



vDRA

- [Dynamic Transport Selection based on Transaction or Origin Host for Wireless Priority Service Messages, on page 1](#)
- [Listening Ports in DRA Deployment, on page 3](#)
- [Preferred Routing for Diameter Update Messages, on page 3](#)
- [Support for New KPIs, on page 4](#)
- [Support to Configure IPC Endpoint Update Interval through CLI, on page 5](#)
- [Support to Enable/Disable Diameter Peer Connections, on page 6](#)
- [Support to Handle Large Number of Peer Connections, on page 8](#)
- [Support to Recreate Mongo Container through CLI, on page 9](#)

Dynamic Transport Selection based on Transaction or Origin Host for Wireless Priority Service Messages

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 Configuration Guide

Table 2: Revision History

Revision Details	Release
First introduced Important This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.	21.1.0

Feature Description

Transactions for certain Wireless Priority Service (WPS) user sessions are sent or received with different DSCP marking. You can create two sets of connections for Rx and Gx each with different DSCP marking. Based on the Rx AAR, the Policy Application Server (PAS) chooses the right connection set for all subsequent transactions related to that session until the P-CSCF indicates a different priority. The DRA allows you to create the following policies for WPS users:

- DSCP marking for peer TCP connections: Use this function for WPS to forward WPS messages received from PAS. The WPS messages are treated as high priority in the network.
- Peer Group Message Class Mapping to configure message class for peer groups.
- Peer Group SRK Mapping.
- Peer Route for Priority Messages: Selects peers based on message priority.
- WPS Message Routing: PAS routes WPS messages over available WPS peer connections. If WPS connections are not available, then PAS routes WPS messages over available normal priority peer connection. PAS does not route non-WPS messages over WPS priority peer connection.
- Priority based destination host Re-routing: Supports rerouting of messages with destination-host based routing when WPS message is addressed to normal priority peer. This is allowed when a peer does not know the FQDN of high priority peer. This message rerouting can be enabled through option in Policy builder.
- DRA Endpoint Message class mapping to configure message class for relay endpoints: Supports dedicated relay links for WPS messages with appropriate DSCP marking for the TCP connection. When forwarding WPS messages, PAS selects relay links matching the message priority.

For more information, see *Dynamic Transport Selection based on Transaction or Origin Host* chapter in the *CPS vDRA Configuration Guide*.

The following new statistics are added:

- diameter_message_route_total
- diameter_message_timeout_total

The following statistics are modified:

- diameter_request_total
- diameter_request_duration_seconds
- relay_message_total

- relay_peer_messages_total
- relay_error_total

For more information on statistics, see [Statistics/KPI Additions or Changes](#).

Listening Ports in DRA Deployment

Feature Summary

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	CPS vDRA Installation Guide for VMware

Feature Description

Added the list of ports used in DRA deployment for various VMs.

For more information, see *Listening Ports in DRA Deployment* appendix in the *CPS vDRA Installation Guide for VMware*.

Preferred Routing for Diameter Update Messages

Feature Summary and Revision History

Table 4: 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

Table 5: Revision History

Revision Details	Release
First introduced	21.1.0

Feature Description

In CPS 21.1.0 release, Destination-Host routing policy is augmented with the following new rule option **Preferred for Update Requests** in the **Peer Group SRK Mapping** window. When Destination-Host routing policy for PCRF Gx peer group is set to **Preferred for Update Requests**, then PAS routes the request as follows.

- PAS resets Destination-Host rule as **Preferred** and route Gx CCR-I request using Table-driven routing when destination host is set as DRA endpoints or destination host is null. If Gx CCR-I request contains destination host AVP as PCRF endpoint, then PAS routes Gx CCR-I request using destination host routing.
- PAS resets Destination-Host rule as **Preferred** and route Gx CCR-U requests using destination host routing and fallback to SRK routing only when PAS failed to find the same PCRF host mentioned in Destination-Host AVP
- PAS resets Destination-Host rule as **Never** and routes Gx CCR-T request using SRK routing



Note

DRA routes second Gx CCR-T request to different PCRF host. PAS supports the new Destination-Host routing rule “Preferred for Update Requests” only for PCRF Gx peer groups. If the new Destination-Host routing rule “Preferred for Update Requests” is configured for any non-Gx peer groups, then PAS sets default Destination-Host rule as “Preferred” for route selection.

For more information, see the *Peer Group for SRK Mapping* section in the *CPS vDRA Configuration Guide*.

The following statistics is updated with new label “message_type” to monitor message type and route type of all diameter messages:

- diameter_message_route_total

For more information on statistics, see [Statistics/KPI Additions or Changes](#).

Support for New KPIs

Feature Summary and Revision History

Table 6: 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 7: Revision History

Revision Details	Release
First introduced	21.1.0

Feature Description

The following new KPIs are implemented to validate CRD update and invalid binding attribute(s).

- crd_cache_load_total
- crd_cache_table_load_failure_total
- crd_cache_table_load_retry_total
- binding_validation_error_total

The following new KPIs are implemented for heap memory statistics and binding read/store.

- late_answer_received_total
- message_processing_time
- message_processing_total
- send_listener_drop
- recv_mesg_process_time
- recv_mesg_processed_total

For more information on statistics, see [Statistics/KPI Additions or Changes](#).

Support to Configure IPC Endpoint Update Interval through CLI

Feature Summary and Revision History**Table 8: 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 Operations Guide

Table 9: Revision History

Revision Details	Release
First introduced	21.1.0

Feature Description

vDRA supports configuring IPC endpoint update interval in milliseconds.

For more information, see *control-plane ipc-endpoint update-interval* section in the *CPS vDRA Operations Guide*.

Support to Enable/Disable Diameter Peer Connections

Feature Summary and Revision History

Table 10: 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 Operations Guide

Table 11: Revision History

Revision Details	Release
First introduced	21.1.0

Feature Description

DRA now supports to select one or more active peers in Peer Monitoring GUI and administratively enable/disable them from connecting to PAS.

Active Peer Endpoints table is enhanced as follows:

- Added a column **Admin State** to indicate the administrative status.
- Ability to administratively disable or disconnect selected peers. **Disconnect** column is generalized as **Actions** and disable option is included in addition to current disconnect option.
- Supports multi-peer selection and administratively disable them. You will be prompted for confirmation before executing the action.



Note In Active Peer Endpoints GUI, after admin disable of active peer, if peer's Admin State gets changed from Enabled to Disabled but still it is shown under Active Peer Endpoints, then peer has to be disconnected by using the disconnect action.

Inactive Peer Endpoints table is enhanced as follows:

- Option to enable peers which are administratively disabled. This option is enabled only for peers which are administratively disabled.
- Table always list admin disabled peers as inactive endpoints even if there are no recent active connections from those peers.
- Ability to multi-select admin disabled peers and enable them. You will be prompted for confirmation before executing the action.

By default, peer connection details for inactive endpoints is retained in the system for 48 hours. If a peer is administratively disabled for more than 48 hours, then last connection details (Peer IP address, DRA endpoint, Event Logs and so on) is not displayed.

The following new APIs are added that can be used to administratively disable and enable multiple peers. The APIs support bulk updates when multiple peers are selected in GUI.

- /custrefdata/peer_admin_disabled_list/_createRows
- /dra/api/localActivePeerEndpoints/disconnect
- /custrefdata/peer_admin_disabled_list/_deleteRows



Attention Peer down alert (DIAMETER_PEER_DOWN) is suppressed for admin disabled peers. There is no change in handling of peer up or peer down state changes and corresponding alerts for admin enabled peers.

For more information, see the following sections: .

- *Peer Admin Disabled List* section in the *CPS vDRA Configuration Guide*
- *View Filtered Data* section in the *CPS vDRA Administration Guide*
- *Admin Disable API* and *Admin Enable API* sections in the *CPS vDRA Operations Guide*

The following new statistics are added:

- cer_message_rejected_admin_disabled_peer
- peer_connection_admin_disconnects

For more information, see [Statistics/KPI Additions or Changes](#).

Support to Handle Large Number of Peer Connections

Feature Summary and Revision History

Table 12: 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 Operations Guide

Table 13: Revision History

Revision Details	Release
First introduced	21.1.0

Feature Description

Director nodes periodically advertise the status of all its peer connections over local and global control plane. All DRA nodes in the network use these peer status messages to keep their peer topology view updated. With this feature, Control Plane load on DRA is reduced enabling to support larger peer connections with the appropriate configurations done for the deployment size.

The following commands are supported:

- control-plane remote-peer-policy global accept
- control-plane remote-peer-policy mated-system id
- control-plane timers peer-status-update-interval
- show control-plane remote-peer-policy

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

The following new statistics are added:

- processed_control_messages_duration
- control_plane_local_publish_queue_drops
- control_plane_remote_peer_policy_accepts
- control_plane_remote_peer_policy_drops
- topology_peer_expirations_total

The following statistics are updated:

- duplicate_control_messages_total

For more information on statistics, see [Statistics/KPI Additions or Changes](#).

Support to Recreate Mongo Container through CLI

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 Operations Guide

Table 15: Revision History

Revision Details	Release
First introduced	21.1.0

Feature Description

vDRA supports removing mongo-s running containers from VMs. This is used to clear the high usage of tmpfs file system memory. In case if any mongo-s container fails to come up or mongod inside it doesn't come up with healthy state then the entire repair operation is aborted.

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

