vDRA

Prometheus Federated Counter Support to Expose Metrics Interface

Feature Summary and Revision History

Table 1: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Always-on
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Operations Guide*

Table 2: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

In CPS vDRA 23.1.0 the Prometheus Federated Counter support is introduced to expose the KPI metrics to the external nodes.

You can configure the Prometheus Federate Server to get the Prometheus API metrics from Prometheus clusters. You can achieve scalable Prometheus monitoring setups or pull related metrics from one service of Prometheus into another.

For more information see, the *Prometheus* section in the *CPS vDRA Operations Guide.*

Configuration and Restrictions

Following are configuration and restrictions:

- To federate metrics from one server to another, configure the destination Prometheus server.
- To enable the honor_labels scrape option and passing in the desired match parameters, scrape from the federate endpoint of a source server.

Note All the federation configuration works on the external server.

- Minimum scrape interval to be configured is >=30 secs.
- Supported for only hi-res interface

Disable Auto Upgrade to the Next Level in Dynamic Peer Throttling

Feature Summary and Revision History

Table 3: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Disabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Configuration Guide*

Table 4: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

In CPS 23.1.0 release, vDRA allows to apply the next level throttling (dynamic peer rate limit throttling) only if there is increase / change in the current DB VM CPU utilization. Use the **Auto Apply Next Level Throttle** check box in the **DRA Configuration** to enable the auto update of the next level CPU.

For more information, see the *Enable DRA Dynamic Peer Rate Limiter* section in the *CPS vDRA Configuration Guide*.

Ability to Configure Prometheus Sampling Interval

Feature Summary and Revision History

Table 5: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Always-on
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Operations Guide*

Table 6: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

Scrape interval configuration is important because it determines the number of data points per minute (DPM) scraped in your active series. In CPS vDRA 23.1.0 and later releases, vDRA allows maximum scrape interval timings configuration using CLI commands. This method helps in taking fewer samples but keeps the data for longer interval.

For more information see, the *CLI Commands* section in the *CPS vDRA Operations Guide*.

Configuration and Restrictions

Prometheus recommends not to configure scrape interval for more than 2 minutess. Due to the default staleness period of 5 minutes, the scrape interval of 2 minutes allows for one failed scrape. Hence, the metrics will no longer be stale.

Support for TLS Certificate In-service Management and Expiry Alert

Feature Summary and Revision History

Table 7: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Configuration Guide*

Table 8: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

In CPS 23.1.0 and later release, vDRA supports the following function:

- Installation of a new certificate on the Directors before expiration of a TLS certificate

Note After installation the same certificate must be installed on the client.

- After replacing a new certificate, the client should re-initiate the connection to make use of new certificate.
- Monitoring of certificate validity will be every hour from the time of application restart.
- Alert notification prior to the certificate expiration date based on the following alert notification metrics.

Table 9: Alert Notification

Expiration in Days	Alert Level
60 days	Minor
40 days	Major
14 days	Critical

Inservice Certificate Management

The vDRA facilitates installation of a new TLS certificate on the Director before the TLS certificate expiration. Ensure to follow the procedure:

- Place the new certificate in the following path `/data/orchestrator/pemKey/`.
- After placing a new updated certificate on the Master VM, use the same CLI command to replace the existing certificate.

  The existing connection from the older certificate remains connected and there should not be a call failure.
- To get the new certificate in place, terminate the existing connection and the new connection must be negotiated by the client.

Configuration and Restrictions

- Ensure to install CA certificates through a CLI before initiating the Stack from the Diameter PB configuration.
- Until the existing connection is terminated, its considered as valid and the replacement of certificate file in the container will not impact the existing connection.
- CLI command is used to place the java key store file to the desired location.

Note Threshold alert configuration does not work for decreasing threshold.

For more information, see the *Creating a new TLS Certificate* section in the *CPS VDRA Configuration Guide*, *Applications Notifications* table and *Enabling Alerts for TLS Certificate Expiration* section in the *CPS vDRA SNMP and Alarms Guide*, and *CLI Commands* section in the *CPS vDRA Operations Guide*.

Apply Dynamic DB Throttling only for IPv6 and Session Cluster

Feature Summary and Revision History

Table 10: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Operations Guide*

Table 11: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

In CPS 23.1.0 and later release, you can dynamically apply throttling to DB VMs based on the configuration. CPU throttling is enabled to only VMs, which has IPv6 session, IMSI, or IPv4 DBs based on the CLI configuration.

If two or more DB types are configured, then all the VMs that have shared types are monitored.

Use the binding monitor-db-vms CLIto monitor only a particular type of DBs based on the cluster name in DB VNF.Also, every 10 seconds CPU gets monitored from the metrics DB from the Worker node.

Configuration and Restrictions

- Monitoring DB VMs starts only after configuration in DB VNF.
- If any one of VMs in which shards of cluster type is breached, then throttling is applied.
- Throttling is applied based on the VM CPU.

For more information, see the *CLI Commands* section in the *CPS vDRA Operations Guide*.

Source IP validation for Diameter connection ACL

Feature Summary and Revision History

Table 12: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*vDRA Configuration Guide*

Table 13: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

In vDRA, you can allow or deny a peer based on the Source-IP validation. The Source-IP validation is an optional check, which an administrator can decide to configure Source-IP with peer FQDN/Realm or not. Source-IP uses Custom Reference Data (CRD) to persist the configuration. Hence the configuration is limited to a site.

You can monitor disconnects and rejections for unknown Source-IP peers in the existing CER_MESSAGE_REJECTED_UNKNOWN_PEER KPI used for the Peer Rejection case.

Configuration and Restrictions

- Source-IP Validation is performed only for a new connection and is not applied on existing connection.
- After an ISO upgrade or patching for this feature, if the CRD contains any existing details, then export the existing details, populate a default value (*) to the **Source-IP** field, and then import back. Otherwise, it restricts to add new entries to the CRD as the existing data doesn't have valid Source-IP value.

  The allowed IPv4/IPv6 subnet formats:

```
(Starting Address of IPv4/IPv6)/(Prefix Length)
Ex.1: 172.10.216.176/28
Ex.2: 2001:420:27c1:906:250:56ff:feae:88c0/124
Ex.3: 2001:420:27c1:906::/64
Ex.4: 2001:420:27c1:906::
```

Note Input IP should be the starting address of that particular subnet range.

- To block a peer from connecting to multiple sites, ensure to disable peer on each site.

For more information, see the *Peer Control Access List* section in the *vDRA Configuration Guide* and *Statistics/KPI Additions or Changes* topic in the *CPS Release Change Reference*.

Monitor Single Subscriber for Non Gx or Rx Protocol

Feature Summary and Revision History

Table 14: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Disabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Administration Guide*

Table 15: Revision History

Revision Details	Release
CPS vDRA supports monitoring of single subscriber activity for Non-Gx / Rx protocols.	23.1.0

Feature Description

In CPS 23.1.0 and later releases, vDRA supports the monitoring of single subscriber activity for Non-Gx / Rx protocols such as Sy/Sd/Gy messages along with Gx/Rx protocols. A new KPI is added in the monitor activity:

- In CPS DRA, click the Subscriber Monitoring tab.
- In the DRA Subscriber Monitor area, click any one of the IMSI/MSISDN/IPv6 options to monitor for a single subscriber.
- Enter the required Subscriber identity values for IMSI/MSISDN/IPv6.

For more information see, the *Managing DRA Operations* section in the *CPS vDRA Administration Guide* and *Statistics/KPI Additions or Changes* section in the *CPS Release Change Reference Guide.*

Enhance Clearzoneinfo Script to Add or Modify the Existing Zone Configuration

Feature Summary and Revision History

Table 16: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Always-on
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Operations Guide*

Table 17: Revision History

Revision Details	Release
In CPS vDRA, the clearZoneInfo script supports the deletion of single zone range configuration.	23.1.0

Feature Description

In previous releases, after performing the initial ipv6 database configuration, vDRA allows you to modify the zones and ranges. Use the clearZoneInfo script to clear the old configuration and to apply the new configuration. The script deletes all zone range configuration which is stored in the Mongo db. This script does not support the deletion of a single zone range configuration.

From CPS vDRA 23.1.0 and later releases, you can delete a single zone range configuration using CLI commands. A new KPI is introduced to track zone range configuration modifications in the ipv6 zone aware configuration.

For more information see, the *CLI Commands* section in the *CPS vDRA Operations Guide* and the *Statistics/KPI Additions or Changes* section in the *CPS Release Change Reference Guide.*

IPv4 DB Support in Orchestrator Mongo Query

Feature Summary and Revision History

Table 18: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Operations Guide*

Table 19: Revision History

Revision Details	Release
In CPS vDRA, the CLI command for a Mongo query function supports. It also supports the existing IMSI, IPv6, MSISDN, and SESSION databases.	23.1.0

Feature Description

The CPS vDRA uses an orchestrator CLI for App sharding queries.

Earlier, the CLI allowed IMSI, IPv6, MSISDN, and SESSION databases. In CPS 23.1.0 and later releases, it allows the IPv4 database with same keys such as staleBindingExpiryTime, srk, session id, and uuid.

For more information, see the *database query* section in the *CLI Commands* chapter in the *CPS vDRA Operations Guide*.

Enhance IPC Queue Processing to Fix Single Point of Failure (SPOF)

Feature Summary and Revision History

Table 20: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable

Default Setting	Enabled – Always-on
Related Changes in This Release	Not Applicable
Related Documentation	• *CPS vDRA Operations Guide* • *CPS vDRA Advanced Tuning Guide*

Table 21: Revision History

Revision Details	Release
The CPS vDRA: • Introduces a new IPC thread pool to process priority messages • Adds an IPC Queue Send Thread priority configuration to handle the slow network peers.	23.1.0

Feature Description

In vDRA, the IPC thread pool is common for both priority and non-priority messages. The slow processing in the nonpriority message affects the priority messages. In CPS vDRA 23.1.0 and later releases, instead of a common pool, two IPC thread pools, one for priority messages and another for non-priority messages are configured through:

- The CLI command *dra ipc-send-thread priority* configuration
- *Policy Builder - qprocessor.priority* threading configuration to process the priority messages.
- *message_class* parameter with the existing parameters in KPI

For more information see, the *CLI Commands section* in the *CPS vDRA Operations Guide* and the *Advanced Tuning section* in the *CPS vDRA Advanced Tuning Guide*.

DSCP Confirmation for Relay and Diameter Peer Connection

Feature Summary and Revision History

Table 22: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Enabled – Always-on
Related Changes in This Release	Not Applicable

Related Documentation	• *CPS vDRA Configuration Guide* • *CPS vDRA Administration Guide* • *CPS vDRA SNMP and Alarm Guide*

Table 23: Revision History

Revision Details	Release
vDRA updates KPI with configured DSCP value for relay and diameter peer connections.	23.1.0

Feature Description

With this configuration of DSCP values for Relay and Diameter peer connections feature, the following activities are automated to reduce the overall time taken during upgrade:

Confirm the configured DSCP values for Relay and Peer through:

- KPIs that are updated with the DSCP parameter.
  1. peer_message_total
  2. peer_connection_status
  3. relay_message_total
  4. relay_peer_status
- Relay and Peer APIs with DSCP value
  1. /dra/api/activePeerEndpoints
  2. /dra/api/localActiveRelayEndpoints
- Monitoring GUIs with DSCP value
  1. Peer Monitoring GUI
  2. Relay Connections GUI

This **$ cps redeploy dra-vnf --healthcheck yes --sysenv dra** command performs redeployment along with healthchecks on the VMs mentioned in `/data/deployer/env/upgradelit.txt` files and order to be maintained. For more information, see the *CPS vDRA Installation Guide for VMware*.

Configuration and Restrictions

PCRF session query API support to display DSCP value is not supported.

For more information, see *DSCP Mapping for DRA Endpoints section* in the *CPS vDRA Configuration Guide*, *Peer Monitoring section and Monitoring Relay Connections section* in the *CPS vDRA Administration Guide* and *Sample Alert Rules section* in the *CPS vDRA SNMP and Alarm Guide.*

vDRA ISSM Automation Improvements

Feature Summary and Revision History

Table 24: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Disabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Installation Guide*

Table 25: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

Currently in consumer DRA, the new version upgrade takes more time and it could take up to 4 maintenance windows for migrating to a higher version.

With vDRA ISSM Automation Improvements feature, the following activities are automated to reduce the overall time taken during upgrade:

- Complete diagnostics report of DRA and DB VNF VMs.
- Automatic redeployment of VMs with required health check performed.

vDRA also supports in upgrading the VMs by performing diagnostics and redeployment health checks to reduce time constraints.Below arguments are added to the CPS commands.

- diagnostics
- --healthcheck
- –sysenv

Following commands are introduced to perform health check and redeployment of VMs:

$ cps diagnostics dra-vnf

The **$ cps diagnostics dra-vnf** command connects to the existing master vm of the corresponding artifact files placed on the system and runs a sequence of health checks and prompts a clear output to the user.

$ cps redeploy dra-vnf --healthcheck yes --sysenv dra

The **$ cps redeploy dra-vnf --healthcheck yes --sysenv dra** command performs redeployment along with healthchecks on the VMs mentioned in `/data/deployer/env/upgradelist.txt` files and order to be maintained as specified in the installation guide.

For more information, see the *Upgrading VMs Using Diagnostics and Redeployment Health Check* section in the *CPS vDRA Installation Guide*.

Support the Integration of CPS Web Interfaces to the External Server (Halo.E)

Feature Summary and Revision History

Table 26: Summary Data

Applicable Product(s) or Functional Area	vDRA
Applicable Platform(s)	Not Applicable
Default Setting	Disabled – Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	*CPS vDRA Installation Guide*

Table 27: Revision History

Revision Details	Release
First introduced	23.1.0

Feature Description

In CPS vDRA, the current authentication works using GTAC LDAP, which is not multifactor aware. For a multifactor user authentication process, DRA Central UI and Grafana use OpenID Connect (OIDC) to integrate to Halo.E and Global Logon.

For more information, see the *Integrating CPS vDRA and Grafana to Halo-E for User Authentication* chapter in the *CPS ATT-specific Features Guide*.