

# **Policy Builder Configuration**

- Plug-in Configuration, on page 1
- Diameter Application, on page 35
- Routing AVP Definition, on page 41
- Custom Reference Data Tables, on page 46
- SVN Repository Changes, on page 69

# **Plug-in Configuration**

Cisco Policy Builder provides core plug-ins for customizing and optimizing your installation.

- Configurations set at the system level are system-wide except as noted in the bullet items below.
- Configurations set at the cluster level apply to that cluster and the instances in it. A value set here overrides the same value set at the system level.
- Configurations set at the instance level apply to the instance only and override the same value set at the cluster or system level.

Select the **Create Child** action in a **Plug-in Configuration** node in the **Systems** tree to define them. You can change any of the variables from the default, or choose not to use a plug-in, as necessary.

When you create a system from the example, the following configuration stubs appear at the cluster and instance level:

#### Figure 1: Create Child Action

Systems	Plugin Configurations Summary	
Summary		
🕨 🌄 lab	<ul> <li>Actions</li> </ul>	
🔺 🌄 default	Create Child:	
🔁 Plugin Configurations	Threading Configuration	
Account Balance Templates	Async Threading Configuration	
Custom Reference Data Tables	Portal Configuration	
Diameter Agents	Customer Reference Data Configuration	
Diameter Clients	Ldap Configuration	
Diameter Defaults	Balance Configuration	
Fault List		
Ldap Server Sets	Diameter Configuration	
Notifications	Unified API Configuration	
Deliau Cofennese to Deinte	Notification Configuration	
Policy Enforcement Points	Voucher Configuration	
RADIUS Service Templates	RADIUS Configuration	
Subscriber Data Sources	ISG Prepaid Configuration	
Tariff Times	USuM Configuration	
	Audit Configuration	

## **Threading Configuration**

A threading configuration utility is provided for advanced users.

Click **Threading Configuration** in the right pane to add the threading configuration to the system. If you are planning to run the system with higher TPS, then you need to configure Threading Configuration. For further information, contact your Cisco Technical Representative.

The Threading Plug-in having thread pools controls the total number of threads in CPS vDRA that are executing at any given time. Each of these thread pools have a queue associated with it.

A configuration example is shown below:

#### Figure 2: Thread Pool Configuration

Threading Configuration			
Thread Pool Configura	ation		
*Thread Pool Name	*Threads	*Queue Size	*Scale By Cpu Core
rules	50	0	
Add Remove 😯 🐥			

The following parameters can be configured under Threading Configuration:

**Table 1: Threading Configuration Parameters** 

Parameter	Description	
Thread Pool Name	Name of the thread pool.	
	For more information on the thread pool names and recommended values that can be configured, refer to <i>Threading Configuration</i> section in the <i>CPS vDRA Advanced Tuning Guide</i> .	
Threads	Number of threads to set in the thread pool.	
Queue Size	Size of the queue before they are rejected.	
Scale By Cpu Core	Select this check box to scale the maximum number of threads by the processor cores.	

## **Async Threading Configuration**

Click Async Threading Configuration in the right pane to add the configuration in the system.

Use the default values for the Async Threading Plug-in. The Async configuration controls the number of asynchronous threads.



Currently, CPS vDRA does not have any asynchronous threads. However, you must add "Async Threading Configuration" and keep this table empty.

The following parameters can be configured under Async Threading Configuration.

Table 2: Async Threading Configuration

Parameter	Description
Default Processing Threads	The number of threads that are allocated to process actions based on priority.
Default Action Priority	The priority assigned to an action if it is not specified in the Action Configurations table.
Default Action Threads	The number of threads assigned to process the action if it is not specified in the Action Configurations table.
Default Action Queue Size	The number of actions that can be queued up for an action if it is not specified in the Action Configurations table.

Parameter	Description		
Default Action Drop	<b>DropOldestWhenFull</b> : The oldest queued action is dropped from the queue when a new action is added to a full queue. Otherwise, the new action to add is ignored.		
	<b>DropWhenFull</b> : A handler for rejected tasks that silently discards the rejected task. No execution for rejected tasks.		
	<b>DoNotDrop</b> : A handler for rejected tasks that runs the rejected task directly in the calling thread of the execute method, unless the executor has been shut down, in which case the task is discarded.		
	Default value is <b>DropOldestWhenFull</b> .		
Action Configurations Ta	able		
Action Name	The name of the action. This must match the implementation class name.		
Action Priority	The priority of the action. Used by the default processing threads to determine which action to execute first.		
Action Threads	The number of threads dedicated to processing this specific action.		
Action Queue Size	The number of actions that can be queued up.		
Action Drop Oldest When	For the specified action only:		
Full	When checked, the oldest queued action is dropped from the queue when a new action is added to a full queue. Otherwise, the new action to add is ignored.		

## **Custom Reference Data Configuration**

Configure your system, cluster, and instance for the first time to use Custom Reference Data Table plug-in. Then you can create as many tables as needed.

(¢

Important

When you add new fields in CRD, manually update the new fields with appropriate values for all the existing entries in CRD. Otherwise DRA doesn't show any values for these new fields for existing entries and this can cause routing failures.

Click Custom Reference Data Configuration from right pane to add the configuration in the system.

- HA example:
  - Primary Database Host/IP Address: sessionmgr01
  - Secondary Database Host/IP Address: sessionmgr02
  - Database Port: 27717

The following parameters can be configured under Custom Reference Data Configuration.

Parameter	Description
Primary Database Host/IP Address	IP address or a host name of the sessionmgr database.
Address	For example, sessionmgr01.
Secondary Database Host/IP Address	(Optional) This field is the IP address or a host name of a secondary, backup, or failover sessionmgr database.
	For example, sessionmgr02.
Database Port	Port number of the sessionmgr.
	<b>Note</b> Make sure that the value for this field is same as filled in for both the Primary Database Host/IP Address and Secondary Database Host/IP Address fields.
	Default value is 27717.
Db Read Preference	Describes how sessionmgr clients route read operations to members of a replica set. Select one of the following options from drop-down list:
	• Primary: All operations read from the current replica set primary member.
	• PrimaryPreferred: In most situations, operations read from the primary database host. However, if this host is unavailable, operations read from the secondary database host.
	• Secondary: All operations read from the secondary members of the replica set.
	• SecondaryPreferred: In most situations, operations read from secondary members. However, if a secondary database host is unavailable, operations read from the primary database host.
	Default value is Primary.
	For more information, see http://docs.mongodb.org/manual/core/ read-preference/.
Connection Per Host	Number of connections that are allowed for each database host.
	Default value is 100.
	Connection Per Host is a performance tuning parameter and can be changed in case of a performance issue according to the call model and hardware.

#### Table 3: Custom Reference Data Configuration Parameters

Parameter	Description
Avp Persists	Use this table to configure certain AVPs that you want to store in the session database. AVPs that are not configured as part of this table, are not persisted.
	• Name: Enter the name for the AVP value.
	• Avp Name: The name of the CRD/policy derived AVP.
	To retrieve the stored AVPs from the session, use the Customer Reference Data Debug AVPs. This retriever is used to send the stored AVPs in any diameter message, and available in the <b>PolicyState/Session data to Custom AVP Mapping</b> under Custom AVP Profiles.
	<b>Restriction</b> When you configure the AVP Persists table in the Policy Builder, for each AVP, configure both the AVP name and name. If no values are added for these fields, then the particular AVP is not added to the Gx session. This scenario leads to unavailability of the specific AVP and hence, no custom AVP are sent.

For more information on Custom Reference Data API Usage, see the CPS Operations Guide for this release.

# **DRA Configuration**

Figure 3: DRA Configuration

Click DRA Configuration from the right pane in Policy Builder to add the configuration in the system.

Stale Session Timer Minutes	Rate Limiter
1	10
Stale Session Expiry Count	*Binding DB Read Preference
6	Nearest
Stale Binding Expiry Minutes	Stale Binding Refresh Minutes
Stale Binding Expiry Minutes 10080 Binding DB Retries Binding Creation, Primary Alt	2880
10080 Binding DB Retries Binding Creation, Primary Alt	2880 rernate System
10080 Binding DB Retries	2880 rernate System
10080 Binding DB Retries Binding Creation, Primary Alt	2880

The following parameters can be configured under DRA Configuration:

Parameter	Descri	ption	
Stale Session Timer Minutes	subseq	es the time after which the audit RAR should be generated (in the uent audit RAR process cycle that runs every minute in CPS for sessions that are stale.	
	Default	:: 180 minutes (recommended value)	
	Minim	um: 10 minutes	
	Maximum: 10080 minutes		
	Note	Once session becomes stale and crosses configured Stale Session Timer Minutes, vDRA generates audit RAR for that session. If there is no audit RAR or the result code in RAA is other than 5002/2001, stale session expiry count gets decremented by one and the same is updated in session database. vDRA performs this operation until stale session expiry count reaches zero. Once stale session expiry count reaches zero, session is deleted.	
Rate Limiter		es the number of audit RARs per second that should be sent out vDRA.	
		mter value is per worker value. Total number of audit RAR ed is calculated as Rate Limiter value * number of workers.	
	Note	• If primary database is Mongo Shard DB, then rate limiter value should be set as follows:	
		The value to be set in the Rate Limit would be $= 1000$	
		• If primary database is Application Shard DB, then rate limiter value should be set as follows:	
		The value to be set in the Rate Limit would be = $1000$ /No. of workers	
	Minim	um: 1	
		um: 1000 (maximum number of RAR messages per second from to PCEF)	
		ormation on recommended value, refer to Audit Rate Limiter in the CPS vDRA Advanced Tuning Guide.	

#### Table 4: DRA Configuration Parameters

I

Parameter	Description
Stale Session Expiry Count	Specifies the number of retries vDRA should do for a stale session if there is no response of audit RAR or if there is Result-Code in RAA (for audit RAR) other than 5002 or 2001.
	Default: 6
	Minimum: 0 (Session deleted without sending RAR)
	Maximum: 10
	For information on recommended value, refer to Audit Rate Limiter section in the CPS vDRA Advanced Tuning Guide.
Binding DB Read Preference	Used to select the mode when reading from Binding DB. Use "nearest" mode for better performance of traffic that needs only read operation on Binding DB.
	Default: Nearest
	For information on recommended value, refer to Audit Rate Limiter section in the CPS vDRA Advanced Tuning Guide.
Stale Binding Expiry Minutes	Duration after which a binding record is validated against a session record to see if the binding should be deleted because it is stale
	The timer is initialized when the session is created.
	The records are deleted when binding expiry time is reached and no active session is found. Otherwise, the timer is updated so the binding record can be audited after another Stale Binding Expiry Minutes.
	Default: 10080 minutes (168 hours or one week) (recommended value)
	Minimum: 10 minutes
	Maximum: 43200 minutes (28 days)
	For more information about binding DB audits and stale records, see Binding DB Audit, on page 12.
Stale Binding Refresh Minutes	Duration for which the expiry time of the binding database records is refreshed.
	Default: 2880 minutes (48 hours or 2 days - recommended value).
	Minimum: 10 minutes
	Maximum: 10080 minutes (one week)
	<b>Note</b> Stale Binding Refresh Minutes should be greater than Stale Session Timer Minutes.
	Important Stale Binding Refresh Minutes parameter has been deprecated from CPS 19.5.0 and later releases. It is recommended to not set this value as zero.

Parameter	Description	
Binding Creation, Primary	Name of vDRA system to retry Gx CCR-i	
Alternative System	When vDRA tries to route a Gx CCR-i request, but is unable to reach the database, the configured values of first the primary, then the secondary systems are used to route the Gx CCR-i to a different vDRA to try the database.	
	The retry is stopped if that vDRA also cannot reach the database.	
	<b>Note</b> The primary system and the current vDRA system must share a common session database.	
Binding Creation, Secondary	Name of secondary vDRA system to retry Gx CCR-i	
Alternative System	<b>Note</b> The secondary system and the current vDRA must share a common session database.	
Binding Routing, Primary Alternative System	Name of vDRA system to retry Rx AAR When vDRA tries to route a Rx AAR request, but is unable to reach the database, the configured values of first the primary, then the secondary systems are used to route the Rx AAR to a different vDRA to try the database.	
	The retry is stopped if that vDRA also cannot reach the database.	
Binding Routing, Secondary Alternative System	Name of secondary vDRA system to retry Rx AAR	
Settings	Refer to Settings.	
Rate Limits	Refer to Rate Limits.	
DRA Feature	Refer to DRA Feature.	
DRA Inbound Endpoints	Refer to DRA Inbound Endpoints, on page 19.	
DRA Outbound Endpoints	Refer to DRA Outbound Endpoints, on page 21.	
Relay Endpoints	Refer to Relay Endpoints, on page 23.	

## Settings

Click **Settings** check box to open the configuration pane.

The following parameters can be configured under Settings:

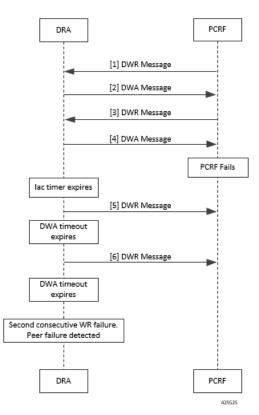
Parameter	Description
Stop Timeout Ms	Determines how long the stack waits for all resources to stop. The delay is in milliseconds.
	Default: 10000 ms (recommended value)
	Minimum: 1000 ms
	Maximum: 60000 ms (one minute)
Cea Timeout Ms	Determines how long it takes for CER/CEA exchanges to timeout if there is no response. The delay is in milliseconds.
	Default: 10000 ms (recommended value)
	Minimum: 1000 ms
	Maximum: 60000 ms (one minute)
Iac Timeout Ms	Determines how long the stack waits before initiating a DWR message exchange on a peer connection from which no Diameter messages have been received. The timeout value is in milliseconds.
	Default: 5000 ms (recommended value)
	Minimum: 1000 ms
	Maximum: 30000 ms (30 seconds)
Dwa Timeout Ms	Determines how long the stack waits for a DWA message in response to a DWR message. If no Diameter message (DWA or other message) is received on the peer connection during the first timeout period, the stack counts a failure, sends another DWR message, and restarts the Dwa timer. If no Diameter messages are received during the second timeout period, the stack counts a second failure. After two consecutive failures, the stack considers the peer connection as failed, and closes the connection.
	The delay is in milliseconds.
	Default: 10000 ms (recommended value)
	Minimum: 1000 ms
	Maximum: 60000 ms (one minute)

#### Table 5: DRA Configuration - Settings Parameters

Parameter	Description
Dpa Timeout Ms	Determines how long it takes for a DPR/DPA exchange to timeout if there is no response. The delay is in milliseconds.
	Default: 5000 ms (recommended value)
	Minimum: 1000 ms
	Maximum: 30000 ms (30 seconds)
Rec Timeout Ms	Determines how long it takes for the reconnection procedure to timeout. The delay is in milliseconds.
	Default: 10000 ms (recommended value)
	Minimum: 1000 ms
	Maximum: 60000 ms (one minute)
Drain Timeout Ms	Indicates the time that a peer connection remains open for responses to be sent to peers even if DPR is sent or received by vDRA.
	If a DPR is sent or received by vDRA, vDRA does not route requests to the disconnecting peer connection via any routing (Dest-Host, SRK, Binding, Table-Driven). However, responses and in-flight requests sent to the corresponding peers till the duration of Drain Timeout. This allows vDRA to gracefully shut down when any remote peer sends a DPR so as to minimize the diameter message loss.
	Default: 2000 ms
	Maximum: Must be less than Dpa timeout Ms
	<b>Note</b> When vDRA initiates DPR and the remote end PCRF/PGW disconnects TCP connection immediately after sending DPA, response for the in-flight requests are dropped before reaching the configured drain timeout value.
Response Timeout Ms	Response timeout in milliseconds.
	Default: 1700 ms

The following figure illustrates the timers in peer detection:





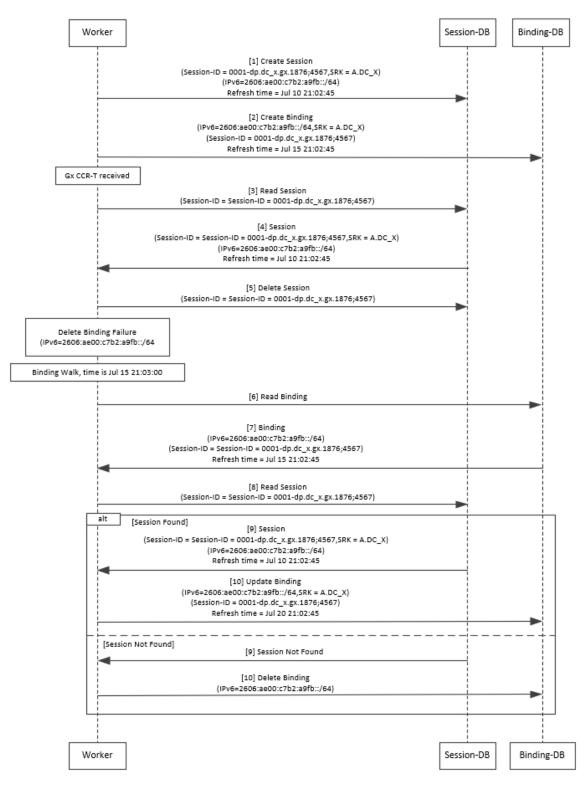
#### **Binding DB Audit**

The Binding DB Audit automatically deletes stale records from the binding DBs. When a Gx session record is created, binding records for the session binding keys are also created. When each binding record is created, the binding record expiry time is initialized to the sum of the session creation time and the Stale Binding Expiry Minutes (that you can configure in Policy Builder).

A binding record is deleted when the corresponding session record is deleted. A binding may become stale if it cannot be deleted when its associated session record is deleted (this occurs typically due to database communication failures). The binding records are audited using a binding audit background process. If the audit process finds a binding record with an expiry time in the past, the binding record is checked for staleness by checking the session database for the corresponding session record. If an active session record is found, the binding record expiry time is updated with sum of current time and the Stale Binding Expiry Minutes. If an active session is not found, the binding is considered stale and is deleted. Note that the binding audit process does not perform any Diameter signaling with the GW before deletion.

The following figures illustrate the working of binding DB:







**Note** There is a housekeeping thread to process stale sessions/bindings which does the following tasks in sequential order:

- 1. Process Stale Session Expiration: Generate Audit RAR OR delete the session if stale session expiry count has reached 0.
- 2. Process expiration of binding: Remove the bindings for which there is no corresponding session.

The stale session expiry task is scheduled to run every minute. This means that the stale session expiry processing is not guaranteed to happen exactly at the configured stale session expiry minutes interval. The stale session expiry processing can happen at any time within the configured stale session expiry minutes to configured stale session expiry minutes + 1 min interval.

However, if the previous task execution of the above mentioned three points takes longer time to complete due to large number of stale sessions/stale bindings, the stale session expiry would run post the previous task completion which can lead to a longer delay than expected 1 minute.

### **Rate Limits**

Rate limit per process instance on Policy Director (lb) VM can be managed using this configuration.

Default is unchecked, that is, no rate limits for Diameter traffic (recommended setting).

If enabled, the following parameters can be configured under Rate Limits:

Parameter	Description	
Rate Limit per Instance on Policy Director	Allowable TPS on a single instance of policy server (QNS) process running on the Policy Director.	
	Minimum: 1	
	Maximum: 5000	
	Note Contact your Cisco representative for usecase-specific recommended values.	
Result-Code in Response	Indicates the error code that must be used while rejecting requests, due to rate limits being reached.	
	Default: 3004	
Error Message in Response	Select the check box to drop the rate-limited messages without sending error response.	
	If the check box is not selected, then the rate limited message are dropped with error response as configured.	

#### Table 6: DRA Configuration - Rate Limits

Parameter	Description
Drop Requests Without Error Response	Select the check box to drop rate limited messages without sending error response.
	If the check box is unchecked, then the rate limited messages are dropped with error response as configured.
	To accommodate configuration to either drop the request or send an error response, a column <i>Discard</i> <i>Behavior</i> can be added under Peer Rate Limit Profile. The column may have one of the two possible values:
	Send Error Response
	• Drop Message
	Default: Unchecked (recommended setting)
	For more information, refer to Peer Rate Limit.
	Important If both Rate Limit Error Code and Rate Limit Error String are provided along with Rate Limit Action as "Drop Message", the Rate Limit Action will take precedence and the other two fields will be ignored.

Here is the list of the available combinations for rate limiting:

#### Table 7: Rate Limiting Combinations

Rate Limiting Type	With Error Code	With Error Code and Error Message	Without Error Code (Drop)
Instance Level	Yes	Yes	Yes
Peer Level Egress	Yes	Yes	Yes
Peer Level Egress with Message Level	Yes	Yes	Yes
Egress Message Level (No Peer Level RL)	Yes	Yes	Yes
Peer Level Ingress	Yes	Yes	Yes
Peer Level Ingress with Message Level	Yes	Yes	Yes
Ingress Message Level (No Peer Level RL)	Yes	Yes	Yes

## **DRA Feature**

Click **DRA Feature** check box to open the configuration pane.

The following parameters can be configured under DRA Feature:

#### Table 8: DRA Features

Parameter	Description
Gx Session Tear Down On5065	By default, <b>Gx Session Tear Down On5065</b> flag is enabled (recommended setting).
	When the PCRF responds with a Experimental Result Code of 5065 in AAAnswer on Rx Interface, DRA deletes its internal binding and session created for the transaction. A RAR with appropriate Session-Release-Cause AVP will also be sent to the PCEF.
	<b>Important</b> When using this flag, there will always be a database query to fetch Gx session id. So this means that the database transactions will linearly increase with AAR traffic on Rx Interface.
Update Time Stamp On Success R A A	When this check box is selected, session timestamp will be updated on receipt of success RAA (Result-Code: 2001) from PCEF. $^{1}$
	Default is checked (recommended setting).
	<b>Important</b> When using this flag, there will always be a database query to fetch Gx session id. So this means that the database transactions will linearly increase with AAR traffic on Rx Interface.
Update Time Stamp On Success C C R U	When this check box is selected, session timestamp will be updated on receipt of success CCR-U (Result-Code: 2001) from PCEF. $^2$
	Default is unchecked (recommended setting).
	<b>Important</b> When using this flag, there will always be a database query to fetch Gx session id. So this means that the database transactions will linearly increase with AAR traffic on Rx Interface.
Enable Proxy Bit Validation	Enables P bit validation.
	vDRA validates the P bit in the Diameter request and, if set, the message maybe proxied, relayed, or redirected.
	If this option is disabled, the P bit in the request is not checked and the request is not considered proxiable.
	Default: Enabled.

Parameter	Description	
Enable Mediation	Enable advanced mediation capabilities in both egress and ingress direction.	
	This feature allows you to configure vDRA to change the value of the Result-Code in Diameter Answer, use mediation to hide topology, prepend label to Destination Host AVP, etc.	
Enable Doic	Enable or disable abatement action for Diameter requests towards PCRF, HSS, AAA, and OCS servers based on reporting of overloaded conditions using the architecture described in RFC 7683 Diameter Overload Indication Conveyance (DOIC).	
	DOIC can be enabled/disabled at peer group level in Peer Group SRK Mapping table. If the destination peer is congested or overloaded, you can choose to either forward, divert, or drop messages.	
Enable PCRF Session Query	Enables or disables the PCRF session query. If you enable this, Policy DRA then supports a fallback routing for Rx AARs for VoLTE using the PCRF session query. This ensures that VoLTE calls can complete in the event that IPv6 binding is not found in the binding database.	
	For an Rx AAR with an IPv6 binding query, vDRA provides the ability to route the Rx AAR based on an API query to the PCRF to determine if it has a session for the IPv6. The queries can be made in parallel to a configured set of query points on PCRFs.	
	The Framed-IPv6 AVP from the Rx must be provided in the request to the PCRF. PCRF returns an SRK to be used for routing, similar to existing binding lookups.	
Create IPv6 Bindings based on PCRF Session Query	Enables creation of IPv6 binding record in the database based or PCRF session query.	
	When PCRF session query result (success) is received and if IPv record is not present in the database, vDRA creates an IPv6 bindin record based on the response from the PCRF.	
	If any CCR-I is received for the same IPv6 record, then it overwrites the IPv6 binding record. For any CCR-T, vDRA deletes the IPv6 binding record from database.	
	<b>Note</b> Ensure you also enable PCRF Session Query for this feature to work.	
	The Stale Binding Expiry and Refresh Minutes are used to clear these binding records from the database. For more information, see Binding DB Audit, on page 12.	

Parameter	Description
Enable Best Effort Binding	When selected allows the operator to enable the best effort binding creation configuration on a per APN basis. The configuration is enabled on a per APN basis and controls any or all of the following bindings (for best effort):
	• IPv6
	• IPv4
	• MSISDN/APN
	• IMSI/APN
	• Session
	Default is unchecked.
	Best effort bindings are those bindings for which DRA does not wait for DB write operations to be completed. DRA forwards the CCR without waiting for DB write and there is an asynchronous write call for best effort bindings.
	If there is no matching APN found in the best effort binding table from CCR-I, DRA takes the legacy behavior and treats all bindings as mandatory. The bindings to be created is primarily decided by binding creation profile and then DRA examines the best effort table to find the best effort and mandatory bindings. The session can be marked as best effort and in such cases session is not created if session Db is down but the CCR is forwarded.
Slf Max Bulk Provisioning TPS	Rate at which subscribers are provisioned in the SLF database.
	SLF bulk provisioning generates high number of database write operations in a short duration of time. To spread out the operations over a period of time and mitigate the performance issue, configure the TPS. The rate limit adds delay between transactions and thereby limits the number of transactions executed per second.
	For more information about SLF bulk provisioning, see the CPS vDRA Operations Guide.
A A R Priority Processing	In vDRA 19.4.0 and later release, this parameter has been deprecated and no longer supported.
	By default, when application-based client sharding is used, AAR processing is prioritized on workers.

<sup>1</sup> The time stamp is updated on generation of Stale RAR. Also, if a success RAR/RAA(2001) comes after generation of Stale RAR, then the Stale RAR counter is reset.

<sup>2</sup> The time stamp is updated on generation of Stale RAR. Also, if a success CCR(U)/CAA(2001) comes after generation of Stale RAR, then the Stale RAR counter is reset.

### **DRA Inbound Endpoints**

The following parameters can be configured under DRA Inbound Endpoints:



**Note** To handle loads of 15 K TPS or more, create multiple TCP connections with PCRF and apply the same configuration to all DRA Directors.

#### Table 9: DRA Configuration - DRA Inbound Endpoints Parameters

Parameter	Description
Vm Host Name	Host Name of the VM that hosts this CPS vDRA endpoint.
Ip Address	Address on which this CPS vDRA endpoint should bind to.
Realm	Realm of the CPS vDRA endpoint.
Fqdn	Fully Qualified Domain Name of the CPS vDRA end point.
Transport Protocol	Allows you to select either 'TCP' or 'SCTP' for the selected DRA endpoint.
	Default value is TCP.
	If the DRA/relay endpoint is to be configured for SCTP, the Transport Protocol should be selected as SCTP for those endpoints.

#### Policy Builder Configuration

Parameter	Description
Multi-Homed IPs	This is a comma separated list of IP addresses that CPS vDRA will use to start the diameter stack with multi-homing enabled for SCTP transport. Diameter stack with TCP transport will still use the existing 'Local Bind Ip' field to specify any specific IP address for TCP stack.
	CPS vDRA will use the 'Local Bind Ip' to bring up SCTP stack and use it along with the 'Multi Homing Hosts' to start the SCTP transport with multi-homing support.
	Note While using SCTP multi-homing functionality review the Linux network and gateway configurations for supporting multiple networks on different subnets. CPS supports Centos 6 release and reverse path filtering kernel parameter (rp_filter) values can be set for allowing packets from different subnets on Policy Director VMs. The default behavior in Centos 6 is to discard the packets in such scenarios.
	<b>Note</b> Both IPv4 and IPv6 are supported in vDRA endpoint configuration. For IPv6, you can enter either short or long format.
	The configuration for multi-homing is validated by netstat command on lb01:
	netstat -apn   grep 3898
Application	Refers to 3GPP Application ID of the interface.
	You can select multiple applications on a peer connection.
	For example, S6a and SLg on a single IPv4/SCTP Multi-homed peer connection.
Enabled	Check to enable the endpoint.
Base Port	Refers to the port on which the CPS vDRA listens for incoming connections.

An example configuration is shown below:

#### Figure 6: DRA Inbound Endpoints - Example Configuration

*Vm Host Name	*Ip Address	*Realm	*Fqdn	Transport Protocol	Multi-Homed IP's	*Application	*Enabled	*Base Port	
ab	10.1.1.1	gx-dra1.cisco.com	gx-dra1	TCP		Gx Application		3868	P
ab	10.1.1.1	gx-dra2.cisco.com	gx-dra2	TCP		Gx Application		3869	
ab	10.1.1.1	gx-dra3.cisco.com	gx-dra3	TCP		Gx Application	$\checkmark$	3870	11
ab	10.1.1.1	rx-dra1.cisco.com	rx-dra1	TCP		<b>Rx</b> Application		4868	
ab	10.1.1.1	rx-dra2.cisco.com	rx-dra2	TCP		<b>Rx</b> Application		<mark>4</mark> 869	
ah	10 1 1 1	sd-dra1 cisco com	sd-dra1	TCP		Sd Application		6868	-

## **DRA Outbound Endpoints**

The following parameters can be configured under DRA Outbound Endpoints:

Table 10: DRA Configuration - DRA Outbound Endpoints Parameters

Parameter	Description
Vm Host Name	Host Name of the VM that hosts this CPS vDRA endpoint.
Ip Address	Address on which this CPS vDRA endpoint should bind to.
Realm	Realm of the CPS vDRA endpoint.
Fqdn	Fully Qualified Domain Name of the CPS vDRA end point.
Transport Protocol	Allows you to select either 'TCP' or 'SCTP' for the selected CPS vDRA endpoint.
	Default value is TCP.
	If the DRA/relay endpoint is to be configured for SCTP, the Transport Protocol should be selected as SCTP for those endpoints.

Parameter	Description	
Multi-Homed IPs	This is a comma separated list of IP addresses that CPS vDRA will use to start the diameter stack with multi-homing enabled for SCTP transport. Diameter stack with TCP transport will still use the existing 'Local Bind Ip' field to specify any specific IP address for TCP stack.	
	<ul> <li>CPS vDRA will use the 'Local Bind Ip' to bring up SCTP stack and use it along with the 'Multi Homi Hosts' to start the SCTP transport with multi-homi support.</li> <li>Note While using SCTP multi-homing functionality review the Linux network ar gateway configurations for supporting multiple networks on different subnets. CPS supports Centos 6 release and rever path filtering kernel parameter (rp_filter values can be set for allowing packets fro different subnets on Policy Director VM The default behavior in Centos 6 is to discard the packets in such scenarios.</li> </ul>	
	<b>Note</b> Both IPv4 and IPv6 are supported in vDRA endpoint configuration. For IPv6, you can enter either short or long format.	
	The configuration for multi-homing is validated by netstat command on lb01:	
	netstat -apn   grep 3898	
Application	Refers to 3GPP Application ID of the interface.	
Enabled	Check to enable the endpoint.	
Peer Realm	Diameter server realm.	
Peer Host	Diameter server host. By default, the connection is initiated on the standard diameter port (3868). If a different port needs to be used than the peer name must be defined using the host:port format.	

An example configuration is shown below:

#### Figure 7: DRA Outbound Endpoints - Example Configuration

*Vm Host Name	*Ip Address	*Realm	*Fqdn	Transport Protocol	Multi-Homed IP's	*Application	*Enabled	*Peer Realm	*Peer Host
lab	10.1.1.1	gx-dra1.cisco.com	gx-dra9	ТСР		Gx Application	1	pcrf2-gx2.cisco.com	gx-pcrf
lab	10.1.1.1	rx-dra1.cisco.com	rx-dra9	ТСР		Rx Application		rx-pcrf.cisco.com	rx-pcrf:4868

### **Relay Endpoints**

The following parameters can be configured under Relay Endpoints:

Table 11: DRA Configuration - Relay Endpoints Parameters

Parameter	Description
Vm Host Name	Host Name of the VM that hosts this Relay endpoint.
Instance Id	Instance Identifier is the ID of the current Instance.
Ip Address	Address on which this DRA endpoint should bind to.NoteThe relay endpoints must be configured on physical IPs and not on virtual IPs.
Port	Port is the listening port for this instance.
Fqdn	Fully Qualified Domain Name of the DRA end point.
Enabled	Check to enable endpoint.

An example configuration is shown below:

#### Figure 8: Relay Endpoints - Example Configuration

*Vm Host Name	*Instance Id	*Ip Address	*Port	*Fqdn	*Enabled
lab	3	10.10.1.1	4868	dra3.rx	

### **Policy Routing for Real IPs with Relay Endpoints**

vDRA relay links consist of a control plane and a data plane.

The control plane uses virtual IPs and the data plane uses real IPs.

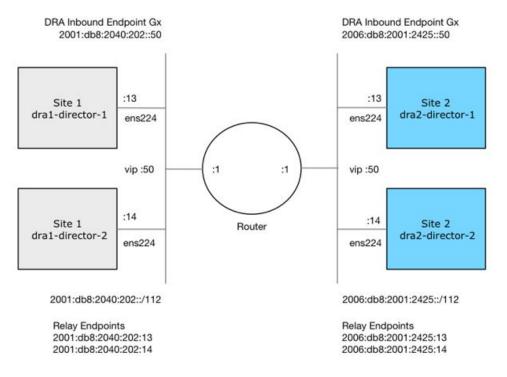
If the control and data plane use the same links, and those links are configured with VIPs, by default, the data plane uses the VIP as its source address for outgoing connections. The data plane uses the VIP as the source address only if the VIP is active on the data plane's outgoing interface.

To avoid this situation, policy routing is used to force the data plane to use the real IP address of the outgoing interface instead of the VIP.

#### **Example of a vDRA Relay Endpoints**

In the following example network, only the DRA director VMs and their relay links are displayed. In a real scenario, many more links may exist on the DRA director VMs.

Figure 9: Example of Relay Endpoints



#### **Policy Routing**

Linux policy routing includes rules and routing tables. The rules identify traffic and point to a user-defined routing table. The routing table contains customized routes.

To prevent the Relay Link's data plane from using the VIP as a source address, a rule is created to identify the real IP in the destination address and identify the desired routing table.

#### **Configure Policy Routing**

The following configuration procedure is performed on Site 1 dra1-director-1. Repeat the procedure for all other dra-directors and modify the IP addresses accordingly.

Perform the following steps on each dra-director VM to configure policy routing:

- **1.** Create a custom routing table
- 2. Create an IP rule for each remote relay endpoint's real IP address
- 3. Add a route to the custom routing table that specifies the real IP source address

#### Set up Custom Routing Table

Set up the custom routing table as shown in the following example:

echo "200 dra.relay" | sudo tee --append /etc/iproute2/rt\_tables

#### Define IP Rules

The following rules match the packets destined to the real IPs of interface ens224 on dra2-director1 and dra2-director2:

```
ip -6 rule add to 2006:db8:2001:2425::13 table dra.relay
ip -6 rule add to 2006:db8:2001:2425::14 table dra.relay
```

#### Define the Route

The following example of the route uses the router's interface as the next hop and specifies ens224's real IP address as the source address for outgoing packets.

```
ip route add 2006:db8:2001:2425::/112 via
2001:db8:2040:202::1 src 2001:db8:2040:202::13 table dra.relay
```

#### Validate the Routing

Use the following example commands to validate the route selection for remote relay real IP and VIP addresses.

ip -6 route show table dra.relay ip -6 route get 2006:db8:2001:2425::13 ip -6 route get 2006:db8:2001:2425::14 ip -6 route get 2006:db8:2001:2425::50

#### Persistent Configuration

In order for the Policy Routing configuration to survive a reboot, add the configuration commands to /etc/network/interfaces under interface ens224 as shown below:

```
auto ens224
iface ens224 inet static
address 192.169.22.13
netmask 255.255.255.0
iface ens224 inet6 static
address 2001:db8:2040:202::13
netmask 112
up ip route add 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1
up ip -6 rule add to 2006:db8:2001:2425::13 table dra.relay
up ip -6 rule add to 2006:db8:2001:2425::14 table dra.relay
up ip route add 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1 src 2001:
db8:2040:202::13 table dra.relay
down ip route del 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1
down ip -6 rule del to 2006:db8:2001:2425::13 table dra.relay
down ip -6 rule del to 2006:db8:2001:2425::14 table dra.relay
down ip route del 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1 src
2001:db8:2040:202::13 table dra.relay
```

#### **Configure Policy Routing with Deployer/Installer**

Configure the VM artifacts and the cloud config to set up policy routing using the deployer.

#### VM Artifacts

Add Policy Route configuration to the DRA director VM's interfaces.esxi file as shown in the following example:

```
cps@installer:/data/deployer/envs/dra-vnf/vms/dra-director
/dra-director-1$ cat interfaces.esxi
auto lo
iface lo inet loopback
auto ens160
```

```
iface ens160 inet static
address 10.81.70.191
netmask 255.255.255.0
gateway 10.81.70.1
auto ens192
iface ens192 inet static
address 192.169.21.13
netmask 255.255.255.0
auto ens224
iface ens224 inet static
address 192.169.22.13
netmask 255.255.255.0
iface ens224 inet6 static
address 2001:db8:2040:202::13
netmask 112
up ip route add 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1
up ip -6 rule add to 2006:db8:2001:2425::13 table dra.relay
up ip -6 rule add to 2006:db8:2001:2425::14 table dra.relay
up ip route add 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1 src
2001:db8:2040:202::13 table dra.relay
down ip route del 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1
down ip -6 rule del to 2006:db8:2001:2425::13 table dra.relay
down ip -6 rule del to 2006:db8:2001:2425::14 table dra.relay
down ip route del 2006:db8:2001:2425::/112 via 2001:db8:2040:202::1 src
2001:db8:2040:202::13 table dra.relay
auto ens256
iface ens256 inet static
address 192.169.23.13
netmask 255.255.255.0
cps@installer:/data/deployer/envs/dra-vnf/vms/dra-director/dra-director-1$
```

#### Cloud Config

Create the dra.relay routing table on the dra-directors by adding the following bootcmd: to user\_data.yml and storing the file at /data/deployer/envs/dra-vnf/vms/dra-director/user\_data.yml. The sed command prevents adding a routing table every time the VM boots.

bootcmd:
 - "sed -i -e '/^200 \*dra.relay/d' /etc/iproute2/rt\_tables"
 - "sh -c \"echo '200 dra.relay' >> /etc/iproute2/rt\_tables\""

#### Example of user data.yml:

```
#cloud-config
debug: True
output: {all: '| tee -a /var/log/cloud-init-output.log'}
```

```
users:
```

```
- name: cps
sudo: ['ALL=(ALL) NOPASSWD:ALL']
groups: docker
ssh-authorized-keys:
```

- ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDzjJjndIvUiBta4VSIbd2gJmlMWcQ8wtejgAbi XtoFZdtMdo9G0ZDEOtxHNNDPwWujMiYAkZhZWX/zON9raavU81gD9+YcRopWUtujIC71YjtoxIjWIBBbrtqt PlUXMUXQsi91RQbUtslENP+tSatS3awoQupyBMMSutyBady/7Wq0UTwFsnYs5Jfs8jIQuMfVQ9uJ4mNn7wJ0 N+Iaf27rE0t3oiY5DRN6j07WhauM61CnZ1JD1zqmTnTHQkgJ3uKmQa5x73tJ10W89Whf+R+dfslVn/yUwK/ vf4extHTn32Dtsxkjz7kQeEDgCe/y7owimaEFcCIfEWEaj/50jegN cps@root-public-key

```
resize_rootfs: true
```

```
write_files:
```

```
- path: /root/swarm.json
   content: |
     {
       "role": "{{ ROLE }}",
       "identifier": "{{ IDENTIFIER }}",
        "master": "{{ MASTER IP }}",
        "network": "{{ INTERNAL_NETWORK }}",
       {% if WEAVE PASSWORD is defined %}"weavePw": "{{ WEAVE PASSWORD }}",
       {% endif %}
        "zing": "{{ RUN_ZING | default(1) }}",
        "cluster id": "{{ CLUSTER ID }}",
        "system id": "{{ SYSTEM ID }}"
    }
   owner: root:root
   permissions: '0644'
  - path: /home/cps/.bash aliases
   encoding: text/plain
   content: |
     # A convenient shortcut to get to the Orchestrator CLI
     alias cli="ssh -p 2024 admin@localhost"
     alias pem="wget --quiet http://171.70.34.121/microservices/latest/cps.pem ;
     chmod 400
cps.pem ; echo 'Retrieved \"cps.pem\" key file'"
   owner: cps:cps
   permissions: '0644'
 - path: /etc/pam.d/common-password
   content: |
    # /etc/pam.d/common-password - password-related modules common to all services
    # This file is included from other service-specific PAM config files,
    # and should contain a list of modules that define the services to be
    # used to change user passwords. The default is pam unix.
    # Explanation of pam unix options:
    # The "sha512" option enables salted SHA512 passwords. Without this option,
    # the default is Unix crypt. Prior releases used the option "md5".
    # The "obscure" option replaces the old `OBSCURE CHECKS ENAB' option in
    # login.defs.
    # See the pam unix manpage for other options.
     # As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
     # To take advantage of this, it is recommended that you configure any
     # local modules either before or after the default block, and use
     # pam-auth-update to manage selection of other modules. See
     # pam-auth-update(8) for details.
    # here are the per-package modules (the "Primary" block)
    password requisite
                                                pam pwquality.so retry=3 minlen=8
    minclass=2
    password [success=2 default=ignore]
                                                pam unix.so obscure use authtok
    try_first_pass sha512 remember=5
    password sufficient
                                                pam sss.so use authtok
     # here's the fallback if no module succeeds
    password requisite
                                                pam deny.so
     # prime the stack with a positive return value if there isn't one already;
     # this avoids us returning an error just because nothing sets a success code
     # since the modules above will each just jump around
    password required
                                                pam permit.so
     # and here are more per-package modules (the "Additional" block)
     # end of pam-auth-update config
```

```
owner: root:root
  permissions: '0644'
runcmd:
 - [vmware-toolbox-cmd, timesync, enable ]
bootcmd:
 - "sed -i -e '/^200 *dra.relay/d' /etc/iproute2/rt_tables"
 - "sh -c \"echo '200 dra.relay' >> /etc/iproute2/rt_tables\""
```

## **SLF** Configuration

You can specify whether the IMSI and MSISDN values are validated in SLF API.

By default, SLF validation is disabled.

To set up SLF validation, create SLF Configuration from the Plugin Configuration in Policy Builder.

Figure 10: SLF Configuration

Systems	SLF Configuration
Summary	or comgaration
<ul> <li>System-1</li> <li>Plugin Configurations</li> <li>Threading Configuration</li> <li>Async Threading Configuration</li> <li>Custom Reference Data Configu</li> <li>Portal Configuration</li> </ul>	*Sif Api Validations Validate IMSI Is Numeric Validate IMSI Length *IMSI Minimum Length
D R A Configuration	15
SLF Configuration	*IMSI Maximum Length
) 👔 cluster-1	15
Custom Reference Data Tables	
Diameter Applications	Validate MSISDN Is Numeric
Fault List	Validate MSISDN Length
Policy Enforcement Points	
Routing Avp Definitions	*MSISDN Minimum Length
Subscriber Data Sources	10
	*MSISDN Maximum Length
	10

The following table describes the SLF API validations that you can configure:

#### Table 12: SLF Configuration

Field	Description
Validate IMSI is Numeric	If checked: IMSI received in the SLF API request must be numeric If unchecked: IMSI numeric validation is not performed on the IMSI received in the SLF API request

Field	Description
Validate IMSI Length	If checked: IMSI length is validated based on the specified IMSI Minimum Length (inclusive) and IMSI Maximum Length (inclusive) If unchecked: IMSI length validation is not performed on the IMSI received in the SLF API request
Validate MSISDN is Numeric	If checked: MSISDN received in the SLF API request
	must be numeric
	If unchecked: MSISDN numeric validation is not performed on the MSISDN received in the SLF API request
Validate MSISDN Length	If checked: MSISDN length is validated based on the specified MSISDN Minimum Length (inclusive) and MSISDN Maximum Length (inclusive)
	If unchecked: MSISDN length validation is not performed on the MSISDN received in the SLF API request

## **Ingress and Egress API Rate limit Configuration**

### **Feature Description**

The vDRA uses PCRF session query to query SRK from PCRF to route the request and then recreates the binding entry. There is no rate limit for a PCRF session query triggered from vDRA. Similarly, Ingress APIs (Binding/Session/SLF/CRD/SVN/Topology/Grafana/Promethus) does not have an overload protection mechanism.

In the CPS 22.1.0 and later releases, vDRA supports a configurable option to rate-limit the incoming traffic and outgoing traffic on the API interface at director level. This rate limiting process protects the system when acting as a client or server. Also, to prevent any back pressure and working on stale messages, vDRA supports configurable queue size and length message SLAs.

### **Egress API Rate Limiting**

vDRA supports PCRF Session Query API rate limits at director level because applying rate limit at worker level can cause uneven distribution of rate limit across Workers.

For example, possibilities of same workers receiving all Rx AAR messages that need PCRF session query, and vDRA can apply rate limit only for that worker. This causes Rx AAR to for that worker even though remaining workers are under rate limit. To avoid this issue, vDRA supports rate limit configurations at the director level.



Note By default, rate limit is not configured for egress API.

The functions of egress rate limiting are:

- The Director triggers PCRF session query based on the configured rate limit. For example, ff configured rate limit is 50, then director allows only first 50 Rx AAR requests per second to trigger PCRF session query and remaining requests are dropped. vDRA sends Rx AAA for dropped PCRF Session query with error message as "PCRF Session Query Throttled". vDRA maintains internal error code as "027".
- If PCRF session query gets triggered due to "No Binding Found" error and PCRF session query got rate limited, then vDRA returns an error message:

"4006:027 - PCRF Session Query Throttled"

• If PCRF session query gets triggered due to "Binding DB Error" error and PCRF session query got rate limited, then vDRA returns error message:

```
"4007:027 - PCRF Session Query Throttled"
```

### Ingress API Rate limiting

Following are the categories of Ingress APIs for which you can set rate limits:

- Binding API
- SLF API
- Topology API (Peer/Relay connections)
- OAM API(CRD/PB/CustRefData/Grafana/Promethues/SVN)

The functions of ingress rate limiting are:

- Ingress API is rate limited in HAProxy service.
- In vDRA, haproxy-common running in master/control-0/control-1/directors is used for load balancing of Policy Builder, Grafana, UI, CC, an so on. The haproxy-common receives request from client and forwards the request to vDRA backend servers.
- Ingress requests reaching haproxy-common is tracked in stick-table with server destination IP as key.
- In frontend, stick-table entries gets compared with configured rate limit for respective ingress API. If the stick-table entries are greater than configured rate limit, then HAProxy sends HTTP deny status to the client. Otherwise, vDRA processes the request and send success status to client.
- vDRA returns error code 429 as deny status to the client for all the failed requests due to rate limit.
- Set the rate limit. For example:
  - If you want to set rate limit as 100 and the clients are configured to send requests only to haproxy-common running in master, then set rate limit as 100.
  - If the clients are configured to send requests to haproxy-common running master/control-0, then rate limit should be set as 50. So that two HAProxy running in master/control-0 provides 100 TPS.

Sample HAProxy configuration to rate limit ingress API:

```
frontend https_all_servers
description Unified API,CC,PB,Grafana,CRD-API,PB-API,Promethues
bind :443
```

```
#ACL for Unified API
acl api path beg /ua/soap /ua/wsdl /dra
http-request deny deny status 429 if api { dst,table http req rate(api servers) gt 50 }
use_backend api_servers if api
#ACL for Grafana
acl grafana path beg /grafana
http-request deny deny status 429 if grafana { dst,table http req rate(grafana servers) gt
100 }
use backend grafana servers if Grafana
backend api_servers
mode http
balance source
option httpclose
option abortonclose
stick-table type ip size 1m expire 10s store http_req_rate(10s)
http-request track-sc1 dst table api servers
server haproxy-api-{{env "CPS SCALING ID" }} haproxy-api-{{env "CPS SCALING ID" }}:80 check
inter 10s resolvers dns resolve-prefer ipv4
{{ if keyExists "crd-api/enabled" }}
acl authoriseReadonlyUsers http auth group(cps user list) qns-ro
acl authoriseAdminUsers http auth group(cps user list) qns
http-request auth realm CiscoApiAuth if !authoriseReadonlyUsers !authoriseAdminUsers
http-request deny if !METH GET authoriseReadonlyUsers
{{ end }}
backend grafana servers
mode http
reqrep ^([^\ ]*\ /)grafana[/]?(.*) \1\2
balance roundrobin
option httpclose
option abortonclose
stick-table type ip size 1m expire 10s store http req rate(10s)
http-request track-sc1 dst table grafana servers
server grafana grafana: 3000 check inter 10s resolvers dns resolve-prefer ipv4
```

### **Configuring Egress API Rate Limit in the Policy Builder**

You can configure egress API rate limit for PCRF Session Query per director in the DRA Configuration.

 In the Policy Builder, click DRA Configuration from the left pane to add the configuration in the system.

#### Figure 11: Director PCRF Session Query Limits

cisco, POLICY BU	Hoshame: policy-builder 41 SVN URL: http://www.heposidm_automation_working_pt SVN Re	vision: 78 Welcome, admin	(ADMIN) POLICY BULLOTR
File Tools			REFERENCE DATA
N 4 5 X 10 41			
Systems Summary Gammary Support System-3 Plugin Configurations	Worker DB Rate Limits DB operations rate limit per Worker ©		
Threading Configuration Anyro: Threading Configuration Custom Reference Data Configu SUF Configuration SUF Configuration	Director PCRF Session Query Limits PCRF session query rate limit per director 0		
D R A Configuration	Dra Dynamic Peer Rate Limiter Reversal Hold Time (Seconds)		
Diameter Applications	30		
Fault List	Reversal Step in %		
Policy Enforcement Points Routing Avp Definitions	20		
Subscriber Data Sources	*D R A Feature		
	<ul> <li>✓ Gx Session Disconnect OnS065</li> <li>✓ Update Time Stamp On Sucess R A A</li> <li>✓ Update Time Stamp On Sucess C C R U</li> </ul>		464855

• Configure the following parameters under DRA Configuration:

#### Table 13: DRA Configuration Parameters

Parameter	Description
DB operations rate limit per	Specifies that the rate limit is per worker for DB operations.
Worker	<b>Default</b> : By default, the rate limit is in disabled state.
PCRF session query rate limit per director	Specifies that the rate limit is for PCRF session query at Director level. Make sure to select the Director PCRF Session Query Limits" in the Policy Builder to view "PCRF session query limits per director" field.
	<b>Default</b> : By default the rate limit is in disabled state.
Reversal Hold Time (Seconds)	Specifies the reversal hold time in seconds.
Reversal Step in %	Specifies the reverstal step in percentage.
Gx Session Disconnect on5065	By default, <b>Gx Session Disconnect On5065</b> flag is enabled (recommended setting).
	When the PCRF responds with a Experimental Result Code of 5065 in AAAnswer on Rx Interface, DRA deletes its internal binding and session created for the transaction.A RAR with appropriate Session-Release-Cause AVP will also be sent to the PCEF.
	<b>Important</b> When using this flag, there is always a database query to fetch Gx session id. This results in linear increase in database transactions with AAR traffic on Rx interface.

Parameter	Description
Update Time Stamp On Success R A A	When this check box is selected, session timestamp will be updated on receipt of success RAA (Result-Code: 2001) from PCEF. $\frac{3}{2}$
	Default is checked (recommended setting).
	<b>Important</b> When using this flag, there is always a database query to fetch Gx session id. This results in linear increase in database transactions with AAR traffic on Rx interface.
Update Time Stamp On Success C C R U	When this check box is selected, session timestamp will be updated on receipt of success CCR-U (Result-Code: 2001) from PCEF. $\frac{4}{2}$
	Default is unchecked (recommended setting).
	<b>Important</b> When using this flag, there is always a database query to fetch Gx session id. This results in linear increase in database transactions with AAR traffic on Rx interface.

<sup>3</sup> The time stamp is updated on generation of Stale RAR. Also, if a success RAR/RAA(2001) comes after generation of Stale RAR, then the Stale RAR counter is reset.

<sup>4</sup> The time stamp is updated on generation of Stale RAR. Also, if a success CCR(U)/CAA(2001) comes after generation of Stale RAR, then the Stale RAR counter is reset.

### **Configuring Ingress API Rate Limit**

You can configure Ingress API rate limits to set the environment variables and use them for checking ingress or egress API rate limit in the *haproxy.cfg.tmpl* file. The CLI updates are applied only in haproxy-common containers because haproxy-common is used for load balancing of Policy Builder, Grafana, UI, API, CC, and so on.

After CLI updates the rate limit in haproxy config file in haproxy-common containers, haproxy is restarted automatically to apply new rate limits.

```
Note
```

Since these CLIs internally applies the rate limit and restart haproxy, you need not manually restart haproxy-common in Master/Control/diameter containers after configuring new rate limits.

You can set common rate limit for all binding API using the CLI **dra set-ratelimit binding-api** *rate limit value*. vDRA provides options to override common rate limits for imsi, imsi-apn, msisdn, msisdn-apn, and ipv6 binding api by specifying binding type in CLI as follows:

```
dra set-ratelimit binding-api-imsi | binding-api-imsi-apn |
binding-api-msisdn
| binding-api-msisdn-apn | binding-api-ipv6]value
```

By default, DRA does not apply any rate limit for ingress APIs.

Use the following CLI commnads to select different ingress API types to set, remove or show rate limits.

- dra set-ratelimit binding-api <rate limit value>
- dra set-ratelimit binding-api-imsi <rate limit value>

- dra set-ratelimit binding-api-imsi-apn <rate limit value>
- dra set-ratelimit binding-api-msisdn <rate limit value>
- dra set-ratelimit binding-api-msisdn-apn <rate limit value>
- dra set-ratelimit binding-api-ipv6 <rate limit value>
- dra set-ratelimit session-api <rate limit value>
- dra set-ratelimit slf-api <rate limit value>
- dra set-ratelimit topology-api <rate limit value>
- dra set-ratelimit oam-api <rate limit value>
- dra remove-ratelimit binding-api
- dra remove-ratelimit binding-api-imsi
- · dra remove-ratelimit binding-api-imsi-apn
- · dra remove-ratelimit binding-api-msisdn
- · dra remove-ratelimit binding-api-msisdn-apn
- dra remove-ratelimit binding-api-ipv6
- dra remove-ratelimit session-api
- dra remove-ratelimit slf-api
- dra remove-ratelimit topology-api
- dra remove-ratelimit oam-api
- · dra show-ratelimit
- · dra show-ratelimit binding-api
- dra show-ratelimit binding-api-imsi
- · dra show-ratelimit binding-api-imsi-apn
- dra show-ratelimit binding-api-msisdn
- · dra show-ratelimit binding-api-msisdn-apn
- dra show-ratelimit binding-api-ipv6
- dra show-ratelimit slf-api
- · dra show-ratelimit session-api
- · dra show-ratelimit topology-api
- dra show-ratelimit oam-api

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

# **Diameter Application**

## **Sd Application**

For Sd, an Application Routing table is used to map specific diameter command codes and CC-Request-Types to a table, typically, an Sd New Session table for routing Sd TSRs to a peer route. The Sd New Session CD table will choose a peer route based on the Destination-Realm. The peer route will then point to a Peer-Group which contains multiple peer connections to a TDF and the DRA will load balance among the TDF peer connections in the Peer Group.

An example configuration is shown below:

Figure 12: Diameter Application - Sd Application Example

lame			*Application Id		
Sd Application		16777303			
endor Ids					
10415		Add	✓ Tgpp Application	n	
		Remove			
Application I		Remove	Cc Request Type	*Destination	HcAction Tables
			Cc Request Type	*Destination	HcAction Tables New Sd Session
Name	*Priority	*Command Code			
Name Sd-TSR	*Priority 0	*Command Code 8388637	0		New Sd Session
Name Sd-TSR Sd-CCR-I	*Priority 0 0	*Command Code 8388637 272	0 1	<b>V</b>	New Sd Session New Sd Session

The following parameters are configured under Sd Application:

#### **Table 14: Sd Application Parameters**

Parameter	Description
Name	Name of the Sd application.
Application Id	16777303, 3GPP specified Application Identifier for Sd interface.
Vendor Ids	Vendor Identifiers that are required to be supported on Sd interface.
Tgpp Application check box	If this check box is selected, indicates this is a 3GPP defined application interface.
Application Route table	
Name	Identifier of the route.

Parameter	Description
Priority	Indicates the priority of the route.
Command Code	Indicates value of command code AVP within the message.
Cc Request Type	Indicates if the Credit Control Request type is Initial(1)/Update(2) or Terminate(3).
Destination Host Null	If this check box is selected, indicates if Destination Host will be null in messages received for this application.
Action Tables	Identifies the request routing table for this interface and message.

## **Gx** Application

For Gx, an Application Routing table is used to map specific diameter command codes and CC-Request-Types to a table. When "Destination Host Null" is checked, it means Destination-Host AVP is null. It will then check for table driven routing.

An example configuration is shown below:

Figure 13: Diameter Application - Gx Application Example

		*Ap	plication Id		
Gx Application		16777238			
endor Ids					
8164					
9		Add	Tgpp Application		
10415		Remove	366 66		
Application Rout	*Priority	*Command Code	Cc Request Type	*Destinal	tion HcAction Tables
Gx Initial	1	272	1		New Gx Session
		272	3		New Gx Session
GxTerminate	1	212			

C-DRA attempts to do Dest-Host routing before doing table driven routing. If the Dest-Host AVP is absent, empty, or equal to the CDRA FQDN, then we skip Dest-Host routing altogether and proceed to Table-Driven routing.

The following parameters are configured under Gx Application:

**Table 15: Gx Application Parameters** 

Parameter	Description	
Name	Name of the Gx application.	

Parameter	Description
Application Id	16777238, 3GPP specified Application Identifier for Gx interface.
Vendor Ids	Vendor Identifiers that are required to be supported on Gx interface.
Tgpp Application check box	If this check box is selected, indicates this is a 3GPP defined application interface.
Application Route table	
Name	Identifier of the route.
Priority	Indicates the priority of the route.
Command Code	Indicates value of command code AVP within the message.
Cc Request Type	Indicates if the Credit Control Request type is Initial(1)/Update(2) or Terminate(3).
Destination Host Null	If this check box is selected, indicates the message will contain a Destination-Host.
Action Tables	Identifies the request routing table for this interface and message.

# **Rx Application**

Identifies the request routing table for this interface and message.

Figure 14: Diameter Application - Rx Application Example

lame			*Application Id		
Rx Application			16777236		
endor Ids					
13019					
8164		Add	Topp Application	1	
9		Remove			
9		Remove			
	6	Remove			
Application Route	*Priority		Cc Request Type	*Destina	tion HcAction Tables
Application Route				*Destina	tion HcAction Tables New Rx Session
	*Priority	*Command Code	Cc Request Type		
Application Route Name Rx Initial	*Priority 1	*Command Code 265	Cc Request Type		New Rx Session

The following parameters are configured under Rx Application:

Parameter	Description
Name	Name of the Rx application.
Application Id	16777236, 3GPP specified Application Identifier for Rx interface.
Vendor Ids	Vendor Identifiers that are required to be supported on Rx interface.
Tgpp Application check box	If this check box is selected, indicates this is a 3GPP defined application interface.
Application Route table	
Name	Identifier of the route.
Priority	Indicates the priority of the route.
Command Code	Indicates value of command code AVP within the message.
Cc Request Type	Not supported for Rx interface.
Destination Host Null	If this check box is selected, indicates if Destination Host will be null in messages received for this application.
Action Tables	Identifies the request routing table for this interface and message.

#### Table 16: Rx Application Parameters

# **Sh Application**

Sh interface is used for communication between AS and HSS for Call data query/Push subscriber profile and subscriber notification procedures.



Note In certain scenarios, the customer might use the Sh interface between PCRF and HSS also.

Figure 15: Diameter Application - Sh Application Example
--

lame		*	Application Id		
Sh Applicat	tion		16777217		
endor Ids					
10415		Add	<ul> <li>Tgpp Application</li> </ul>		
pplication	Route				
<b>pplication</b> Name	Route *Priority	*Command Code	Cc Request Type	*Destinat	ion HcAction Tables
Name		*Command Code 306	Cc Request Type	*Destinat	
Name UDR	*Priority				ion HcAction Tables Sh_Application Sh_Application
	*Priority 0	306	0		Sh_Application

The following parameters are configured under Sh Application:

Table 17: Sh Application Parameters

Parameter	Description
Name	Name of the Sh application.
Application Id	16777217, 3GPP specified Application Identifier for Sh interface.
Vendor Ids	Vendor Identifiers that are required to be supported on Sh interface.
Tgpp Application check box	If this check box is selected, indicates this is a 3GPP defined application interface.
Application Route table	
Name	Identifier of the route.
Priority	Indicates the priority of the route.
Command Code	Indicates value of command code AVP within the message.
Cc Request Type	CC-Request-Type is not applicable for Sh interface.
Destination Host Null	If this check box is selected, indicates the message will contain a Destination-Host.

Parameter	Description
Action Tables	Identifies the request routing table for this interface and message.

# **S6a Application**

DRA supports S6a interface with the implementation of Subscriber Location Function(SLF) feature. S6a is an interface which supports the mobility management and subscriber data management procedures between MME and HSS in an LTE EPC network.

An example configuration is shown below:

Figure 16: Diameter Application - S6a Application Example

Name		*Ap	plication Id		
S6a Applicatio	n	16	777251		
Vendor Ids					
10415					
		Add	Tgpp Application		
		Remove	SFFORF		
		Remove			
Application Ro					
Name	ute *Priority	*Command Code	Request Type	*Destination Host Null	Action Tables
		*Command Code 318	Request Type	*Destination Host Null	Action Tables S6a_Application
Name	*Priority				

The following parameters are configured under S6a Application:

Parameter	Description
Name	Name of the S6a application.
Application Id	16777251, 3GPP specified Application Identifier for S6a interface.
Vendor Ids	Vendor Identifiers that are required to be supported on S6a interface.
Tgpp Application check box	If this check box is selected, indicates this is a 3GPP defined application interface.
Application Route table	
Name	Identifier of the route.

Parameter	Description		
Priority	Indicates the priority of the route.		
Command Code	Indicates value of command code AVP within the message.		
Cc Request Type	CC-Request-Type is not applicable for S6a interface.		
Destination Host Null	If this check box is selected, indicates the message will contain a Destination-Host.		
Action Tables	Identifies the request routing table for this interface and message.		

# **Routing AVP Definition**

# **Gx Session**

An example configuration is shown below:

Figure 17: Routing AVP Definition - Gx Session

Name	
New Gx Session	
Routing Avp Lookup	
*Search Table Group	
apn_mapping_table	
TB_GX_NEW_SESSION	

# **Rx Session**

Figure 18: Routing AVP Definition - Rx Session

Name	
New Rx Session	
Routing Avp Lookup	
*Search Table Group	
TB_RX_NEW_SESSION	
apn_mapping_table	

## **Rx New Session Rules - CRD Table**

An example configuration is shown below:

Figure 19: Rx New Session Rules - CRD Table

Name		Display Name							
TB_RX_NEW_SESSION		Rx New Session Rules	Cache Re	esults					
Activation Condition			*Evaluation	Order					
Rx	select dear	<ul> <li>Best Match</li> </ul>	0						
Columns									
"Name		Display N	ame		*Use In 0	Conditi "Type		Key	Required
logical_apn		Logical Al	PN .		<i>.</i>	Text		2	~
origin_host		Origin Ho	st		1. Contraction (1. Contractio)	Text		×	~
peer_route		Peer Rou	te		1	Text			
destination_host		Destinatio	on Host		1	Text		1	۲.
Column Details			v	stalidation			Bustino Bisting		
olumn Details Valid Values The values allowed in Contr (a) All	ol Center for this colu	umn	v	Validation Validation used by Control Center Regular Expression			Runtime Binding Which rows match when a message is received None Bind to Subscriber AVP code		
olumn Details Valid Values The values allowed in Contr (a) All		umn Visplay Name	V R	Validation used by Control Center			Which rows match when a message is received None		
Column Details			V R	Validation used by Control Center Regular Expression			Which rows match when a message is received None Bind to Subscriber AVP code		
Column Details			V R	Validation used by Control Center Regular Expression			Which rows match when a message is received None : Bind to Subscriber AVP code Bind to Session/Policy State Field		
Column Details Valid Values The values allowed in Contr a All Clist of valid Values			V R	Validation used by Control Center Regular Expression			Which rows match when a message is received None: Bind to Subscriber AVP code: Bind to Session/Policy State Field Retrieve Dession/Policy State Field Dind to a result column from austher table		
olumn Details			V R	Validation used by Control Center Regular Expression			Which rows match when a message is received None Bind to Subscriber AVP code Bind to Subscriber AVP code Bind to Session/Policy State Field Retrieve Destination Host (Cisco: Select) clean Bind to a result column from another table		
Unit of Valid Values	0	isplay Name	V R	Validation used by Control Center Regular Expression			Which rows match when a message is received None: Bind to Subscriber AVP code: Bind to Session/Policy State Field Retrieve Dession/Policy State Field Dind to a result column from austher table		
Column Details Valid Values The values allowed in Contr All Cust of valid values "Name	0	isplay Name	V R	Validation used by Control Center Regular Expression			Which rows match when a message is received None Bind to Subscriber AVP code Bind to Subscriber AVP code Bind to Session/Policy State Field Retrieve Destination Host (Cisco: Select) clean Bind to a result column from another table		

## **Gx New Session Rules - CRD Table**

For Gx, an Application Routing table is used to map specific diameter command codes and CC-Request-Types to a table, typically, for routing Gx CCR-Is. The Gx CCR-I should be routed based on a logical APN and the Origin-Host attribute. Regular expression matching of logical APNs and Origin-Hosts can also be configured. The implementation should be flexible to allow CRDs to be configured for routing of other attributes such as Destination-Realm and Origin-Realm.

Figure 20: Gx New Session Rules - CRD Table

*Name		Display Name								
TB_GX_NEW_SESSION		Gx New Session	Rules	Cache Results						
Activation Condition				*Evaluation Order						
Gx	select dear	<ul> <li>Best Match</li> </ul>		1						
Columns										
"Name			Display Name		*Use In	Conditi "Type		Key	Required	
peer_route			Peer Route		1	Text				
origin_realm			Origin Realm		9	Text		4	<b>a</b>	
destination_realm			Destination Rea	alm	2	Text		2	2	17
origini_host			Origin Host		1	Text		4	1	
logical_apn			Logical APN		1	Text		1	2	
imsi Add Remove 😚 😣			IMSI		1	Text		1	1	
Valid Values The values allowed in Contr (e) All (c) List of Valid Values				Validation Validation used by Control Center Regular Expression			Runtime Binding Which rows match when a message is received None Bind to Subscriber AVP code			
"Name	1	Display Name		Regular Expression Description			Bind to Session/Policy State Field     Retrieve Origin Realm (Cisco DR select dear     Bind to a result column from another table			
							Bind to Diameter request AVP code			
							Matching Operator			

# **Sd New Session Rules - CRD Table**

An example configuration is shown below:

Figure 21: Sd New Session Rules - CRD Table

*Name		Display Name	-						
TB_SD_NEW_SESSION		SD_NEW_SESSION	Cache Results						
Activation Condition			*Evaluation Order						
	select dear	Best Match	0						
Columns									
"Name		Display Na		"Use In	Conditi *Type		Key	Required	
peer_route		Peer Route			Text				
origin_realm		Origin Rea		1	Text		4	9	
destination_realm		Destinatio		1	Text		1	1	
destination_host		Destinatio	n Host	1	Text		1	7	
logical_apn		Logical API	4	7	Text		1	~	
msisdn		MSISDN		1	Text		1	1	
Add Remove 😯 🚸									
Column Details									
Valid Values			Validation			Runtime Binding			
The values allowed in Contro	Center for this col	lumn	Validation u	sed by Control Center		Which rows match when a message is received			
(e) Al			Regular Exp	ression		None .			
"Name		Display Name	Regular Exp	ression Description					
						entert de r			
						Matching Operator			

# **Logical APN List - CRD Table**

Figure 22: Logical APN List - CRD Table

Name	Display Name	Cache Results	Activation Condition					
logical_apn_list	Logical APN List	Cache Results	select	lear				
Columns								
"Name		Display Name		*Use In Co			Кеу	Required
logical_apn		Logical APN		1	Text		1	9
Add Remove 😯 🚸 Column Details								
Valid Values			Validation			Runtime Binding		
The values allowed in Co	ntrol Center for this column		Validation used by Control Center			Which rows match when a message is received		
<ul> <li>All</li> </ul>			Regular Expression			(e) None		
"Name	Display Name		Regular Expression Description					
	0					C Bind to Diameter request AVP code		
						Matching Operator		

## **Dynamic AVP Retriever for Routing**

DRA supports routing messages based on the following AVPs from request message:

- Destination-Host
- Destination-Realm
- Origin-Host
- Origin-Realm
- APN (from Called-Station-ID)
- IMSI (from Subscription-ID)
- MSISDN (from Subscription-ID)

Regular-expression matching and combinations of AVPs is supported. This requirement is not applicable across all messages on different interfaces. The following table shows applicability of the AVP's at a message and interface level.

Interface	Message	Origin Host	Origin Realm	Destination Host	Destination Realm	APN (Called-Station-ID)	IMSI	MSISDN
Gx	CCR-I	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	CCR-U	No	No	No	No	No	No	No
	RAR	No	No	Yes	No	No	No	No

Table 19: Regular-expression Matching and Combinations of AVPs

L

Interface	Message	Origin Host	Origin Realm	Destination Host	Destination Realm	APN (Called-Station-ID)	IMSI	MSISDN
Sd	TSR	Yes	Yes	Yes	Yes	No	No	No
	CCR-I	Yes	Yes	Yes	Yes	No	No	No
	CCR-U/T	No	No	Yes	No	No	No	No
	RAR	No	No	Yes	No	No	No	No
Rx	RAR	No	No	Yes	No	No	No	No

Dynamic AVP Retrievers are used mostly used in Custom Reference Data where data has to be fetched from messages at runtime.

### **Configure Dynamic AVP Retriever**

The following sample configuration shows how to retrieve the AVP and bind it to a Key Column in the CRD.

- Step 1Select the column name from the Columns table and click select near Bind to Session/Policy State Field to open the<br/>Please select an object... dialog box.
  - **Note** You can use **Bind to Session/Policy State Field** only for those columns in the **Columns** table where **Key** column has been selected.
- **Step 2** Select the required object from the dialog box and click **OK**.

#### Figure 23: Adding AVPs

*Name	Display Name		*Use In C	onditi *Type		Key	Required
calledStationId	APN		9	Text		1	$\overline{\checkmark}$
logical_apn	Logical APN		1	Text			$\sim$
		Please select an ob	ject		o x		
dd Remove 👔 🔶			ofile Charging Id		-		
Valid Values The values allowed in Contro All List of Valid Values	ol Center for this column	Retrieve AP     Retrieve Ap     Retrieve Bin	bscriber Id Retrier N (Cisco DRA) plication Id (Cisco ading FQDN (Cisco stination Host (Ci	DRA) DRA)	-	when a messa	age is received
"Name	Display Name	<ul> <li>Retrieve IM</li> <li>Retrieve MS</li> <li>Retrieve Ori</li> </ul>	stination Realm ( SI (Cisco DRA) ISDN (Cisco DRA) igin Host (Cisco D igin Realm (Cisco	RA)	Cisc	/Policy State F to DRA) column from a	select <u>clear</u>
Add Remove 🕢 🕹		-	E	ок		er request AVP	selection <u>clear</u>
		-					

**Step 3** Repeat these steps to add additional AVPs.

# **Custom Reference Data Tables**

## **Search Table Groups**

### **Peer Rate Limit Profile**

This is a Search Table Group whose key columns are Peer Group, Peer FQDN or Origin Host in the message and Message Direction.

Using this search table group, the user can configure a maximum rate for each of the configured and defined diameter peers. It also allows the user to configure a maximum rate for each server process.

The peer rate limit is shown below:

#### Figure 24: Peer Rate Limit - STG

*Name	Display Nar	ne						
peer_rate_limit_profile	Peer Rate L	imit Profile	Cache Results					
Activation Condition	Best Mat	ch	*Evaluation Order					
Columns	select dear		0					
*Name	Dissistant biose		Alles To d				Beering	
peer_group	Display Name Peer Group		-Use In C	Conditic *Type Text		Key	Required	1
peer_fqdn	Peer FODN		9	Text		-	÷	
direction	Message Dire	ction		Text		-	÷.	
rate limit profile	Rate Limit Pro		~	Text		-	-	
peer_rate_limit	Peer Rate Lim		~	Number				
discard behavior	Discard Beha	tion.	5	Number				
Column Details Valid Values The values allowed in Control Ce All List of Valid Values	inter for this column	Vali	idation idation used by Control Cen gular Expression		Runtime Binding Which rows match whe None Bind to Subscriber J		eived	
*Name	Display Name	Rej	gular Expression Descript	tion	Bind to Session/Poli	cy State Field	i dear	
					Bind to a result colu	mn from another b	able	
						select	clear	
Add Remove A					O Bind to Diameter re	quest AVP code		
O Valid values pulled from anot	ther table's column (key)							
	selecti dear				Matching Operator			
					1.00			

- Peer Group: This is the group of peers classified together using Peer Group and Peer Group Peer values initiating the message.
- Peer FQDN: The origin host of the peer. A specific diameter peer with its Fully Qualified Domain Name can be specified in this field or use wildcards specified by \* in this field for any peer or matching peers like hss\*.
- Direction: Message direction (Ingress and Egress).
  - Ingress: Any diameter messages received by CPS vDRA from diameter peer. The routing decision by CPS vDRA will be taken after the ingress side rate limiting has been applied.
  - Egress: Any diameter messages forwarded/routed by CPS vDRA to diameter peer. The egress side rate limiting will be applied after the routing decision has been taken by CPS vDRA.

- Peer Rate Limit: This field is to specify the threshold in TPS above which the diameter messages are discarded. This can be left empty if none of the messages are to be dropped or only message level rate limit is to be applied.
- Rate Limit Profile: Profile Name applicable for this Peer Group and Peer, if specified. This profile maps to Rate Limiting at message level. This field enables the rate limit at per message/command code level. See Message Rate Limit Profile for more details.
- Rate Limit Result Code: The result code sent by CPS vDRA for response message towards diameter peer when Discard Behavior is configured as Send Error Answer. In case Discard Behavior is configured as Drop Message, this field is ignored.
- Error String: The string specified in this field is populated by CPS vDRA in AVP Error Message for response message towards diameter peer when Discard Behavior is configured as Send Error Answer. In case Discard Behavior is configured as Drop Message, this field is ignored. This is an optional field when Discard Behavior is configured as Send Error Answer.

Note

If both Rate Limit Error Code and Rate Limit Error String are provided along with Rate Limit Action as "Drop Message", the Rate Limit Action takes precedence and the other two fields will be ignored.

For more information, see Peer Rate Limit Profile.

### **Peer Group Mapping**

#### Figure 25: Peer Group Mapping - STG

Name	Display Nam	e				
peer_group_mapping	Peer Group	Mapping	Cache R	lesults		
ctivation Condition			*Evaluatio	n Order		
	selecti clear 🛛 🐼 Best Match		0			
Columns						
*Name	Display Name		*Use In C	onditic *Type		Кеу
realm_pattern	Realm Pattern		1	Text		1
fqdn_pattern	FQDN Pattern		<b>V</b>	Text		$\checkmark$
peer_group	Peer Group			Text		
weight	Weight		2	Number		
vdd) Remove) 🔐 👪 olumn Details						
/alid Values		Validati			Runtime Binding	
The values allowed in Control Center	er for this column	Validatio	on used by Control	Center	Which rows match w	hen a messag
All		Regular	Expression		None	
List of Valid Values					Bind to Subscribe	r AVP code
*Name I	Display Name	Regular	Expression Desc	ription		
					Bind to Session/P	

For more information, see Peer Group Mapping.

### Message Retry Profile

Message retry profile has been added.

#### Figure 26: Message Retry Profile - STG

*Name		<b>Display Name</b>	-	_				
message_retry_profile		Message Retry	Profile	Cache Resu	ts			
Activation Condition			*1	Evaluation Or	der			
	select <u>clear</u>	Best Match	C	)				
Columns								
*Name			Display Name	*Use Ir	Conditi *Type	Key	Required	
peer_group			Peer Group		Text	$\overline{\checkmark}$	<b>V</b>	
app_id			Application Id	<b>V</b>	Text	$\overline{\checkmark}$		
cmd_code			Command Code	~	Text	$\overline{\checkmark}$		
rc_in_resp			Result Code	$\overline{\checkmark}$	Text	$\overline{\checkmark}$	Image: A start and a start	
exp_rc			Experimental RC		True/False			
num retries			Number Of Retries		Text			
Valid Values			lation		Runtime Binding			
The values allowed in Cont	rol Center for this colu	umn Valio	lation used by Contro	l Center	Which rows match	h when a m	essage is receive	d
<ul> <li>All</li> </ul>		Reg	ular Expression		None			
O List of Valid Values					) Bind to Subsc			
*Name	Display Name	Reg	ular Expression Desc	ription				
					O Bind to Sessic		ite Field	
							select <u>cle</u>	
					O Bind to a resu	lt column fr	om another table	
					) Bind to a resu	lt column fr		
Add Remove 😚 🐣					<ul> <li>Bind to a resu</li> <li>Bind to Diame</li> </ul>		om another table	
Add) Remove 😚 🕀	another table's colur	nn (key					om another table	

- Peer Group: Peer group for which the retry has to be happen.
- Application Id: Application Id of the diameter applications.
- Command Code: Command Code of the message.
- Result Code: Result code received from PCRF for timeout. The value is 7000.
- Experimental RC: Indicates whether result code is experimental or not. This is for future purpose and value in this has no effect on the message retry functionality.
- Number of Retries: Number of retries for the message.

For more information, see Message Retry Profile.

### **Message Mediation Profile**

The message mediation profile is used to provide support for mediation of AVPs in Diameter request and answer.

- For Diameter requests, only remove is supported.
- For Diameter answers, the following actions are supported:
  - "remove" meaning remove all matching AVPs in the request.
  - "copy" meaning copy from the request if no AVPs are present in the answer.

• If the AVP is present in answer, no action is performed.

• "overwrite" meaning first remove and then copy from the request.

- Check if the AVP is present in answer, if so remove and add from request.
- If AVP is not present in answer, copy from request.

#### A new Message Mediation Profile STG has been added:

#### Figure 27: Message Mediation Profile - STG

*Name		Display Name							
message_mediation_profile		Message Mediation Profile	Cache Re	isults					
Activation Condition		Best Match	*Evaluation	Order					
Columns	select dear		0						
*Name		Display Name		Use In Condi	tic *Type		Key	Required	
app_id		Application Id		7	Text		V		2
cmd_code		Command Code		1	Text		~	v	
msg_type		Message Type		1	Text		4	1	
avp_code		Avp Code		2	Text		2	1	
vendor_id		Avp Vendor Id		2	Text		v .	2	
avo action		Avp Action		-	Text				
Valid Values The values allowed in Control Center All Ust of Valid Values	r for this colu	mn Valid Regu	lation lation used by Cor ular Expression			Runtime Binding Which rows match when a None Bind to Subscriber AVP			
*Name	Display Nar	ne Regi	ular Expression	Description		<ul> <li>Bind to Session/Policy 1</li> </ul>	State Field		
							selecti de	ar	
						O Bind to a result column	from another table		
							select. de		
							Carana		
Add Removes in the						<ul> <li>Bind to Diameter reque</li> </ul>		_	

- Application Id: Application ID of the Diameter applications.
- · Command Code: Command code of the message.
- Message Type : Request/Answer for which the rule has to be applied.
- Avp Code : AVP code of the Diameter message.
- Vendor Id : AVP vendor ID.
- Avp Action : Provides options for copy/remove/overwrite.



Note

Application ID, Command Code, AVP Code and Vendor Id are used as key, so no duplicate rows could be defined for this combination and the same AVP action. For example, you cannot define both "remove" and "Copy from request" for the same set of Application ID, Command Code, AVP Code and Vendor Id.

Best Match check box needs to be checked if you want to use the wildcard feature.

For more information, see Message Mediation Profile in Custom Reference Data Tables chapter.

### **Peer Group Answer Timeout**

New search table Peer Group Answer Timeout has been added.

Figure 28: Peer Group Answer Timeout - STG

*Name	Display Name	Cache Results			
peer_group_answer_timeout	Peer Group Answer Timeout	Cache Results			
Activation Condition		*Evaluation Order			
	elear Best Match	0			
Columns					
*Name		Display Name		*Use In (	Conditic *Typ
peer_group		Peer Group		<ul> <li>Image: A set of the set of the</li></ul>	Text
app_id		Application Id		<b>V</b>	Text
cmd_code		Command Code		<b></b>	Text
answer_timeout		Timeout Milliseconds		2	Text
Add Remove 😥 🚸					
Valid Values			Validation		
The values allowed in Control Center for	this column		Validation used by Control Center		
() All			Regular Expression		
C List of Valid Values					
*Name	Display Name		Regular Expression Description		

- Application Id: Application Id of the diameter applications.
- Peer Group: Peer group for which the timeout is applied.
- · Command code (to enable different timeouts for different Diameter commands)
- Timeout: Timeout in milliseconds.

For more information, see Peer Group Answer Timeout.

### **Error Result Code Profile**

Error result code profile can be used to map errors to Result-Code value and an error message string for the Error-Message AVP. It also provides support for configurable error result codes.

#### Figure 29: Error Result Code Profile - STG

internal_err Error   rc_In_resp Result Code   exp_rc_in_resp Exp Result Code   exp Result Code Exp Result Code   Exp Result Code Exp Result Code   Finder Subscripter AvP code End to Subscripter AvP code   Internet Regular Expression Description End to Session/Policy State Field   Internet Regular Expression Description End to Session/Policy State Field   Internet Regular Expression Description End to Session/Policy State Field   Internet Regular Expression Description End to Session/Policy State Field   Internet Regular Expression Description End to Session/Policy State Field   Internet Regular Expression Description End to Session/Policy State Field   Internet Regular Expression Description End to Session/Policy State Field   Internet Regular Expression Description End to Dianeter request AVP code	*Name	Display Name							
* Columns     * Name   Bisplay Name   * Name   * Display Name   * Name   * Display Name   * Name   * Display Name   * Name   * Name   * Display Name   * Name   * Name   * Name   * Name   * Name   * Display Name   * Name   <	error_profile	Error Result Code	e Profile	Cache Results					
'solume     'Soluma	Activation Condition			*Evaluation Order					
**Name       Display Name       **Use In Conditik **Type       Key       Required         app_id       Application Id       Image       Text       Image       Image         internal_err       Error       Text       Image       Im		selecti clear Best Match		0					
app_id Application Id Text Image in the image	Columns								
Internal_err recip_ce_fin_resp Result Code Text Code Resp. cc_fin_resp Result Code Text Code Text Code Resp. cc_fin_resp Result Code Text Code Tex	*Name	Display Name		*Use In C	onditic *Type		Key	Required	
rc_in_resp Result Code   exp_rc_in_resp Exp Result Code   exp_rc_in_resp Err Msa   exp response Err Msa   Exp Result Code Exp Result Code   Exp Result Code Exp Result Code   It st of Valid Values Regular Expression Description   Name Display Name Regular Expression Description   It st of Valid Values It st of Valid Code   It st of Valid Values It st of Valid Code   It st of Valid Values It st of Valid Code   It st of Valid Values It st of Valid Values	app_id	Application Id		<b>v</b>	Text		~	1	8
exp_rc_in_resp Exp Result Code   exp_rc_in_resp Exp Result Code   exp_rc_in_resp Exp Result Code   exp_rc_in_resp Exp Result Code   exp_rc_in_resp Fr Mso	internal_err	Error		×	Text		<b>v</b>	2	
exp_vendr_jd vendor Id rext rest rest rest rest rest rest rest res	rc_in_resp	Result Code		1	Text				
err mso Err Mso	exp_rc_in_resp	Exp Result Code		1	Text				
Addi       Termore       Image: Column Details         Valid Values       Validation       Runtime Binding         The values allowed in Control Center for this column       Validation used by Control Center       Which rows match when a message is received         Image: All Column Details       Regular Expression       Image: Bind to Subsorber AVP code         Image: Name       Display Name       Regular Expression Description       Image: Bind to Subsorber AVP code         Image: Name       Display Name       Regular Expression Description       Image: Bind to Subsorber AVP code         Image: Image: Display Name       Image: Expression Description       Image: Bind to Subsorber AVP code         Image: I	exp_vendor_id	Vendor Id		<b>a</b>	Text				
Column Details       Validation       Runtime Binding         Yalidation used by Control Center       Which rows match when a message is received         Image: All       Regular Expression       Image: None         Image: Used of Valid Values       Bind to Subscriber AVP code       Image: Bind to Subscriber AVP code         Image: Name       Display Name       Regular Expression Description       Image: Bind to Subscriber AVP code         Image: Regular expression       Bind to Subscriber AVP code       Image: Bind to Subscriber AVP code         Image: Regular expression       Bind to Subscriber AVP code       Image: Bind to Subscriber AVP code         Image: Regular expression       Bind to Subscriber AVP code       Image: Bind to Subscriber AVP code         Image: Regular expression       Bind to Subscriber AVP code       Image: Bind to Subscriber AVP code         Image: Regular expression       Bind to Subscriber AVP code       Image: Bind to Subscriber AVP code         Image: Regular expression       Bind to Subscriber AVP code       Image: Bind to Diameter request AVP code         Image: Regular expression       Bind to Diameter request AVP code       Image: Bind to Diameter request AVP code	err msg	Err Msa			Text				
Name       Display Name       Regular Expression Description       Index to the session/Policy State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield       Image: State Pield       Image: State Pield         Image: State Pield <t< th=""><th>The values allowed in Control Center</th><th>r for this column</th><th>Validatio</th><th>n used by Control Cent</th><th>er</th><th>Which rows match wh</th><th></th><th>eived</th><th></th></t<>	The values allowed in Control Center	r for this column	Validatio	n used by Control Cent	er	Which rows match wh		eived	
Att Ramow @ @@     Bind to Session/Policy State Field       Image: State Field     Image: Sta	<ul> <li>List of Valid Values</li> </ul>				_	<ul> <li>Bind to Subscriber</li> </ul>	AVP code		
add:       Ramove:       Bind to a result column from another table         add:       Ramove:       Bind to Diameter request AVP code         Valid values pulled from another table's column (key)       Emotion of the pulled from another table's column (key)	*Name	Display Name	Regular	Expression Descript	ion				
Add     Sind to a result column from another table       Index     Sind to Diameter request AVP code       Valid values pulled from another table's column (key)     Sind to Diameter request AVP code						O Bind to Session/Po	licy State Field		
Add:     Remove:     Sind to Diameter request AVP code       Valid values pulled from another table's column (key)     Image: Column (key)							select	clear	
Add Remove of Bind to Diameter request AVP code						Bind to a result col	umn from another t	able	
Valid values pulled from another table's column (key)							select	i clear	
Valid values pulled from another table's column (key)						O Blad to Dismaker a	anuart AUR cade		
Matching Operator						C) bind to Diameter r	equest Ave coole		

Valid values is the place where all the valid error values can be configured in STG so that they are visible in CRD drop-down.

- ApplicationId: Application ID for which the mapping of Result-Code has to be done.
- Error: Internal error list.
- ResultCode: Result Code to be sent in answer.
- ExpResultCode: Experimental result code to be sent in answer. Vendor-Id will be sent in Answer only for Experimental result-Code.
- ErrMsg: Error message AVP sent in answer.



Note

Experiment result code will be sent when Result-Code is not configured. If both Result-Code and experimental Result-Code are present, Result-Code would take precedence.

For more information, see Error Result Code Profile.

### **Gx Session Routing**

Gx Session Routing table is required for "table driven routing". Here an example for Gx New Session Rules is provided. If table driven routing is required for Rx or Sd, user needs to create similar tables for Sd and Rx as well.

#### Figure 30: Gx Session Routing

Name		Display Name		_					
gx_session_routing		Gx Session Routing	9	Cache R	esults				
Activation Condition		_		*Evaluation	n Order				
	select clear	Best Match		0					
*Columns									
*Name	Disp	olay Name		*Use In C	onditic *Type		Key	Required	
logical_apn	Log	ical APN		<b>V</b>	Text			Image: A start and a start	ŀ
origin_host	Orig	gin Host		$\checkmark$	Text				
peer_route	Pee	r Route			Text				
origin_realm	Orig	jin Realm		$\checkmark$	Text			~	
destination_host	Des	tination Host		~	Text		<b>V</b>	×	
destination realm Add Remove 🔐 🐥	Des	tination Realm		2	Text				[
Column Details									
Valid Values The values allowed in Control Ce			Validation	ised by Control	Cartan	Runtime Binding	<b>g</b> h when a message i		
	enter for this colu	imn			Center		n when a message i	s received	
<ul> <li>All</li> </ul>			Regular Ex	cpression		None			
O List of Valid Values						O Bind to Subsc	riber AVP code		
*Name	Display Name		Regular Ex	pression Des	cription				
						Bind to Session	on/Policy State Field		
								select clear	
						Bind to a result	It column from anot	her table	
								select clear	

For more information, see Gx New Session Rules.

### **SLF Trigger Profile**

This table is used to derive SLF destination type and SLF lookup type. Keys used for this table are: Application Id, cmd\_code, and dest\_realm. Output of this table are slf\_lookup\_type and slf\_destination\_type.

An example configuration is given.

#### Figure 31: SLF Trigger Profile - STG

Name	Dis	splay Name							
slf_trigger_profile	S	LF Trigger Profile		Cache Resu	lts				
Activation Condition				*Evaluation O	rder				
	select clear	Best Match		0					
Columns									
*Name	Dis	play Name			Jse In Con	ditic *Type		Key	Required
application_id	Ap	plication ID			Ē	Text		1	<b>Z</b>
cmd_code	Co	mmand Code				Text		1	v
dest_realm	De	stination Realm		-		Text		1	4
slf_lookup_type	SU	F Lookup Type		6	ē	Text			2
slf_destination_type	SU	F Destination Type			i i	Text			<b>v</b>
	r for this column		Validati Validati	ion on used by Contri	d Center		Runtime Binding Which rows match when a me	ssage is received	
	er for this column		Validatio		ol Center				
The values allowed in Control Cente	er for this column Display Name		Validatio Regula	on used by Contro			Which rows match when a me		
The values allowed in Control Cente All     Ust of Valid Values			Validatio Regula	on used by Contro r Expression			Which rows match when a me	le	
The values allowed in Control Cente All     Ust of Valid Values			Validatio Regula	on used by Contro r Expression			Which rows match when a me None Bind to Subscriber AVP con	le	
The values allowed in Control Cente All     Ust of Valid Values			Validatio Regula	on used by Contro r Expression			Which rows match when a me None Bind to Subscriber AVP con	ie Field (select) de	
C List of Valid Values			Validatio Regula	on used by Contro r Expression			Which rows match when a me  None  Bind to Subscriber AVP con  Bind to Session/Policy State  Bind to Session/Policy State	te Field (select) cie m another table	ar
The values allowed in Control Cente  All  Ust of Valid Values  Name			Validatio Regula	on used by Contro r Expression			Which rows match when a me  Which rows match when a me  Bind to Subscriber AVP coll  Bind to Session/Policy Stat  Bind to a result column fro	de re l'ield (select) de manother table	ar
The values allowed in Control Cente All Ust of Valid Values *Name Add Remove () ()	Display Name		Validatio Regula	on used by Contro r Expression			Which rows match when a me  None  Bind to Subscriber AVP con  Bind to Session/Policy State  Bind to Session/Policy State	de re l'ield (select) de manother table	ar
The values allowed in Control Cente  All  Ust of Valid Values  Name	Display Name	zy)	Validatio Regula	on used by Contro r Expression			Which rows match when a me  Which rows match when a me  Bind to Subscriber AVP coll  Bind to Session/Policy Stat  Bind to a result column fro	de re l'ield (select) de manother table	ar

For more information, see SLF Trigger Profile.

## **SLF Routing**

This table is used to derive SLF session route key from SLF Destination. An example configuration is given.

#### Figure 32: SLF Routing - STG

Name		Display Name						
slf_routing		SLF Routing	Cac	he Results				
ctivation Condition	select dear	Best Match	*Evalu	ation Order				
Columns								
*Name		Display Name		*Use In Cor	nditic *Type		Key	Required
slf_destination		SLF Destination		<b>2</b>	Text		<b>V</b>	1
slf_session_route_key		SLF Session Route Key			Text			7
The values allowed in Control C All List of Valid Values	enter for this col	umn	Validation used b Regular Expres			Runtime Binding Which rows match when a m None Bind to Subscriber AVP o		U.
*Name	Display Na	me	Regular Expres	sion Description				
					]	Bind to Session/Policy St	ate Field	
							select de	3.0
						Bind to a result column f	rom another table	
							select de	ar
Add Barrows & D						O Bind to Diameter request	AVP code	
Add Ramova 🙀 🕹						Bind to Diameter request	AVP code	
Add Remove 🔐 💀	ther table's colur					Bind to Diameter request Matching Operator	: AVP code	

For more information, see SLF Routing.

### **S6/Sh Table Driven Rules**

This table is used for the table driven routing of S6/Sh messages. Fields origin\_host, origin\_realm, dest\_realm, dest\_host, msisdn, imsi are used as keys to derive the peer\_route.

An example configuration is given.

Figure 33: S6 Table Driven Rules - STG

*Name		<b>Display Name</b>						
TB_S6		S6_TB_Rules		Cache Results				
Activation Condition				*Evaluation Order				
	select clear	<ul> <li>Best Match</li> </ul>		0				
Columns								
*Name			Display Name		*Use In C	Conditi *Type	Key	Required
origin_host			Origin Host			Text	$\overline{\checkmark}$	~
origin_realm			Origin Realm		$\overline{\checkmark}$	Text	1	~
destination_host			Destination Ho	st	<b>V</b>	Text	1	<b>V</b>
destination_realm			Destination Re	alm	$\overline{\checkmark}$	Text		
imsi			IMSI		<b>V</b>	Text	1	~
neer route			Peer Route			Text		
olumn Details	enter for this col	umn	Validation Validation us	ed by Control Center	Runtime Bin Which rows	<b>ding</b> match when a me	ssage is rece	eived
volumn Details	enter for this col	umn	Validation us		Which rows		ssage is rece	ived
olum Details Valid Values The values allowed in Control Ce All	nter for this col	umn			Which rows	match when a me		lived
olumn Details Valid Values The values allowed in Control Ce			Validation us Regular Exp	ression	Which rows			tived
All		umn visplay Name	Validation us Regular Exp		Which rows	match when a me		eived
Valid Values Valid Values All List of Valid Values			Validation us Regular Exp	ression	Which rows <ul> <li>None</li> <li>Bind to S</li> </ul>	match when a me		ived
olumn Details Valid Values The values allowed in Control Ce			Validation us Regular Exp	ression	Which rows <ul> <li>None</li> <li>Bind to S</li> </ul>	match when a me		
olumn Details Valid Values The values allowed in Control Ce			Validation us Regular Exp	ression	Which rows <ul> <li>None</li> <li>Bind to S</li> <li>Bind to S</li> </ul>	match when a mer ubscriber AVP code	e Field	dear
Valid Values Valid Values All All Clist of Valid Values			Validation us Regular Exp	ression	Which rows  None Bind to S Bind to S	match when a me	e Field select	dear ble
Jumn Details			Validation us Regular Exp	ression	Which rows  None Bind to S Bind to S	match when a mer ubscriber AVP code	e Field	dear ble
Valid Values Valid Values All All Clist of Valid Values			Validation us Regular Exp	ression	Which rows None Bind to 5	match when a mer ubscriber AVP code	e Field select) n another ta	dear ble
olumn Details		visplay Name	Validation us Regular Exp	ression	Which rows None Bind to 5	match when a mes ubscriber AVP code lession/Policy State result column from	e Field select) n another ta	dear ble

For more information, see S6/Sh Table Driven Rules.

## **Custom Reference Data Tables**

### **APN Mapping**

This table provides information related to APN Mapping. The read-only APN Mapping are shown below:

#### Figure 34: APN Mapping - CRD Table

Name	Display Name	_					
apn_mapping	APN Mapping	✓	Cache Res	ults			
ctivation Condition	_	*Ev	aluation (	Order			
	select clear Best Match	0					
Columns							
Name	Display Name		*Use In Co	onditic *Type		Key	Required
called_station_id	Called Station Id		$\checkmark$	Text		$\checkmark$	$\checkmark$
ogical_apn	Logical APN		~	Text			
dd Remove 😚 🐥							
olumn Details							
alid Values		Validation			Runtime Binding		
he values allowed in Control (	Center for this column	Validation used by	Control Ce	enter	Which rows match whe	en a message is r	eceived
<ul> <li>All</li> </ul>		Regular Express	ion		None		
List of Valid Values					O Bind to Subscriber	AVP code	
*Name	Display Name	Regular Express	ion Descri	ption			
					Bind to Session/Pol	icy State Field	
						sel	ect clear
					Bind to a result col	umn from anothe	r table
						sel	ect clear

- Called-Station-Id: This is the AVP from which APN is derived. This also is the key column for this table. It is bound to the session or Policy State field as shown in the snapshot.
- Logical\_APN: This is the mapped logical name that is used for referencing and processing the message within the system.

Note

For sample data configuration, refer the CPS Control Center Interface Guide for Full Privilege Administrators for this release.

### **Peer Access Control List**

You can use the Peer Access Control List to specify the list of peers (by realm, FQDN, and applications) that can establish peer connections to vDRA so that unknown peers are not permitted to create Diameter peer connections.

#### Figure 35: Peer Access Control List

Name	Display Name						
peer_access_control_list	Peer Access Control List	t	Cache Results				
Activation Condition		*Evaluation Order					
	enletti cipar		0				
Columns							
*Name	Display Name		*Use In C	onditic *Type		Key	Required
origin_host	Origin Host		Q.	Text		1	1
origin_realm	Origin Realm		8	Text		1	1
auth_action	Authorization Action		V.	Number			1
error_code	Authorization Action Deny - Re	esult Code	1	Number			
error_msg	Authorization Action Deny - Er	rror Message	2	Text			
annlication id	Application Id		1	Text		100	9
Add Hemove &							
Column Details							
Valid Values	Va	alidation			Runtime Binding		
The values allowed in Control Cent	er for this column Va	alidation use	d by Control	Center	Which rows match	when a message is	s received
<ul> <li>All</li> </ul>	R	egular Expr	ession		None		
C List of Valid Values	[				Bind to Subscriber AVP code		
*Name	Display Name	egular Expr	ession Des	cription			
					O Bind to Session	/Policy State Field	
							electi clear

### **Peer Routes**

This tables provides the information related to Peer Routes available in the system. The read-only peer routes are shown below:

#### Figure 36: Peer Routes - CRD Table

*Name	Display Name		Activation Co	ondition			
peer_route	Peer Routes	Cashe Results			selected dear		
Columns							
*Name	Display Name		*Use In Co	nditi *Type		Key	Required
peer_route	Peer Route		2	Text		~	[✓]
Add Remove 6 6	8						
Valid Values		Validation			Runtime Binding		
The values allowed in	Control Center for this column	Validation use	d by Control C	Center	Which rows match wh	nen a message is	received
() All		Regular Expr	ession		None		
*Name	Display Name	Regular Expr	ession Descri	ption			
					O Bind to Session/P		
						-00	lette clear

### **Peer Group SRK Mapping**

This table provides the information related to Peer Groups in the system. The read-only peer groups are shown below:

#### Figure 37: Peer Group - CRD Table

Name	Display Name		Activation Con	dition			
peer_group_srk_mapping	Peer Group SRK Mapping	Cache Results			select clear		
Columns							
*Name	Display Name		*Use In C	Conditic *Type		Key	Require
peer_group	Peer Group		<b>v</b>	Text			~
session_routing_key	Session Routing	Key	1	Text			
dest_host_routing_rule	Destination Host	Routing Rule	1. Contraction (1. Contraction	Text			1
dest_host_replace_rule	Destination Host	Replace	1	Text			
dest_realm_replace_rule	Destination Real	n Replace	~	Text			
The values allowed in Control	Center for this column	Validation used	by Control Cente	r	Which rows match when	a message is receive	be
		Regular Expre	ssion		<ul> <li>None</li> <li>Bind to Subscriber A</li> </ul>	VP code	
	Display Name		ssion ssion Descriptio	an		VP code	
All     Ust of Valid Values     Name	Display Name			on			
Ust of Valid Values	Display Name			on .	Bind to Subscriber A		lear
Ulst of Valid Values	Display Name			2n	Bind to Subscriber A	y State Field	
Ulst of Valid Values	Display Name			2m	Bind to Subscriber A	y State Field	
Ulst of Valid Values	Display Name				Bind to Subscriber A	y State Field select) c no from another table select) c	
Ust of Valid Values				20	Bind to Subscriber A Bind to Session/Polic Bind to Session/Polic Bind to a result colur	y State Field select) c no from another table select) c	

- Peer Group: Name of the peer group.
- Session Routing Key: Routing token for this Peer Group.
- Destination Host Routing Rule: Defines Routing behavior of this group.

### **Peer Routing**

This table provides the information related to peer routing in the system. The read-only peer routings are shown below:

Figure 38: Peer Routing - CRD Table

peer_routing Columns "Name peer_route system_id	Peer Routing Display Name	🖉 Godia Results					
peer_route							
peer_route							
			*Use In O	Conditi *Type		Key	Required
system_id	Peer Route		1	Text		<b>V</b>	$\checkmark$
	System Id		1	Text		$\sim$	1
peer_group	Peer Group		~	Text		1	1
precedence	Precedence		2	Number			1
weight	Weight		1	Number			$\overline{\checkmark}$
Column Details Valid Values		Validation			Runtime Binding		
The values allowed in Control Co	enter for this column	Validation use		Center	Which rows match whe	n a message is	received
		Regular Expre	ession		None		
*Name	Display Name	Regular Expre	ession Desc	ription			

• Peer Route: Identifier of this Peer Route.

- System ID: System Identifier for this VM.
- Peer Group: Identifier of the Peer group on this peer Route.
- Precedence: of the peer group on this Peer Route.
- Weight: Weight of the peer group on this Peer Route.

### **PCRF Session Query Peers**

Use this CRD to configure the REST API parameters for Rx AAR fallback routing.

Policy DRA supports a fallback routing for Rx AARs for VoLTE using the PCRF session query.

For an Rx AAR with an IPv6 binding query, vDRA provides the ability to route the Rx AAR based on an API query to the PCRF to determine if it has a session for the IPv6. The queries can be made in parallel to a configured set of query points on PCRFs.

V

Note Ensure you have enabled PCRF Session Query in the DRA plugin configuration to use this feature.

#### Figure 39: PCRF Session Query Peers CRD

*Name	Display Name	-	Activation Condi	ition	
pcrf_session_query_peers	pcrf_session_query_peers	Cache Results		selec	t <u>dear</u>
Svn Crd Data					
Columns					
*Name	Display Name	*Use In	Conditi *Type		Ke
base_url	BASE_URL	<i></i>	Text		9
pcrf_group	PCRF GROUP	<i>w</i>	Text		
session_query_parameter	SESSION QUERY PARAME	TER 🗸	Text		
user_id	USER ID	1	Text		
password	PASSWORD	v.	Text		
timenut ms	TIMEOUT MS	3	Number		125
Add Remove 😚 😣					
Column Details					
Valid Values		Validation		Runtime Binding	
The values allowed in Control	Center for this column	Validation used by C	ontrol Center	Which rows match	when a
		Regular Expression		( None	
E List of Valid Values					
"Name	Display Name	Regular Expression	Description		
framedIpv6PrefixKev	framedIpv6PrefixKev				

This CRD contains the following fields:

- base\_url: The HTTP URL for the PCRF REST API, supports both HTTP and HTTPS. This does not contain the Rest API endpoint name.
- pcrf\_group: The PCRFs can be configured in logical groups by defining the common pcrf\_group. vDRA triggers the REST API request one after another for multiple PCRFs configured with same group name. This is to support PCRF with primary and secondary API endpoints. (Optional)
- session\_query\_parameter: PCRF session query parameter. Currently, only one value is supported: framedIpv6PrefixKey
- user\_id: User ID for REST API request if PCRF requires any basic authentication. (Optional)
- password: Password for REST API request if PCRF requires any basic authentication. (Optional)

• timeout\_ms: REST API equest timeout value. Default: 250ms. (Optional)

You can also configure a session route key for the PCRF response. When vDRA makes REST API requests to multiple PCRFs for session query using the Framed-IPv6-Prefix received in the Rx AAR message, the PCRF that has the corresponding Gx session sends a session route key in the response. vDRA then uses this key to look up the peer group and route the Rx AAR message to the correct PCRF. To configure a session route key in the response, see the Unified API Plugin Configuration in *CPS Mobile Configuration Guide*.

Additionally, diameter load balancing ensures that when a PCRF is connected to two directors and the PCEF traffic passes on one director, the traffic is then equally distributed to both directors.

vDRA can also load balance session query REST requests across multiple PCRF API endpoints. Previously, all REST queries were sent to the primary endpoint and only if the primary query fails, then the request is sent to secondary. Now, the requests are load balanced across the different PCRF endpoints within a peer group. If the session query results indicate that the PCRF does not have the corresponding Gx session for the IPv6 prefix, then vDRA does not send the query to the other PCRF configured in the same group. Similarly, for all other failures, vDRA sends the session query request to a different PCRF REST API in the same group. It is recommended that a group may contain a maximum of four PCRF REST API endpoints. If there is no group name, the PCRF API endpoint is considered as a standalone PCRF.

### IPv6 Ranges System ID Mapping

Use this CRD to specify a range of IPv6 addresses and the relay vDRA system ID.

This CRD is used to relay Rx AAR messages to other vDRA clusters based on the IPv6 range defined in the CRD.

When an Rx-AAR reaches vDRA, the AAR is checked for an IPv6 prefix. If there is an IPv6 prefix, then this CRD is checked for IPv6 ranges and to find the related primary and secondary vDRA system ID.

If the primary or secondary system is the current vDRA system-ID, then AAR message is processed locally. If the primary/secondary system ID is not the current vDRA, then current vDRA checks the relay links between current system and primary system. If the relay link is up, the the AAR is relayed to the primary system; else vDRA checks link to the secondary system.

Figure 40: IPv6 Ranges System ID Mapping CRD

*Name	Display Name		Activation Condition				
ipv6_range_sys_id_map	IPV6 Ranges System ID Mapping	Cache Results		5	ielect clear		
Svn Crd Data							
Columns							
*Name	Display Name		*Use In	Conditic *Type		Key	Require
ipv6_start_range	IPV6 Start Range		9	Text			1
ipv6_end_range	IPV6 End Range		9	Text		1	2
primary_system_id	Primary System Id	1	1	Text			2
secondary_system_id	Secondary System	n ID	1.5	Text			

Table 20: IPv6 Ranges System ID Mapping Fields

Fields	Description
IPV6 Start Range	Starting IP of IPv6 range in long format.
IPV6 End Range	Ending IP of IPv6 range in long format.

Fields	Description
Primary system ID	Mandatory field. Indicates the System ID of vDRA in a vDRA cluster to which the request can be relayed.
Secondary system ID	Secondary vDRA to which the request can be relayed if the primary is not present.

Note

The ranges are expected to be mutually exclusive and unique. Verify the values when provisioning the same.

### **Binding Key Profile**

This table provides the information related to binding key profile in the system. The read-only keys are shown below:

#### Figure 41: Binding Key Profile - CRD Table

binding_key_profile			ectivation Cond				
	Binding Key Profile	Cache Results			select dear		
olumns							
Name	Display Name		*Use In Co	onditic *Type		Key	Required
rofile_name	Profile Name		· ·	Text		×	×
msi_apn	IMSI APN Key Enab	led	2	True/False			
nsisdn_apn	MSISON APN Key E	nabled	4	True/False			
ramed_ipv6_prefix	Framed IPv6 Enable	b	~	True/False			
ramed_ipv4	Framed IPv4 Enable	ed.	×.	True/False			
dd Remove 👉 😽							
alid Values		Validation			Runtime Binding		
The values allowed in Control Cer	nter for this column	Validation used b	v Control Center		Which rows match when a m	essage is received	
All		Regular Expres			None		
		regular express		1			
Uist of Valid Values					O Bind to Subscriber AVP o	ode	
*Name	Display Name	Regular Expres	sion Description	0			
					O Bind to Session/Policy St	ate Field	
						select clear	
					Bind to a result column f	rom another table	
						select clear	
Add Remove 👔 🕹					O Bind to Diameter request	AVP code	
Valid values pulled from anot					Matching Operator		
	select dear				18		

- Profile Name: This is the name given to the Bind profile that is associated with keys that are either enabled and/or disabled.
- MSI APN Key Enabled: Enabling this field would mean that bindings will be stored in IMSI APN collections in bindings database.
- MSISDN APN Key Enabled: Enabling this field would mean that bindings will be stored in MSISDN APN collections in bindings database.
- Framed IPv6 Enabled: Enabling this would mean binding data would be stored in "ipv6bindings" collection.
- Framed IPv4 Enabled: Enabling this would mean binding data getting stored in "ipv4bindings" collection.

Refer to Binding Key Profile for configuration in Control Center.

### **Appld Key Profile Mapping**

This table stores the mapping between Application Identifiers and Bind Key Profile Names. The Application Identifiers are pre-provisioned for two Application Identifiers as Gx and Rx. Similarly, the BindingKeyProfile is also tied to the Profile Name column of the "BindingKeyType\_Profile" table:

Figure 42: Appld Key Profile Mapping- CRD Table

Columns "Name application_id profile_name wide Democra of the other blumn Details Valid Values The values allowed in Control Center for t	Id Key Profile Mapping Display Name Application Id Profile Name his column	Validation Validation	<u>5</u>	onditi: *Type Text Text	Runtime Binding	Key V	Required
Columns  *Name application_id profile_name  Add: Removes for the column Details  Valid Values  The values allowed in Control Center for t  All List of Valid Values	Application Id Profile Name		<u>5</u>	Text	Runtime Binding		
application_id profile_name Add: Remove @	Application Id Profile Name		<u>5</u>	Text	Runtime Binding		
profile_name Add() Remove () () () () () () () () () () () () () () (	Profile Name		2	Text	Runtime Binding		V
Add Samoon Samoo					Runtime Binding		
olumn Details Valid Values The values allowed in Control Center for t	his column		by Control Cente		Runtime Binding		
The values allowed in Control Center for t	his column		by Control Cente		Runtime Binding		
III (	his column	Validation used	by Control Cente				
				t	Which rows match when a	a message is received	
C List of Valid Values		Regular Expre	ssion	22	None		
					Bind to Subscriber AVI	P code	
*Name Disp	play Name	Regular Expre	ssion Descriptio	n			1
					Bind to Session/Policy	State Field	
						select clear	
					Bind to a result column		
						select dear	
Add Remove 😚 🚯					Bind to Diameter requ	lest AVP code	
O Valid values pulled from another table	's column (key)						
selec					Matching Operator		
					100		

### **Message Rate Limit Profile**

This table gives a provision to configure Message Rate Limits at a profile level.

#### Figure 43: Message Rate Limit Profile - CRD Table

Name	Display Name		Activa	tion Condition			
message_rate_limit_profile	Message Rate Limit Profile	Cache Results			select clear		
Columns							
*Name	Display Name		*Use In C	onditic *Type		Key	Required
profile_name	Rate Limit Profile Name		<b>V</b>	Text			$\checkmark$
app_id	Application Identifier		<b>V</b>	Number			~
command_code	Command Code		~	Number			$\checkmark$
mesg_type	Message/Request Type		~	Number		~	$\checkmark$
rate_limit	Message Rate Limit		~	Number			$\checkmark$
Add) Remove 🔐 😺	center for this column	Validation Validation used by	<sup>7</sup> Control C	enter	Runtime Binding	when a message is r	eceived
Valid Values The values allowed in Control C	ienter for this column	Validation used by		enter	Which rows match	when a message is n	eceived
Valid Values The values allowed in Control C	ienter for this column			enter	Which rows match	-	eceived
valid Values The values allowed in Control C	center for this column	Validation used by	ion		Which rows match	-	eceived
Julum Details <b>Jalid Values</b> The values allowed in Control C All List of Valid Values		Validation used by Regular Express	ion		Which rows match	ber AVP code	eceived
Jumn Details /alid Values The values allowed in Control C All List of Valid Values		Validation used by Regular Express	ion		Which rows match  None Bind to Subscri	ber AVP code	
Jumn Details /alid Values The values allowed in Control C All List of Valid Values		Validation used by Regular Express	ion		Which rows match None Bind to Subscri Bind to Susscri Bind to Session	ber AVP code /Policy State Field	ect clear
Valid Values Valid Values All All List of Valid Values		Validation used by Regular Express	ion		Which rows match None Bind to Subscri Bind to Susscri Bind to Session	Policy State Field	ect) <u>clear</u> r table

- Profile Name: Unique Identifier for a profile.
- Application ID: Application Identifier for this row. 3GPP App Ids only are allowed here.
- Command Code: Command Code of the message that is applicable on the said interface specified by Application Id above.
- Message Type: Initial/Update/Terminate or None for messages that do not have them. The message request type should be same as specified for the command code in Policy Builder under Diameter Application.
- Rate Limit: This field is to specify the threshold in TPS above which the diameter messages are discarded. This value should be more than the Peer Rate Limit in order for message level rate limit to be applied.
- Profile Name: Unique Identifier for a profile.

Refer to Message Rate Limit Profile for configuration in Control Center.

### **Reserved IMSI**

You can configure the Reserved IMSI CRD table to validate a parsed IMSI for SLF routing against a configured list of reserved MCC ranges.

The CRD has two main columns : MCC Start range and MCC End Range. The MCC consists of the first three digits of an IMSI.

If the IMSI matches a reserved IMSI, the value is ignored for SLF routing.

You can provide support up to ten distinct (non-overlapping) MCC ranges as Reserved IMSIs.

The DRA/SLF ignores AVPs that contain such IMSIs, and continues searching other AVPs in the Diameter request, for a valid address to be used for address resolution.

The following image shows a sample Reserved IMSI configuration:

#### Figure 44: Reserved IMSI

*Name	Display Name		Activition	Condition	
reserved_mcc	Reserved MCC	Cache Results			anness char
*Columns					
*Neme	Display Name		*Use In Cond	tic *Type	
mcc_start	MCC Start		1	Number	
mcc_end	MCC End		2	Number	
Column Details	8				
Valid Values		Validation			Runtime Binding
The values allowed in Ci	ontrol Center for this column	Validation used by	Control Centrol	11 <sup>4</sup>	Which rows match
8.41		Regular Express	lon		· North
					O Bind to Subscrit
C Dat of Valid Values					
O bit of valid Values	Display Name	Regular Express	ion Descripti	on	

### **Trusted Realm Profile**

Trusted Realm Profile is used for topology hiding. The CRD includes the following columns:

- Trusted Profile Name: Profile Name having a trusted realm mapped to it.
- Trusted Realm: Realm for which Topology Hiding is not required.

#### Figure 45: Trusted Realm Profile

Name	Display Name				
trusted_realm_profile	Trusted Realm Profile	Cadre Rei			
ctivation Condition	Svn Crd Data	P Best Matz			
Evaluation Order	aninti dear				
0					
Columns					
		and the second second	onditic *Type	Key	Required
Name	Display Name	"Use In C			
	Display Name Trusted Profile Name	-Ose in C	Text	2	1
*Name profile_name trusted_realm				2 2	3.5

### **Protected Realm Trusted Profile Mapping**

Protected Realm Trusted Profile Mapping is used for topology hiding. The CRD includes the following columns:

- Protected Realm: Realm that is protected (topology hiding is required).
- Profile Name: Profile having realms that are trusted for this protected realm and that do not require topology hiding.

#### Figure 46: Protected Realm Trusted Profile Mapping

Name	Display Name				
protected_realm_trusted_profile	Protected Realm Trusted Profile #				
ctivation Condition	The Ort Date	2 Inst Parch			
Evaluation Order					
0					
Columna					
0 Columns	Display Name	*Use In Care	DOX *Type	Key	Required
0 Columna Name	Display Name Protected Realm	120000	DDX *Type Text	Key	2
0					Required

### **MME Alias Map**

MME Alias Map is used for topology hiding. The CRD includes the following columns:

- MME FQDN: FQDN of MME that requires topology hiding.
- Alias1: Mandatory. An alias identity used for the protected host that belongs to an MME in the network.
- Alias 2: Optional. Alternate Alias that can be used for Topology Hiding for the given MME FQDN.
- Alias 3: Optional. Alternate Alias that can be used for Topology Hiding for the given MME FQDN.

#### Figure 47: MME Alias Map

Name	Display Name		Activati	ion Condition			
mme_allas_map	MME Allas Map	Cadre Results	1		mainith Cent		
The Crd Deca							
Columns							
			Alter In the	inditic *Type		Key	Required
*Name	Display Name		-Use in Co	motor - type		No.4	
	MME FQON		-Use In Co	Text		3	1
*Name mme_host allas1	12.22 - 24.22		4				
mme_host	MME FQON			Text			9

Add Harmon 44

### **HSS Aliases**

HSS Aliases is used for topology hiding. The CRD includes the following columns:

- HSS Alias FQDN: Alias FQDN used to replace a protected HSS FQDN.
- Shared Alias: Boolean variable used to indicate whether the Alias FQDN is shared across multiple HSS servers or not.

#### Figure 48: HSS Aliases

hss_aliases HSS Aliases	Cache Results			chiar	
Sive Ord Data					
Columns					
*Name Display Name		Use In Co	onditik *Type	Key	Required
hss_alias HSS Alias FQDN		2	Text	10 C	1
is_shared_allas Shared Allas		2	True/False		2

#### Add Harmon Q .

### **HSS Alias Map**

HSS Alias Map is used for topology hiding. The CRD includes the following columns:

- HSS FQDN: FQDN of HSS peer.
- Alias1: Required field which is derived from HSS Alias CRD.
- Alias2: Optional. Alias for the HSS FQDN.
- Alias3: Optional. Alias for the HSS FQDN.

#### Figure 49: HSS Alias Map

Name	Display Name		Activet	ion Condition			
hss_alias_map	HSS Allas Map	Ceche Results			animh) cear		
Svn Crd Owta							
Columns							
*Name	Display Name		*Use In Co	ondibic *Type		Key	Required
hss_host	HSS FQON		9	Text		1	8
alias1	Alias1		9	Text			2
alias1 alias2	Alias2		9	Text			
allas3	Alias3		(a) -	Text			

### **Binding Key Profile Creation Map**

This table provides the information related to binding key type profile creation map in the system. The read-only keys are shown below:

#### Figure 50: Binding Key Profile Creation Map - CRD Table

Name		Display Name	-			
bind_key_profile_creation_map	]	Binding Key Profile Creation Map	Cache Results			
Activation Condition	select clear	Svn Crd Data	Best Match			
*Evaluation Order						
0	]					
Columns						
*Name	Disp	olay Name	*Use In Condition	*Туре	Key	Required
appl_id	App	lication Identifier	<b>V</b>	Text	$\checkmark$	
a h h		ed Station Id		Text	~	
called_station_id	Call					1



**Note** If there is no profile configured for any Application ID and Called Station ID pair, then a default profile is automatically selected. This profile has only Framed-IPv4-Enabled as false/disabled, while all other keys are true/enabled.

- Application Identifier: Application ID of the message.
- Called Station Id: Called-Station-Id AVP value from the Diameter message.
- Binding Key Profile: Profile name from binding key profile.

Refer to Binding Key Profile Creation Map for configuration in CPS Central.

### **Binding Key Profile Read Map**

This table provides the information related to binding key type profile read map in the system. The read-only keys are shown below:

Figure 51: Binding Key Profile Read Map - CRD Table

*Name	Display Name				
bind_key_profile_read_map	Binding Key Profile Read Map	Cache Res	ults		
Activation Condition	electi clear	🛃 Best Match			
*Evaluation Order					
0					
0 *Columns					
Columns	Display Name	*Use In Co	onditic *Type	Key	Required
Columns	Display Name Application Identifier	*Use In Co	onditic *Type Text	Key	Required
Columns *Name					
Columns *Name appl_id	Application Identifier	Image: A start of the start	Text		$\sim$

• Application ID: Application ID from the message.

- Origin Host: Origin host from the message.
- Origin Realm: Origin realm from the message.
- Binding Key Profile: Profile name from binding key profile.

Refer to Binding Key Profile Read Map for configuration in CPS Central.

### **Best Effort Binding**

This table enables you to configure best effort binding on APN basis. The Caller Station Id column accepts regular expressions.

Figure 52: Best Effort Binding - CRD Table

				F	Filter CRD Tab	oles 🛞
		Framed	Framed	IMSI APN	MSISDN	
2 Called	Session	IPv6	IPv4	Key	APN Key	
Station Id *	Enabled	Enabled	Enabled	Enabled	Enabled	Actions
ms.com	true	true	true	true	true	e 🗎

### **Peer Admin Disabled List**

Peer Admin Disabled List table is used by PAS to dynamically add/remove peer FQDN to administratively disable/enable peers. To administratively disable a peer, its FQDN should be added to "Peer Admin Disabled List" table. To enable the peer, FQDN should be removed from the table. This table could also be updated by external systems using CRD API. The configuration changes take effect once CRD table is updated.

CRD table only supports exact matches (equality) of origin FQDN and realms. Pattern based rules are not supported. Since each peer is required to use unique origin-host FQDN, CRD table is designed to just include FQDN to identify a peer.

The CRD is used to persist the configuration. So, the configuration is limited to a site (scope of CRD). To block a peer from connecting to multiple sites, the peer must be disabled on each site.



Note

Peer Admin Disabled List is applied only for inbound diameter connections. Outbound diameter connections from PAS could be disabled by disabling the corresponding outbound endpoint.

When restoring CRD from backup, Peer Admin Disabled List should be excluded from import so that current configurations are not lost. The table should be included only if the intent is to reset the configuration.

When you add an entry for active peer in **Peer Admin Disabled List** CRD table, it takes effect only after the peer is disconnected and the peer attempts to reconnect. You can use **Active Peer Endpoints** GUI under **DRA Peer Monitoring** to disconnect the peer connection. For more information, refer to *View Filtered Data* section in the *CPS vDRA Administration Guide*.

If you need active peer connections to be administratively disabled, it is recommended to disable the peers using the **DRA Peer Monitoring** GUI only. For more information, refer to *CPS vDRA Administration Guide*.

		Filter CRD Tab	les 🙁
& Origin Host *	د Origin Realm *	Admin Disable Time	Actions
x8-tcpdra	gx8-tcpdra.cisco.com	Fri Jan 15 05:00:36 UTC 2021	e 🗊
dpcrf-tcpsite	sdpcrf-tcpsite.cisco.com	Fri Jan 15 05:00:36 UTC 2021	e 🗊
x10-tcpdra	gx10-tcpdra.cisco.com	Fri Jan 15 05:00:36 UTC 2021	e 🗊
×13-tcpdra	gx13-tcpdra.cisco.com	Fri Jan 15 05:00:36 UTC 2021	e 🗊
×11-tcpdra	gx11-tcpdra.cisco.com	Fri Jan 15 05:00:36 UTC 2021	e 🗊
×7-tcpdra	gx7-tcpdra.cisco.com	Fri Jan 15 05:00:36 UTC 2021	e 🗊
×14-tcpdra	gx14-tcpdra.cisco.com	Fri Jan 15 05:00:36 UTC 2021	e 🗊
×4-tcpdra	gx4-tcpdra.cisco.com	Fri Jan 15 05:00:36 UTC 2021	e 🗈
×5-tcpdra	gx5-tcpdra.cisco.com	Fri Jan 15 05:00:36 UTC 2021	e 🗊
x15-tcpdra	gx15-tcpdra.cisco.com	Fri Jan 15 05:00:36 UTC 2021	e 🗎

#### Figure 53: Peer Admin Disabled List

The CRD table contains the following fields:

- Origin Host: Origin FQDN of peer to be administratively disabled.
- Origin Realm: Origin realm of the peer.

- Admin Disable Time: Time at which disable rule was created. This is read-only field.
- Actions: Edit or delete the current configuration.

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

- Disable APIs:
  - API to create multiple rows in CRD: /custrefdata/peer\_admin\_disabled\_list/\_createRows
  - API to disconnect multiple endpoints: /dra/api/localActivePeerEndpoints/disconnect
- Enable API:
  - API to delete multiple rows in CRD: /custrefdata/peer\_admin\_disabled\_list/\_deleteRows

For more information on APIs, refer to API Endpoints And Examples section in the CPS vDRA Operations Guide.



```
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.

# **SVN Repository Changes**

Note

This feature has not been validated for all customer deployment scenarios. Please contact your Sales Account team for support.

## Viewing Summary of SVN Repository Changes in the Policy Builder

The CPS DRA provides GUI support to view history of Policy Builder configuration changes. .

Perform the following steps to view the summary of publish changes:

1. In CPS DRA, choose Policy Builder > Policy Builder > SVN repository changes, click the History of configuration changes link to open the History of configuration changes window.

#### Figure 54: SVN Repository Changes

cisco CPS DRA	Hostname: policy-builder-s1 System: system-1
A Policy Builder   Reference Da	ta - ♀ Repository: export_admin ≓   Publish ⊙

# **DRA Policy Builder Overview**

## Reference Data

Data referenced from services or used for system wide configuration

🖂 Environment specific data

- Systems for initial setup of environment.
- I Custom Reference Data Schemas
  - Search Table Groups allow setting custom reference data for installation
  - · Custom Reference Data Tables are basic tables without search functionality
- .II Diameter Application specific data
  - Diameter Applications
- Routing AVP
  - Routing AVP Definitions
- SVN repository changes
  - · History of configuration changes
- 2. From the **Choose repository to view history** drop-down list box, choose a repository, and then click **Submit**. The following parameters are displayed for all the published commit changes published.

Table 21: History of Configuration Changes Parameters	Table 21: Histor	v of Configuration	Changes Parameters
---	------------------	--------------------	--------------------

Field	Description
Revision	Revision number of the SVN commit.
Date and Time	Shows the date and time of the last changes made.
User	Name of the user who made changes.
Commit Message	Commit message entered by user into GUI while publishing summary of changes.
Files Impacted	Shows impacted files during SVN commit changes.
Changes	Click the icon to view differences between two adjacent revisions. To download and save changes, click the Download icon at the top-right corner of the window.



Note

DRA Central GUI retrieves the SVN log and SVN differences by using an underlying SVN containers. If SVN container is down then GUI will have issues.