

OAC Private Access Channel

20.02.2024, Version 1
Copyright © 2024, Oracle and/or its affiliates
Public

Table of Contents

Introduction.....3

- Data Source and Private Access Channel in the Subnet in the same VCN.....4**
- Data Source and Private Access Channel in different Subnets in the same VCN.....9**
- Data Source and Private Access Channel in different VCNs 11**
- Data Source in corporate network peered to an Oracle Cloud Infrastructure VCN 20**
- Data Source in corporate network (accessible only by IP address) peered to an Oracle Cloud Infrastructure VCN..... 21**

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**.

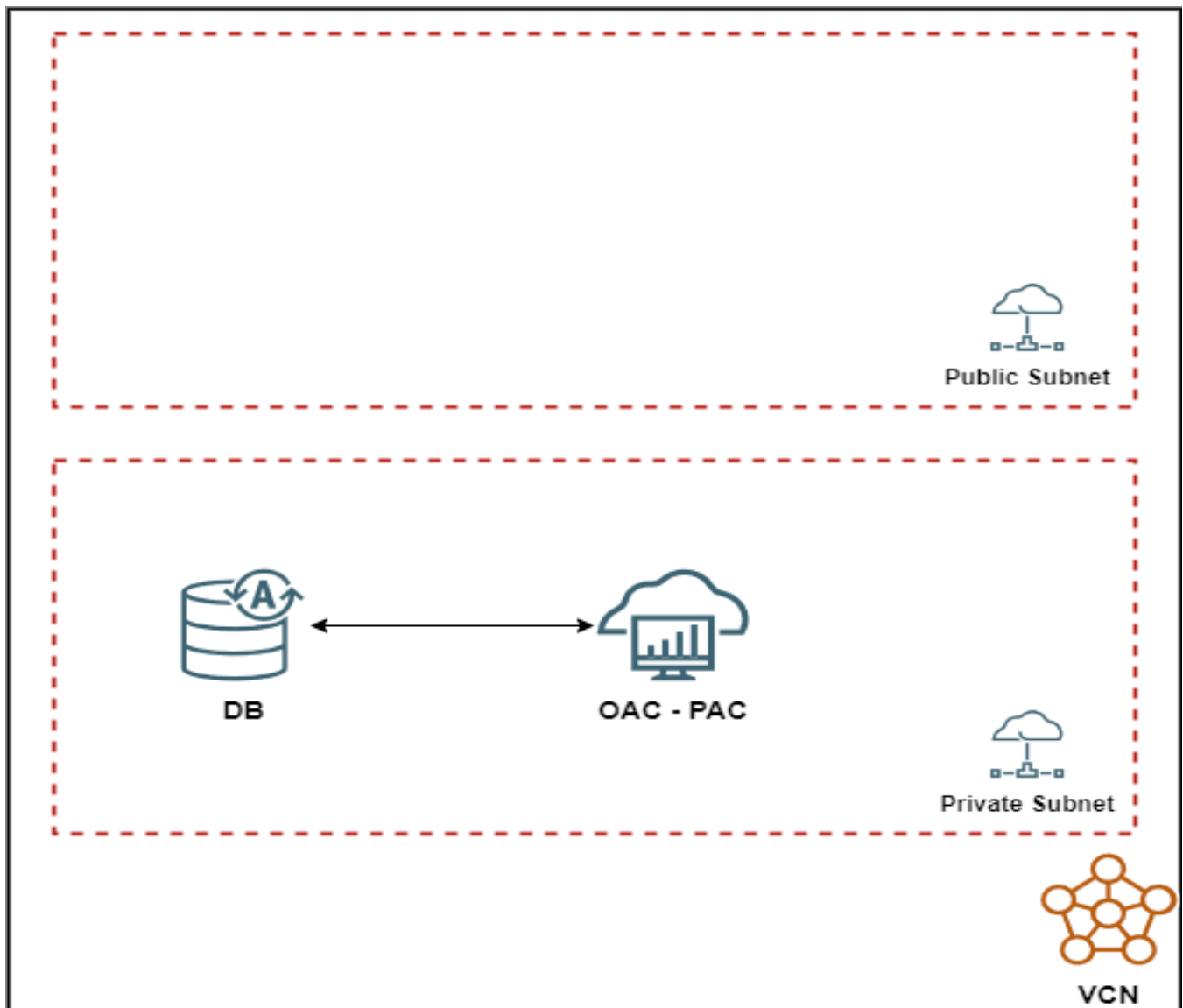
Document Scope

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.



ACTIVE

NortheastOAC

Northeast-OAC

[Analytics Home Page](#) [Resume](#) [Pause](#) [Change Capacity](#) [More Actions](#)
[Instance Details](#) [Additional Details](#) [Tags](#)

General Information

OCID: ...ij2hkva [Show](#) [Copy](#)
 Compartment: oraseemeaanalytics (root)/Northeast
 Created: Fri, Dec 17, 2021, 07:18:16 UTC
 Capacity: 2 OCPUs
 Edition: Enterprise Edition
 License: Bring Your Own License (BYOL)
 Encryption Key: Oracle-managed key [Assign](#)

Network Access

Access Type: Public ⓘ
 Access Control: Not Configured [Edit](#)

Access Information

URL: <https://northeastoac-fraap2zhtzbe-fr.analytics.ocp.oraclecloud.com/ui/> [Copy](#)
 Vanity URL: Not Configured [Create](#)

Resources

[Activity Log](#)[Private Access Channel](#)[Metrics](#)

Private Access Channel

[Configure Private Access Channel](#)

Name	Virtual Cloud Network	Subnet	Private Sources
No private access channels configured			

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.

Configure Private Access Channel

Name

ADB-PAC

Must start with a letter and contain only alphanumeric characters, hyphen(-) or underscore(_).

Virtual Cloud Network in **Northeast** [\(Change Compartment\)](#)

VCN-1

Subnet in **Northeast** [\(Change Compartment\)](#)

Private Subnet-VCN-1

Private Sources

DNS Zones

☐ Virtual Cloud Network's domain name as DNS zone (vcn1.oraclevcn.com)


DNS Zone

adb.eu-frankfurt-1.oraclecloud.com

Description *Optional*

×

(1/30 DNS zones) [+ Another DNS zone](#)



Configure

Cancel

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

Overview > [Autonomous Database](#) > Autonomous Database Details

ADW

AVAILABLE

WIEZADW

Database Actions

DB Connection

Performance Hub

Manage Scaling

More actions

Autonomous Database Information

Tools

Tags

General Information

Database name:

WIEZADW

Workload type:

Data Warehouse

Compartment:

oraseemeaanalytics (root)/Northeast

OCID:

...pysk4a [Show](#) [Copy](#)

Created:

Wed, Aug 17, 2022, 12:43:43 UTC

OCPU count:

1

OCPU auto scaling:

Enabled ⓘ

Storage:

1 TB

Storage auto scaling:

Disabled ⓘ

License type:

Bring Your Own License (BYOL), Standard Edition

Database version:

19c

Lifecycle state:

Available [Check database availability](#)

Instance type:

Paid

Character set:

AL32UTF8

National character set:

AL16UTF16

Auto Start/Stop schedule:

Disabled [Schedule](#)

Mode:

Read/Write [Edit](#)

Infrastructure

Dedicated infrastructure:

No

Autonomous Data Guard ⓘ

Status:

Disabled [Enable](#)

Backup

Last automatic backup:

Wed, Aug 24, 2022, 00:17:17 UTC

Manual backup store:

Not Configured

Network

Access type:

Virtual Cloud Network

Virtual Cloud Network:

VCN-1

Subnet:

Private Subnet-VCN-1

Private Endpoint IP:

...1.111 [Show](#) [Copy](#)

Private Endpoint URL:

...ud.com [Show](#) [Copy](#)

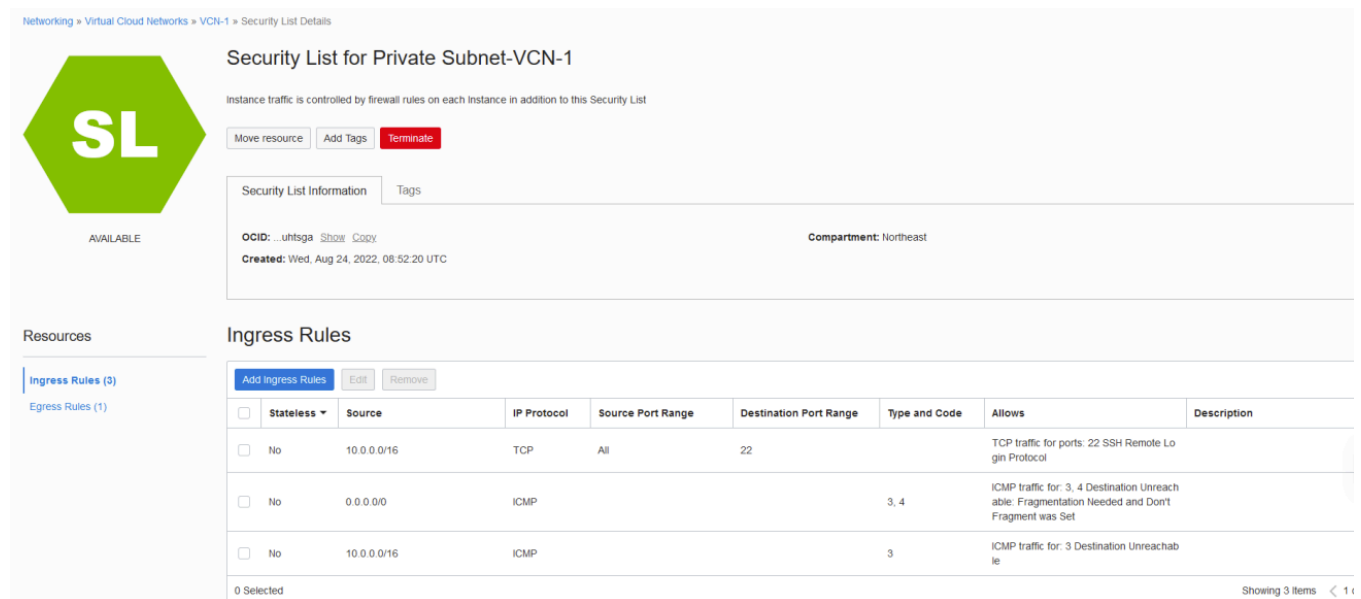
Network Security Groups:

None [Edit](#)

Mutual TLS (mTLS) authentication:

Required [Edit](#)

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**.



Networking » Virtual Cloud Networks » VCN-1 » Security List Details

Security List for Private Subnet-VCN-1

Instance traffic is controlled by firewall rules on each instance in addition to this Security List

Move resource Add Tags Terminate

Security List Information Tags

OCID: ...uhtsga Show Copy Compartment: Northeast
Created: Wed, Aug 24, 2022, 08:52:20 UTC

Resources

Ingress Rules (3)
Egress Rules (1)

Ingress Rules

Add Ingress Rules Edit Remove

<input type="checkbox"/>	Stateless ▾	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
<input type="checkbox"/>	No	10.0.0.0/16	TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	
<input type="checkbox"/>	No	0.0.0.0/0	ICMP			3, 4	ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set	
<input type="checkbox"/>	No	10.0.0.0/16	ICMP			3	ICMP traffic for: 3 Destination Unreachable	

0 Selected Showing 3 items < 1

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**.

Add Ingress Rules

Ingress Rule 1

Allows TCP traffic 1522

☐ Stateless ⓘ

Source Type

CIDR

Source CIDR

10.0.0.0/16

Specified IP addresses: 10.0.0.0-10.0.255.255 (65,536 IP addresses)

IP Protocol ⓘ

TCP

Source Port Range Optional ⓘ

All

Examples: 80, 20-22

Destination Port Range Optional ⓘ


1522

Examples: 80, 20-22

Description Optional

Maximum 255 characters

+ Another Ingress Rule

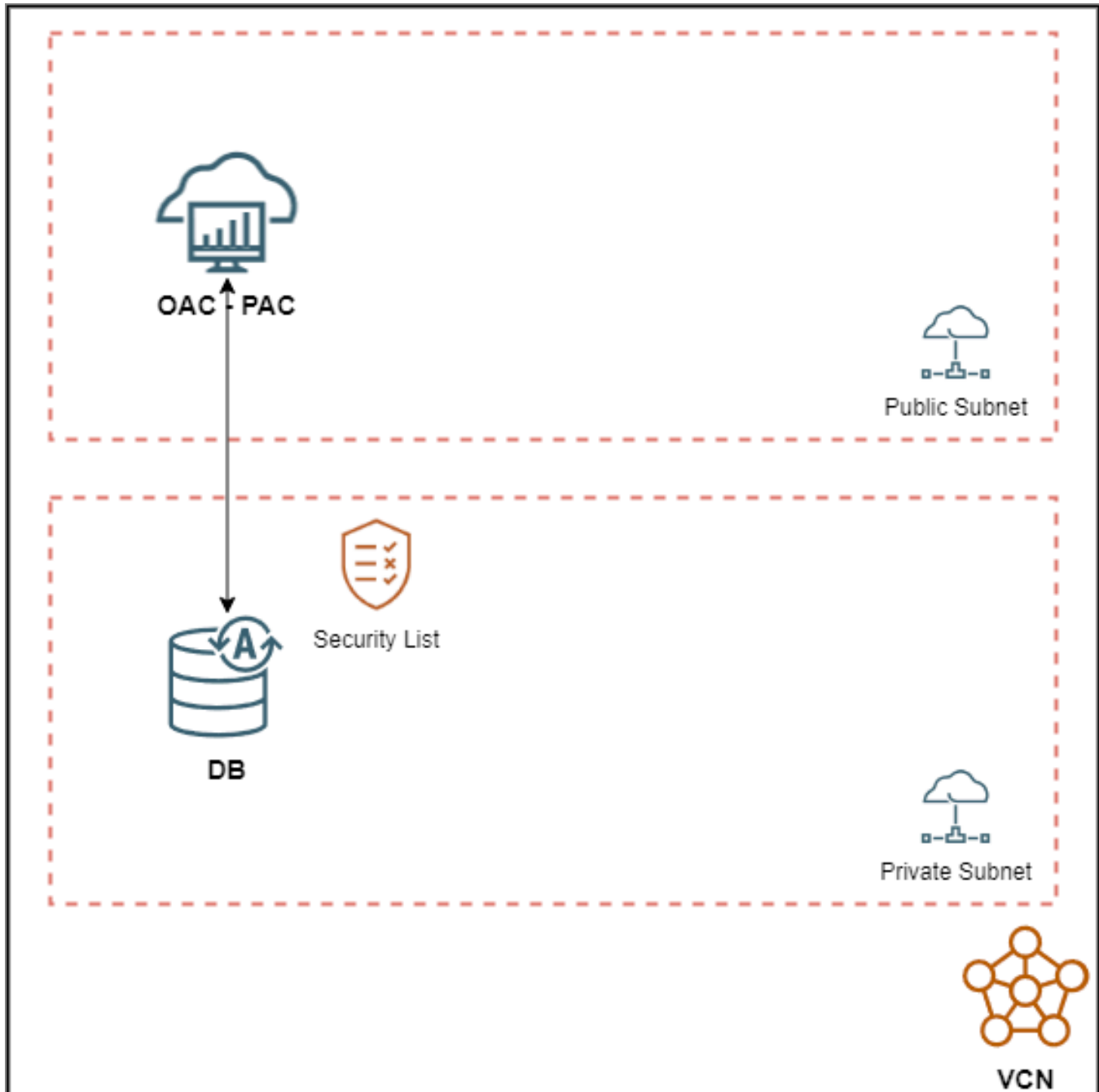


Add Ingress Rules

Cancel

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 an 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**.

Add Ingress Rules

Ingress Rule 1

Allows TCP traffic 1522

☐ Stateless ⓘ

Source Type

CIDR

Source CIDR

10.0.0.0/24

Specified IP addresses: 10.0.0.0-10.0.0.255 (256 IP addresses)

IP Protocol ⓘ

TCP

Source Port Range Optional ⓘ

All

Examples: 80, 20-22

Destination Port Range Optional ⓘ

1522

Examples: 80, 20-22

Description Optional

Maximum 255 characters

+ Another Ingress Rule

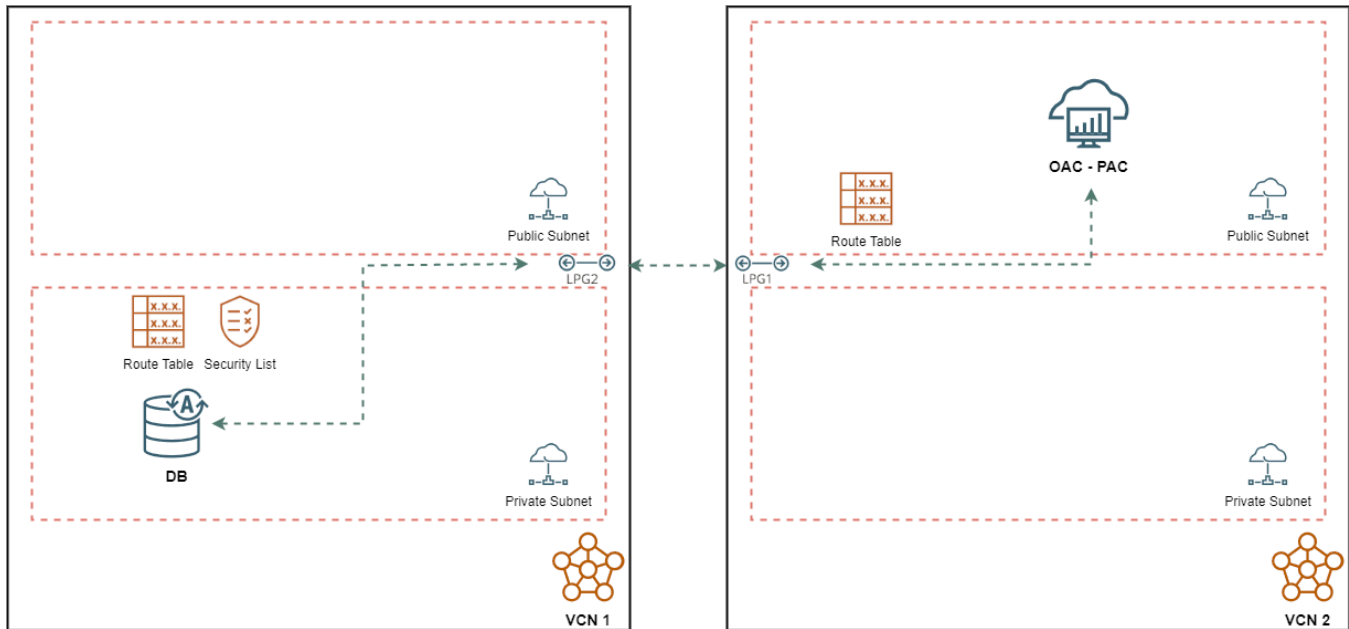
Add Ingress Rules

Cancel

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**.

Create Local Peering Gateway

Name

LPG-VCN1

Create In Compartment

Northeast

oraseemeanalytics (root)/Northeast

Show Advanced Options

Create Local Peering Gateway

Cancel

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.

Resources

Subnets (2)

CIDR Blocks/Prefixes (1)

Route Tables (2)

Internet Gateways (1)

Dynamic Routing Gateways Attachments (0)

Network Security Groups (0)

Security Lists (2)

DHCP Options (1)

Local Peering Gateways (1)

NAT Gateways (1)

Service Gateways (1)

VLANs (0)

Work Requests (0)

Scope

Local Peering Gateways in Northeast Compartment

Create Local Peering Gateway

Name	State	Peering Status	Route Table ⓘ	Peer Advertised CIDRs	Cross-Tenancy
LPG-VCN2	● Available	New - Not connected to a peer.			

- 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.

Establish Peering Connection [Help](#)

Specify the Local Peering Gateway
☒ Browse Below ☐ Enter Local Peering Gateway OCID

Virtual Cloud Network Compartment
 Northeast
oraseemeaanalytics (root)/Northeast

Virtual Cloud Network
 VCN-1

Local Peering Gateway Compartment
 Northeast
oraseemeaanalytics (root)/Northeast

Unpeered Peer Gateway
 LPG-VCN1

Establish Peering Connection [Cancel](#)

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.

Add Route Rules

[Help](#)

 **Important:**
For a route rule that targets a Private IP, you must first enable "Skip Source/Destination Check" on the VNIC that the Private IP is assigned to.

Route Rule


Target Type
Local Peering Gateway

Destination CIDR Block
10.0.0.0/16
Specified IP addresses: 10.0.0.0-10.0.0.255 (65,536 IP addresses)

Target Local Peering Gateway in **Northeast** [\(Change Compartment\)](#)
LPG-VCN2

Description *Optional*
Maximum 255 characters

[+ Another Route Rule](#)



[Add Route Rules](#) [Cancel](#)

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*.

Add Route Rules

[Help](#)

Important:

For a route rule that targets a Private IP, you must first enable "Skip Source/Destination Check" on the VNIC that the Private IP is assigned to.

Route Rule

Target Type

Local Peering Gateway

Destination CIDR Block

192.0.0.0/16

Specified IP addresses: 192.0.0.0-192.0.255.255 (65,536 IP addresses)

Target Local Peering Gateway in **Northeast** [\(Change Compartment\)](#)

LPG-VCN1

Description Optional

Maximum 255 characters

+ Another Route Rule



Add Route Rules

[Cancel](#)

- 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**.

Add Ingress Rules

Ingress Rule 1

Allows TCP traffic 1522

☐ Stateless ⓘ

Source Type

CIDR

Source CIDR

192.0.0.0/16

Specified IP addresses: 192.0.0.0-192.0.255.255 (65,536 IP addresses)

IP Protocol ⓘ

TCP

Source Port Range Optional ⓘ

All

Examples: 80, 20-22

Destination Port Range Optional ⓘ


1522

Examples: 80, 20-22

Description Optional

Maximum 255 characters

+ Another Ingress Rule



Add Ingress Rules


[Cancel](#)

- 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.



VCN-1

Move resource Add Tags Terminate

VCN Information Tags

Compartment: Northeast
Created: Wed, Aug 24, 2022, 08:52:18 UTC
IPv4 CIDR Block: 10.0.0.0/16
IPv6 Prefix: No Value

OCID: ...lthvda [Show](#) [Copy](#)
DNS Resolver: VCN-1
Default Route Table: [Default Route Table for VCN-1](#)
DNS Domain Name: vcn1.oraclevcn.com

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**.

Create Endpoint [Help](#)

Name

Listener

Choose a subnet in **Northeast** [\(Change Compartment\)](#)

Private Subnet-VCN-1

Endpoint Type

Listening
 An IP address in the subnet used to listen for queries. If a listening address is not provided then it will be assigned by the system. ✓

Forwarding
 An IP address in the subnet that queries may be forwarded from. If a forwarding address is not provided then it will be assigned by the system.

Listening IP Address *Optional*

☐ Use Network Security Group to control traffic *Optional*
 Select up to a maximum of (5) network security groups.

[Create Endpoint](#) [Cancel](#)

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

Create Endpoint

[Help](#)

Name

Forward

Choose a subnet in **Northeast** [\(Change Compartment\)](#)

Private Subnet-VCN-1

Endpoint Type

Listening

An IP address in the subnet used to listen for queries. If a listening address is not provided then it will be assigned by the system.


Forwarding

An IP address in the subnet that queries may be forwarded from. If a forwarding address is not provided then it will be assigned by the system. ✓

Forwarding IP Address *Optional*

☐ Use Network Security Group to control traffic *Optional*

Select up to a maximum of (5) network security groups.



Create Endpoint

[Cancel](#)

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

Endpoints

The private endpoints used for forwarding and listening to DNS queries to or from another private DNS system such as a peered VCN or an on-premises network.

Create Endpoint				
Name	State	Subnet	Forwarding address ⓘ	Listening address ⓘ
Forward	● Active	Private Subnet-VCN-1	10.0.1.118	—
Listener	● Active	Private Subnet-VCN-1	—	10.0.1.132

OAC-Private Access Channel – Endpoints

Endpoints

The private endpoints used for forwarding and listening to DNS queries to or from another private DNS system such as a peered VCN or an on-premises network.

Create Endpoint				
Name	State	Subnet	Forwarding address ⓘ	Listening address ⓘ
FWD	● Active	Public Subnet-VCN-2	192.0.0.243	—
LST	● Active	Public Subnet-VCN-2	—	192.0.0.66

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.

<div>Manage Rules Remove</div>						
<input type="checkbox"/>	Order	Rule Condition ⓘ	Client CIDR Blocks/Domains ⓘ	Rule Action	Source Endpoint ⓘ	Destination IP Address
<input type="checkbox"/>	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).

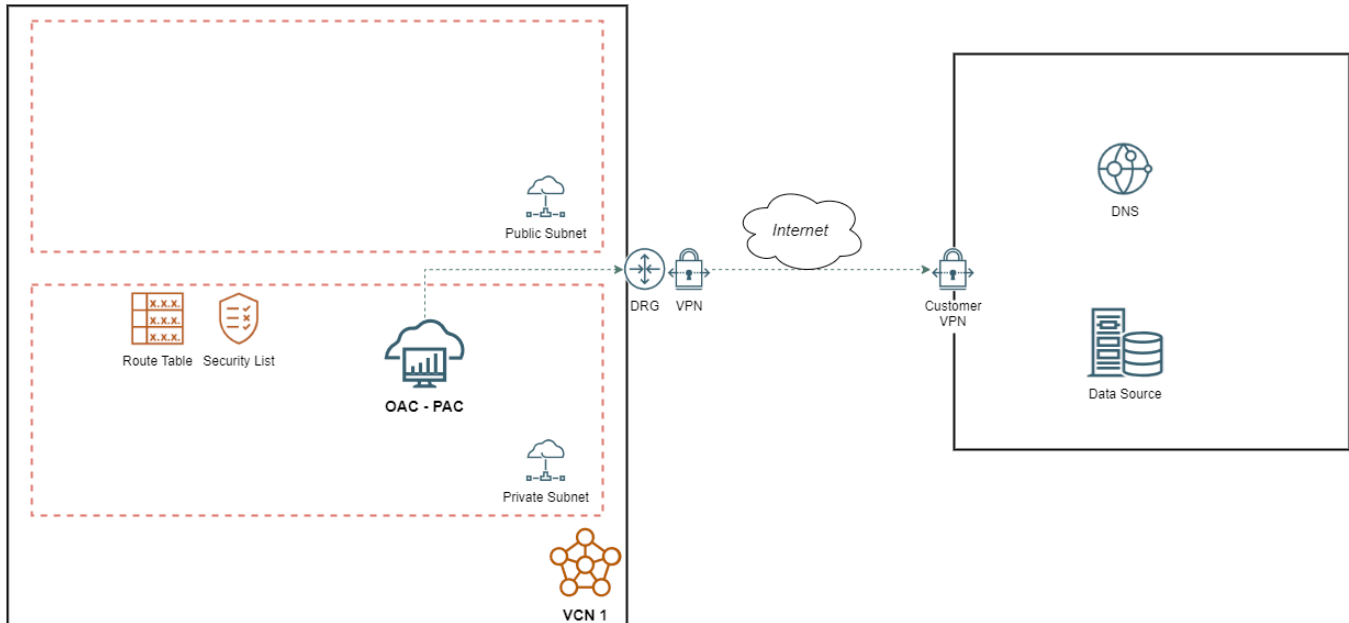
Rules

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.

<div>Manage Rules Remove</div>						
<input type="checkbox"/>	Order	Rule Condition ⓘ	Client CIDR Blocks/Domains ⓘ	Rule Action	Source Endpoint ⓘ	Destination IP Address
<input type="checkbox"/>	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**



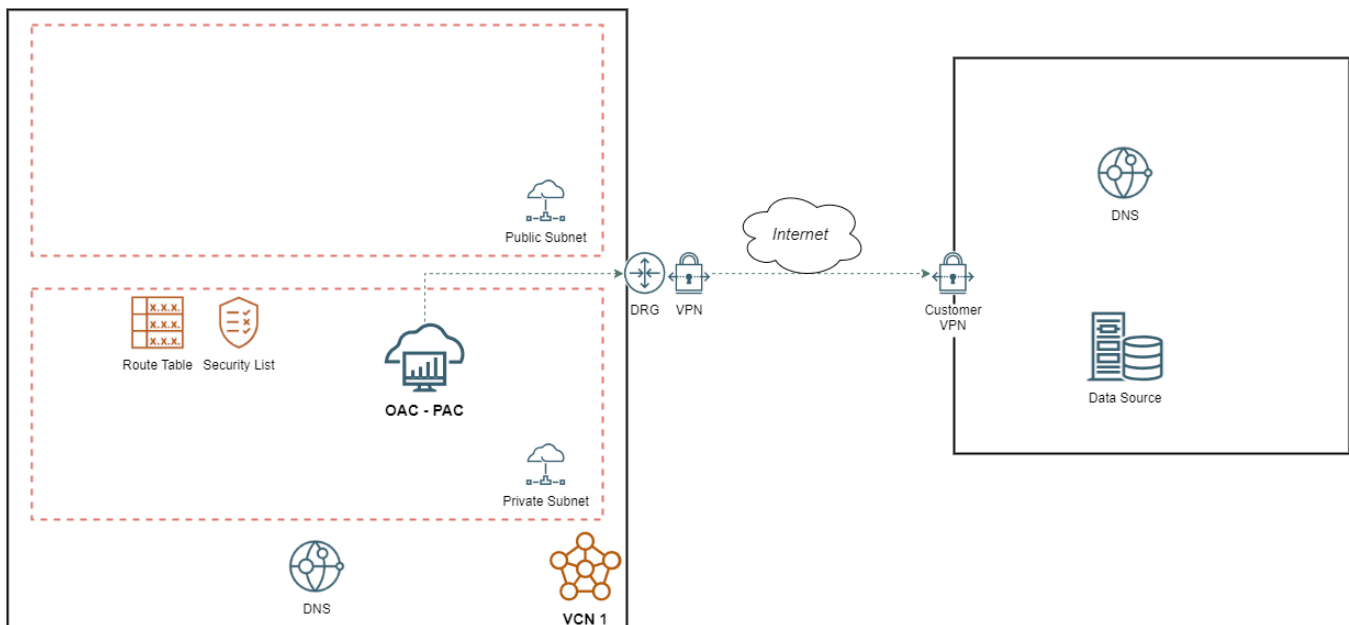
In this scenario, the Data Source resides in a corporate network and the OAC-Private Access Channel in an Oracle Cloud Infrastructure VCN. The steps to make the connections between them is similar with the ones from the previous scenario, with the difference that we will not setup an LPG connection and 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 Private Zone

[Help](#)

You can only view or manage a zone when working in the region where it was created. This zone will not be visible when working from another region.

Zone Name ⓘ

companyabc.com

Create in Compartment

Northeast

oraseemeanalytics (root)/Northeast

Zone Type Read-Only ⓘ

Primary

DNS Private View ⓘ

A private zone must be attached to a private zone view in order for the resolver to direct traffic to the correct location.

When a private zone is attached to a private zone view, the private zone cannot be moved to a new private zone view.

Selecting existing DNS Private View

Create new DNS Private View

Name Optional

pac_vcn

This resource will be created in the compartment selected above.

Show Advanced Options

Create

Cancel

- 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.

DNS - companyabc.com

Move Resource

Add Tags

Delete

Zone Information

Tags

Zone Scope: Private

Zone Type: Primary

Private View: [pac_vcn](#)

Nameservers: vcn-dns.oraclevcn.com.

Created: Thu, Aug 25, 2022, 12:30:51 UTC

OCID: ...o4szva [Show](#) [Copy](#)

Compartment: Northeast

Protected: No ⓘ

Records

Publish Changes

Add Record

Actions

Search...

	Domain	TTL	Type	RDATA	Protected	State
<input type="checkbox"/>	companyabc.com	86400	NS	vcn-dns.oraclevcn.com.	Yes	Protected
<input type="checkbox"/>	companyabc.com	86400	SOA	vcn-dns.oraclevcn.com. hostmaster.oracle.com. 1 3600 3600 3600 10	Yes	Protected

0 Selected

Showing 2 Items < Page

22 OAC Private Access Channel / Version 1
Copyright © 2024, Oracle and/or its affiliates / Public

ORACLE

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**.

Add Record

Record Type

A - IPv4 Address

Host record, used to point a hostname to an IPv4 address.

Name Optional

datasource01

.companyabc.com

TTL

30

TTL Unit

Seconds

All A records in datasource01.companyabc.com will be updated to reflect last changes to TTL [Lock](#)

Rdata Mode

Basic

Address

196.0.0.2

☐ Add Another Record

Submit

Cancel

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.

Manage Private Views

[Help](#)

Manage which private views are associated with this resolver. The resolver will answer to private views based on order.

Choose a Private View in **Northeast** [\(Change Compartment\)](#)

1. pac_vcn (Not Protected) - ...sdjctq

+ Additional Private View



Save Changes

[Cancel](#)

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*).