Oracle® Retail Data Store Private Endpoint

Database Access Implementation Guide

Release 24.1.101.0
F91162-01
February 2024

Oracle Retail Data Store Private Endpoint Database Access Implementation Guide, Release 24.1.101.0

F91162-01

Contents

Preface

This guide describes the Implementation considerations for database access, for Retail Data Store Private Endpoint.

Audience

This guide is intended for administrators and describes the administration and implementation tasks for Oracle Retail Data Store Database Access.

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 following website https://docs.oracle.com/en/industries/retail/html

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

Oracle Retail Merchandising Cloud Services is hosted in the Oracle Cloud with the security features inherent to Oracle technology and a robust data center classification, providing significant uptime. The Oracle Cloud team is responsible for installing, monitoring, patching, and upgrading retail software.

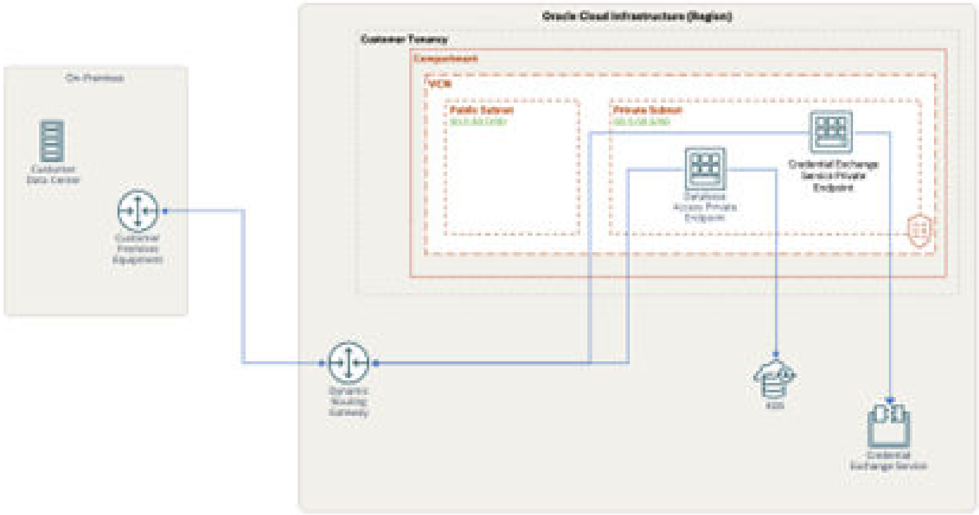
Included in the service is continuous technical support, access to software feature enhancements, hardware upgrades, and disaster recovery. The Cloud Service model helps to free customer IT resources from the need to perform these tasks, giving retailers greater business agility to respond to changing 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 Data Store (RDS) is accessible through the APEX Developer Environment as well as through custom APEX applications and services developed by the customer. Private endpoints extend access to RDS within your virtual cloud network (VCN) on Oracle Cloud Infrastructure or to other networks peered to the VCN such as your corporate network. That is, you can access RDS from hosts within your virtual cloud network (VCN) or from your on-premises network.

Figure 1-1 RDS Access through a Private Endpoint


On-Premises
Customer Data Center
Customer Premises Equipment
Oracle Cloud Infrastructure (Region)
Customer Tenancy
Compartment
VCN
Public Subnet
Private Subnet
Database Access Private Endpoint
Credential Exchange Service Private Endpoint
Dynamic Routing Gateway
RDS
Credential Exchange Service

With a private endpoint, traffic does not go over the internet. A private endpoint is a private IP address within your VCN that you can use to access a given service within Oracle Cloud Infrastructure. The service sets up the private endpoint in a subnet of your choice within the VCN. You can think of the private endpoint as 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 RDS, 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.

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 RDS, 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 RDS begin by creating a private subnet in a 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 vnics 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>
```

3
Client-side Configuration

When private endpoint setup is complete, Oracle Support provides you with details for each of your private endpoints, two per environment. To access RDS from within OCI, you need to edit the security list Ingress Rules of your private subnet. Typical values are shown in the table below.

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
TYPE AND CODE	(Blank)
ALLOWS	All
DESCRIPTION	(Optional)

4 Credentials

You still need database credentials to access RDS through your private endpoint. You obtain these credentials by using the Credential Exchange Service, a REST endpoint, through its own private endpoint.

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

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.

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>" }

Registered mailto endpoints are sent a notification email.

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, currently a single entry
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
   }
  ]
}
```

5 Supported and Unsupported Use Cases

Private endpoint does not alter your privileges. Anything you can currently do as an APEX developer, through a custom RDS service, or a custom APEX application you are able to do from a private endpoint. Any ADW feature that is currently unavailable due to lack of sufficient privileges is still unavailable when using a private endpoint. Below is a list of known supported and unsupported use cases. These use cases are not exhaustive. They are provided for your convenience.

Known Support Use Cases

- Connecting Oracle Analytics Cloud to RDS using a private access channel

Known Unsupported Use Cases

- Using RDS as a GoldenGate Source