Managing DRA Operations

Operations Overview

The Operation page enables you to access various interfaces and perform operations, maintenance, and troubleshooting activities. It assists system administrators and network engineers to operate and monitor the Policy Server.

Monitoring DRA

DRA monitoring page under operations includes the following options:

- DRA Peer Monitoring
- DRA Binding Monitoring
- DRA SLF Bindings
- DRA Relay Connection
- Grafana

DRA Peer Monitoring

DRA peer monitoring page displays the active peer endpoints (by default) for the cluster node. You can click the toggle for active/inactive peers to view the active or inactive peer endpoints.

The active and inactive peer monitoring screens have resize option for each column. You can use the scrollbar to view multiple values.

When the page is loaded, the Autorefresh checkbox is enabled by default which refreshes peers data every 30 seconds. You can stop this functionality by disabling the checkbox. After every refresh, the Data Last Refreshed field is updated with the locale time.

You can use the filter option to filter active and inactive peer endpoints. You can also view all event logs and peer details for specific active or inactive peer endpoints of the cluster node.

Pagination support is provided in active and inactive peer endpoints table data. A number of rows per page drop-down are displayed below each table which contains the different set of numbers indicating the number of rows which can be shown per page. This option enables you to perform the following tasks:

- Select the number of rows to be displayed in each page.
- Specify the page to which you want to navigate.

Through Pagination toolkit, you can view records count displayed in the webpage link out of total number of records fetched by API. This value changes as per the change in filtering of records through filter toolbar.

You can use the **Close All** option to close all the displayed popups. By default the **Close All** option is disabled. If you have many popups open, the **Close All** option gets enabled.

View Filtered Data

Step 1 In CPS DRA, navigate to **DRA Peer Monitoring**.

Step 2 Select the **Filter by** drop-down and click on any one of the following data options displayed:

- Peer Host Name
- Peer IP Address
- Admin State
- DRA Host Name
- DRA IP Address
- Application Id
- Peer Group
- Details/Event Logs
- Actions

In the **Search** field, enter a search value and click either the Search icon or press Enter to view details. Based on inputs the vDRA searches the entry and displays the output. You can also use Regex/Wildcard filter criteria to view peer endpoint details. For example, if the input value is "ndc2c*" then the search results displayed are ndc2c.gx.xom,ndc2c.gxx.com and so on.

Step 3 Enter a value in the **Filter Peer Endpoints** option.

Step 4 Click **Toggle for Active Peers** to view filtered active peer endpoints or **Toggle for Inactive Peers** to view filtered inactive peer endpoints.

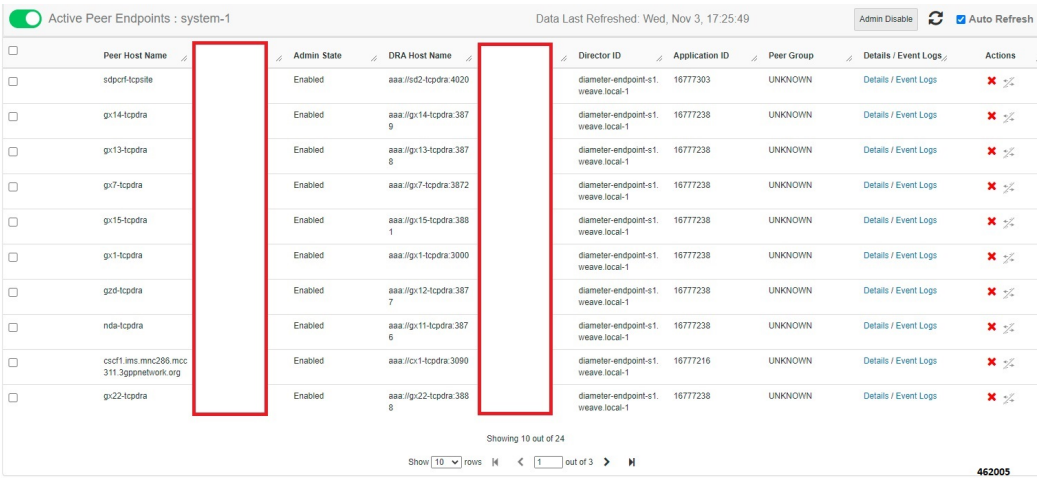
Under Active Peer Endpoints:

- You can administratively disable or disconnect selected peers.

- You can multi-select peer connections and administratively disable them. You will be prompted for confirmation before executing the action.

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

Figure 1: Active Peer Endpoints



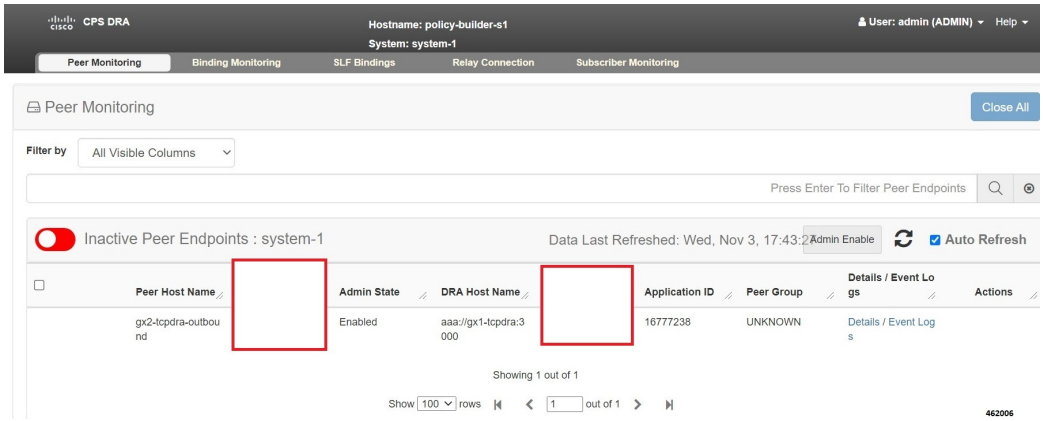
Under Inactive Peer Endpoints:

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

  Note You can administratively disable maximum 20 peer connections in a single operation using multi-selection. If more than 20 peer connections are selected, an error is prompted with an option to proceed with disabling the first 20 of selected connections.

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

Figure 2: Inactive Peer Endpoints



The following tables describe the details displayed under Peer Endpoints section:

Table 1: Active Peer Endpoint Details

Parameter	Description
Peer Host Name	Peer host name.
Peer IP Address	Peer IP address
Admin State	Indicate the admin state of the peer. You can filter the inactive peers by admin state.
DRA Host Name	DRA host name and port.
DRA IP Address	DRA IP address
Application Id	Identifier of the Diameter application (Gx, Rx, Sy, Sh and so on).
Peer Group	Peer group of the connected peer.
Details/Event Logs	When selected provides Details and Event Logs links. To view details of a particular peer, click **Details**. To view event logs of a particular peer, click **Event Logs**.
Actions	Options are Disconnect and Disable. Disconnect: Disconnects an active peer by confirming from the user and sends the request to the API for disconnecting the active peer. Disable: Disables admin active peer by confirming from the user and sends the request to the API for disabling the active peer.

Table 2: Inactive Peer Endpoint Details

Parameter	Description
Peer Host Name	Peer host name.
Peer IP Address	Peer IP address
Admin State	Indicate the admin state of the peer. You can filter the inactive peers by admin state.
DRA Host Name	DRA host name and port.
DRA IP Address	DRA IP address
Application Id	Identifier of the Diameter application (Gx, Rx, Sy, Sh and so on).
Peer Group	Peer group of the connected peer.
Details/Event Logs	When selected provides Details and Event Logs links. To view details of a particular peer, click **Details**. To view event logs of a particular peer, click **Event Logs**.
Actions	Used to enable the peer which was disabled by admin earlier.

You can use the refresh option provided next to the toggle for active/inactive peer endpoints to refresh the table data.

You can enable the **Auto-refresh** checkbox to refresh data every 30 seconds. The **Data Last Refreshed** field displays time when data is fetched from server.

View Details

Step 1 In CPS DRA, navigate to **DRA Peer Monitoring**.

Step 2 Click **Toggle for Active Peers** to view active peer endpoints or **Toggle for Inactive Peers** to view inactive peer endpoints.

Step 3 To view details of a particular peer, click **Details**.

Figure 3: Peer Endpoint Details

Peering Information for Peer Key: gx24-tcpdra@gx24-tcpdra:3891@16777238@1

Data Last Refreshed: Fri, Jan 15, 10:36:25

Name	Value
Key	gx24-tcpdra@gx24-tcpdra:3891@16777238@1
Realm	gx24-tcpdra.cisco.com
Host	gx24-tcpdra
Application Ids	16777238
Peer Group	UNKNOWN
Peer Weight	100
Session Routing Key	
Direction	Inbound
Transport Protocol	TCP
Peer Status	UP
Last Connect Time	Fri Jan 15 03:26:29 UTC 2021
Own Host	aaa://gx24-tcpdra:3891
Own IP Addresses	
Own Port	3891
Peer Uri	aaa://gx24-tcpdra:55851
Remote IP Addresses	
Remote Port	55851
Instance Id	diameter-endpoint-s1.weave.local-1
Peer Message Class	0
Admin State	Enabled

The following details are displayed:

Table 3: Peer Endpoint Details

Parameter	Description
Application ID	Identifier of the Diameter application (Gx, Rx, Sy, Sh and so on).
Peer Group	Peer group of the connected peer.
Session Routing Key	Identifier to select peer for routing.
Realm	Realm of the connected peer.
Last Connect Time	Last connection time.
Own Host	Own host name and port of CPS vDRA.
Peer Status	Peer connection status (up/down).
Direction	Inbound/Outbound.
Key	Internal key/identifier assigned by CPS vDRA.
Host	Host name of the connected peer.

If the **Auto-refresh** checkbox is enabled, the **Data Last Refreshed** field is displayed at the top of the Details dialog box of the selected peer.

When you select **Details** modal, the **Data Last refreshed** field displays the time at which peers data was last refreshed. If the a**Auto-refresh** is performed when modal is opened, **Data Last refreshed** time in the modal is not updated and you have to re-open the modal to view the updated data.

View Event Logs

Step 1 In CPS DRA, navigate to **DRA Peer Monitoring**.

Step 2 Click **Toggle for Active Peers** to view active peer endpoints or **Toggle for Inactive Peers** to view inactive peer endpoints.

Step 3 To view event logs of a particular peer, click **Event Logs**.

The **Peer Status Logs** is displayed.

If the **Auto-refresh** checkbox is enabled, the **Data Last Refreshed** field is displayed at the top of the Event Logs dialog box of the selected peer.

When you select **Event Logs** modal, the **Data Last Refreshed** field displays the time at which modal is opened. The data is not updated when the modal is opened. You have to re-open the modal to get the updated data. Event log data is independent of auto refresh data.

DRA Binding Monitoring

CPS vDRA stores bindings in the mongo database. A binding database is needed to map search keys to PCRF binding information. Each binding has a search key and binding data associated with it.

You can access CPS vDRA binding information based on the following supported search keys:

- IMSI
- IMSI + APN
- MSISDN
- MSISDN + APN
- IPv6
- IPv4

View DRA Binding Details

Perform the following steps to view DRA binding details:

Step 1 In CPS DRA, navigate to **DRA Binding Monitoring**.

Step 2 To view CPS vDRA binding information for a supported search key, click on any one of the following options displayed in the **DRA Binding** page:

- IMSI
- IMSI + APN
- MSISDN
- MSISDN + APN
- IPv6
- IPv4

Step 3 Enter the required value. The search button is enabled which when clicked displays the following binding details:

Table 4: DRA Binding Details

Parameter	Description
APN	Access Point Name (Called Station ID).
Gx Session ID	Gx Session Identifier (unique) assigned by PCEF.
Session Routing Key	Identifier to select peer for routing.
Origin Host	Host name of the connected peer.

Parameter	Description
Age	Duration of session establishment. Age format is as follows: `xxxd xxh xxm xxs,` Where: • d is days • h is hours • m is minutes • s is second
Details	CPS vDRA binding details.

View Gx Session Details

Step 1 In CPS DRA, navigate to **DRA Binding Monitoring**.

Step 2 Select a supported search key and provide an input value in the search input field.

Step 3 Click **Search**.

CPS vDRA Bindings is displayed with two links for **Gx Session ID** and **Details** in each row.

Step 4 To view Gx session details, click **Gx Session ID**.

The following details are displayed in a Gx session details popup:

Table 5: Gx Session Details

Parameter	Description
Age	Duration of session establishment.
Gx Session ID	Gx Session Identifier (unique) assigned by PCEF.
IMSI	International Mobile Subscriber Identity (15 digits).
APN	Access Point Name (Called Station ID).
IPv4	IPv4 PDN address.
MSISDN	Mobile Subscriber ISDN Number (11 digits).
Origin Realm	Origin-Realm AVP from Gx CCR-I message.
Destination Realm	Destination-Realm AVP from Gx CCR-I message.
Origin Host	Origin-Host AVP from Gx CCR-I message.
Destination Host	Destination-Host AVP from Gx CCR-I message.

Parameter	Description
IPv6	IPv6 PDN address.
App Id	Identifier of the Diameter application (Gx, Rx, Sy, Sh and so on).
Session Route Key	Identifier to select peer for routing.

View Details

Step 1 In CPS DRA, navigate to **DRA Binding Monitoring**.

Step 2 Select a supported search key and provide an input value in the search input field.

Step 3 Click **Search**.

CPS vDRA Bindings is displayed with two links for **Gx Session ID** and **Details** in each row.

Step 4 To view details, click **Details**.

The following details are displayed in a details popup:

Table 6: DRA Binding Details

Parameter	Description
Age	Duration of session establishment.
Gx Session ID	Gx Session Identifier (unique) assigned by PCEF.
IMSI	International Mobile Subscriber Identity (15 digits).
APN	Access Point Name (Called Station ID).
Origin Host	Host name of the connected peer.
Session Route Key	Identifier to select peer for routing.

DRA SLF Bindings

This section describes how to view SLF Bindings details.

View SLF Bindings Details

Perform the following steps to view SLF binding details:

In CPS DRA, navigate to **DRA SLF Monitoring**.

The **DRA SLF Monitoring** page is displayed. You can access SLF binding information based on the following supported search keys:

- Subscriber ID
- IMSI
- MSISDN

View Subscriber ID Details

Step 1 Select **Subscriber ID**.

Step 2 Enter a valid subscriber ID.

Step 3 Click **Search**.

The following details are displayed in a Subscriber Details popup:

Parameter	Description
Subscriber ID	Unique identifier to identify the subscriber.
Destination	Destination specified in the map.
SLF Destination Type	Type of SLF destination specified in the map.
SLF Destination	SLF Destination specified in the map.

Step 4 Click **Details**.

The following details are displayed in a Subscriber Details popup:

Parameter	Description
Subscriber ID	Unique identifier to identify the subscriber.
IMSI	International Mobile Subscriber Identity (15 digits).
MSISDN	Mobile Subscriber ISDN Number (11 digits).
Destination	Destination specified in the map.
SLF Destination Type	Type of SLF destination specified in the map.
SLF Destination	SLF Destination specified in the map.

View IMSI Details

Step 1 Select **IMSI**.

Step 2 Enter a valid IMSI.

Step 3 Click **Search**.

The following details are displayed in a Subscriber Details popup:

Parameter	Description
IMSI	International Mobile Subscriber Identity (15 digits).
Subscriber ID	Unique identifier to identify the subscriber.
Destination	Destination specified in the map.
SLF Destination Type	Type of SLF destination specified in the map.
SLF Destination	SLF Destination specified in the map.

Step 4 Click **Details**.

The following details are displayed in a Subscriber Details popup:

Parameter	Description
Subscriber ID	Unique identifier to identify the subscriber.
IMSI	International Mobile Subscriber Identity (15 digits).
MSISDN	Mobile Subscriber ISDN Number (11 digits).
Destination	Destination specified in the map.
SLF Destination Type	Type of SLF destination specified in the map.
SLF Destination	SLF Destination specified in the map.

View MSISDN Details

Step 1 Select **MSISDN**.

Step 2 Enter a valid MSISDN.

Step 3 Click **Search**.

The following details are displayed in a Subscriber Details popup:

Parameter	Description
MSISDN	Mobile Subscriber ISDN Number (11 digits).
Subscriber ID	Unique identifier to identify the subscriber.
Destination	Destination specified in the map.
SLF Destination Type	Type of SLF destination specified in the map.

Parameter	Description
SLF Destination	SLF Destination specified in the map.

Step 4 Click **Details**.

The following details are displayed in a Subscriber Details popup:

Parameter	Description
Subscriber ID	Unique identifier to identify the subscriber.
IMSI	International Mobile Subscriber Identity (15 digits).
MSISDN	Mobile Subscriber ISDN Number (11 digits).
Destination	Destination specified in the map.
SLF Destination Type	Type of SLF destination specified in the map.
SLF Destination	SLF Destination specified in the map.

Monitoring Relay Connections

You can monitor different relay connections to remote DRAs using the DRA Relay Connection option.

View Relay Connections

Perform the following steps to view relay connections:

Step 1 Navigate to **DRA Relay Connection**.

Step 2 Select the **Filter by** drop down and click on any one of the following data options displayed:

- All Visible Columns
- Remote System
- Peer
- Remote IP Address
- Local Host Name
- Status
- Direction
- Details/Event Logs
- All Data

Step 3 Enter a value in the **Filter Relay Connections** field.

Step 4 Click **Toggle for Active Relays** to view filtered active relay endpoints or **Toggle for Inactive Relays** to view filtered inactive relay endpoints.

The following table describes the details displayed under Relay Connections:

Table 7:

Parameter	Description
Remote System	Connected relay system.
Peer	Connected relay host name.
Remote IP Address	Connected relay IP address.
Local Host Name	DRA's own host name and port.
Local IP Address	DRA's own IP address.
Status	Relay connection status (up/down).
Direction	Inbound or outbound.
Details/Event Logs	Relay details/relay connection history log.

You can check the **Auto-refresh** checkbox to refresh data every 30 seconds. The **Data Last Refreshed** field displays time when data is fetched from server

View Relay Details

Perform the following steps to view relay details:

Step 1 Navigate to **DRA Relay Connection**.

Step 2 Click **Toggle for Active Relays** to view filtered active relay endpoints or **Toggle for Inactive Relays** to view filtered inactive relay endpoints.

Step 3 To view details of a particular relay connection, click **Details**.

The following details are displayed:

Table 8:

Parameter	Description
Key	Internal key or identifier assigned by DRA.
Last Connect Time	Last connection time.
Peer Status	Relay connection status (up/down).
Direction	Inbound or outbound.
Own Host	DRA's own host name and port

Parameter	Description
Own IP Address	DRA's own IP address.
Own Port	DRA's own port.
Peer Uri	Connected relay host name.
Remote I P Address	Connected relay host port.
Remote Port	Connected relay IP address.
Remote System Id	Connected relay system.

If the **Auto-refresh** checkbox is checked, the **Data Last Refreshed** field is displayed at the top of the Details dialog box of the selected peer.

When you select the **Details** modal, the **Data Last Refreshed** field displays the time at which data was last refreshed. If the **Auto-refresh** is performed when the modal is opened, **Data Last refreshed** time in the modal is not updated and you have to reopen the modal to view the updated data.

View Relay Event Logs

Perform the following steps to view relay event logs:

Step 1 Navigate to **DRA Relay Connection**.

Step 2 Click **Toggle for Active Relays** to view filtered active relay endpoints or **Toggle for Inactive Relays** to view filtered inactive relay endpoints.

Step 3 To view event logs of a particular relay connection, click **Event Logs**.

The **Event Logs for Relay Key** is displayed.

If the **Auto-refresh** checkbox is enabled, the **Data Last Refreshed** field is displayed at the top of the Event Logs dialog box of the selected peer.

When you select **Event Logs** modal, the **Data Last Refreshed** field displays the time at which modal is opened. The data is not updated when the modal is opened. You have to re-open the modal to get the updated data. Event log data is independent of auto refresh data.

Message Tracing and Activity Monitoring for Single Subscriber

Message Tracing for Single Subscriber

CPS vDRA stores audit logs based on modules. If you enable the debug or trace logging function, it stores detailed logs in the log file for all the subscribers for those modules. To overcome this situation, in the CPS 21.2.0 release, vDRA supports tracing function of incoming and outgoing messages for a single subscriber in PCAP format.

The main functions are:

- vDRA captures diameter request and response messages across all vDRA sites for a single subscriber and stores all messages in configured DB in PCAP format.
- Captures Request and Answer messages as received from peer and as sent to the peer on ingress and egress director, respectively.
- Starts or Stops the message trace by getting subscriber identity, which is IMSI/MSISDN/IPv6.
- Retrieves the PCAP based on subscriber identity. By default, vDRA stores PCAP in admin-db.
- DRA configures any other mongo db uri.

Note Make sure that configured mongo-db uri is having reachability for directors and workers.

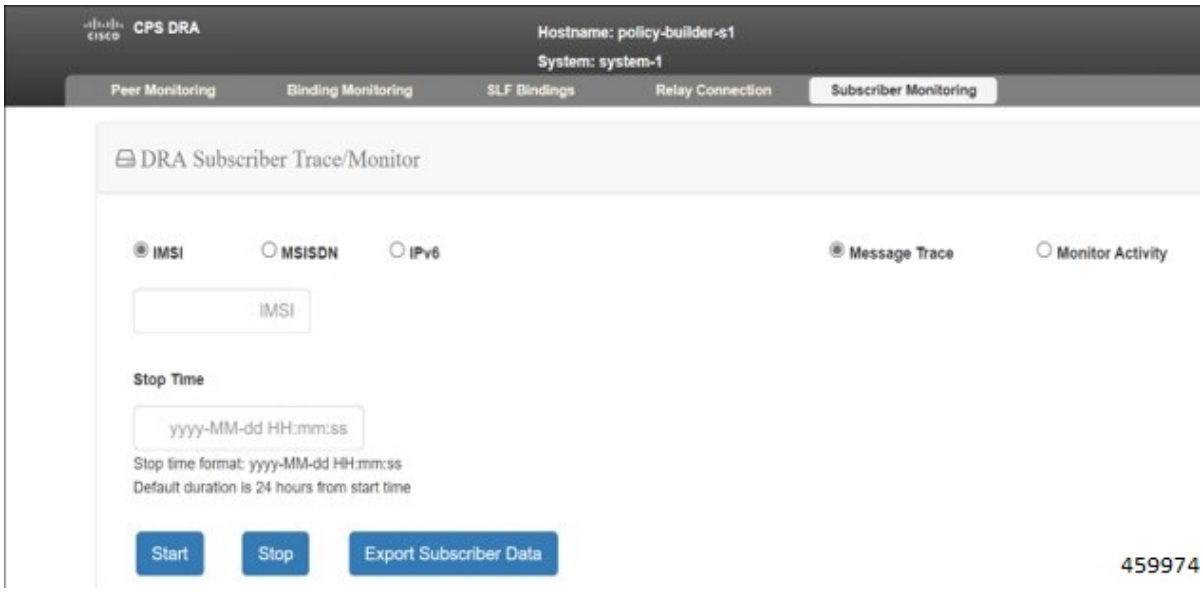
View Trace Messages

Perform the following steps to view trace messages:

Before you begin

Step 1 In CPS DRA, click the **Subscriber Monitoring** tab.

Figure 4: Subscriber Monitoring



Step 2 In the **DRA Subscriber Trace/ Monitor** area, click any one of the following options displayed to trace messages for a single subscriber:

- IMSI

- MSISDN
- IPv6

Step 3 Enter the required subscriber identity values for IMSI/MSISDN/IPv6.

Note You can enter subscriber identity values for IMSI/MSISDN/IPv6, where trace was already started and click **Export Subscriber Data** to download pcap files from DRA.

Step 4 Click the following radio button:

Table 9: DRA Subscriber Monitoring Details

Parameter	Description
Message Trace	Click the **Message Trace** radio button to trace subscriber messages. vDRA creates database "trace_db" in admin-db or any configured mongo db. In trace_db, DRA creates collection pcap_files, trace_key_version, trace_keys to store pcap files, version number and IMSI/MSISDN/IPv6 values, respectively. For more information about configuration parameters, refer the **dra subscriber-trace db-connection** and **dra subscriber-trace db-pcap-collection-max-size** CLI Commands in the *CPS vDRA Operations Guide*.

Step 5 In the **Stop Time** field, enter the time to stop the trace for single-subscriber.

- Supports date/time formats:
  - yyy-MM-dd HH:mm::ss – Supports date and time format in ISO format.
  - HH:mm:ss – Allows to enter only time where DRA internally considers date as current date.
- By default, DRA traces each subscriber for 24 hours duration and after that DRA automatically stops the message trace.
- Manually you can change the duration before starting the message trace.

Step 6 Click **Start** to start the message trace.

Step 7 Click **Export Subscriber Data** to download pcap files from DRA.

Workflow for Capturing Subscriber-Based Information

In the audit log, vDRA captures traces across different containers such as Diameter-Endpoint, Binding and so on for success and failure messages. To overcome the difficulties of consolidating and getting the trace for complete session creation to termination from existing audit logs, vDRA captures subscriber-based logs based on IMSI/MSISDN/IPv6.

How it works:

- Enable message trace in all possible sites where peer can connect. This is because, only those sites that are configured with trace detects the session.
- Ingress director processing CCR-I/AAR maps the subscriber to the monitor session and notifies the start of session to all other sites. Thus subsequent messages for that session are captured in other sites. DSCP values are captured only for outbound messages.
- On Start trace, other sites are notified with configured subscriber identity and any messages related to that configured subscriber identity/session are captured in other sites. On stop trace, other sites are notified with configured subscriber identity and capturing sessions are stopped for that configured subscriber identity. Other nodes in the system and other sites are notified on session monitoring through Control Plane advertisement.
- vDRA captures Request and Answer message as received from peer and as sent to the peer on ingress and egress director, respectively.
- After vDRA receives CCR-I for trace enabled subscriber, vDRA parses subscriber identity values (IMSI/MSISDN/IPv6) from CCR-I messages and stores them in internal cache along with session ids. This information is used for tracing initial AAR based on IPv6.
- vDRA traces all other messages Gx CCR-U/T/RAR and Rx AAR update/RAR/STR based on session IDs stored on internal cache.

Limitations

Following are the limitations:

- DSCP value is captured only for outbound messages. For inbound messages, DSCP value is not captured.
- For inbound messages, only diameter messages along with ip address and port are captured.
- If same subscriber connects with different identity, then you need to configure a separate trace request for subscriber. DRA does not resolve the multiple identities for a subscriber automatically.
- Enable message trace in all possible sites where peer can connect.
- Supports only Gx, Rx application messages
- By default, DRA can monitor maximum of 50 subscribers.
- Message trace should be enabled only during maintenance window or in lab for any debugging purpose. By default, Trace is disabled.
- DRA starts session trace only after receiving CCR-I message for that session. Until that even though message trace is configured, DRA does not capture trace for any messages related to that session.

Monitoring Single Subscriber Activity

The vDRA supports following functions to store live subscriber-based logs:

- In vDRA, enable monitor activity in all possible sites where peer can connect. This is because, only those sites enabled with monitoring activity detect the session.
- After monitor activity starts, vDRA captures and stores all possible logs related to the Policy Builder (PB), Customer Reference Data (CRD) configuration, Route selected, Shard selected, and traces of logs in different containers in **monitor_activity_db** DB.

- If monitor activity stops, vDRA notifies other sites to stop capturing activity logs.
- vDRA notifies other nodes in the system and other sites on session monitoring through Control Plane advertisement.
- Once DRA receives CCR-I for monitor activity enabled subscriber, DRA parses subscriber values (IMSI/MSISDN/IPv6) from CCR-I messages and stores them in internal cache along with session ids. This information is used for monitoring initial AAR based on IPv6.
- vDRA monitors all other messages Gx CCR-U/T/RAR and Rx AAR update/RAR/STR based on Session IDs stored on internal cache.
- When monitor activity is enabled for a particular subscriber and set logger level of DRA.trace to trace, then DRA logs all activities of particular subscriber in a consolidated qns log under trace level.
- DRA monitors activity only for Gx/Rx messages.
- vDRA monitors maximum of 50 subscribers.
- By default, vDRA monitors subscriber activity for 24 hours.
- By default, DRA stores monitor activity keys and activity logs in mongo-admin-a: 27017, mongo-admin-b: 27017, and mongo-admin-c: 27017.
- By default, vDRA sets activity collection size as 1024 MB.

Limitations

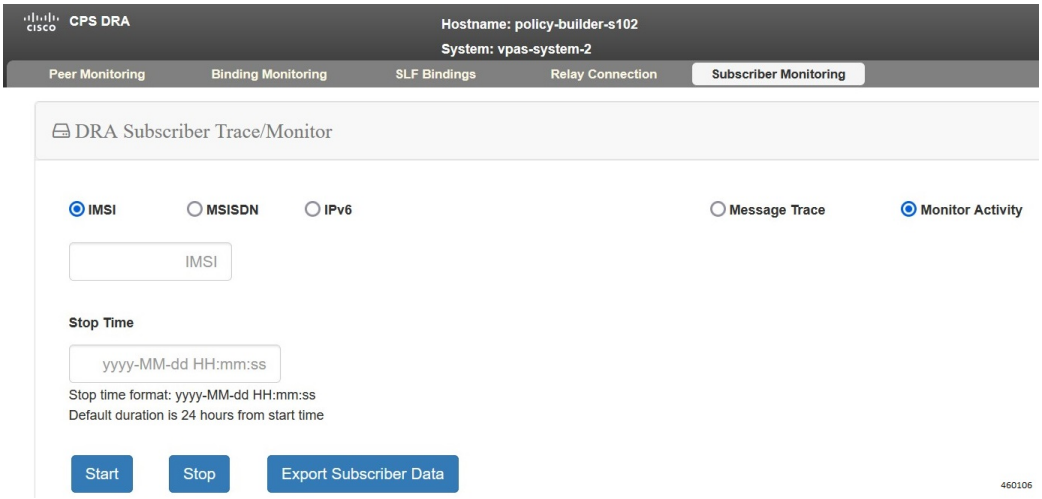
Following are the limitations:

- Logs contain:
  - Monitor subscriber activity configurations-related to CRD and Policy Builder
  - Activity flows in each container
  - Shard selection logs
  - Routing information
- DRA starts session monitoring only after receiving CCR-I message for that session. Until that even though monitor activity is configured, DRA does not capture activity for any messages related to that session.
- Does not support monitoring activity of the same subscriber with multiple times.
- Recommended to use only during debugging session or testing.

View Subscriber-Based logs

1. In CPS DRA, click the **Subscriber Monitoring** tab.

Figure 5: Subscriber Monitoring



2. In the **DRA Subscriber Trace/ Monitor** area, click any one of the following options displayed to tmonitor subscriber activities for a single subscriber:
   - IMSI
   - MSISDN
   - IPv6
3. Enter the required subscriber identity values for IMSI/MSISDN/IPv6.
4. Click the following radio button:

Table 10: DRA Subscriber Monitoring Details

Parameter	Description
Monitor Activity	Click the **Monitor Activity** radio button to monitor subscriber activity in the vDRA. For more information about configuration parameters, refer the **dra subscriber-monitor-activity db-connection** and **dra subscriber-monitor-activity db-activity-collection-max-size** CLI Commands in the *CPS vDRA Operations Guide*.

5. In the **Stop Time** field, enter the time to stop the monitor activity for single-subscriber.
   - Supports date/time formats:
     - yyy-MM-dd HH:mm::ss – Supports date and time format in ISO format.
     - HH:mm:ss – Allows to enter only time where DRA internally considers date as current date.
   - By default, DRA monitors each subscriber for 24 hours duration and after that DRA automatically stops the monitoring subscriber activity.

- Manually you can change the duration before starting the monitor activity.

6. Click **Start** to start the monitor activity.
7. Click **Export Subscriber Data** to download subscriber activity files from DRA.

Monitor Live Subscriber Activity

Use the **monitor subscriber-activity** CLI command to monitor live subscriber activity logs in the vDRA. This **monitor subscriber-activity** CLI command is used only to view live logs. For example, use the following Syntax to view subscriber identity logs:

```
monitor subscriber-activity imsi <IMSI value> user <admin>
monitor subscriber-activity msisdn <MSISDN value> user <admin>
monitor subscriber-activity ipv6 <IPv6 value> user <admin
```

For more information, see *monitor subscriber-activity* section in the *CPS vDRA Operations Guide*.

DRA Health Checks

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

CRD, Metadata DB connectivity, and Consul failures leads to improper processing of diameter messages in the Worker node. To enhance product resiliency in the Worker CRD failure, Worker Metadata DB, and Worker consul readiness scenarios, vDRA supports health checks to ensure that all prerequisites are met before traffic is accepted by nodes.

As a best practice, the following validation is done during Worker or Diameter node start up:

- **CRD Validation for Diameter and Binding Initiation**: Applicable only for binding node:
  - During container startup (Diameter or Worker node), vDRA performs the CRD validation, and if the CRD is not loaded properly, then the container is marked as unhealthy.
  - During runtime state, if there's any validation performed for CRD update and if there are any errors during CRD cache loading, that node is revoked from IPC message processing and marked as unhealthy.
- **Metadata DB Access Check from Binding Node**: Applicable for Worker node. During container startup the metadata DB connection validation is performed. If there's any failure/issue, then the node is marked as unhealthy and gets removed from the IPC message processing.

  During runtime, if there are any errors during Metadata DB cache reloading, that node gets revoked from IPC message processing and marked as unhealthy.
- **DRA App Configuration Validation**: Applicable only during application startup in Worker/Director node.

  Use the `consul-health` CLI configuration command to monitor consul failures during startup. This script is part of `supervisorctld`.

Monitoring Installation Using Grafana

You can access the Grafana interface under DRA Monitoring to monitor installation. It is a third-party metrics dashboard and graph editor. Grafana provides a graphical or text-based representation of statistics and counters collected in the Prometheus database.

Note After the DRA Director (DD) failover/reboot, the TPS values in Grafana dashboards takes approx. 5 minutes to fetch and display the latest updated values. Until the values are updated, Grafana displays the old data.

For more information about Grafana in vDRA, refer to the *Prometheus and Grafana* chapter in the *CPS vDRA Operations Guide*.

Viewing CPS APIs

API information option enables you to view API related information:

- Service Orchestration API: to manage Policy Builder data

Select the link to view the documentation and usage examples.