionIds collection. Skipping. Logs Flooding
CSCvo38487	Concurrent CCR-I results in missing STR
CSCvo39778	WSP file are getting deleted from pcrfclient within 5-6 Days
CSCvo41305	Multiple UDC update messages generated during APN termination
CSCvo43288	not showing correct log for geotag configuration failure via curl api
CSCvo43963	CRD should not clean old cache until the new cache is built
CSCvo44198	PB timedout when svn commit is running in background
CSCvo46242	soft delete not null check is erroneously deleting the singleSy session
CSCvo46672	disable tcpconnections listening port statistics
CSCvo48484	IllegalArgumentException: Cannot find class [com.broadhop.utilities.<200b>keystore.IKeyStoreManager]
CSCvo55244	out of date collision is causing spr_linked_sessions_key value to be inaccurate - singleSh
CSCvo56186	TC- Cross site messaging of stale session RARs from lb of one site to lb of peer site2--> failing
CSCvo58219	BEMS923318 - capture_env parameter -a (age) does not work
CSCvo61912	P-bit is not set in Binding Db Check Rxb AAR and Dest-Host AVP omission in Rxb AAR

CDETS ID	Headline
CSCvo62437	Under certain conditions, resync-db-traps.sh generates a false "sync needed" alert
CSCvo64314	Trap file is not getting updated.
CSCvo64324	Need to handling the remote site queries without local session affinity
CSCvo64343	monit showing "aido_client" status OK, But process is not running,
CSCvo66005	More updates needed in QPS_statistics
CSCvo66404	After ISSU from CPS18.2 to CPS 19.2 drop 4, observed qns process are not coming up in all qns nodes
CSCvo69799	Error "ShardInterface - Unexpected error" after failover on GR for CPS19.2
CSCvo70726	ERROR c.b.blueprint.master.MasterBlueprint - An error occurred while updating a session
CSCvo71117	vPCRF - no "Resource-Allocation-Notification" parameter in TableDrivenChargingRule
CSCvo82113	File Parameter Shell Command Injection vulnerability observed during CPS PB URL AppScan
CSCvo83636	many call failures with 3004 after "/mnt/iso/migrate.sh traffic restore" cli
CSCvo84430	java.lang.NullPointerException - DiameterGxTGPPDeviceMgr.getSessionLifecycle
CSCvo85222	ERROR c.b.c.s.mongosk.MongoSkJanitor - Exception while scrubbing sk shard
CSCvo87719	AIDO unable to bring up arbitervip member in replica sets (Ipv6 address has ::1)
CSCvo88020	enable_tacacs + clustermgr failed with nscd package not compatible with glibc on 18.3
CSCvo89540	PATS is not able to connect to K8-Master when using sshkey based login
CSCvo91994	load average is very high on pcrfclient
CSCvo98582	message Timeouts when Message Count Threshold per PD Configured
CSCvo98865	SY-OCS session stale. no next eval set and expiration hours crossed

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 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.