



vDRA

- [Apply Filter for Specific Column in CRD Table, on page 1](#)
- [Create and Manage API Dedicated User, on page 2](#)
- [Debug Log Collection Statistics Support, on page 3](#)
- [Display Last Published Repository in Policy Builder, on page 4](#)
- [Error Code Classification per Peer/End Node in Grafana, on page 4](#)
- [Limit Permissions to Subset of CRD Tables, on page 5](#)
- [Support Alerts for Monitoring Primary DB, on page 6](#)
- [Support TLS for Gy and Sy, and MTLS Support for Diameter Application, on page 7](#)

Apply Filter for Specific Column in CRD Table

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	<i>CPS vDRA Configuration Guide</i>

Table 2: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

In vDRA, the CRD table supports filter option to select a specific column and search the required data in the selected column



Note By default, the CRD table is set with the **All Visible Columns** option. It selects and searches the keyword against all the columns of that table.

Configuration and Restrictions

- The **All Visible Columns** option displays all the table data if any of the column data matches with the search string.
- If you select any particular column, the filter option of the table displays all the table data of the selected column data that matches with the search string.

For more information, see the *Custom Reference Data Configuration* chapter in the *CPS vDRA Configuration Guide*.

Create and Manage API Dedicated User

Table 3: 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	<i>CPS vDRA Operations Guide</i>

Table 4: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

In vDRA, by default the local users have access to API, CLI and read-only access for central and Grafana and the external users can access VM, API, CLI, central and Grafana.

From this release, you can create and manage users only with the API and restrict other accesses.

The **api-user add** and **api-user remove** CLI commands allow to create and remove API users either with the user-name or gid value.

The following CLI commands help to manage the API dedicated users and to map the external users:

- **api-user add/remove group-details gid <GID> auth-type local/external write-enable true/false**
- **api-user add/remove user-details name <USER_NAME> auth-type local/external write-enable true/false**

- `external-aaa pam username-mapping <USER-NAME> <ROLE>`

Configuration and Restrictions

- In previous releases, the user part of Grafana-admin and Grafana-editor have admin or editor access and the user part of remaining groups have viewer access. From this release, if the user is not a part of any Grafana groups (grafana-admin/editor/viewer), they cannot access the Grafana.
- To convert the read-only and read-write API user roles, remove the access from API user CLI and add a flag with the required write-enable flag.
- Configure the below nacm rule in the configuration mode for CLI restriction.

```
config
nacm rule-list restricting-CLI-access group [ rest-api-ro rest-api-rw ] cmdrule
restrict-CLI-access command * access-operations create,read,update,delete,exec context
cli action deny
```

- The pem file should be in the `/data/keystore` path of the orchestrator.
- If the Halo-E is enabled, the API user is still able to access Grafana in viewer mode using the Halo-E login as the user is getting assigned with default viewer role.

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

Debug Log Collection Statistics Support

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	<i>CPS vDRA Operations Guide</i>

Table 6: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

In vDRA, the log collection CLIs collect the logs to support the troubleshooting based on timestamps.

In CPS 23.2.0 and later releases, you can track the log collection status through the `log_collection_stats` KPI.

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

Display Last Published Repository in Policy Builder

Table 7: 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	<i>CPS vDRA Configuration Guide</i>

Table 8: Revision History

Revision Details	Release
Display the last published and commit repository details in the last commit order in the history page of DRA Policy builder.	23.2.0

Feature Description

In CPS 23.2.0 and later releases, the policy builder displays the last published and commit repository details using the newly added API from the SVN commands. It displays the following details:

- Last committed repository and published repository in the history page.
- List of repositories sorted based on the last commit order in DRA central.

Limitation

DRA Central GUI retrieves the SVN last publish and SVN commit repositories by using an underlying SVN containers. If SVN container is down then GUI will have issues.

For more information, see *SVN Repository Changes* topic in *Policy Builder Configuration* chapter from the *CPS vDRA Configuration Guide*.

Error Code Classification per Peer/End Node in Grafana

Table 9: 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	Not Applicable

Table 10: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

In CPS vDRA, the Grafana monitors the per peer message failures as 3XXX or 5XXX error codes. From CPS vDRA 23.2.0 and later releases, the peer traffic monitor in Grafana includes the following monitoring panels as a part of the **peer_message_total** KPI enhancement:

- destination_host
- destination_realm
- peer_group

The Grafana updates the KPI based on the error code type. It does not consider the DRA rejection messages and the 4XXX error codes in the KPI.

For more information, see the *Statistics/KPI Additions or Changes* topic in the *CPS Release Change Reference*.

Limit Permissions to Subset of CRD Tables

Table 11: 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	<i>CPS vDRA Operations Guide</i>

Table 12: Revision History

Revision Details	Release
First Introduced.	23.2.0

Feature Description

In vDRA, the Custom Reference Data (CRD) REST API supports the query for selection, creation, deletion, and update of CRD table data with the read-only and read-write access. From this release, the CRD REST API allows the following CRD groups to limit the read or write access to a subset of the CRD Table:

- `crd-table-restrict-read-write` - read and write access to the configured subset of CRD tables
- `crd-table-restrict-read-only` - read only access to the configured subset of CRD tables
- `crd-table-restrict-write-only` - read only access to all the CRD tables and write access to the configured subset of CRD tables

Configuration and Restrictions

Use the CLI commands to:

- manage the CRD table group
- manage the mapping of local and external users to the CRD table group

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

Support Alerts for Monitoring Primary DB

Table 13: 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	<i>CPS vDRA SNMP and Alarm Guide</i>

Table 14: Revision History

Revision Details	Release
Enhanced the NO_PRIMARY_DB alert and added a new alert to monitor the status of primary DB in vDRA.	23.2.0

Feature Description

vDRA supports the following alerts and KPI extensions:

- **PREFERRED_PRIMARY_NOT_RUNNING** - Use the alert to know if the the primary DB is not running on the server seed.

- **NO_PRIMARY_DB** - Enhancement to this alert provides information on the DB name and replica set name.
- The **mongo_primary_reachable** KPI includes the following labels added along with the existing labels:
 - preferredprimary
 - seed

Configuration and Restrictions

- In database configuration, the server seed should be the highest priority member.
- If the low priority member is configured as server seed and when the server-seed is down, it triggers the **PREFERRED_PRIMARY_NOT_RUNNING** alert.
- If there are two highest priority members configured and the server seed goes down, another highest priority becomes a primary member. This raises the **PREFERRED_PRIMARY_NOT_RUNNING** alert even if the server seed rolls back. There is no automatic switchover of primary to server seed because of the same priority
- If the seed member is restoring from site 2 to site 1 (inter site primary transition), the alert status may flap for a few seconds before becoming stable.

For more information, see the *Notification and Alerts* section in the *CPS vDRA SNMP and Alarm Guide* and *Statistics/KPI Additions or Changes* topic in the *CPS Release Change Reference*.

Support TLS for Gy and Sy, and MTLS Support for Diameter Application

Table 15: 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	<i>CPS vDRA Configuration Guide</i>

Table 16: Revision History

Revision Details	Release
The feature supports both TLS and MTLS in the policy builder page of vDRA.	23.2.0

Feature Description

In CPS 23.2.0 and later releases, the vDRA supports both TLS and MTLs encryption by enabling them from the PB GUI.

The following DRA applications support TLS and MTLs encryption.

- Gx interface
- Rx interface
- Gy interface
- Sy interface

Configuration and Restrictions

- The open stack supports either TLS or MTLs for data encryption.
- The connecting peer must be inline with the DRA peers.
 - If the DRA peer is TLS enabled, then the connecting peer should be TLS enabled
 - If the DRA peer is MTLs enabled, then the connecting peer should be MTLs enabled

For more information, see the *Policy Builder Configuration* chapter in the *CPS vDRA Configuration Guide*.