Oracle® Retail AI Foundation Cloud Service

AI Foundation Private Endpoint Cloud Service: Database Access Implementation Guide

Release 25.1.201.0
G32927–01
April 2025

Oracle Retail AI Foundation Cloud Service AI Foundation Private Endpoint Cloud Service: Database Access Implementation Guide, Release 25.1.201.0

G32927–01

Contents

Preface

Audience

This document is intended for the users and administrators of Oracle Retail AI Foundation Cloud Service.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Oracle Help Center (docs.oracle.com)

Oracle Retail product documentation is available on the Oracle Help Center at https://docs.oracle.com/en/industries/retail/index.html.

(Data Model documents can be obtained through My Oracle Support.)

Comments and Suggestions

Please give us feedback about Oracle Retail Help and Guides. You can send an e-mail to: retail-doc_us@oracle.com

Oracle Retail Cloud Services and Business Agility

Included in the service is continuous technical support, access to software feature enhancements, hardware upgrades, and disaster recovery. The Cloud Service model helps to free customer IT resources from the need to perform these tasks, giving retailers greater business agility to respond to changing technologies and to perform more value-added tasks focused on business processes and innovation.

Oracle Retail Software Cloud Service is acquired exclusively through a subscription service (SaaS) model. This shifts funding from a capital investment in software to an operational

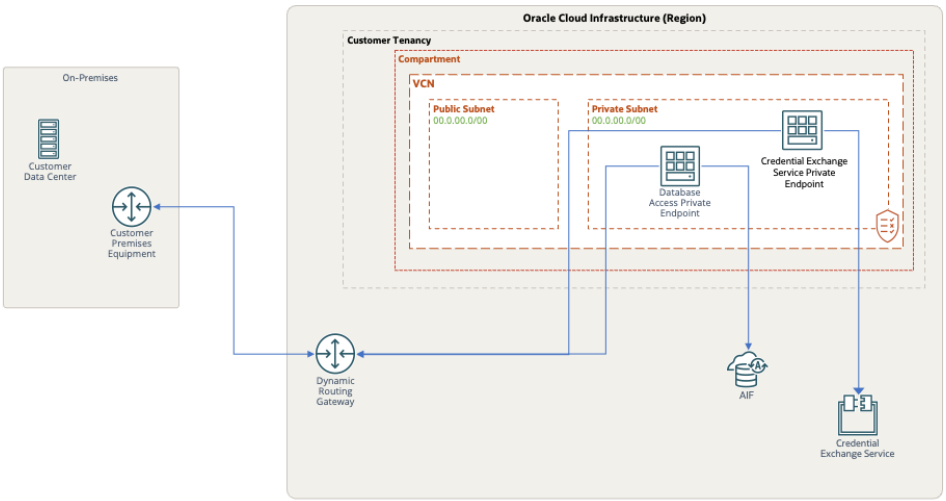
expense. Subscription-based pricing for retail applications offers flexibility and cost effectiveness.

1

Introduction

The Oracle Retail AI Foundation Cloud Service database is accessible through Innovation Workbench including APEX and Notebook development environments. Private endpoints extend access to Retail AI Foundation Cloud Service within the virtual cloud network (VCN) on Oracle Cloud Infrastructure or to other networks peered to the VCN such as your corporate network. You can access Retail AI Foundation Cloud Service data from hosts within the virtual cloud network (VCN) or from the on-premises network.

Figure 1-1 Retail AI Foundation Cloud Service Access through a Private Endpoint



With a private endpoint, traffic does not go over the internet. A private endpoint is a private IP address within your VCN that can be used to access a given service within the Oracle Cloud Infrastructure. The service sets up the private endpoint in a subnet of your choice within the VCN. The private endpoint is just another Virtual Network Interface Card (VNIC) in your VCN.

You control access to it as you would for any other VNIC by using security rules. When you set up a private endpoint for Retail AI Foundation Cloud Service, however, the VNIC is set up for you, and its availability is maintained on your behalf. Your only responsibility is to maintain the subnet and the security rules. See Figure 1.

Be aware; taking full advantage of your private endpoint requires substantial networking skills. For additional information, consult Oracle documentation on *OCI networking, OCI private access, FastConnect, and site-to-site VPN*.

When you request a private endpoint for Retail AI Foundation Cloud Service, you receive an endpoint for each of your environments: production, stage, and so on. You also receive a second private endpoint that gives you access to a Credential Exchange Service (discussed in more detail below). Establishing a private endpoint requires some lead time and a short outage

on each environment (two to eight hours depending on environment size). The outage on each environment precedes the availability of the endpoint by several days. In short, the time between your request for private endpoint access and its availability is measured in days not hours or minutes. Oracle support will contact you to schedule environment outages.

2
Prerequisites

When you request a private endpoint for Retail AI Foundation Cloud Service begin by creating a private subnet in an ideally dedicated compartment and VCN of your choice. Oracle Support will ask for the following information:

- Tenancy OCID
- Compartment Name
- Compartment OCID
- VCN OCID
- Subnet OCID

This information is readily available on the OCI Console and is accessible when you create your subnet. You may create a new child compartment as well as a new VCN if you choose. Once you have completed this task, put the following policies in place using the **Identity > >Policies** screen on your OCI Console.

```
Allow service ORACLE_INDUSTRY_SAAS to manage vnic in compartment <Customer
Compartment Name>
```

```
Allow service ORACLE_INDUSTRY_SAAS to use subnets in compartment <Customer
Compartment Name>
```

```
Allow service ORACLE_INDUSTRY_SAAS to use network-security-groups in compartment
<Customer Compartment Name>
```

```
Allow service ORACLE_INDUSTRY_SAAS to inspect work-requests in compartment
<Customer Compartment Name>
```

Notification of database credential rotation can be done through email, an http or https endpoint, or neither. If you choose neither, then credentials are fetched as needed. Note, if you use an http or https endpoint for notification, you will need to create an additional private subnet in a dedicated (ideally) compartment and VCN of your choice. Oracle Support will ask for the following information about your subnet and endpoint:

- VCN OCID
- Subnet OCID
- Subnet
- Fully qualified domain name of notification endpoint

  In addition, if you use an http or https endpoint for notification, you may need to add an ingress rule to ensure that the notification endpoint is reachable from the Credential Exchange Server. If you are uncertain as how you wish to be notified of credential rotation or are uncertain about the specifics, you may provide endpoint details in a later request. See Credentials.

Note:

Concerning OCI regions, and the number of availability domains (AD). If your service is within a 3-AD region, you are done. If, however, you are within a single AD region, you will also need to complete the above prerequisites for the standby region as well. The standby details will be provided in your requests. In the event of a Disaster Recovery situation in a single AD region, the customer must perform a number of DNS updates. When the disaster is mitigated, the customer must reverse those updates. The details are found in My Oracle Support Doc ID: 2991525.1.

3
Client-Side Configuration

When private endpoint setup is complete, Oracle Support provides details for each private endpoint, two per environment. To access Retail AI Foundation Cloud Service from within OCI, edit the security list Ingress Rules of the private subnet. Typical values are shown in the table below.

> **Note:**
>
> Concerning OCI regions, and the number of availability domains (AD). If your service is within a 3-AD region, you are done. If, however, you are within a single AD region, you will also need to complete the security ingress rules of your private subnet in your standby region.

Table 3-1 Example Ingress Rules for Private Endpoint

Attribute	Value
STATELESS	No
SOURCE	CIDR (10.0.0.0/16)
IP PROTOCOL	TCP
SOURCE PORT RANGE	All
DESTINATION PORT RANGE	1521-1522, 443
TYPE AND CODE	(Blank)
ALLOWS	All
DESCRIPTION	(Optional)

4
Credentials

Database credentials are needed to access Retail AI Foundation Cloud Service through your private endpoint. Obtain these credentials by using the Credential Exchange Service, a REST endpoint.

The endpoint provides a means of fetching the database credentials required to connect. Credentials are periodically refreshed when passwords are rotated. Notification of password rotation is received by registering one or more callback services or email addresses with the Credential Exchange Service.

It is recommended that at least an email address be registered through the rotation-notification endpoint as a fallback means of notification, otherwise the credentials may be rotated without your knowledge.

Any callback service should be accessible through the Private Endpoint. Repeatedly unavailable endpoints may be removed. Finally, credentials are not conveyed through the callback; you are only notified that they have changed.

The Credential Exchange Service uses OAuth 2.0for authentication. That token is generated using a well-known OCI IAM service, which authenticates using basic authentication. The client credentials for this (that is,, client id and client secret) are obtained from Retail Home.

Bear in mind, the OCI IAM service is rate limited (see API Rate Limits). Best practice is to reuse tokens until they expire (one hour). If you encounter an HTTP- 429 error when requesting a token or authenticating, you have hit the rate limit. When you encounter a rate limit, pause any further requests for one minute to reset the rate limiter.

Obtaining Credential Exchange Server Credentials

Base URL

The base URL mentioned below has the following form:

<host-name>/<sub-name-space-name>

The host-name can be further decomposed into:

https://home.retail.<region>.ocs.oracle.com

Likewise, the sub-namespace-name can be further decomposed into:

rgbu-common<customerid>-<env>

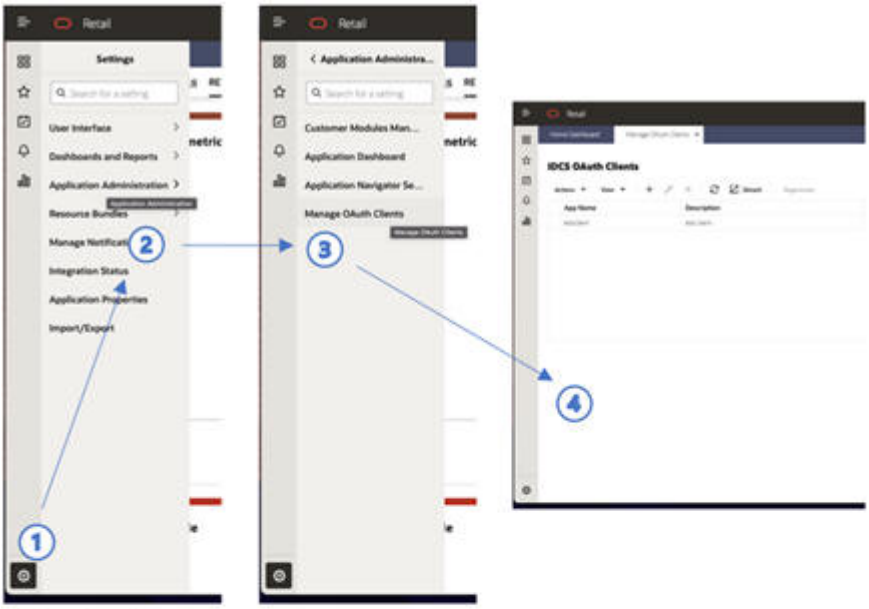
You can extract region, customerid, and env from your Retail Home URL. The host port of the base URL is 443.

If you are still uncertain as to how to construct the base URL or the base URL you have constructed is not working as expected, submit a Support Request for further assistance.

The Credential Exchange Service uses OAUTH 2 for authentication. What this means in practice is that a short-lived token is used for authentication. That token is generated using a well-known service, which authenticates using basic auth. The basic auth credentials (i.e., client id and client secret) are obtained from Retail Home.

1. In Retail Home, navigate to Manage OAUTH Clients page by tapping settings (1), then tapping the Application Administration menu item (2), and lastly tapping the Manage OAUTH Clients menu item to arrive at the Manage OAUTH Clients page (4).

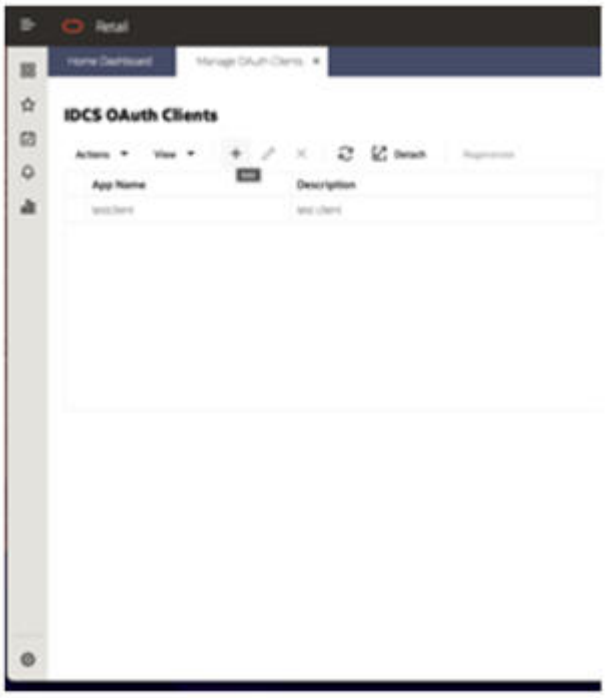
Figure 4-1 Mange OAUTH Client



Select the + button.

2. Select the +

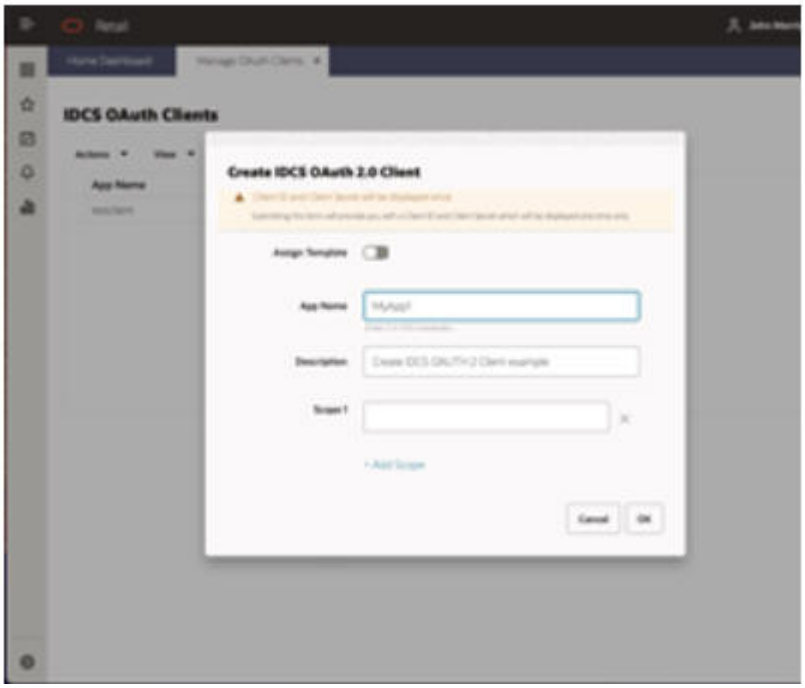
Figure 4-2 Selecting + Button



button.

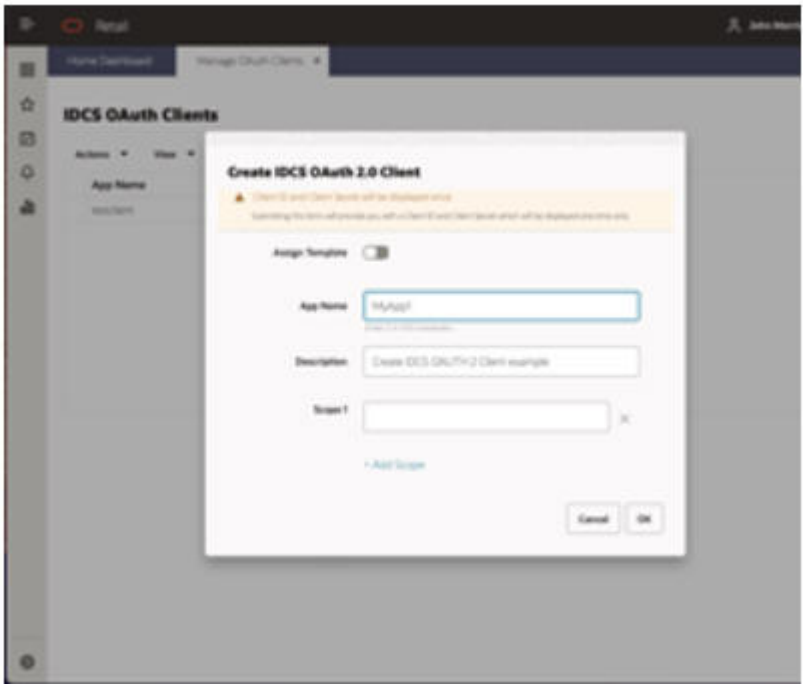
3. A popup dialog appears. Provide an App Name and Description. Leave Scope blank. Select OK.

Figure 4-3 Provide App name and Description



4. A new dialog appears with a Display Name, Client ID and Client Secret. You *must* retain this information. It will not be displayed again. Select Done when the information has been copied. Note: New credentials can be created at any time and that production, stage, and development will have different credentials.

Figure 4-4 Descriptive Information



Consult the Retail Home Application Administration Guide for additional details on managing OAUTH clients.

Remember that the OCI IAM service is rate-limited (see API Rate Limits). Best practice is to reuse tokens until they expire (one hour). If you encounter a 429 error when requesting a token or authenticating, you have hit the rate limit. When you encounter a rate limit, back off for one minute to reset the rate limiter.

Before proceeding:

- Verify that a client ID and secret can be created in Retail Home.
- Retain the client ID and secret for future use.

There is no need to create multiple OAuth clients for each OCI IAM service. A single OAuth client can be used across all environments secured by a given IDCS.

Generating a Credential Exchange Server Access Token

You will need an IDCS Authorization Server endpoint URL and ORDS service credentials to perform the steps described below.

You will use an IDCS Authorization Server to generate an ORDS access token. There are multiple techniques for generating an access token. The example below employs cURL.

The cURL command for generating an access token has five components:

1. The IDCS Authorization Server endpoint URL

2. The IDCS Authorization Server endpoint URL
3. An Authorization
4. A grant type
5. A scope

   Only the IDSC Authorization Server endpoint url and authorization are customer-specific. content type, grant type, and scope are the same for all customers.

IDSC Service Host

The IDCS endpoint URL has the following form: https://<idcs authorization server host>/oauth2/v1/token

To obtain your IDCS service host, navigate to Retail Home. When you navigate to Retail Home you will be redirected to an IDCS authorization server URL. The host of that URL is the IDCS authorization server that you will use to obtain your access token.

Basic Auth Encoding

```
To fetch a token, you need to use Basic Auth and Base 64 encode the credentials. For
example, you could use the following script to obtain an access token on Oracle Linux 8:

CLIENT_ID=”your_client_id”
CLIENT_SECRET=”your_client_secret”

# Combine the client ID and secret, then encode in Base64
ENCODED_CREDENTIALS=$(echo -n “${CLIENT_ID}:${CLIENT_SECRET}” | base64 -w 0)

# Output the result
echo “Encoded Base64 credentials: $ENCODED_CREDENTIALS”

Replace your_client_id and your_client_secret with the credentials obtained when
creating your OAUTH client.

Use the cURL command to generate a token is the following:

RESPONSE=$(curl --location --request \
POST "https://<idcs authorization server host>/oauth2/v1/token" \
--header "Content-Type: application/x-www-form-urlencoded" \
--header "Authorization: Basic ${ENCODED_CREDENTIALS}" \
--data-urlencode "grant_type=client_credentials" \
--data-urlencode "scope=urn:opc:idm:__myscopes__")

ACCESS_TOKEN=$(echo ${RESPONSE} | jq -r .access_token)
echo ${ACCESS_TOKEN}
```

Before proceeding:

1. Verify that you can generate an access token.
2. Retain the access token if you plan to use it within the next hour.

Credential Exchange Endpoints

Fetching Credentials

Method	Endpoint
GET	/api/data-pe/v1/fetch-credentials

Returns the wallet and credentials for the schemas exposed by the Database Private Endpoint.

Fetching Wallet

Method	Endpoint
GET	/api/data-pe/v1/fetch-wallet

This REST call returns the wallet as a compiled zip file for use with the Database Private Endpoint. The wallet does not contain credentials, these need to be fetched from the fetch-credentials endpoint.

Registering Notification Endpoints

Method	Endpoint
PUT	/api/data-pe/v1/rotation-notification

```
JSON payload: {"usecase": "credentialRotationNotification", "endpoint": "http://
example.org:80/foo/bar/baz/notification1" }
```

This method inserts unique endpoints into the notification endpoint list. Duplicates are silently ignored (intended for repeat registrations from restarted callback services). The notification endpoint can be a URL in the form of http, https, or mailto (e.g., mailto:foo@bar.baz).

Registered http or https endpoints are called with an http POST containing a JSON payload describing the scope of the change: `{usecase:"credentialRotation", change:"<all|credentials|wallet>" }`

> **Note:**
>
> If an http or https endpoint is registered, you may need to add an ingress rule for <base_url> to ensure that the endpoint is reachable.

Registered mailto endpoints are sent a notification email. SMTP notifications are sent from the regional OCI Email Delivery Service to the email address that the customer specifies.

After receiving this notification, the consuming applications should refresh their credentials.

Method	Endpoint
DELETE	/api/data-pe/v1/rotation-notification

```
JSON payload: {"usecase": "credentialRotationNotification", "endpoint": "http://
example.org:80/foo/bar/baz/notification1" }
```

Removes endpoints from a list. Non-existent endpoints are silently ignored.

Method	Endpoint
GET	/api/data-pe/v1/rotation-notification?tenantId=abc123

Returns endpoints[...] containing a list of registered endpoints, or empty endpoints [] if none exist.

Example

```
{"endpoints": [ "http://example.org:80/foo/bar/baz/notification", "mailto:
nobody@example.org" ] }
```

Serialized Wallet and Credential Format

Credentials are serialized into JSON and, within that payload, Oracle Wallet file contents are base64 encoded.

Content	Purpose
wallets	Array of wallets
walletName	Name of database wallet and instance, derived from tnsnames.ora within wallet
walletPassword	(Currently unused)
comment	(Currently unused)
certificateEndDate	Expiration date of wallet, derived from truststore certificate within wallet
certificateStartDate	Start date of wallet, derived from truststore certificate within wallet
lastRotationDate	Date of last rotation
schemas	Map of database credentials (username):(password)
wallet	Map of wallet file contents, (filename):(base64 encoded file)

Example

```
{
  "wallets": [
    {
      "certificateEndDate": 1746276157000,
      "certificateStartDate": 1588596157000,
      "comment": null,
      "lastRotationDate": 1624305815466,
      "schemas": {
        "username1": "password1",
        "username2": "password2",
        "username3": "password3",
        "username4": "password4",
      },
    "wallet": {
      "README": "...base64-encoded-file...",
      "cwallet.sso": "...base64-encoded-file...",
      "ewallet.p12": "...base64-encoded-file...",
      "keystore.jks": "...base64-encoded-file...",
      "ojdbc.properties": "...base64-encoded-file...",
      "sqlnet.ora": "...base64-encoded-file...",
      "tnsnames.ora": "...base64-encoded-file...",
      "truststore.jks": "...base64-encoded-file..."
    },
    "walletName": "Wallet_RDSADWABC123",
    "walletPassword": null
   }
```

```
    ]
}
```

Table 4-1 Troubleshooting

HTTP Status Code	Problem	Solution
404	Incorrect API URL	Verify API URL
401	Invalid, expired, or missing token	Verify that you are using the a client ID and secret from the correct IAM service, that the token has not expired, that the token is valid (e.g., echo cURL script), and the token is not missing.
403	Internal error	Submit a support ticket with the details of the API invocation (e.g., a cURL script)
200	Response is: {"msg":"Internal error, cannot connect to upstream service", "detail":"java.net.ConnectException: Connection refused (Connection refused)"}	Submit a support ticket with the details of the API invocation (e.g., a cURL script)

5
Verifying Your Private Endpoint from OCI VM

Verifying Access to the Credential Exchange Server

Begin by obtaining an access token using the steps described above. The example below assumes the token is in an environment variable named ACCESS_TOKEN. Next, using cURL, fetch the database credentials as show in the example below. This example assumes you are using Oracle Linux 8.

```
# Fetch wallet
$ curl --location "https://<base-url>/api/data-pe/v1/fetch-credentials" \
    --header "Authorization: Bearer ${ACCESS_TOKEN}" > response.json
 # Store wallet and schema information
cat response.json | jq -r '.wallets[0]' > wallets.json
cat response.json | jq -r .schemas > schemas.json

# Decode wallet
mkdir -p wallet
cat wallets.json | jq -r '.wallet.README' | base64 -d > wallet/README
cat wallets.json | jq -r '.wallet."cwallet.sso"' | base64 -d > wallet/
cwallet.sso
cat wallets.json | jq -r '.wallet."ewallet.p12"' | base64 -d > wallet/
ewallet.p12
cat wallets.json | jq -r '.wallet."keystore.jks"' | base64 -d > wallet/
keystore.jks
cat wallets.json | jq -r '.wallet."ojdbc.properties"' | base64 -d > wallet/
ojdbc.properties
cat wallets.json | jq -r '.wallet."sqlnet.ora"' | base64 -d > wallet/
sqlnet.ora
cat wallets.json | jq -r '.wallet."tnsnames.ora"' | base64 -d > wallet/
tnsnames.ora
cat wallets.json | jq -r '.wallet."truststore.jks"' | base64 -d > wallet/
truststore.jks
```

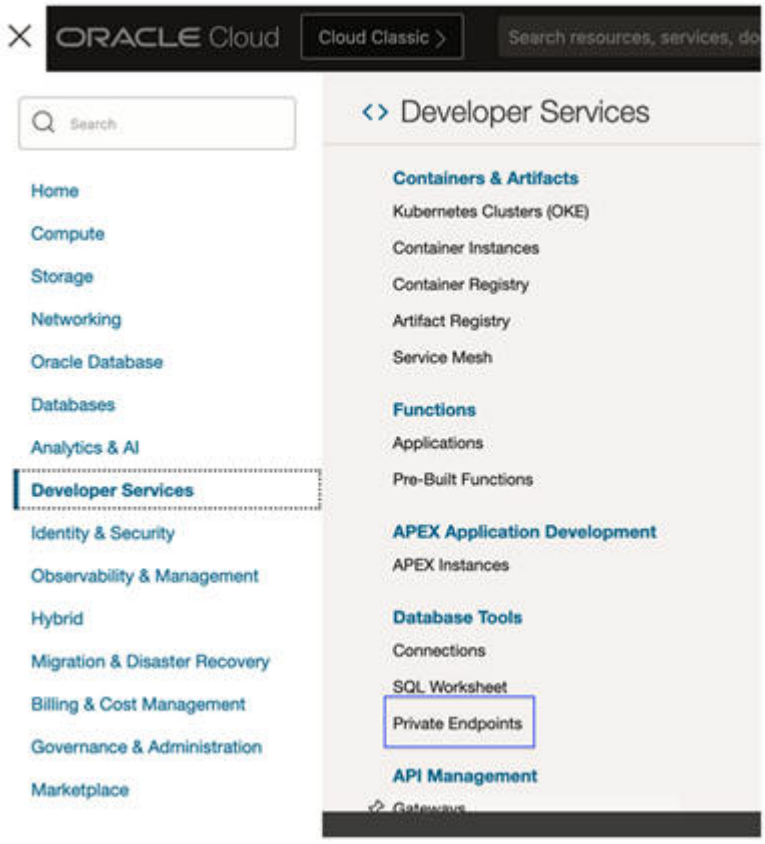
Verifying Access to your Database Through the Private Endpoint

Create Private Endpoint

To create a Private Endpoint:

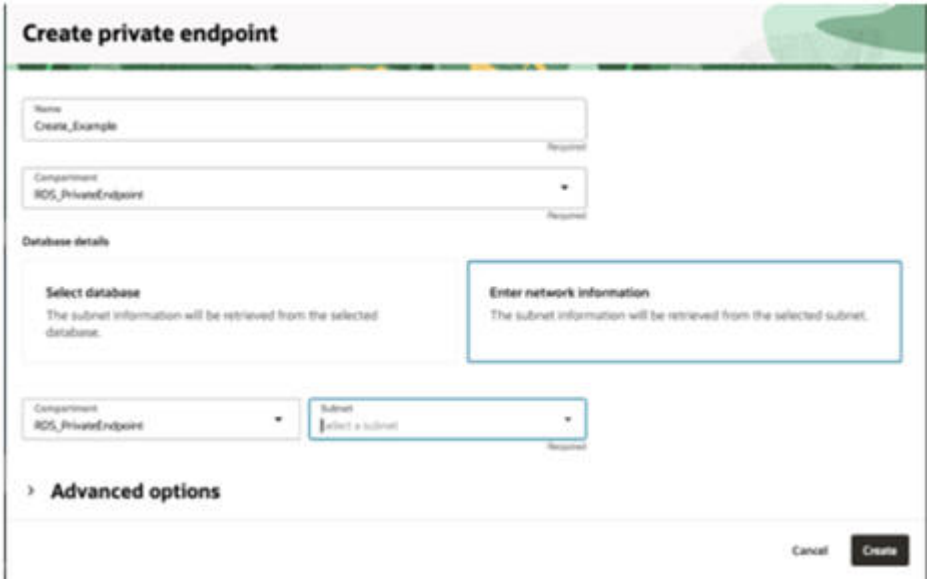
1. Log-in to the Cloud Console in your OCI tenancy. Navigate to Developer Services > Database Tools > Private Endpoints.

Figure 5-1 Private Endpoint



2. Click Create Private Endpoint.
3. Create the Private Endpoint in the compartment where the Data Private Endpoint was created.
4. Select Enter network information.
5. Select the compartment in which the private endpoint was created.
6. Select the private subnet.
7. Click Create.

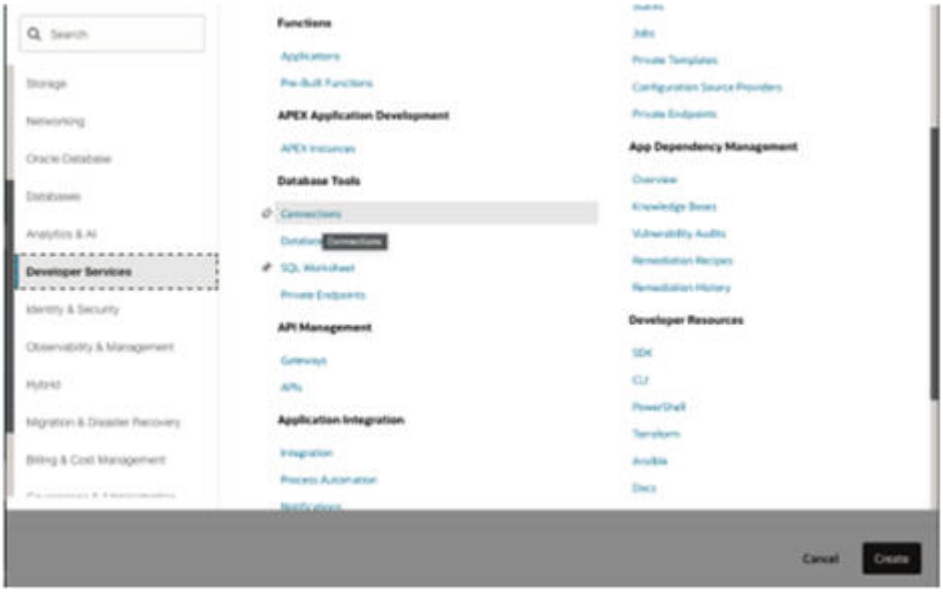
Figure 5-2 Create Private Endpoint



Create Connection

1. Log-in to the Cloud Console in your OCI tenancy. Navigate to Developer Services Database Tools Connections.

Figure 5-3 Create Connection

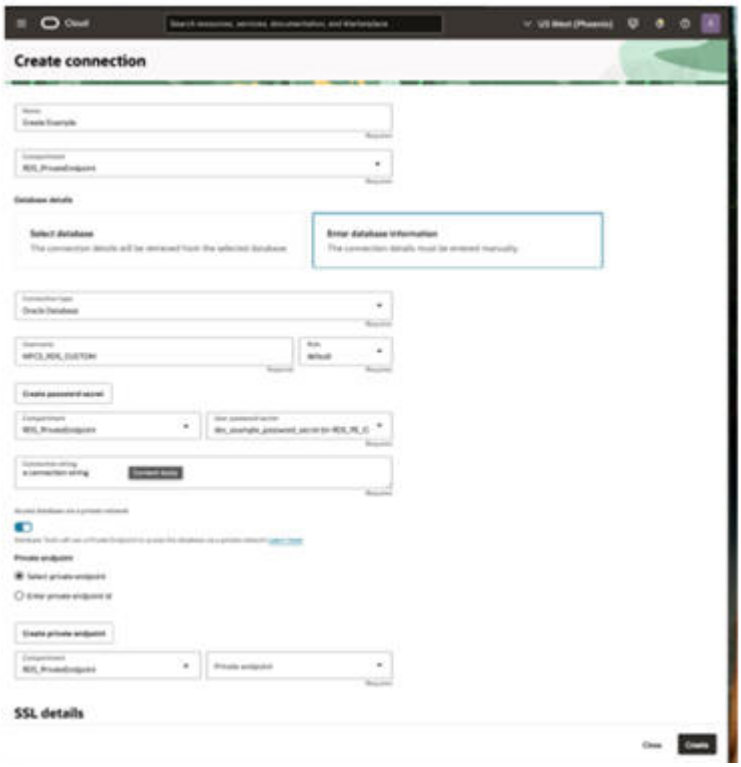


2. Click Create Connection.
3. Enter the connection information:

- Connection name: Your ADW Database connection name.
- Compartment: Choose compartment where Data PE is created.
- Choose Enter Database Type and select the Connection Type Oracle Database.
- Username: ADW schema name you want to connect to.
- User password secret: Create a secret that contains the username password. The password is in the schemas.json file extracted from the response.json file.

4. Click Create.

Figure 5-4 Click Create



Open SQL Worksheet

1. Log-in to the Cloud Console in your OCI tenancy. Navigate to Developer Services Database Tools SQL Worksheet.
2. Select the compartment in which your private endpoint was created.
3. Select the connection created above.

Figure 5-5 Open SQL Worksheet