OAC Private Access Channel

20.02.2024, Version 1

Public

Table of Contents

Introduction

The Oracle Analytics platform is a cloud-native service that provides the capabilities required to address the entire analytics process from data ingestion and modelling, through data preparation and enrichment, to visualization and collaboration without compromising security and governance. Embedded machine learning and natural language processing technologies help increase productivity and build an analytics-driven culture in organizations.

A private access channel enables a direct connection between Oracle Analytics Cloud and your private data sources. It can give Oracle Analytics Cloud access to private data sources within your virtual cloud network (VCN) on Oracle Cloud Infrastructure or other networks peered to the VCN such as your corporate network.

You can set up a private access channel for Oracle Analytics Cloud instances deployed with the **Enterprise Edition**. Private access channels aren't available to Oracle Analytics Cloud instances with the **Professional Edition**.

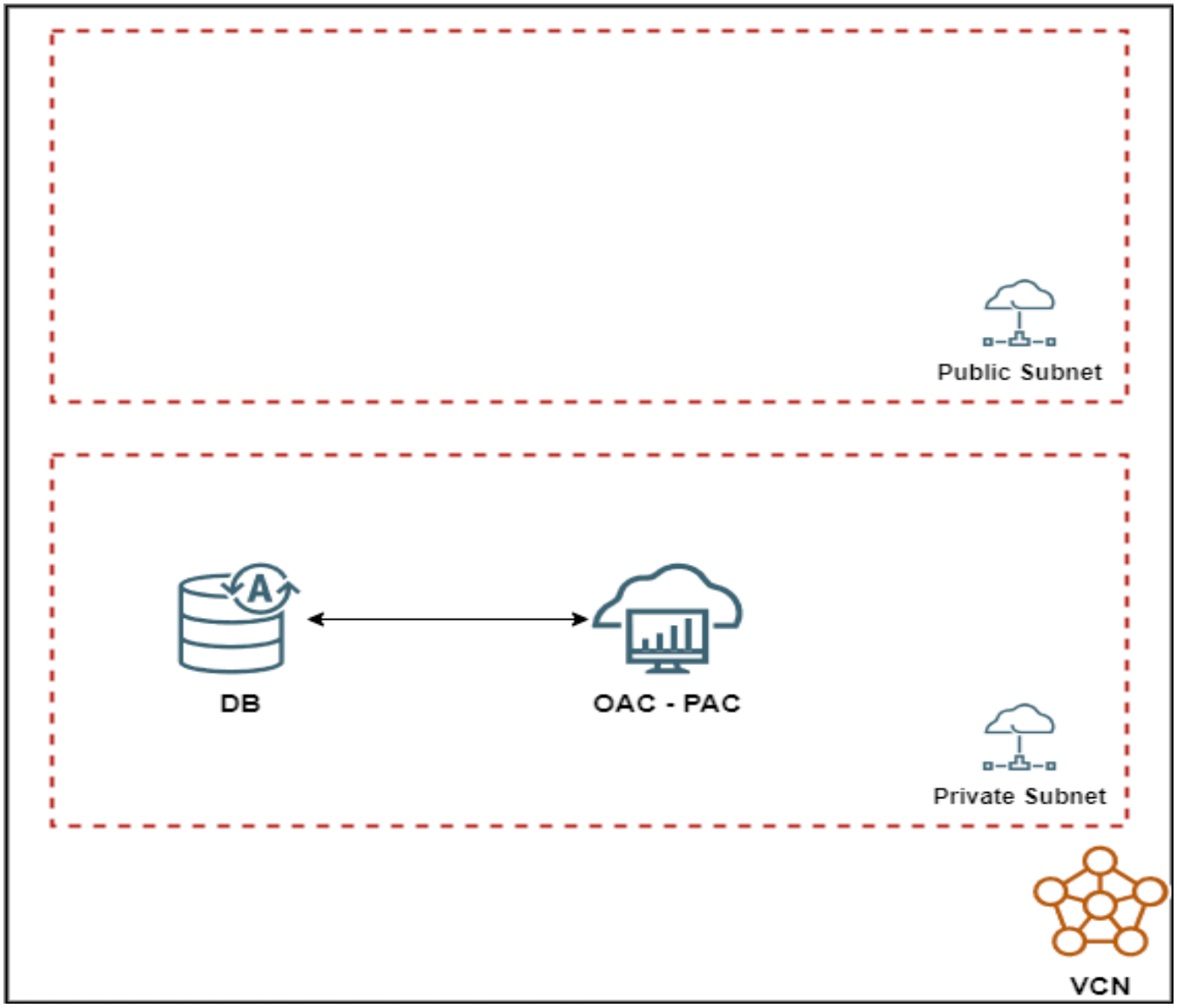
Document Scope

The scope of this document is to provide a better understanding of different scenarios where a Private Access Channel can be used. Information regarding the Supported Data Sources and Prerequisites for Private Access Channel can be found in the respective documentation pages.

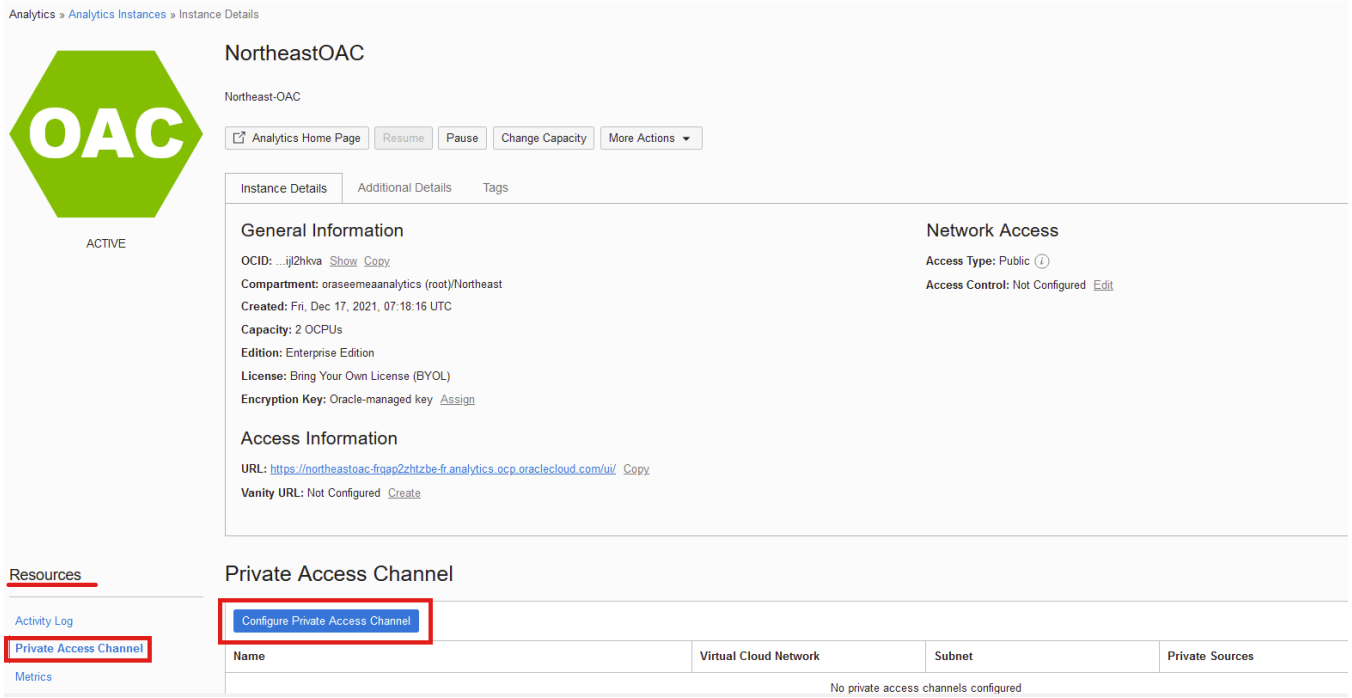
Scenarios

We will focus on the main scenarios where a Private Access Channel in Oracle Analytics Cloud is suitable, and we will try to go a step-by-step approach to achieve the final setup. To simplify things, we will use as a data source an Autonomous Database.

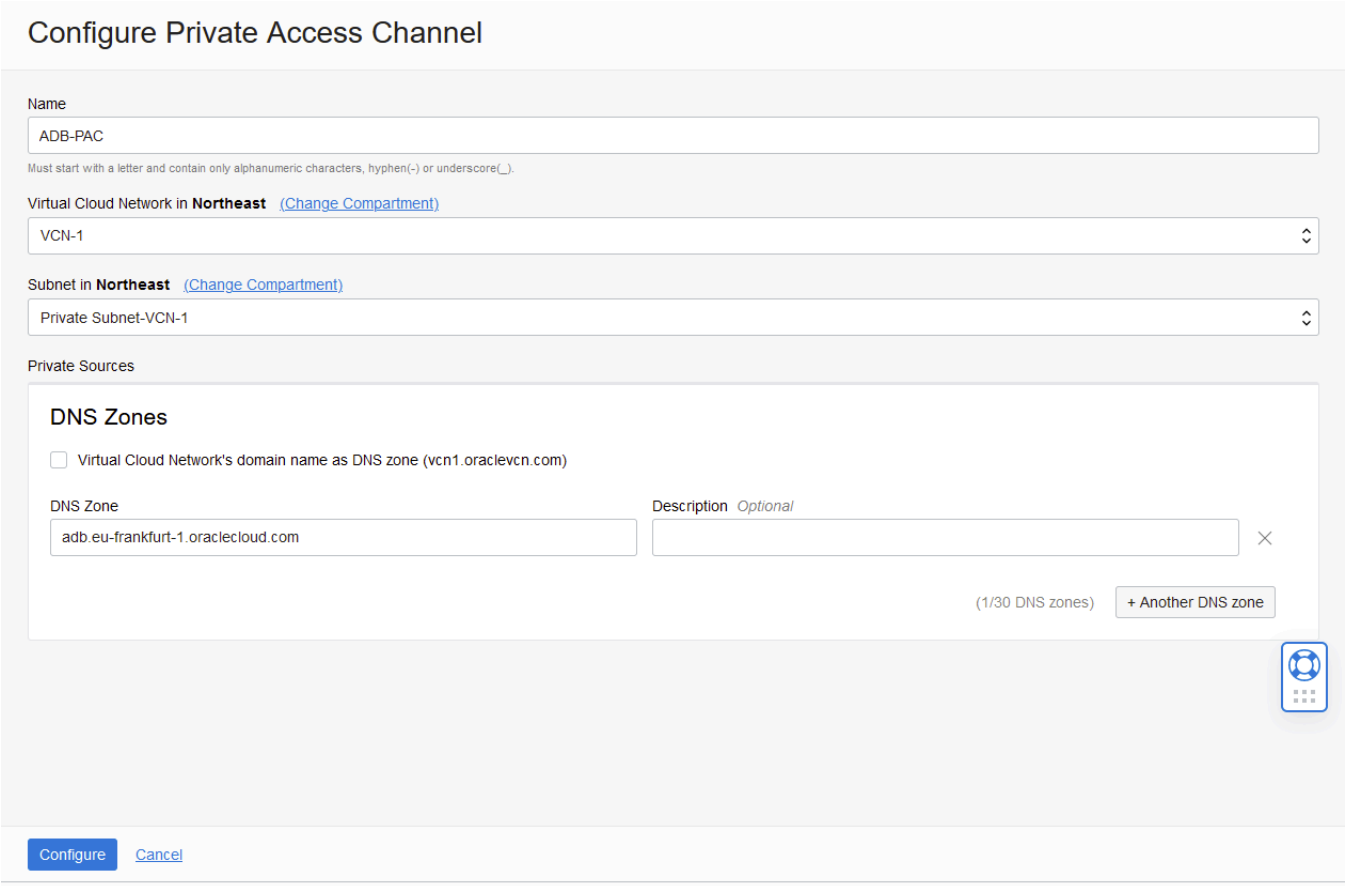
- **Data Source and Private Access Channel in the Subnet in the same VCN**



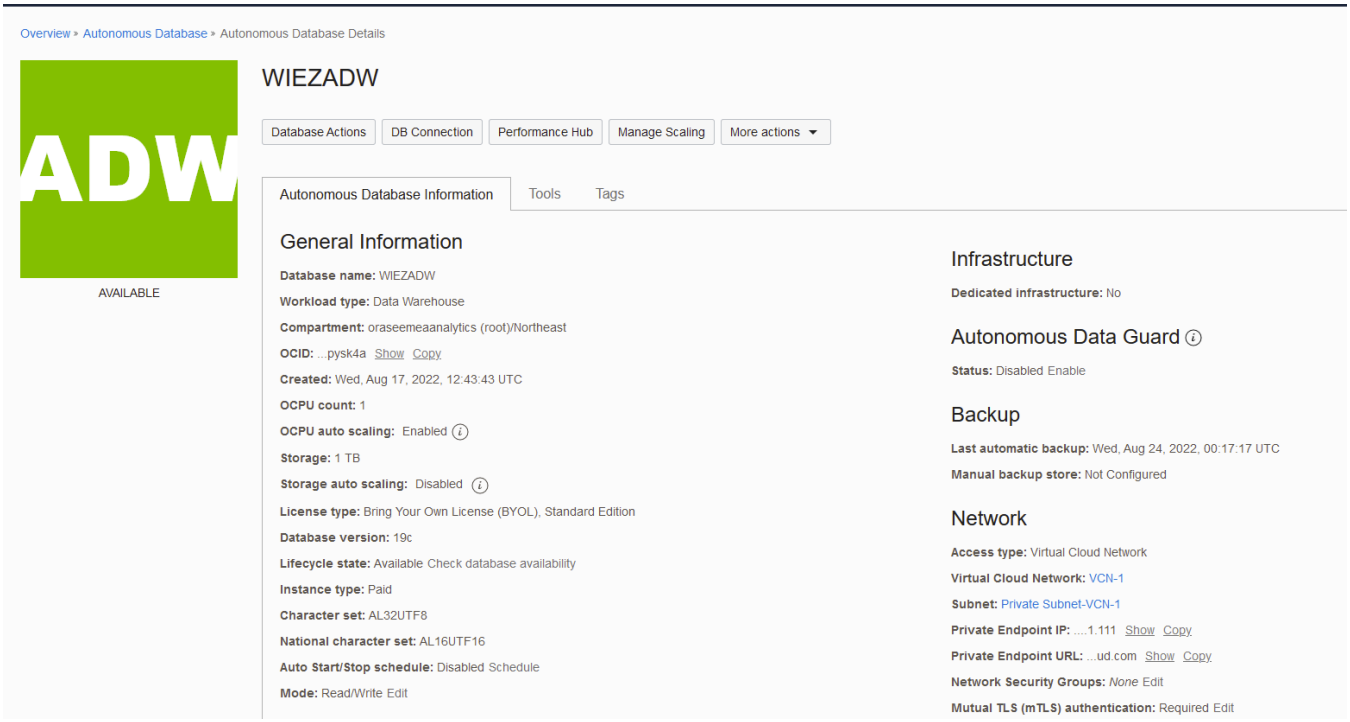
If the Oracle Analytics Cloud is provisioned with a private endpoint, when we will provision the Private Access Channel the Private Subnet is already preselected.
In the Analytics Details page, from the left side under Resources, click on Private Access Channel.



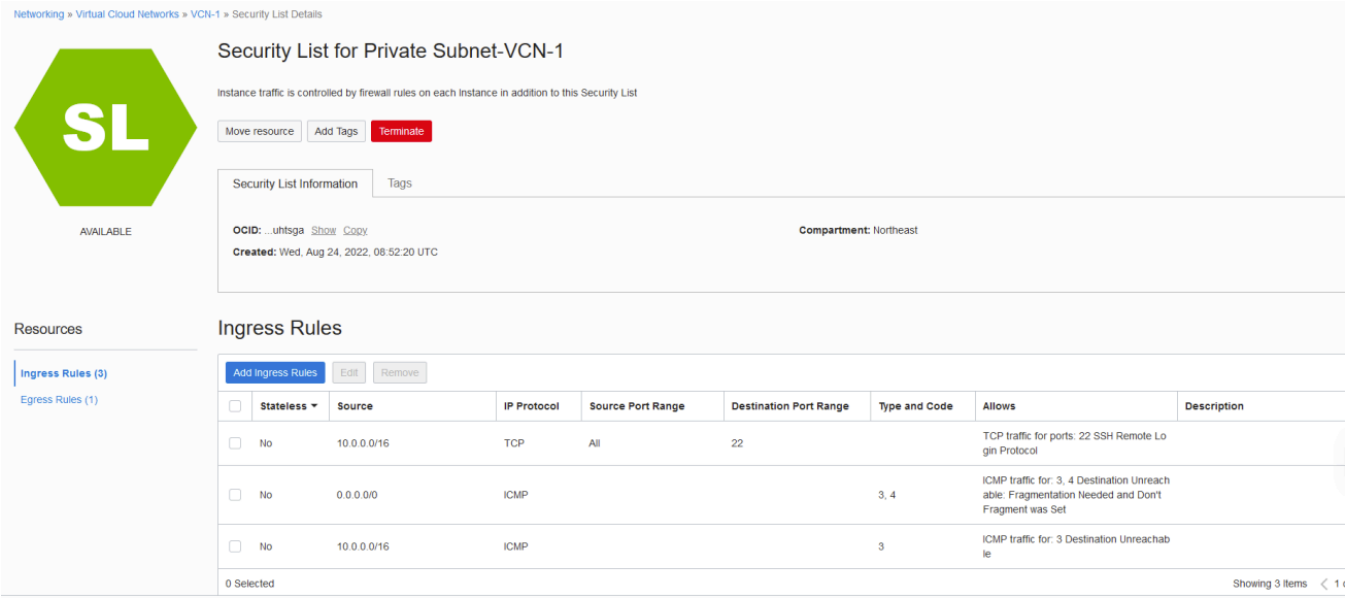
In the popup window we need to fill in the ***Name*** for the Private Access Channel, select the ***Virtual Cloud Network*** and ***Subnet*** (if the Oracle Analytics Cloud instance is provisioned with a public endpoint) and add the **DNS zone** for the Data Sources (in our case the ADB DNS name - *adb.<region>.oraclecloud.com*). After this, click on ***Configure*** and wait for the process to finish.



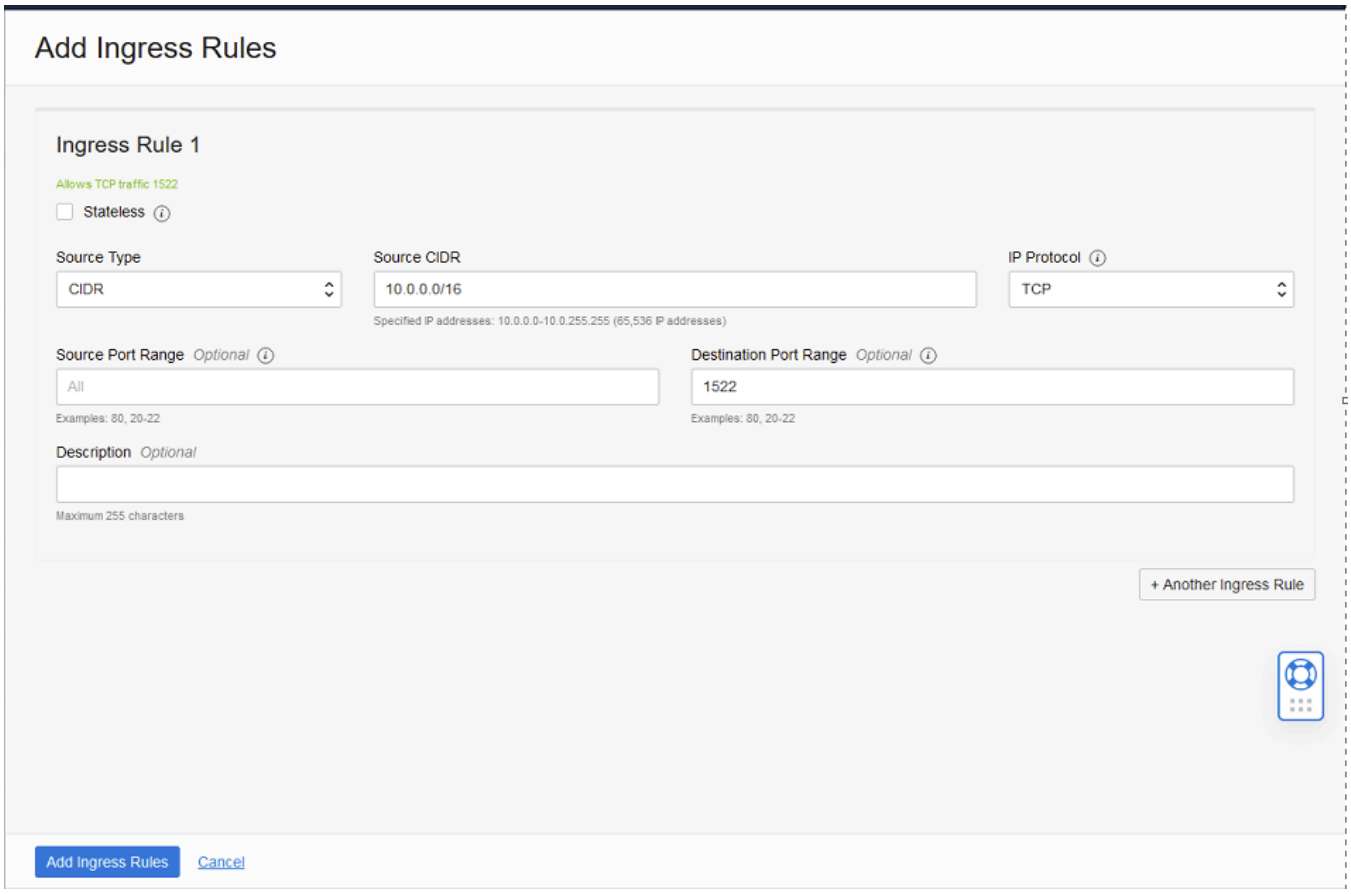
For the Data Source, check the Network configuration and download the wallet to be used when setting up the Connection in Oracle Analytics Cloud.



If the Subnet does not have an Ingress rule to open TCP connection through the Data Source port (1522 in our example is the ADB port), you need to add this in the VCN. From the left side, under *Resources - > Security Lists*. Select the Security List for *Private Subnet*, since this is where our Data Source is located, and click on ***Add Ingress Rule***.

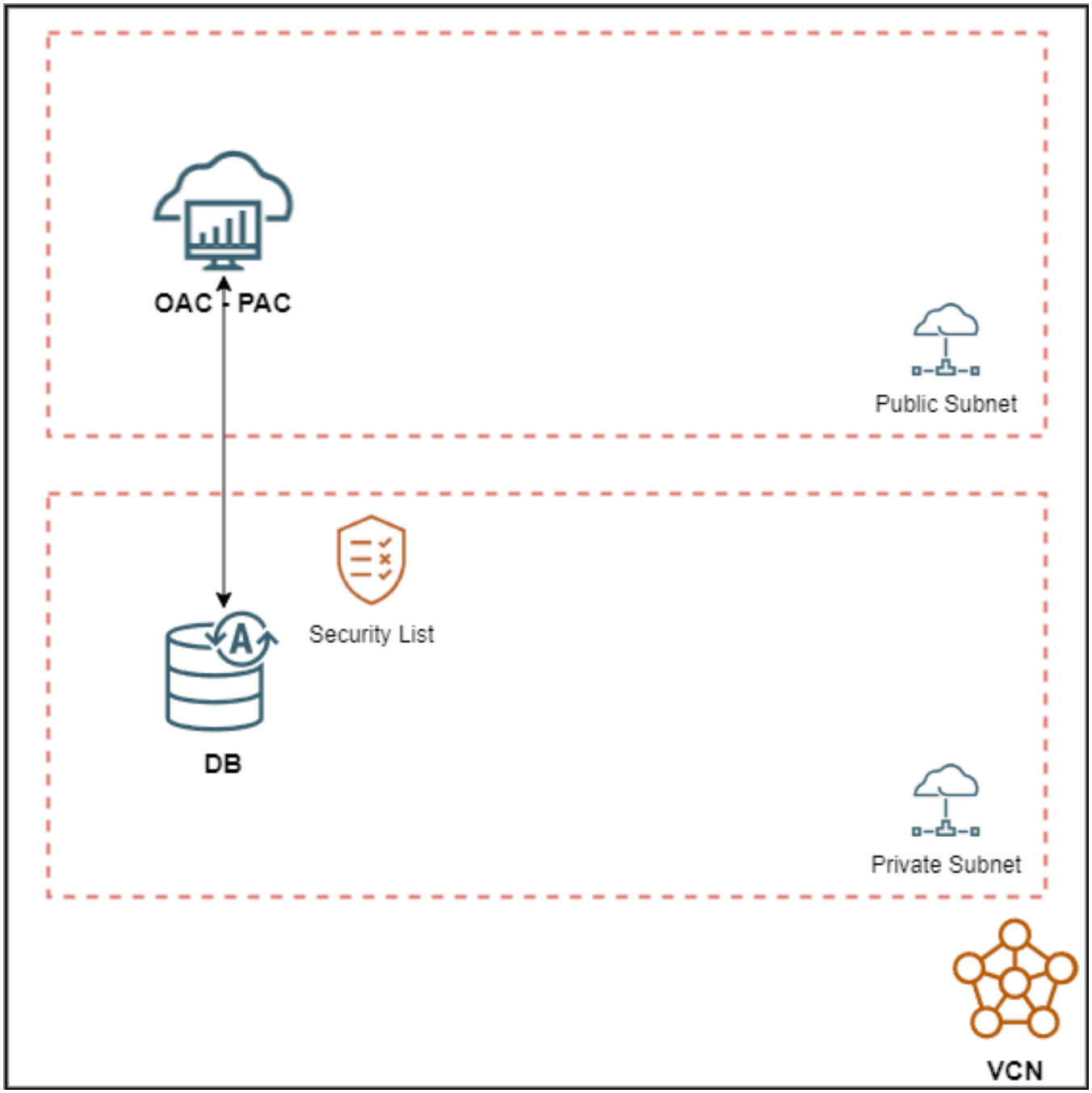


Keep ***Stateless*** option unchecked, add the ***CIDR*** of the source, leave *TCP* as the ***IP Protocol*** and leave the ***Source Port Range*** to *All* and fill in the ***Destination Port Range*** with the port of the Data Source (*1522* in our example). Submit by clicking on ***Add Ingress Rule***.

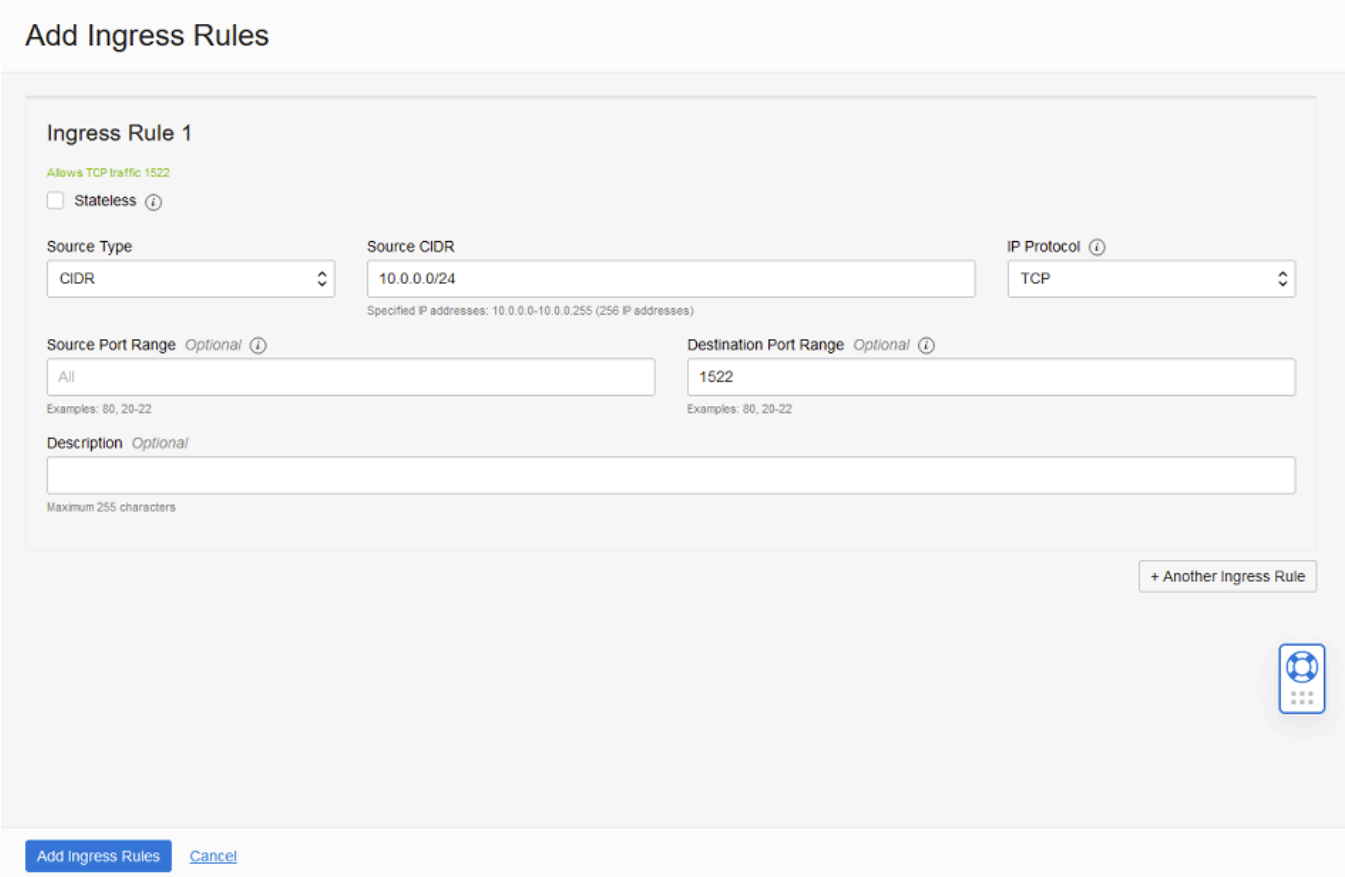


After setting this up, create the connection in Oracle Analytic Cloud to the Data Source (using the wallet in our example or the domain name setup at the PAC provisioning (e.g., if you registered the domain *companyabc.com* as a private source, set up a connection that includes this domain name).

- **Data Source and Private Access Channel in different Subnets in the same VCN**

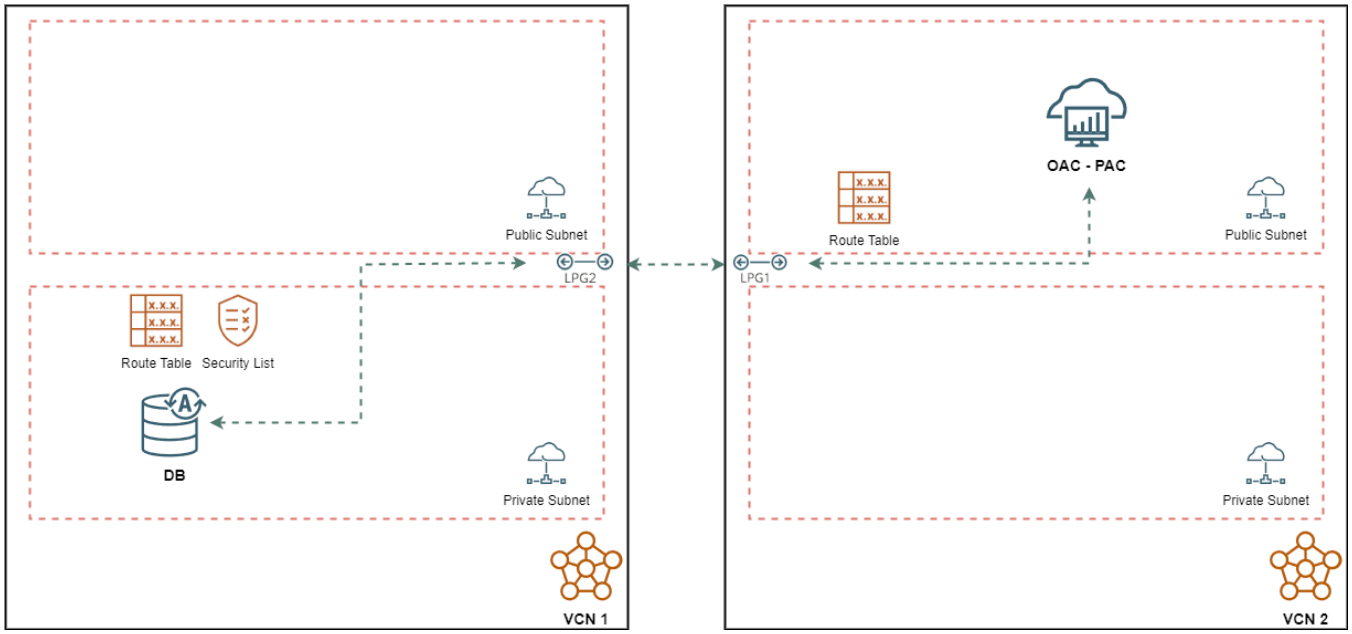


In this scenario, the Data Source is in a *Private Subnet* and the OAC - Private Access Channel is set in the *Public Subnet* of the same Virtual Cloud Network. The setup is the same as in the previous scenario, we just need to select the Public Subnet in the PAC configuration.
To be able to connect to the private Data Source from the Public Subnet, we need to open to connection between the two subnets by adding and Ingress rule in the Private Subnet.
We first need to get the ***IPv4 CIDR Block*** of the *Public Subnet*, since we will use it for the Ingress rule.
As in the above scenario, navigate to the Virtual Cloud Network, under Resources, click on the Subnets. Note down the ***IPv4 CIDR Block*** of the Public Subnet.
Then from the left side of the window, under *Resources - > Security Lists*. Select the *Security List* for *Private Subnet*, since this is where our Data Source is located, and click on ***Add Ingress Rule***.



Keep ***Stateless*** option unchecked, add the ***CIDR*** of Public Subnet, leave *TCP* as the ***IP Protocol*** and leave the ***Source Port Range*** to *All* and fill in the ***Destination Port Range*** with the port of the Data Source (*1522* in our example). Submit by clicking on ***Add Ingress Rule***.
After setting this up, create the connection in Oracle Analytic Cloud to the Data Source (using the wallet in our example or the domain name setup at the PAC provisioning (e.g., if you registered the domain *companyabc.com* as a private source, set up a connection that includes this domain name).

- **Data Source and Private Access Channel in different VCNs**



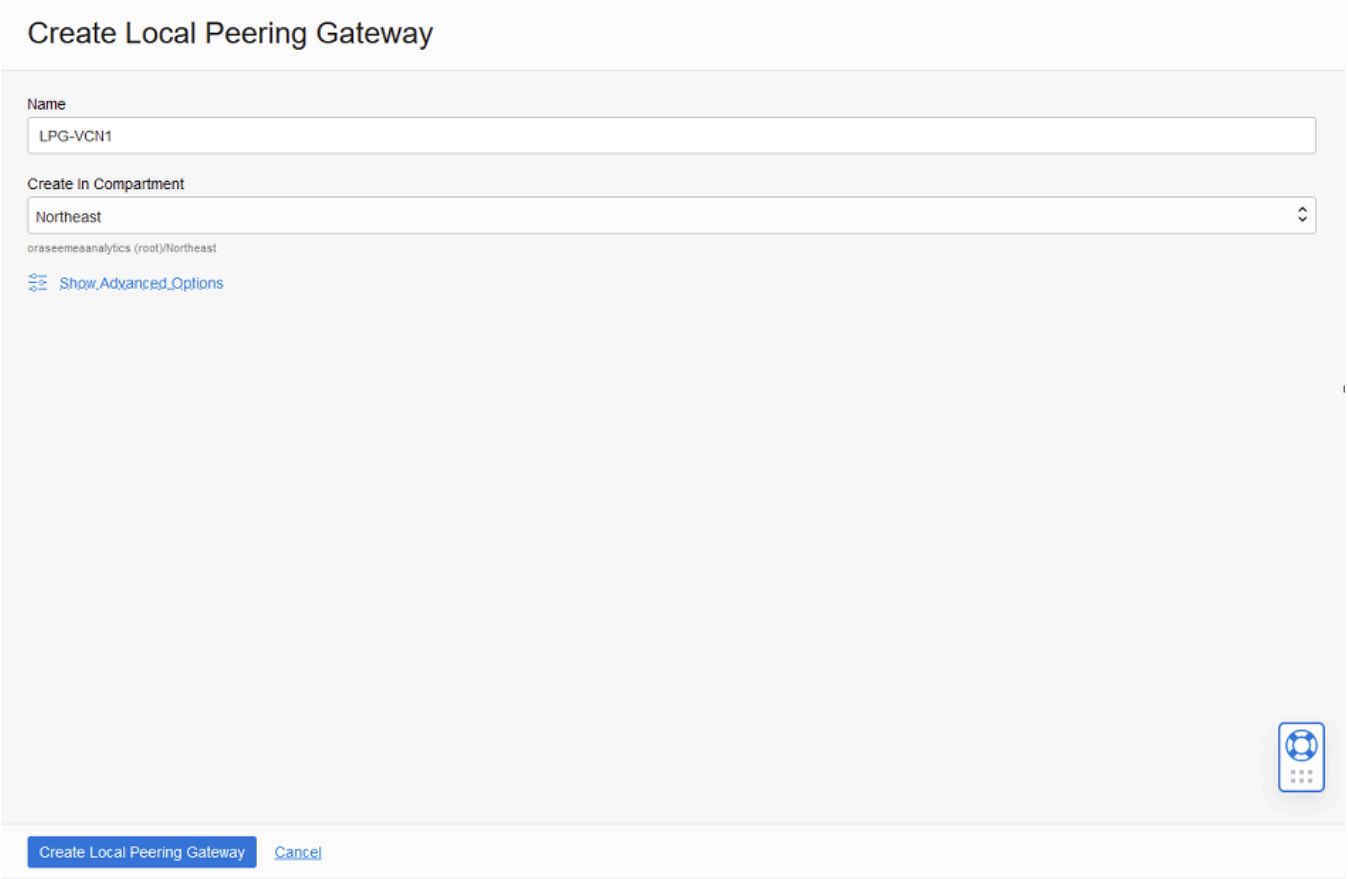
In this scenario, the Data Source and OAC - Private Access Channel are set in different VCNs in the same region. So, for the resources to communicate, we will need to create a Local VCN Peering using Local Peering Gateway.
At a high level, the Networking service components required for a local peering include:

• Two VCNs with non-overlapping CIDRs, in the same region
• A local peering gateway (LPG) on each VCN in the peering relationship.
• A connection between those two LPGs.
• Supporting route rules to enable traffic to flow over the connection, and only to and from select subnets in the respective VCNs (if wanted).
• Supporting security rules to control the types of traffic allowed to and from the instances in the subnets that need to communicate with the other VCN.
In our example, the Data Source is provisioned in a Private Subnet in VCN 1 (CIDR block 10.0.0.0/16) and the OAC – _Private Access Channel is provisioned in a Public Subnet in VCN 2 (CIDR block 192.0.0.0/16).

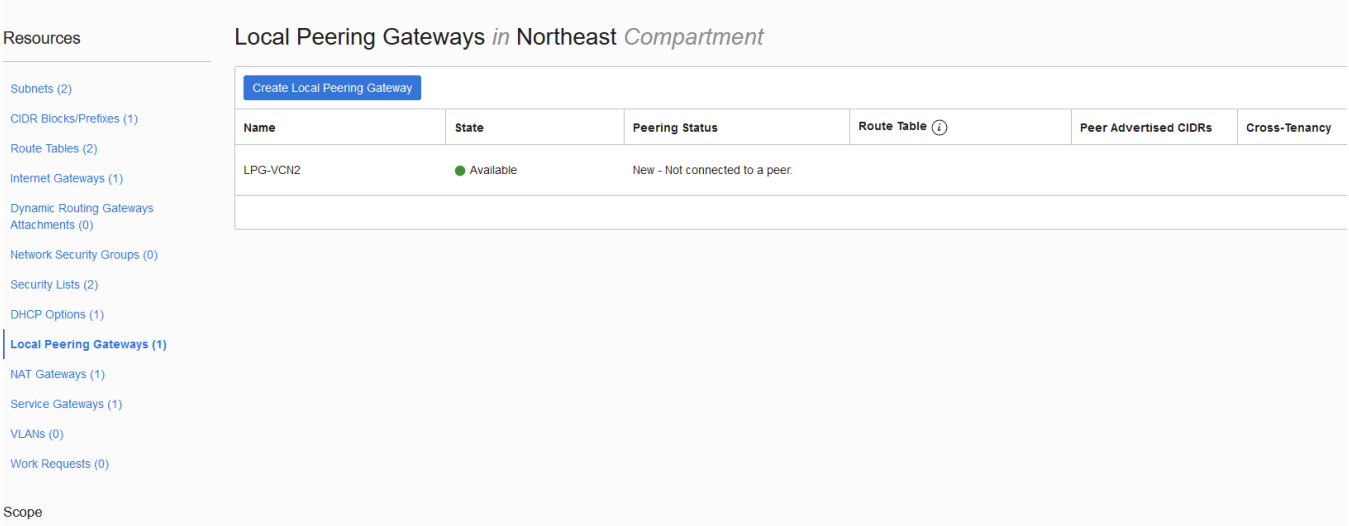
- Create the LPG

In the Console, confirm you're viewing the compartment that contains the ***VCN*** that you want to add the LPG to. Open the navigation menu, click ***Networking***, and then click ***Virtual Cloud***

Networks. Click the ***VCN*** you're interested in. Under ***Resources***, click ***Local Peering Gateways***. Click Create ***Local Peering Gateway***.

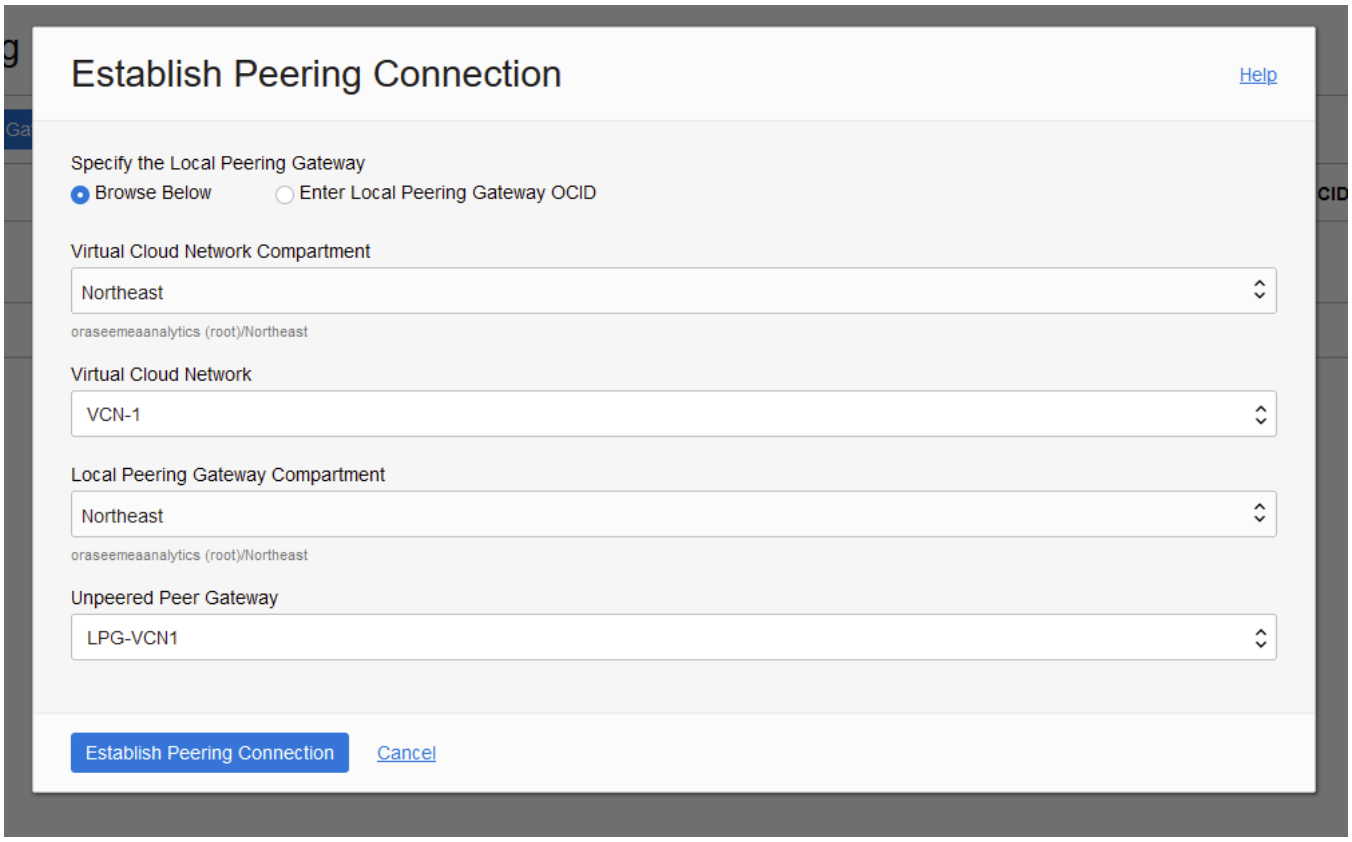


Fill in the ***Name*** of the LPG and leave the other fields with the default settings. Click ***Create Local Peering Gateway***.
Repeat the steps for the second VNC.



• Establish the connection between the two LPGs

From the Console, on the ***VCN*** where the OAC – _Private Access Channel is set, under ***Resources*** -> ***Local Peering Gateways***, click the ***Actions*** menu, and then click ***Establish Peering Connection***. Specify which LPG you want to peer with: Select Browse Below, and then select the Data Source VCN and LPG from the lists provided.



Click Establish Peering Connection.

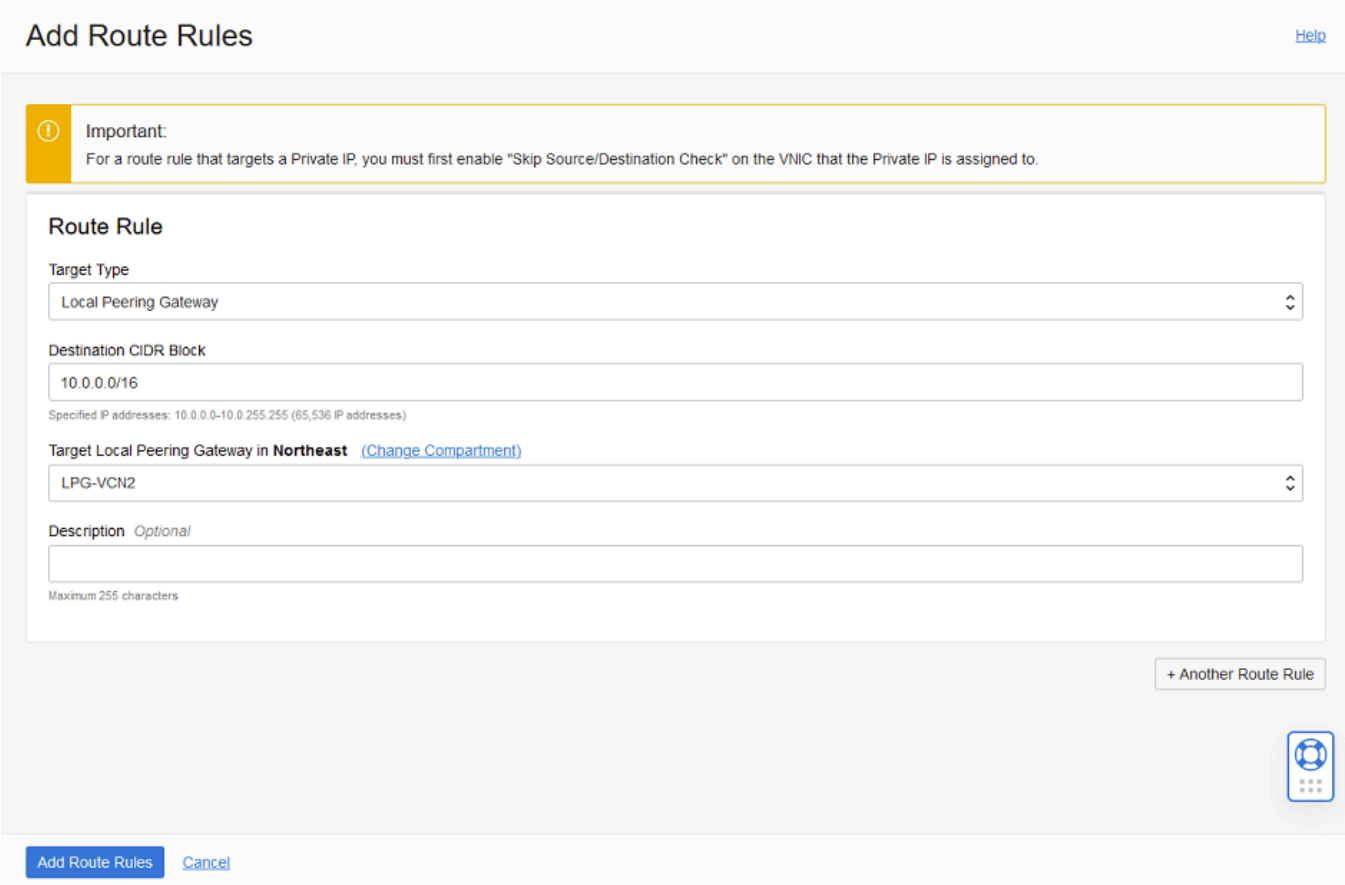
- Configure the Route Tables

Determine which subnets in your VCN need to communicate with the other VCN. In the bellow example we will add in parenthesis the example for the Route Table setup for OAC – _Private Access Channel.
Update the route table for each of those subnets to include a new rule that directs traffic destined for the other VCN's CIDR to your LPG. Open the navigation menu, click ***Networking***, and then click ***Virtual Cloud Networks***. Click the ***VCN*** you're interested in (*VCN-2*). Under ***Resources***, click ***Route***

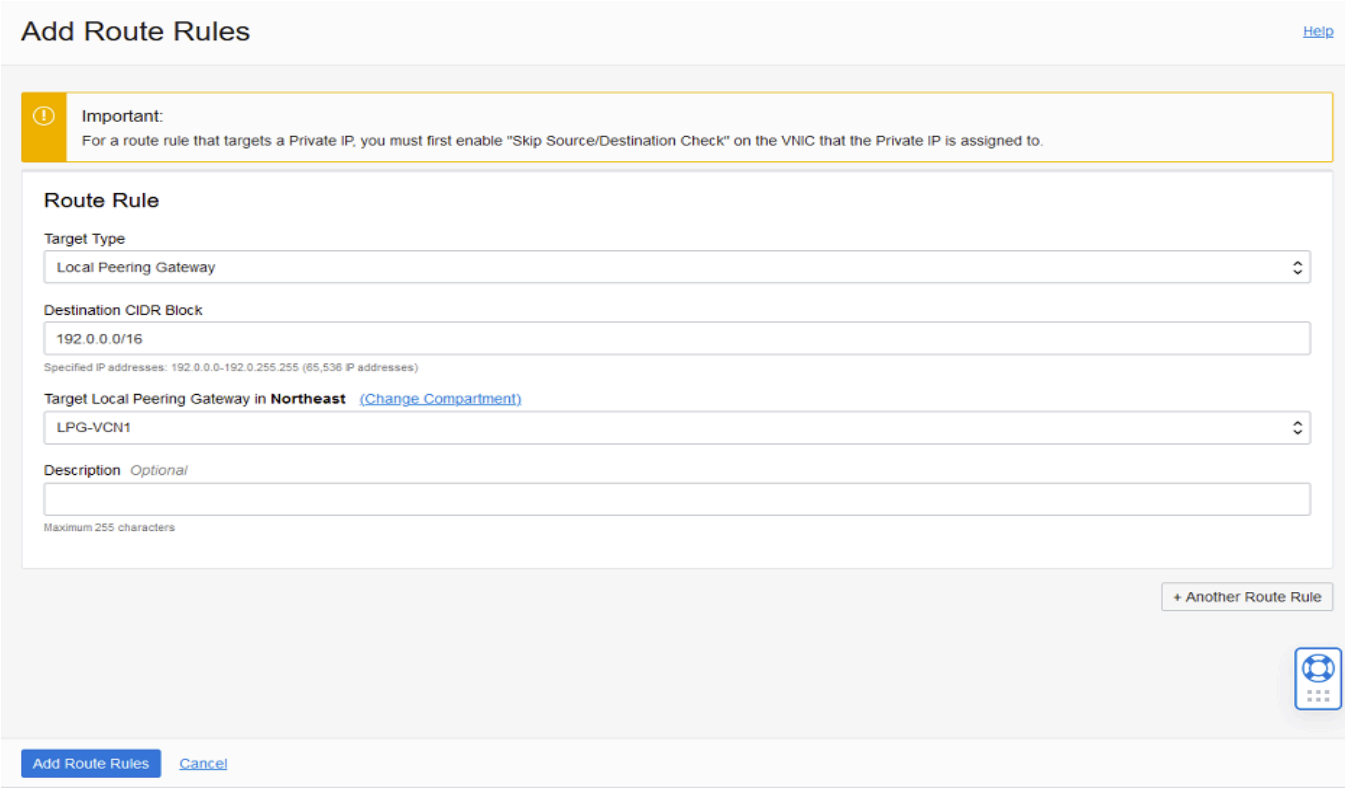
Tables. Click the route table you're interested in (*Default Route table for VCN-2*). Click ***Add Route Rule*** and enter the following:
- **Target Type**: Local Peering Gateway.

- **Destination CIDR Block**: The other VCN's CIDR block. If you want, you can specify a subnet or particular subset of the peered VCN's CIDR. (*10.0.0.0/16*)
- **Target Compartment**: The compartment where the LPG is located, if not the current compartment.
- **Target**: The LPG. (*LPG-VCN2*)
- **Description**: An optional description of the rule.

Click Add Route Rule.

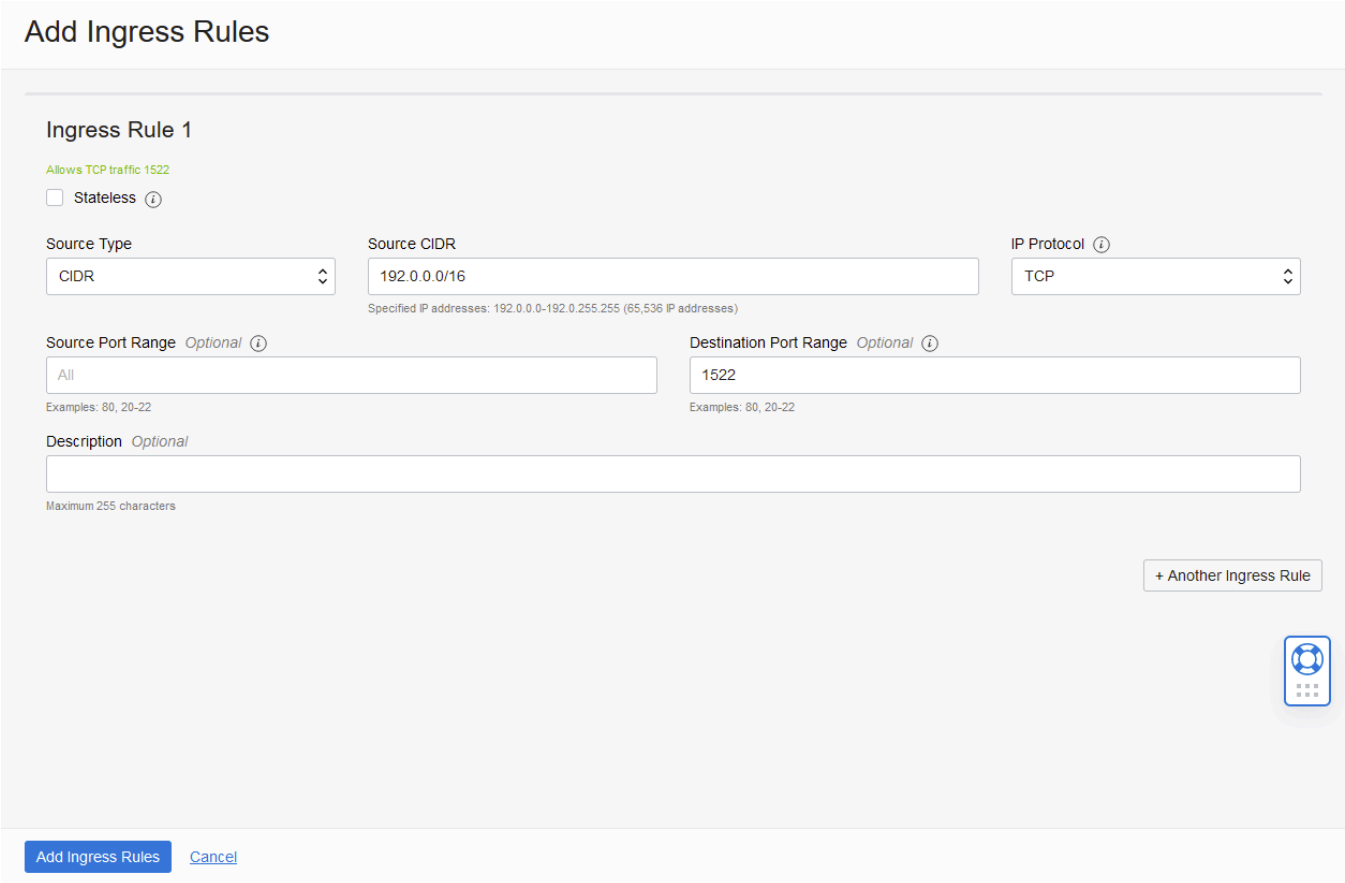


Repeat the same steps for the other VCN (*VCN-1* in our example). In the Route Table, click on the *Route Table for Private Subnet-VCN-1* and use the CIDR block for *VCN-2.*



- Configure the Security Rules

Determine which subnets in your VCN need to communicate with the other VCN.
Update the security list for each of those subnets to include rules to allow the intended egress or ingress traffic specifically with the CIDR block or subnet of the other VCN.
In the Data Source VCN (*VCN-1* in our example), click ***Security Lists***, click the security list you're interested in (*Security List for Private Subnet-VCN-1*). Under ***Resources***, click ***Ingress Rules***.
Keep ***Stateless*** option unchecked, add the ***CIDR*** of Public Subnet, leave *TCP* as the ***IP Protocol*** and leave the ***Source Port Range*** to *All* and fill in the ***Destination Port Range*** with the port of the Data Source (*1522* in our example). Submit by clicking on ***Add Ingress Rule***.

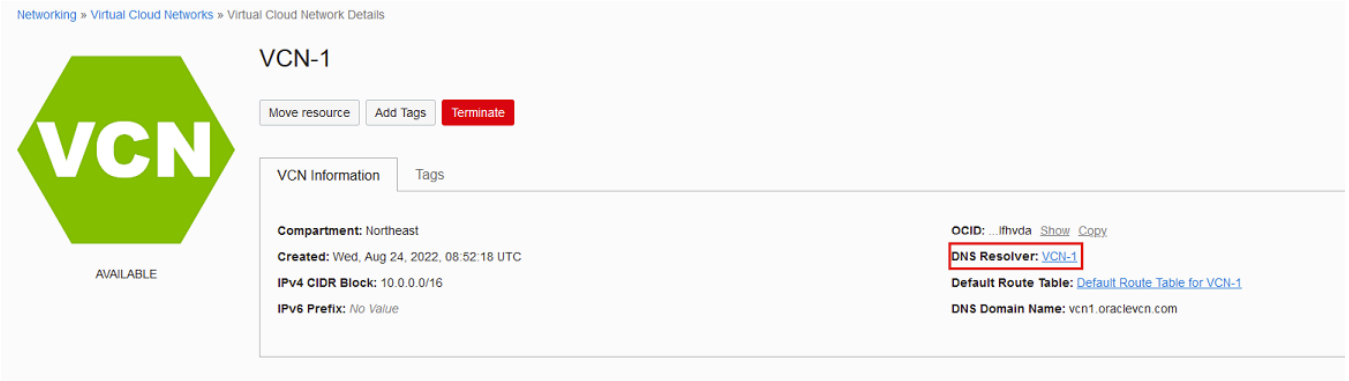


- DNS Peering Between VCNs

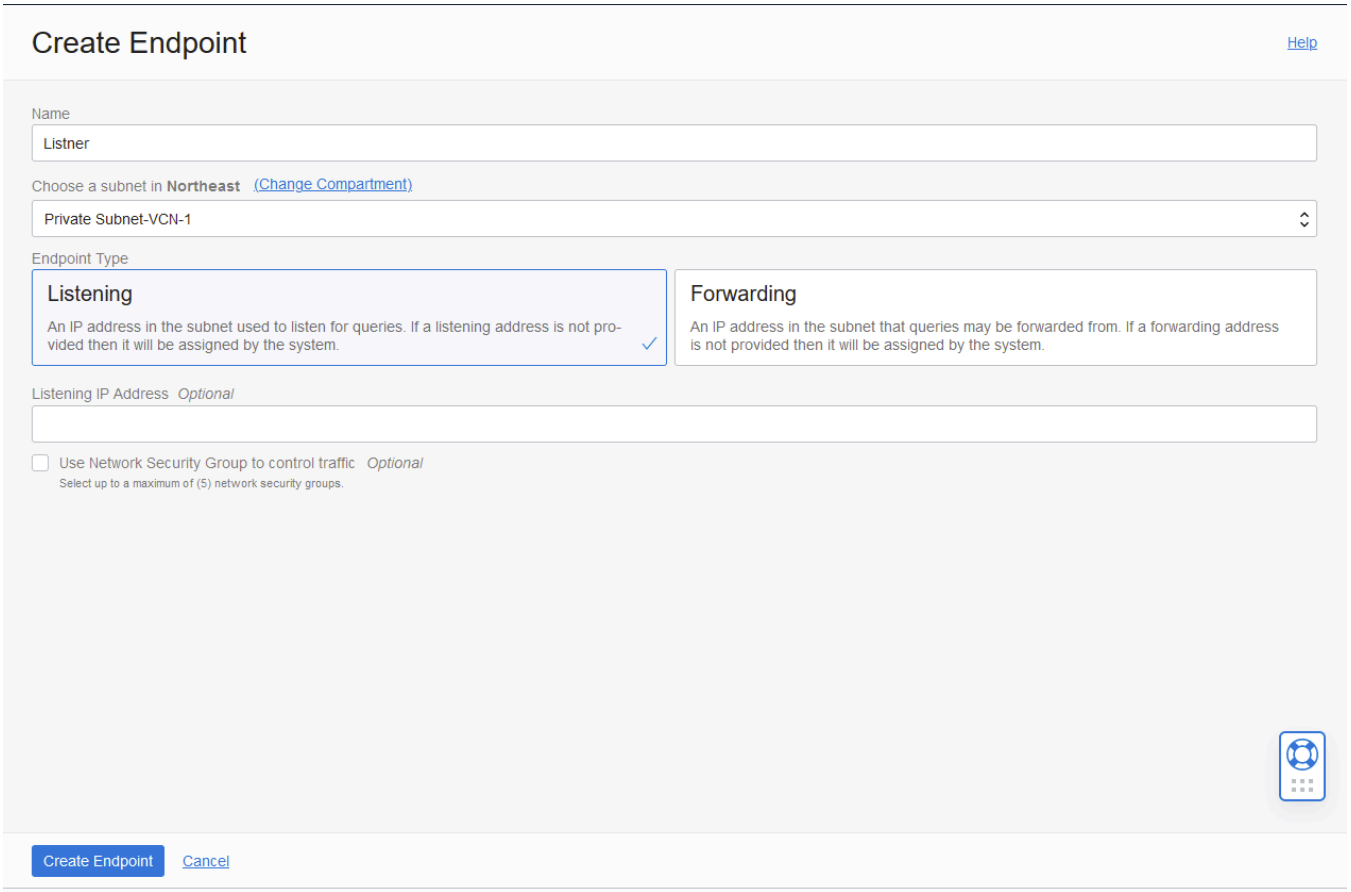
Since the OAC – _Private Access Channel works only with DNS names and not IPs and since DNS resolver is local to each VCN, the local resolver does not have any information about the resolver or hosts in any other VCN in the same region or in other region. To be able to connect to the Data Source from the other VCN, we need to configure one last step in this scenario, the DNS Peering Between VCNs. To achieve this, for every ***VCN DNS Resolver***, we will need to create two ***Endpoints*** for *Listening* and *Forwarding* and one ***Rule*** to tell the DNS resolver where to forward the request for a particular domain.

From the ***Console***, select ***Networking***, select ***Virtual Cloud Network***, select the ***VCN***. Click the ***DNS Resolver***.

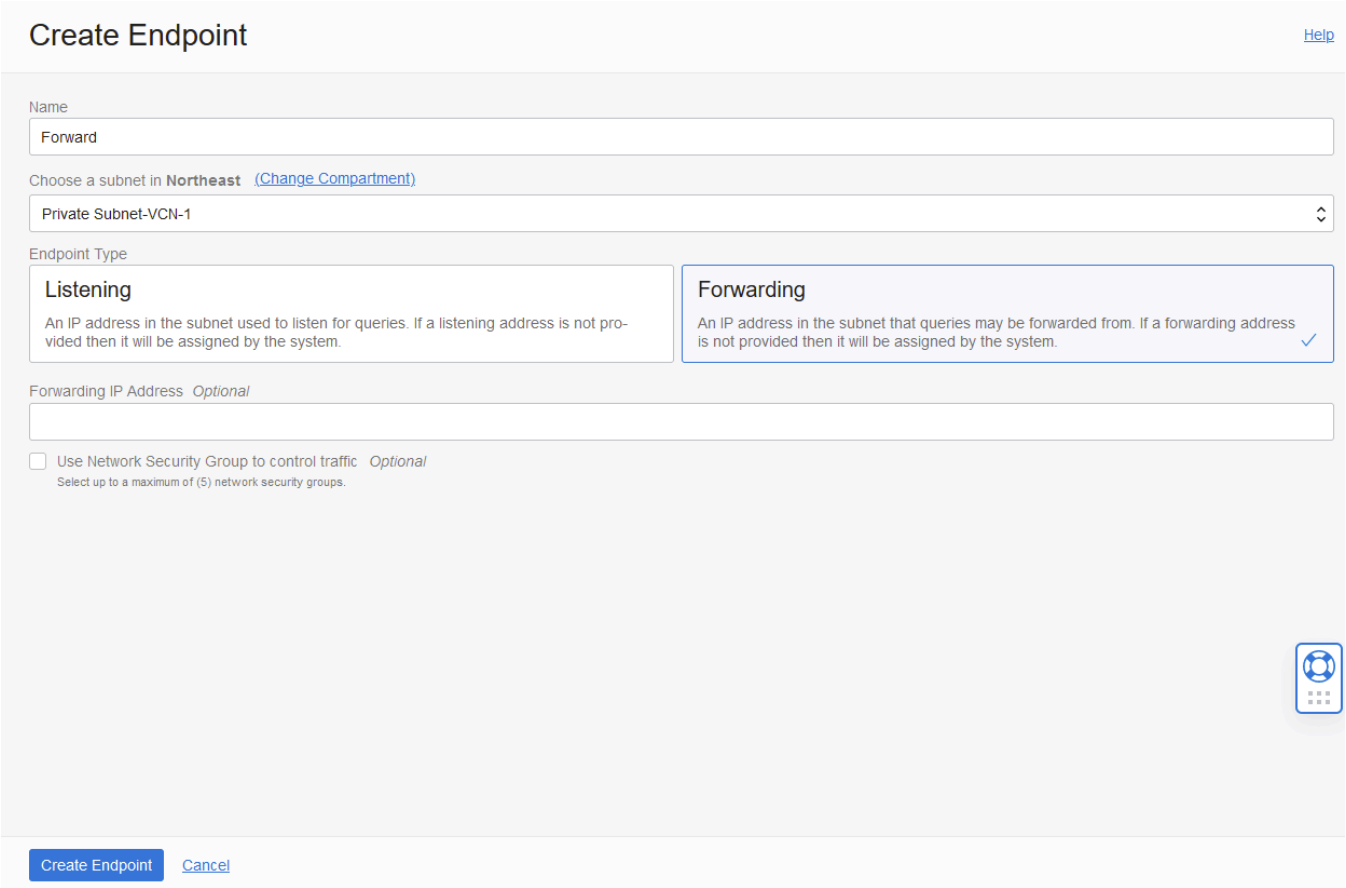
The following example is focusing on the Data Source VCN. The same steps should be applied for the OAC-Private Access Channel VCN.



Under ***Resources***, click ***Endpoints***.
- Create a **Listener** endpoint. Click ***Create Endpoint***, give it a **Name**, choose the **Subnet** (*Private Subnet – _VCN-1*, since this is where the Data Source resides), select **Endpoint Type** – *_Listening*, click ***Create Endpoint***.

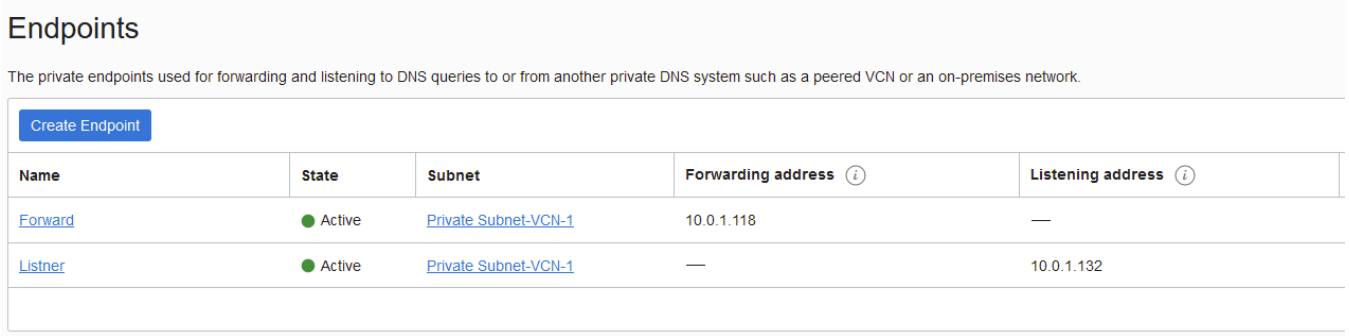


- Repeat the steps to create a **Forward** endpoint.



We will need to create the **Endpoints** for the other VCN also. Repeat the steps from above using the appropriate **Subnet** for the other **VCN**.

Data Source VCN – Endpoints



OAC-Private Access Channel – Endpoints

Now that all the resolvers have Listening and Forwarding endpoints the next step is to create some rules to forward DNS queries to the respective resolver.
On the DNS Resolver page (Data Access VCN), under ***Resources***, click on ***Rules***. Click ***Manage Rules***. We will create a rule for the OAC-Private Access Channel VCN using as a condition the Domains. From the ***Rule Condition*** drop-down, select ***Domains,*** in the Domain fill in the other VCN DNS domain name, ***Source Endpoint*** – *_Forward* (the forward endpoint that was setup previous), ***Destination IP address*** – _this will be the Listening IP address of the OAC-PAC VCN (VCN-2) DNS Resolver. Click on ***Save Changes***.

Rules

Queries that match the rule condition or conditions will be handled by the rule. If no rules match, the query will be resolved from internet DNS.

Manage Rules | Remove

Order	Rule Condition	Client CIDR Blocks/Domains	Rule Action	Source Endpoint	Destination IP Address
1	Domains	vcn2.oraclevcn.com	Forward	Forward	192.0.0.66

0 Selected

Following the same steps, we will setup a ***Rule*** at the DNS Resolver for the OAC – _Private Access Channel level. The same ***Rule Condition*** will be selected, and the ***Domain*** will be the Data Source DNS name (*adb.eu-frankfurt-1.oraclecloud.com*, in our example).

Rules

Queries that match the rule condition or conditions will be handled by the rule. If no rules match, the query will be resolved from internet DNS.

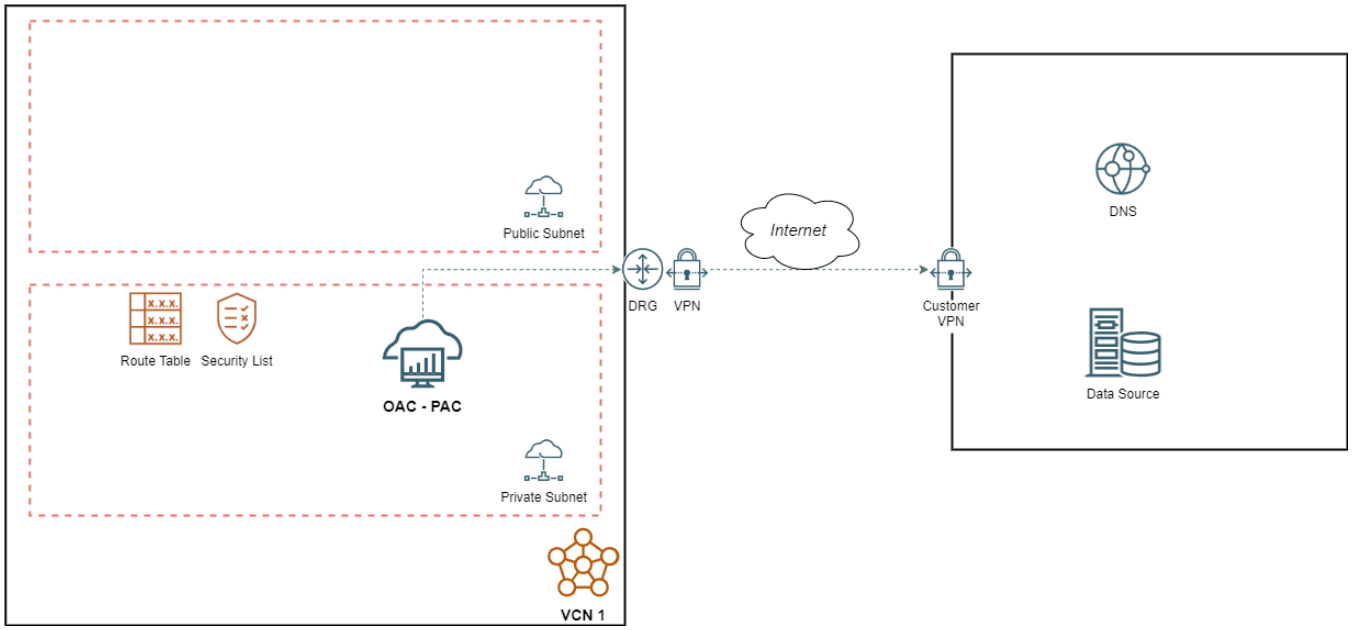
Manage Rules | Remove

Order	Rule Condition	Client CIDR Blocks/Domains	Rule Action	Source Endpoint	Destination IP Address
1	Domains	adb.eu-frankfurt-1.oraclecloud.com	Forward	FWD	10.0.1.132

0 Selected

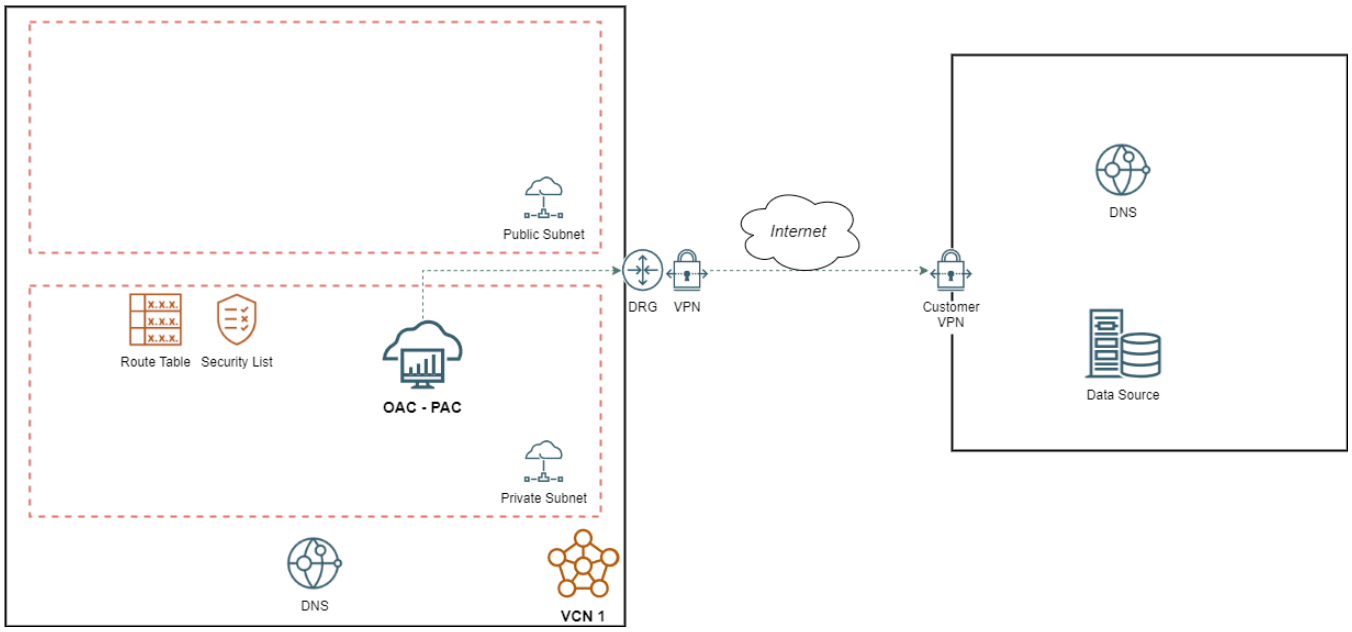
After setting this up, create the connection in Oracle Analytic Cloud to the Data Source (using the wallet in our example or the domain name setup at the PAC provisioning (e.g., if you registered the domain *companyabc.com* as a private source, set up a connection that includes this domain name)).

- **Data Source in corporate network peered to an Oracle Cloud Infrastructure VCN**



In this scenario, the Data Source resides in a corporate network and the OAC-Private Access Channel in an Oracle Cloud Infrastructure VCN. The steps to make the connections between them is similar with the ones from the previous scenario, with the difference that we will not setup an LPG connection and instead we will do a Dynamic Routing Gateway and using a Virtual Private Network to connect securely to the corporate network.
The steps to setup the Dynamic Routing Gateway and attached to the VCN where the OAC-Private Access Channel reside can be found here.
After setting up the connection, as in the previous scenario, we will need to do the DNS peering. On-prem DNS server also has a Listening and Forwarding endpoint that can be used to peer with the DNS resolver in OCI, the process is like what was implemented in the previous use case for VCNs within OCI.
After setting this up, create the Private Access Channel using the DNS name used in the DNS peering setup and check that everything works by creating a connection in Oracle Analytic Cloud to the Data Source (e.g., if you registered the domain *companyabc.com* as a private source, set up a connection that includes this domain name).

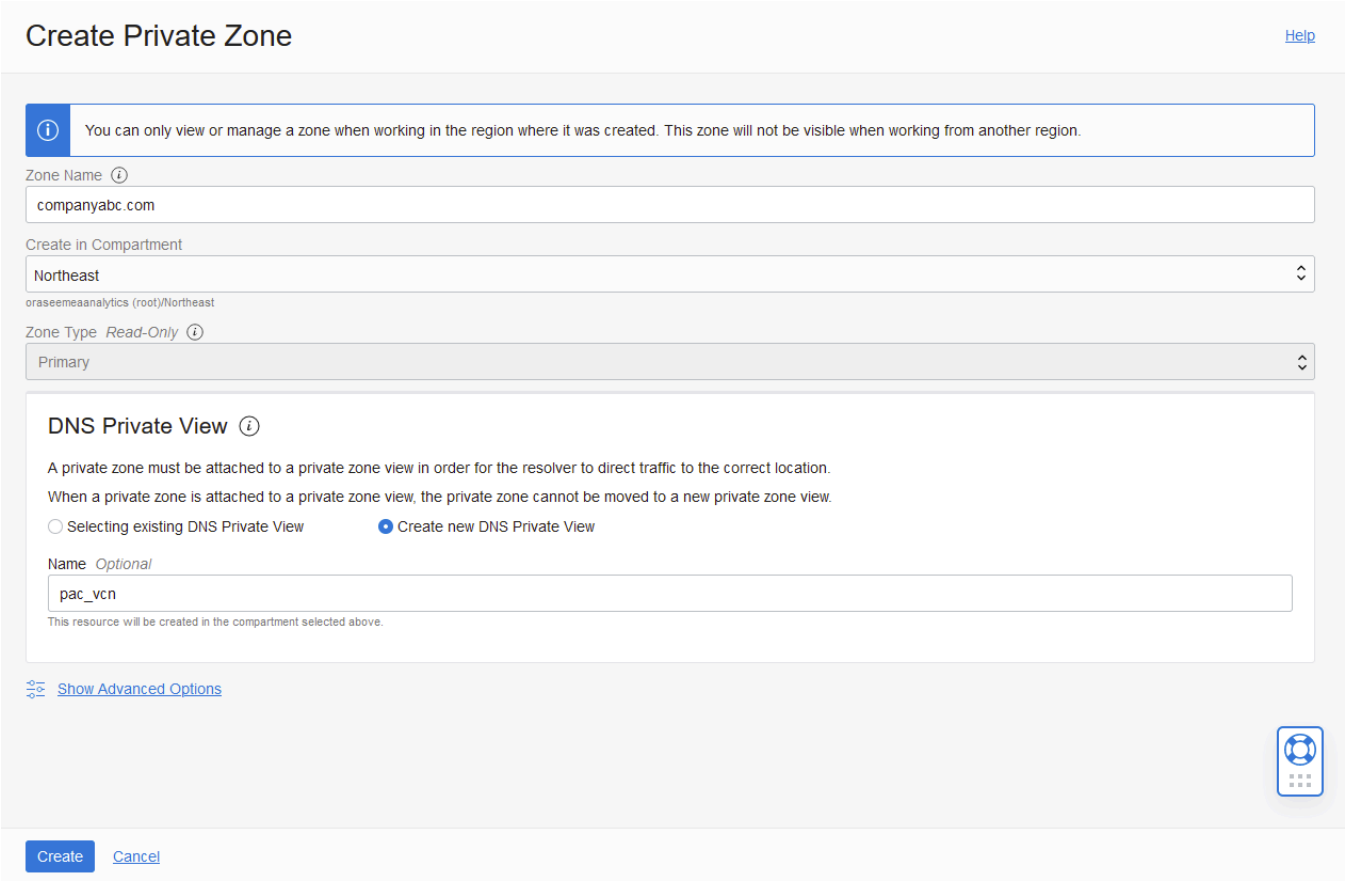
- **Data Source in corporate network (accessible only by IP address) peered to an Oracle Cloud Infrastructure VCN**



Similar with Scenario 4, the only difference is that the Data Source from the corporate network is accessible only by the IP address. In this case, after setting the proper connectivity between the corporate network and Oracle Cloud Infrastructure VCN, we need to create a Private DNS Zone, Views, and Resolvers.

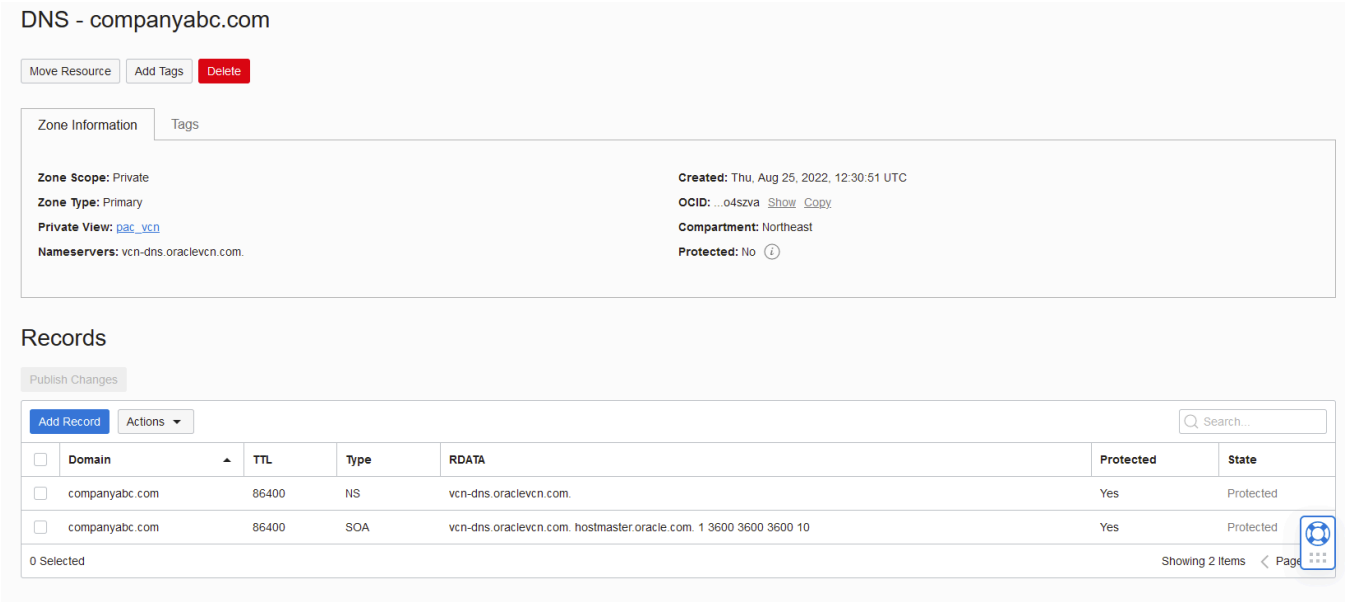
- Create Custom Private Zone

From the OCI services menu, click ***DNS Management*** under ***Networking***. Then, click on ***Zones***, and then ***Private Zones***. You should see the private zones that are created automatically for your subnets. Click on ***Create Zone*** and create zone *companyabc.com*. Select ***Create new DNS Private View*** and name it *pac_vcn*.

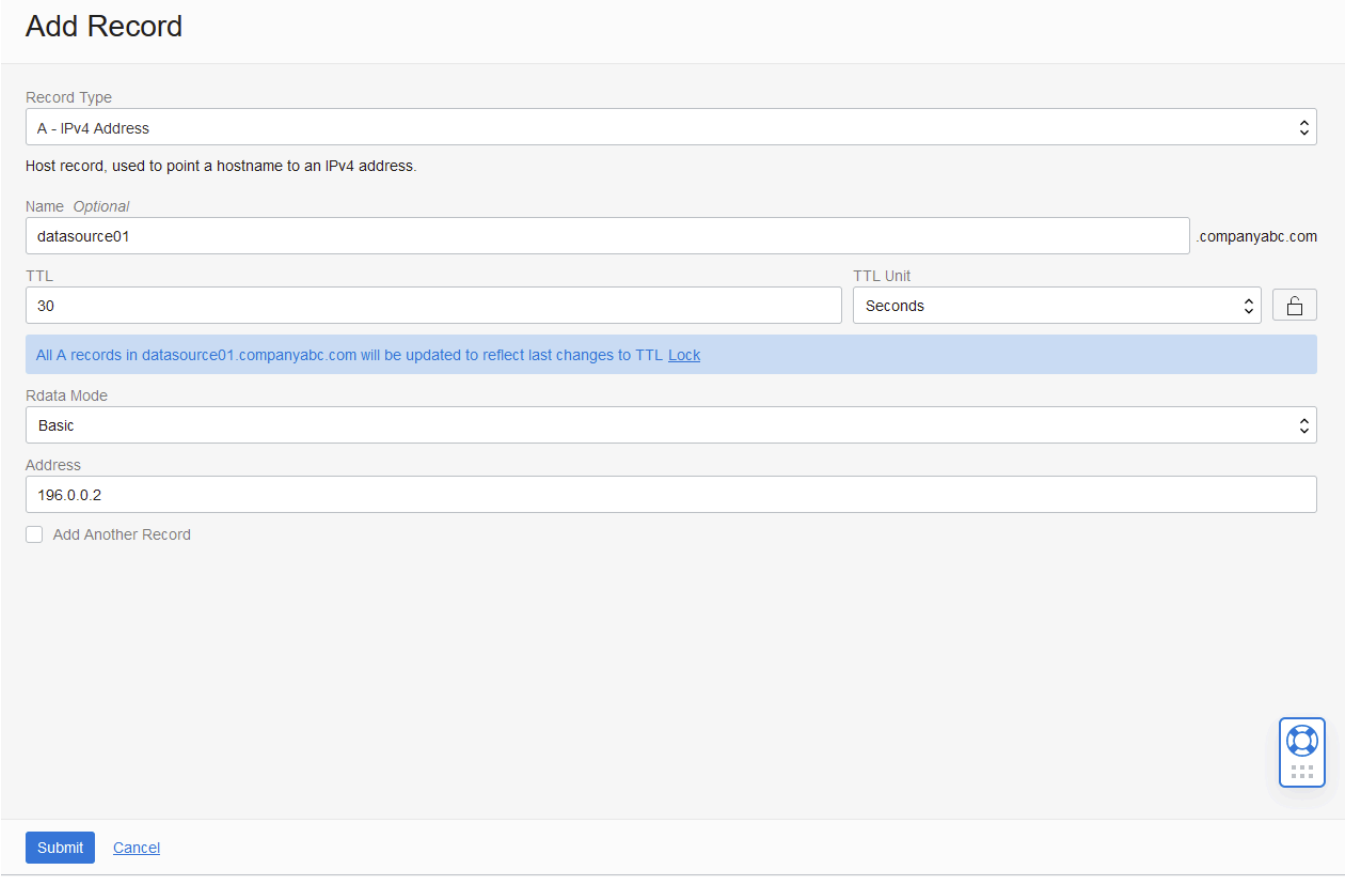


- Create A record in *companyabc.com*

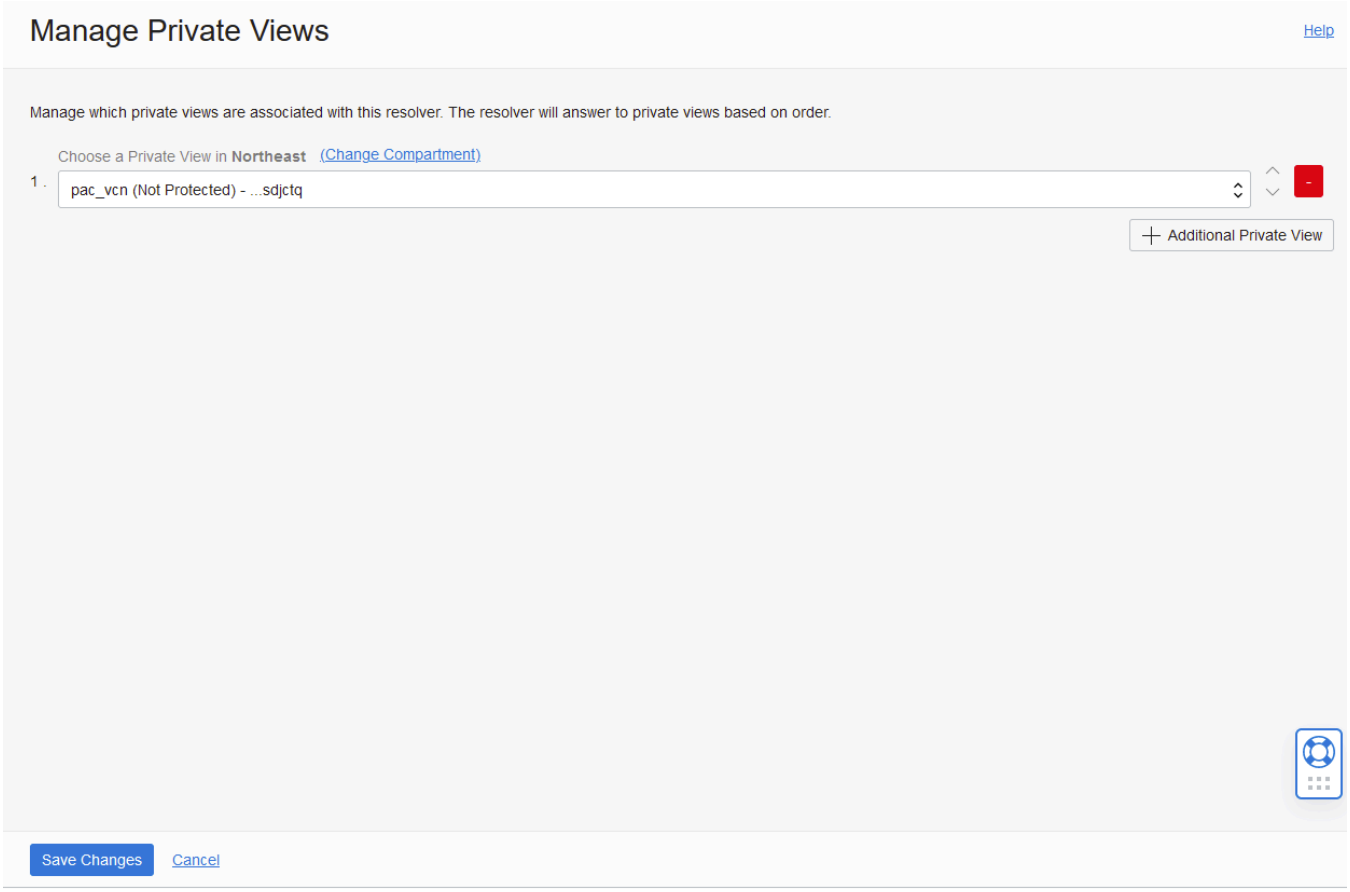
After the zone is created, the details page will be presented. We need to add an A record to map the IP address of our Data Source.



Under ***Records***, click on ***Add Record.*** For the ***Record Type***, select ***A - IPv4 Address***, add a ***Name,*** Set ***TTL*** to 30 seconds. If the lock icon is engaged, click on it to disengage and enable the field. Set ***Address*** to your Data Source IP (in our example we will use 196.0.0.2). Click ***Submit***.



Click on ***Publish Changes*** and then ***Publish Changes*** again in the new window.
Navigate to the DNS Resolver option for your VCN where PAC resides and associate the private DNS VCN you created.
In ***Virtual Cloud Networks*** under ***Networking,*** Click on *VCN-1* from the VCNs' list. Locate the DNS Resolver and click on *vcn-1.* Click on ***Manage Private Views,*** select *pac_vcn* under Choose a ***Private View in private-DNS.*** Save.



After this step, we need to configure a DNS forwarder in the private DNS resolver to forward corporate hostname resolution to your company's DNS server (as we did in the previous scenarios). Create/update the Private Access Channel using the DNS name used in the DNS peering setup and check that everything works by creating a connection in Oracle Analytic Cloud to the Data Source (e.g., if you registered the domain *companyabc.com* as a private source, set up a connection that includes this full qualified domain name: *datasource01.companyabc.com*).