Lab 2: IPSec VPN

Introduction

Local VCN peering is the process of connecting two VCNs in the same region so that their resources can communicate using private IP addresses without routing the traffic over the internet or through your on-premises network. The VCNs can be in the same Oracle Cloud Infrastructure tenancy or different ones. Without peering, a given VCN would need an internet gateway and public IP addresses for the instances that need to communicate with another VCN.

Objective

This lab walks you to the steps needed to create a hub and spoke topology. We will reuse the resources created in the previous labs.

Pre-requisites

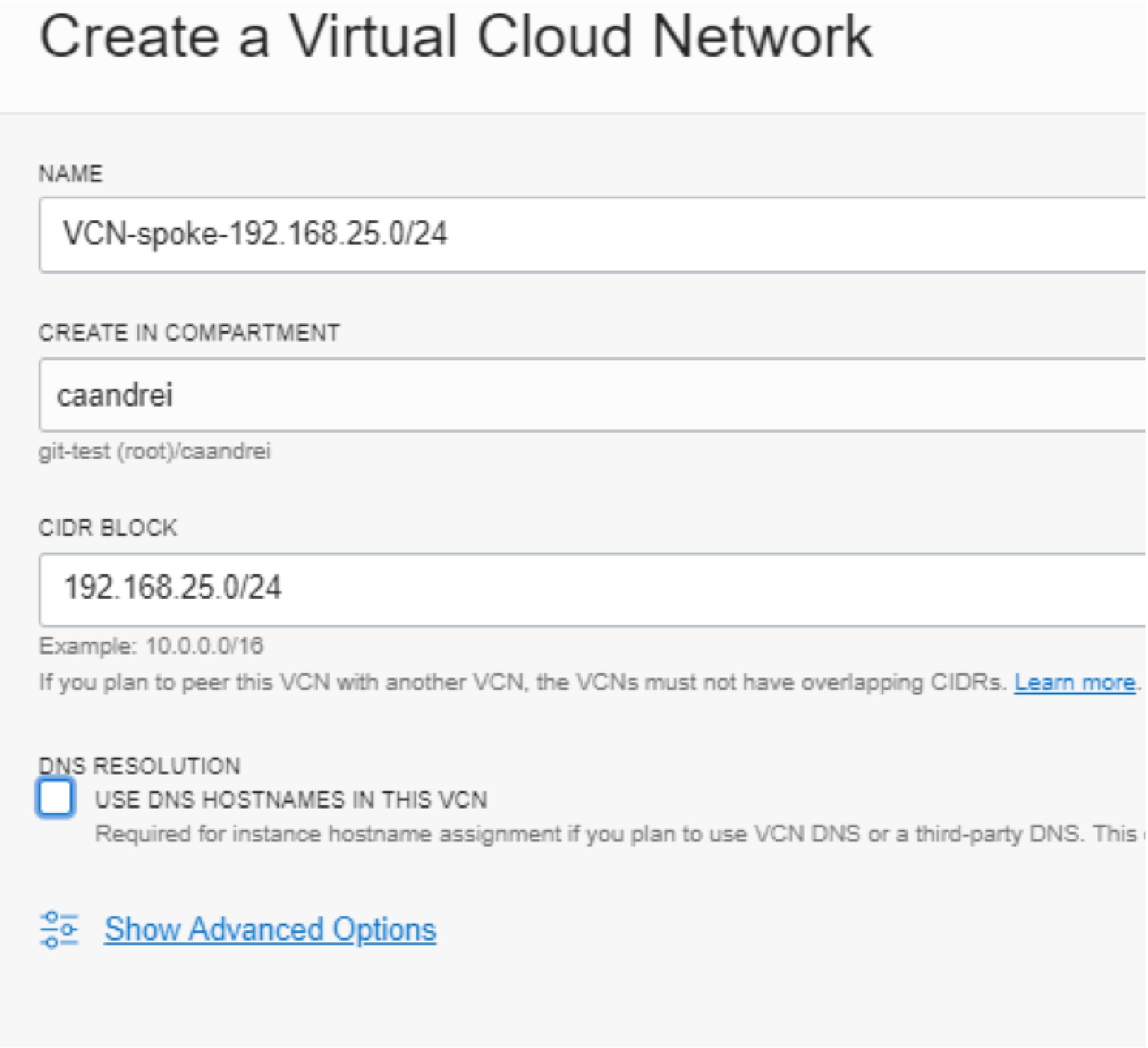
To perform this lab, you must finish the first two labs

Process Overview

- Create Spoke VCN
- Create Routing for the VCN Peering
- Create VCN peering
- Adjust Routing for the connectivity
- Test the Connectivity

Create Spoke VCN

Navigate to Networking > Virtual Cloud Networks and create a new VCN



Create a Virtual Cloud Network

NAME

VCN-spoke-192.168.25.0/24

CREATE IN COMPARTMENT

caandrei

git-test (root)/caandrei

CIDR BLOCK

192.168.25.0/24

Example: 10.0.0.0/16

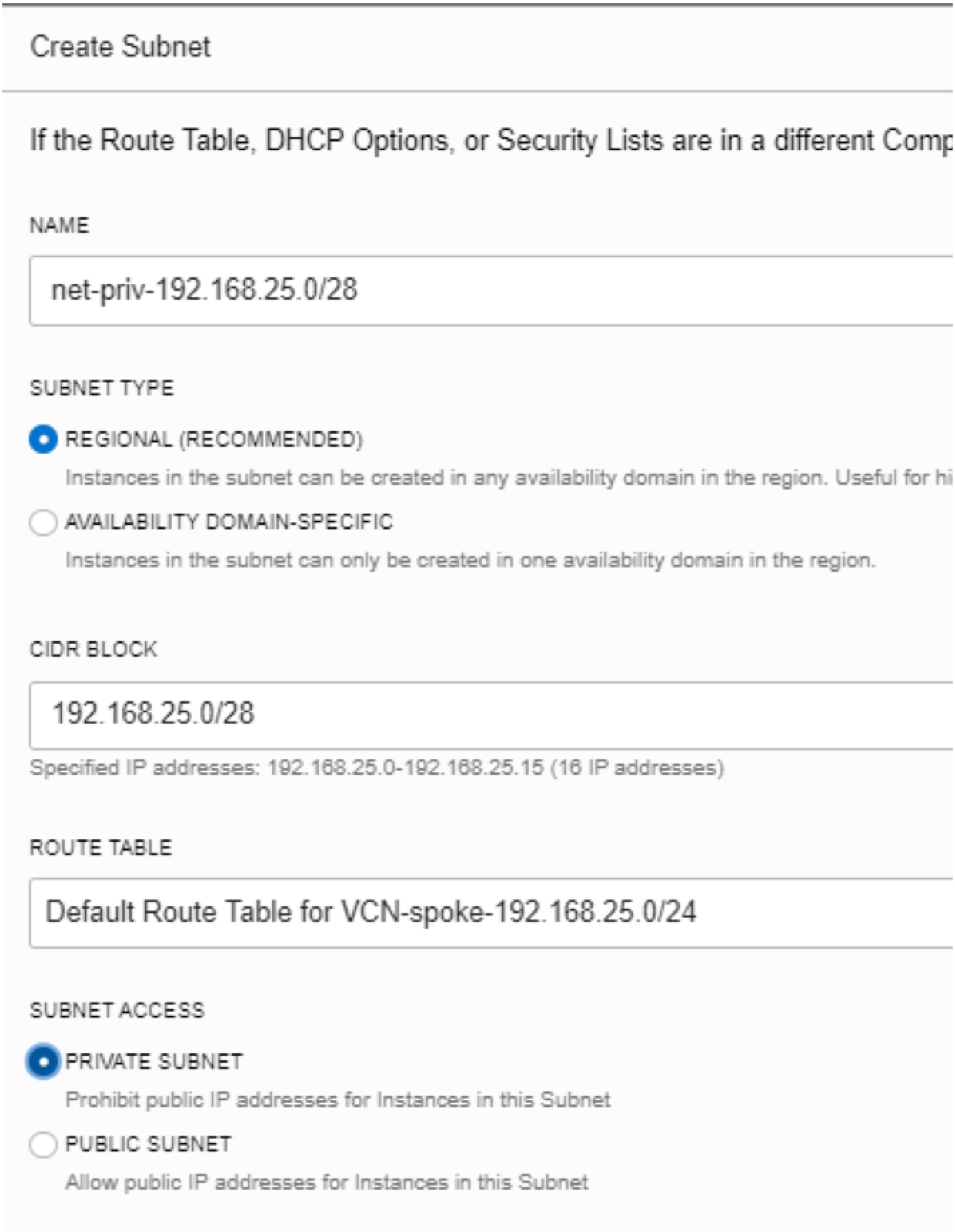
If you plan to peer this VCN with another VCN, the VCNs must not have overlapping CIDRs. Learn more.

DNS RESOLUTION

□ USE DNS HOSTNAMES IN THIS VCN

Required for instance hostname assignment if you plan to use VCN DNS or a third-party DNS. This

Create a private subnet



Create Subnet

If the Route Table, DHCP Options, or Security Lists are in a different Comp

NAME

net-priv-192.168.25.0/28

SUBNET TYPE

● REGIONAL (RECOMMENDED)

Instances in the subnet can be created in any availability domain in the region. Useful for hi

○ AVAILABILITY DOMAIN-SPECIFIC

Instances in the subnet can only be created in one availability domain in the region.

CIDR BLOCK

192.168.25.0/28

Specified IP addresses: 192.168.25.0-192.168.25.15 (16 IP addresses)

ROUTE TABLE

Default Route Table for VCN-spoke-192.168.25.0/24

SUBNET ACCESS

● PRIVATE SUBNET

Prohibit public IP addresses for Instances in this Subnet

○ PUBLIC SUBNET

Allow public IP addresses for Instances in this Subnet

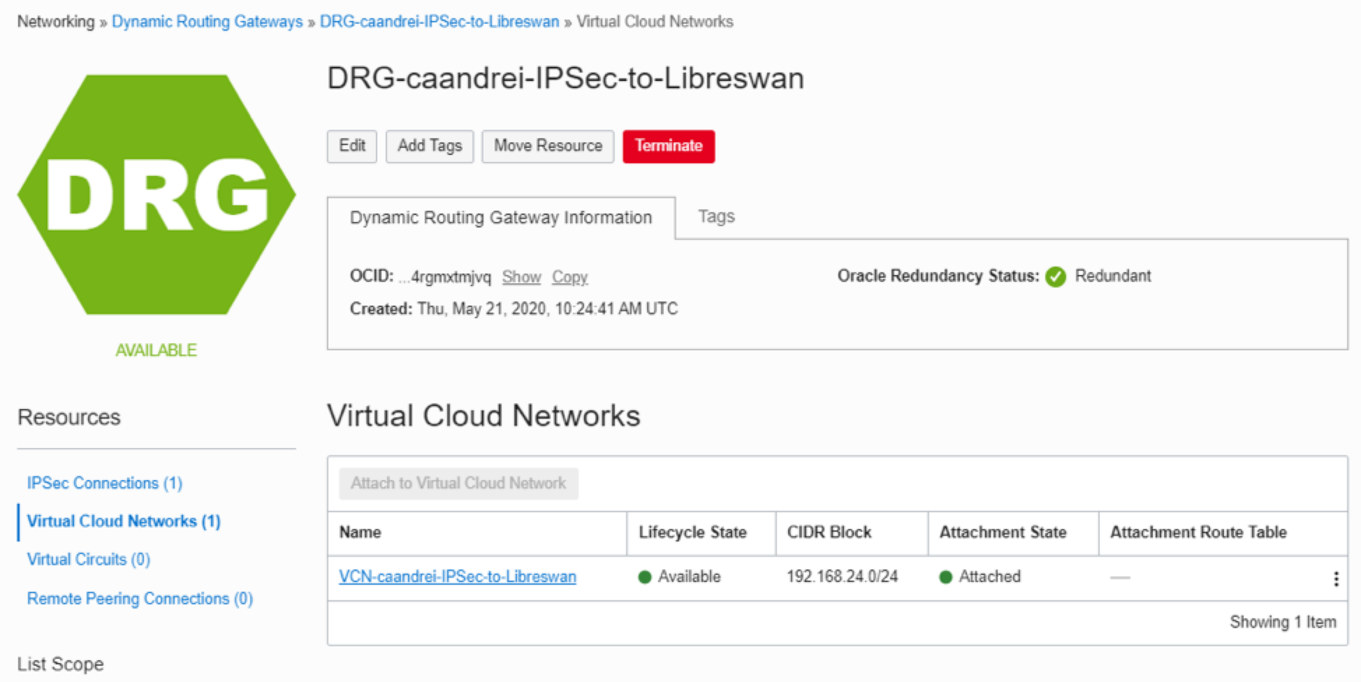
Create Routing for the VCN Peering

Navigate to Networking > Virtual Cloud Network > {VCN from the second Lab} > Route Tables and create a two new Route Tables

- Rt-drg
- Rt-lpg-hub

Associate the rt-drg to the DRG

Navigate to Networking >Dynamic Routing Gateway, click on the DRG and under the Virtual Cloud Networks associate the route table



Networking » Dynamic Routing Gateways » DRG-caandrei-IPSec-to-Libreswan » Virtual Cloud Networks

DRG-caandrei-IPSec-to-Libreswan

OCID: ...4rgmxtmjvq Show Copy

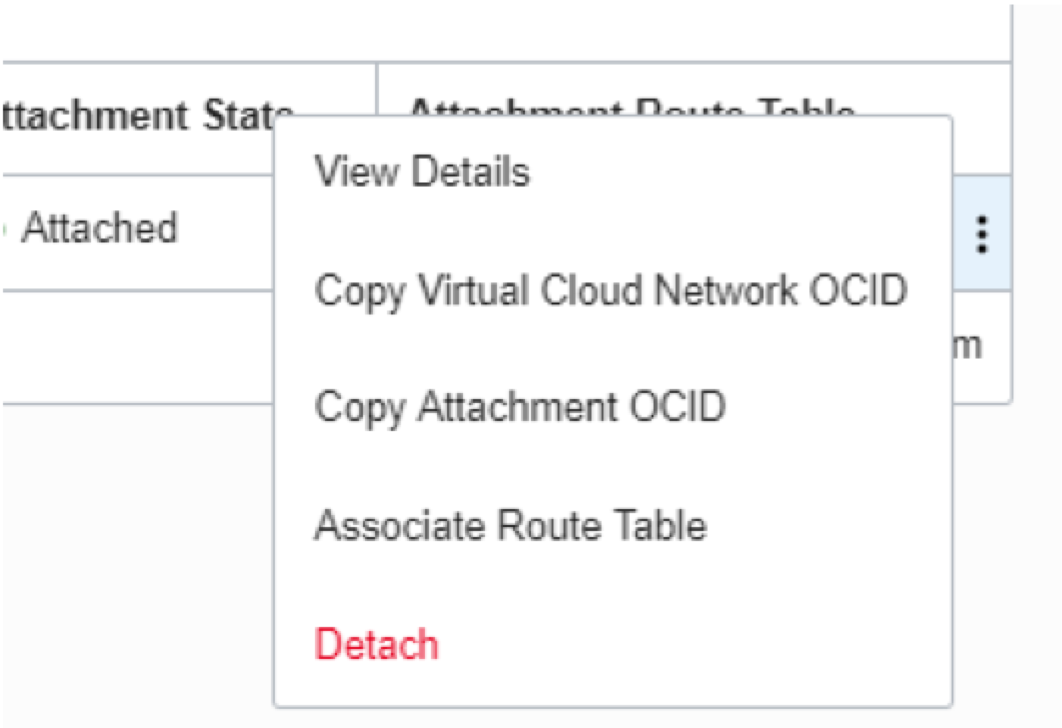
Oracle Redundancy Status: ✓ Redundant

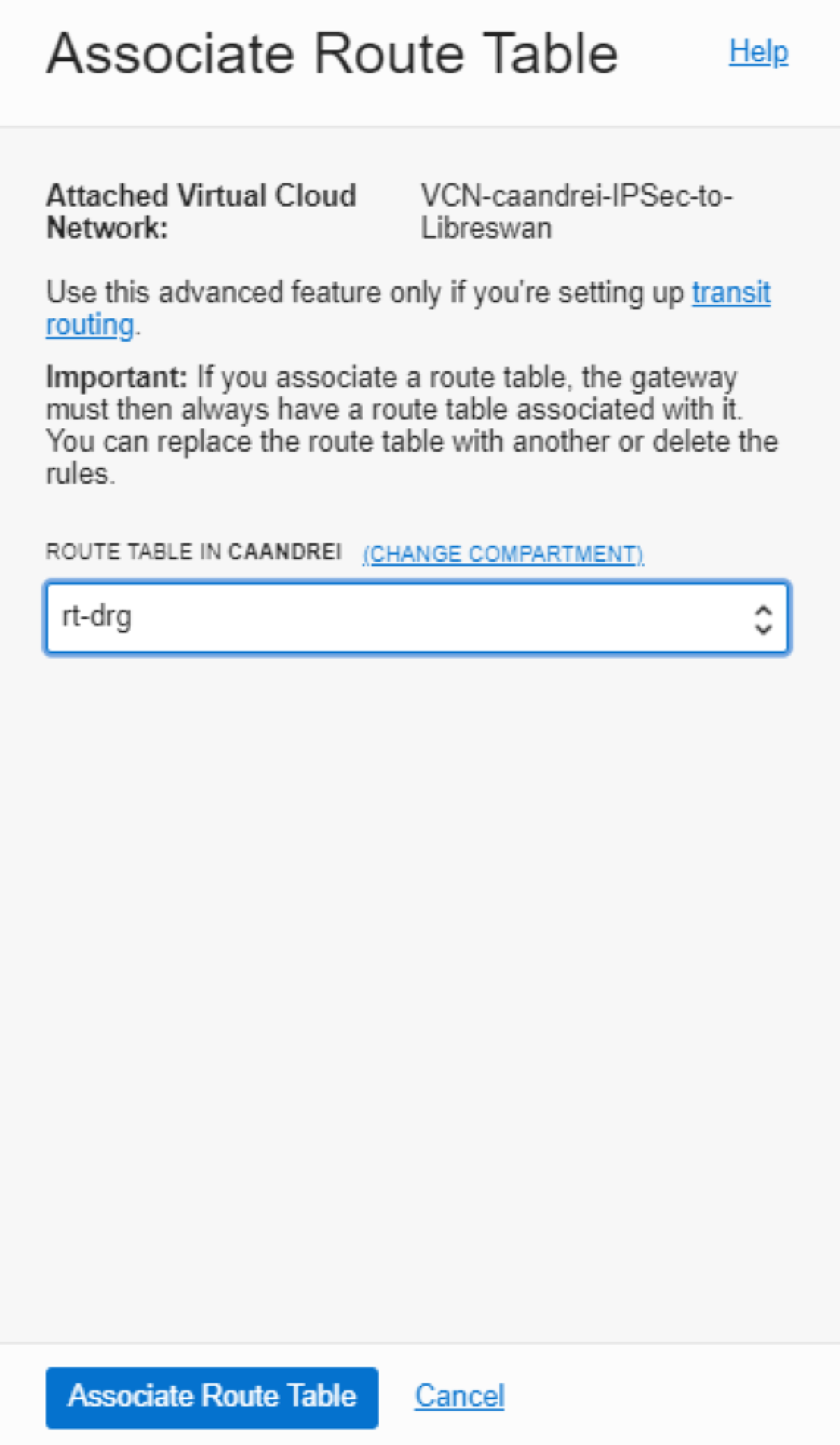
Created: Thu, May 21, 2020, 10:24:41 AM UTC

Resources
IPSec Connections (1)
Virtual Cloud Networks (1)
Virtual Circuits (0)
Remote Peering Connections (0)
List Scope
Virtual Cloud Networks
Attach to Virtual Cloud Network

Name	Lifecycle State	CIDR Block	Attachment State	Attachment Route Table
VCN-caandrei-IPSec-to-Libreswan	● Available	192.168.24.0/24	● Attached	—

Showing 1 Item





Associate Route Table

Attached Virtual Cloud Network: VCN-caandrei-IPSec-to-Libreswan

Use this advanced feature only if you're setting up transit routing.

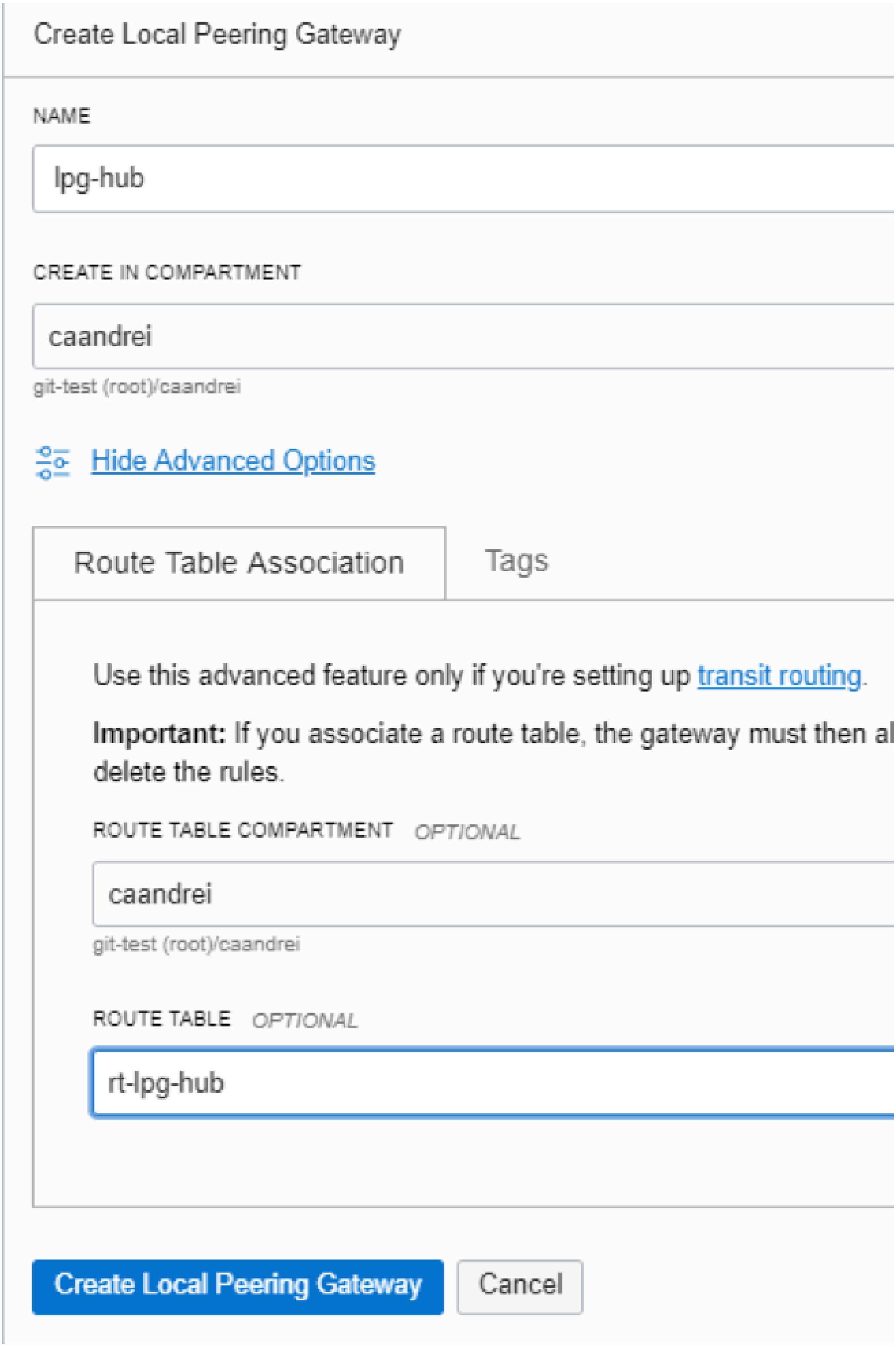
Important: If you associate a route table, the gateway must then always have a route table associated with it. You can replace the route table with another or delete the rules.

ROUTE TABLE IN CAANDREI (CHANGE COMPARTMENT)

rt-drg

Create VCN peering

Navigate to Networking > Virtual Cloud Network > {VCN from the second Lab} > Local Peering Gateways and create a LPG. Under Advanced Options, associate the route table created earlier



Create Local Peering Gateway

NAME

lpg-hub

CREATE IN COMPARTMENT

caandrei

git-test (root)/caandrei

Use this advanced feature only if you're setting up transit routing.

Important: If you associate a route table, the gateway must then al
delete the rules.

ROUTE TABLE COMPARTMENT *OPTIONAL*

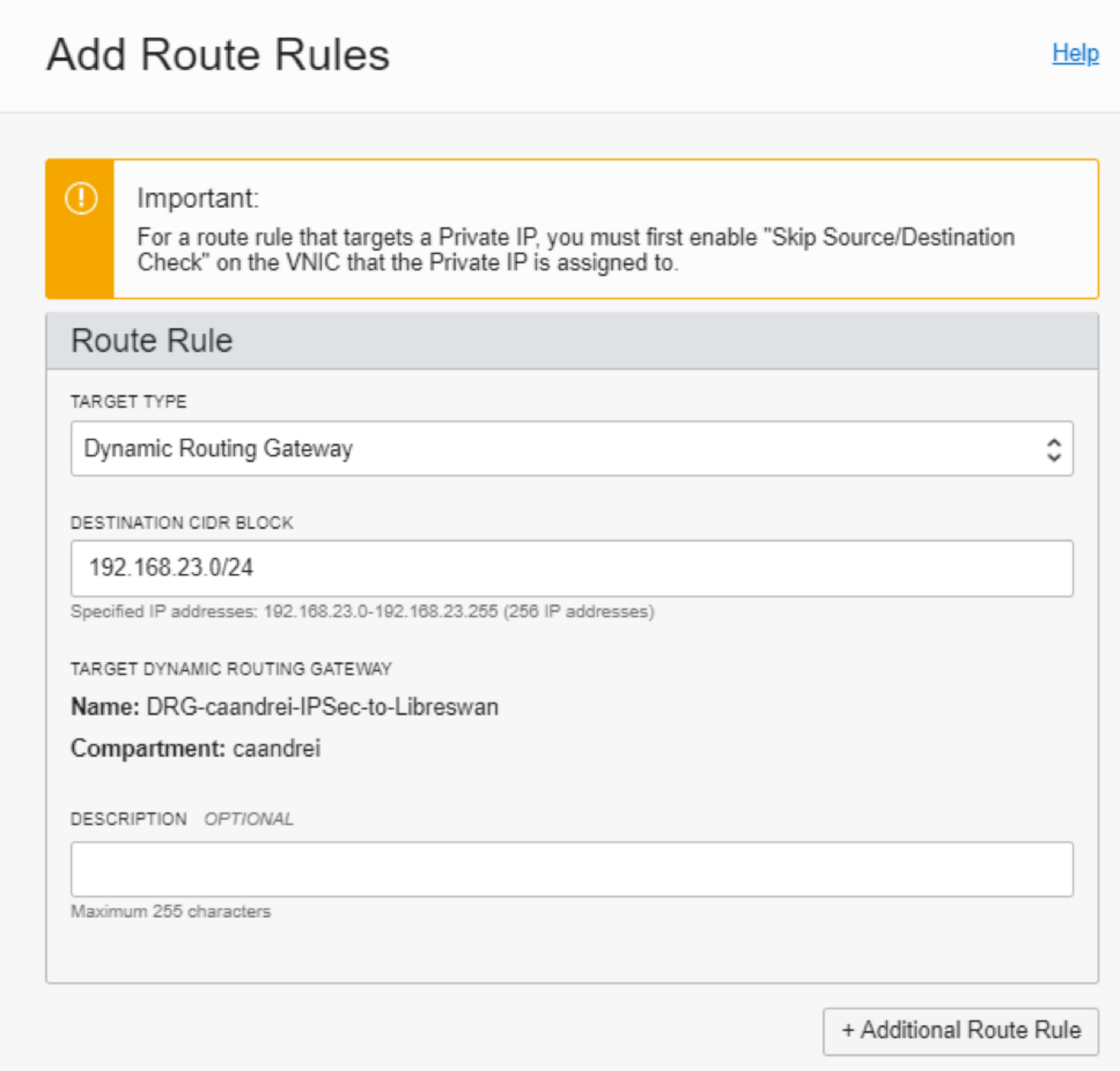
caandrei

git-test (root)/caandrei

ROUTE TABLE *OPTIONAL*

rt-lpg-hub

In the rt-lpg-hub add a route for the subnets that are behind the Libreswan (192.168.23.0/24)



Add Route Rules

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: Dynamic Routing Gateway

DESTINATION CIDR BLOCK: 192.168.23.0/24

Specified IP addresses: 192.168.23.0-192.168.23.255 (256 IP addresses)

TARGET DYNAMIC ROUTING GATEWAY

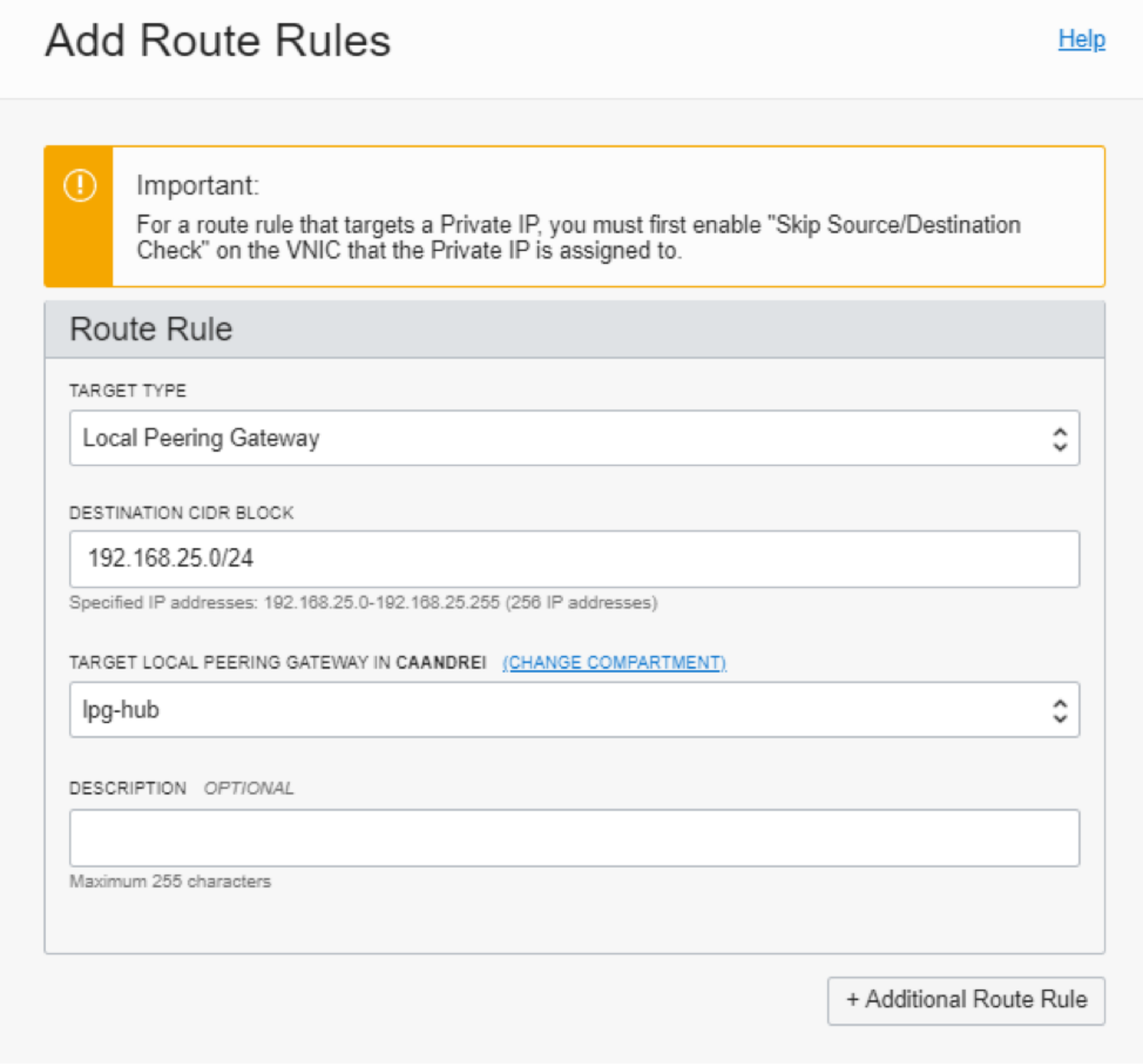
Name: DRG-caandrei-IPSec-to-Libreswan

Compartment: caandrei

DESCRIPTION *OPTIONAL*

Maximum 255 characters

In the rt-lpg-drg add a route for the subnets that are in the spoke VCN (192.168.25.0/24)



Add Route Rules

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: 192.168.25.0/24

Specified IP addresses: 192.168.25.0-192.168.25.255 (256 IP addresses)

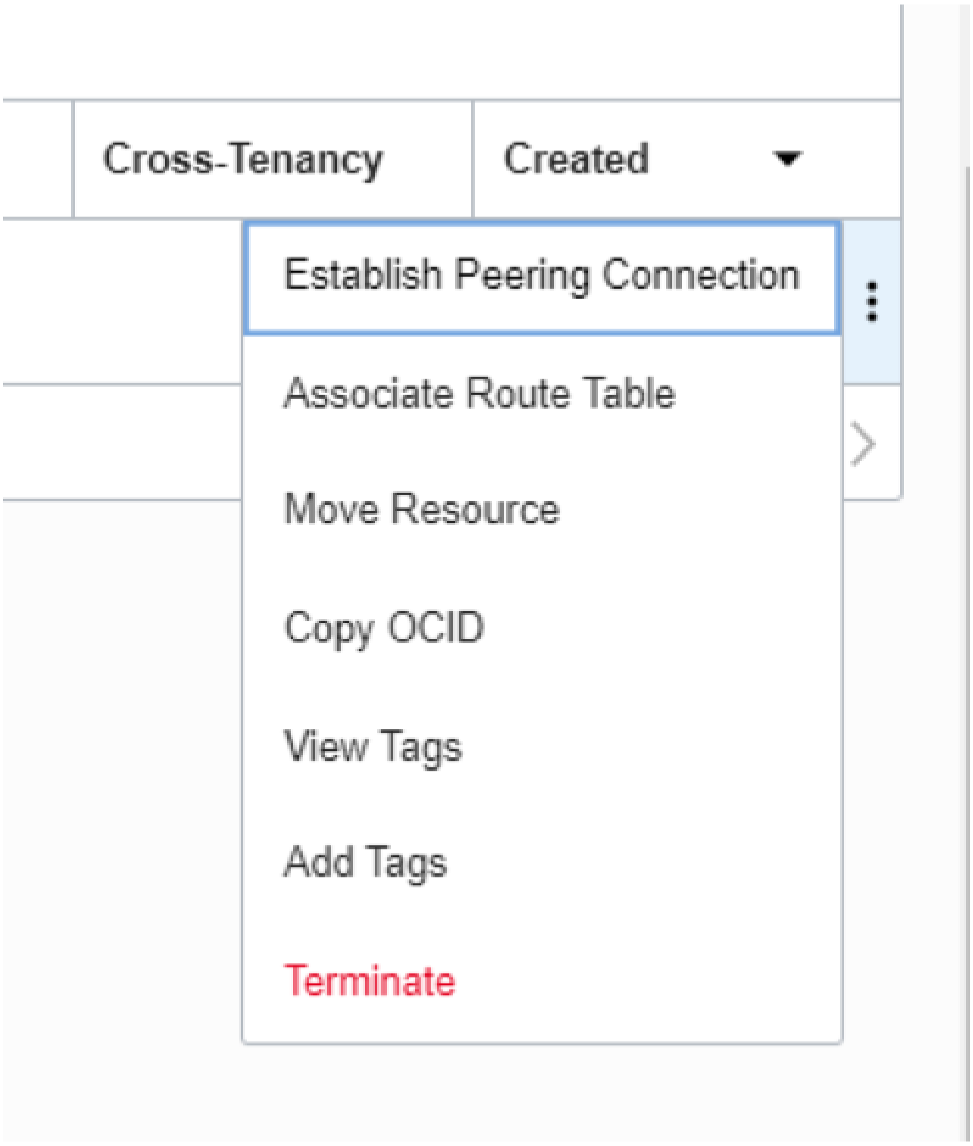
TARGET LOCAL PEERING GATEWAY IN **CAANDREI** (CHANGE COMPARTMENT): lpg-hub

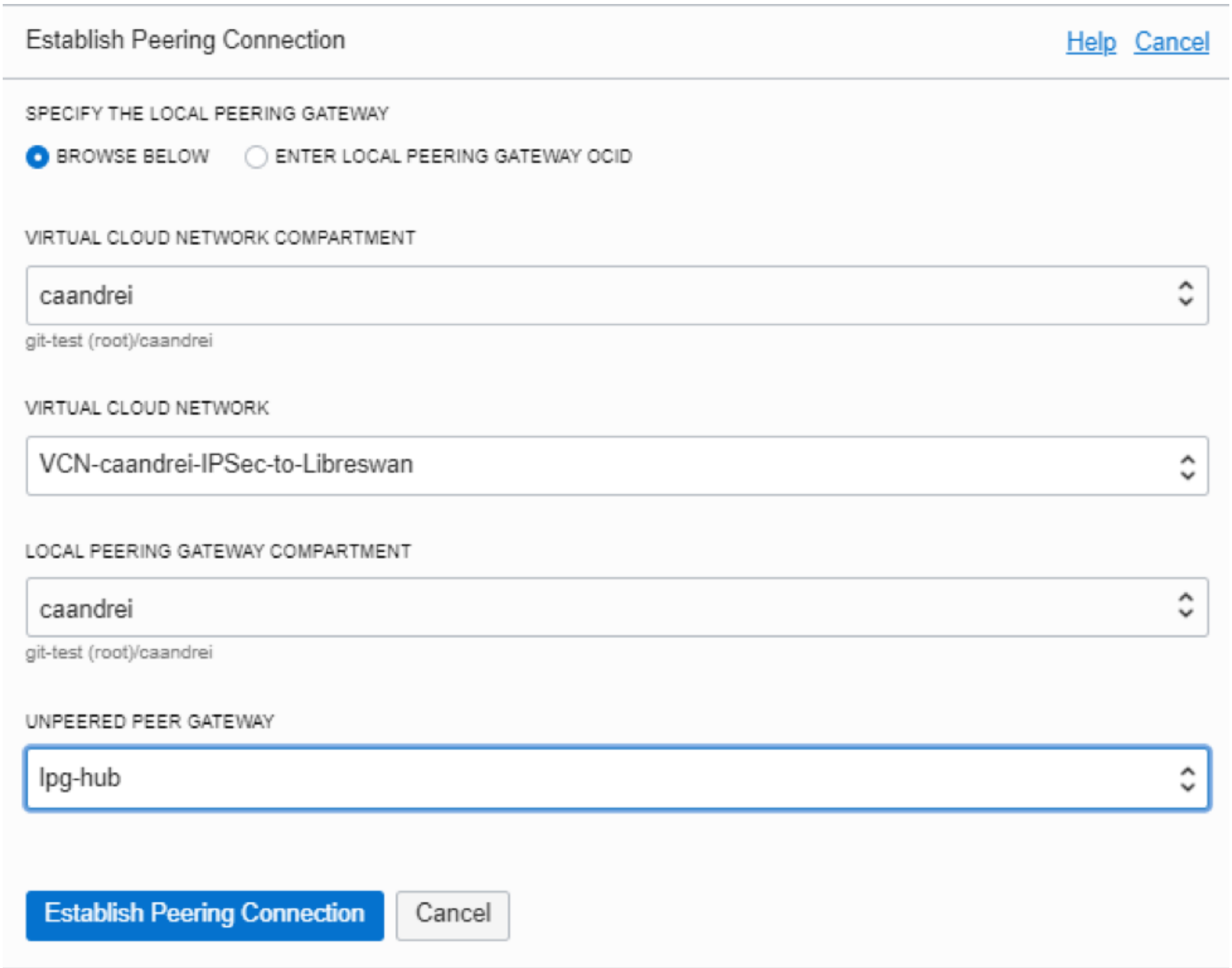
DESCRIPTION *OPTIONAL*

Maximum 255 characters

Navigate to Networking > Virtual Cloud Network and click on the spoke vcn created.

Go under Local peering gateways and create a new LPG. Establish peering Connection with the hub lpg


Cross-Tenancy
Created
Establish Peering Connection
Associate Route Table
Move Resource
Copy OCID
View Tags
Add Tags
Terminate



Establish Peering Connection

SPECIFY THE LOCAL PEERING GATEWAY

● BROWSE BELOW ○ ENTER LOCAL PEERING GATEWAY OCID

VIRTUAL CLOUD NETWORK COMPARTMENT: caandrei

git-test (root)/caandrei

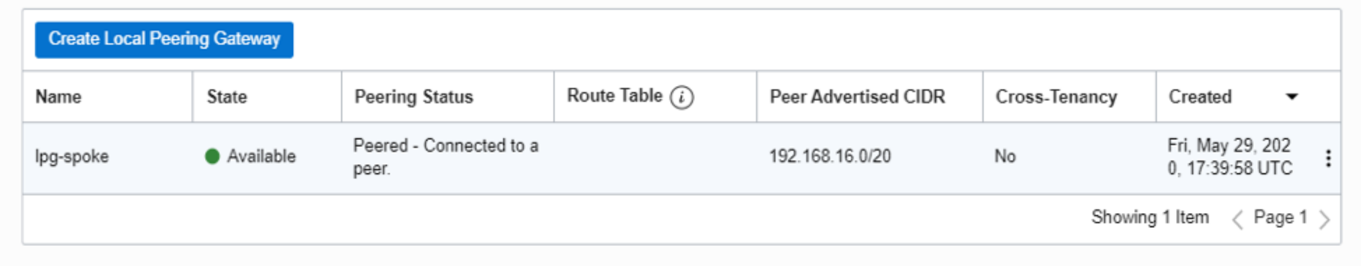
VIRTUAL CLOUD NETWORK: VCN-caandrei-IPSec-to-Libreswan

LOCAL PEERING GATEWAY COMPARTMENT: caandrei

git-test (root)/caandrei

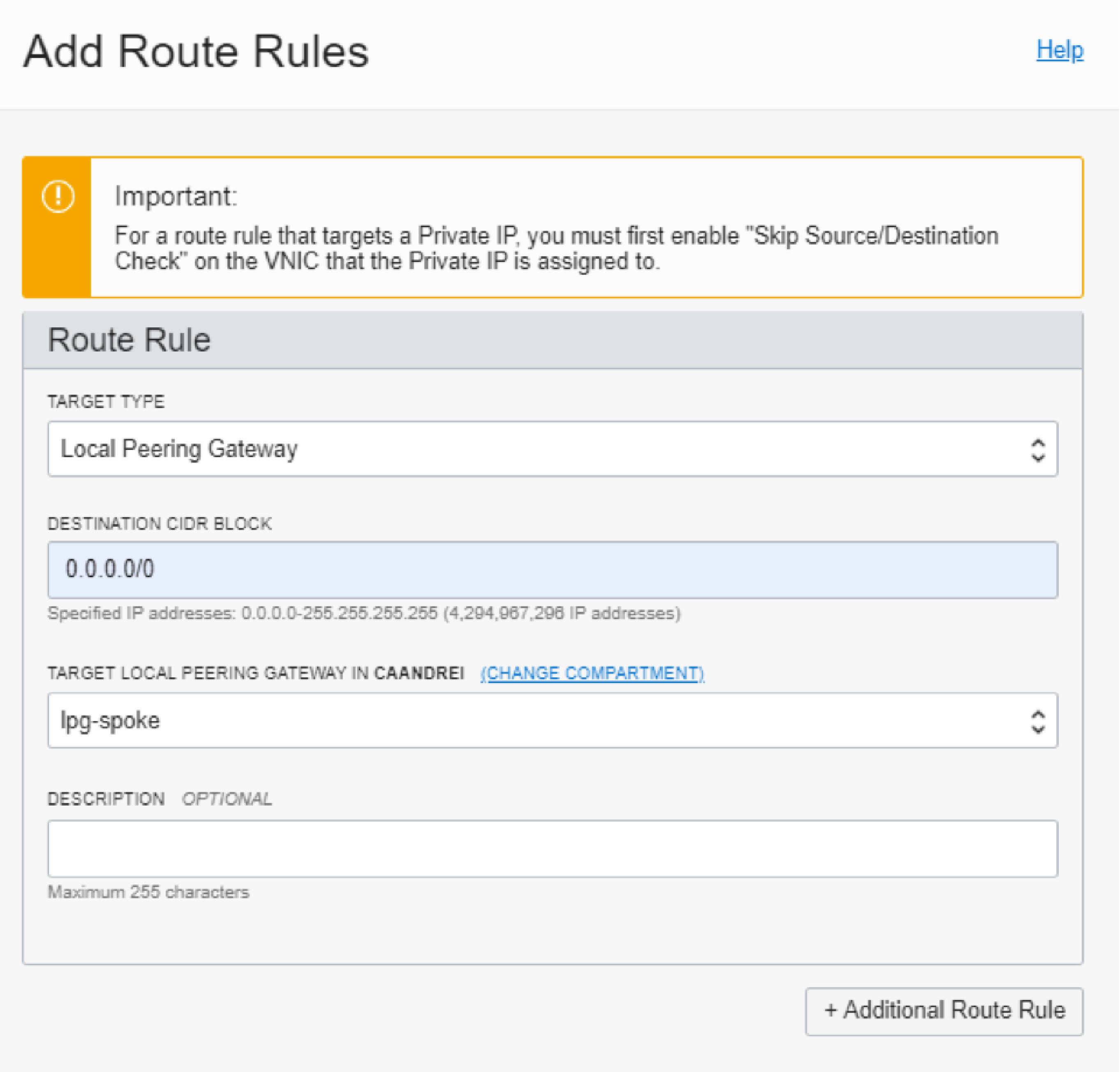
UNPEERED PEER GATEWAY: lpg-hub

The LPG will receive a summary route of the hub vcn CIDR and the CIDR space of the VCN that Libreswan is located



Name	State	Peering Status	Route Table	Peer Advertised CIDR	Cross-Tenancy	Created
lpg-spoke	● Available	Peered - Connected to a peer.		192.168.16.0/20	No	Fri, May 29, 2020, 17:39:58 UTC

Modify the Default route table of the spoke vcn and add a default route to the spoke lpg



Add Route Rules

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: 0.0.0.0/0

Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)

TARGET LOCAL PEERING GATEWAY IN **CAANDREI** (CHANGE COMPARTMENT): lpg-spoke

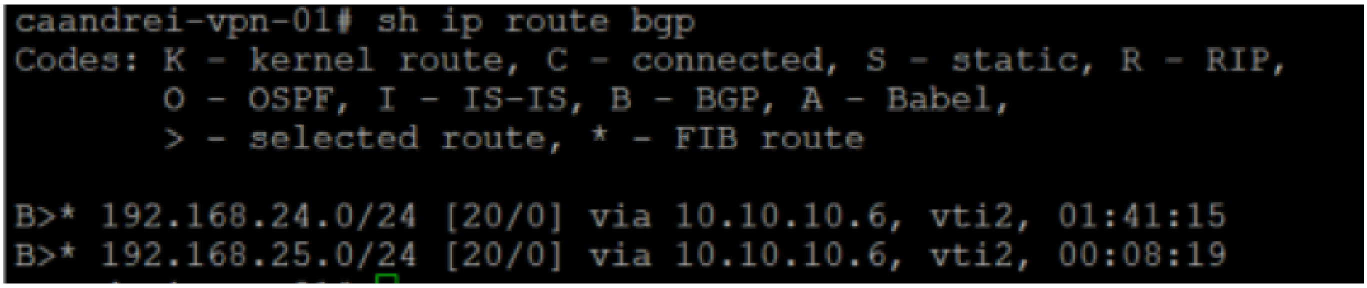
DESCRIPTION *OPTIONAL*

Maximum 255 characters

Adjust Routing for the connectivity

Let's adjust routing for cooncetivity from 192.168.23.0/24 to 192.168.24.0/23

Connect to the Libreswan VM and in quagga check the received routes

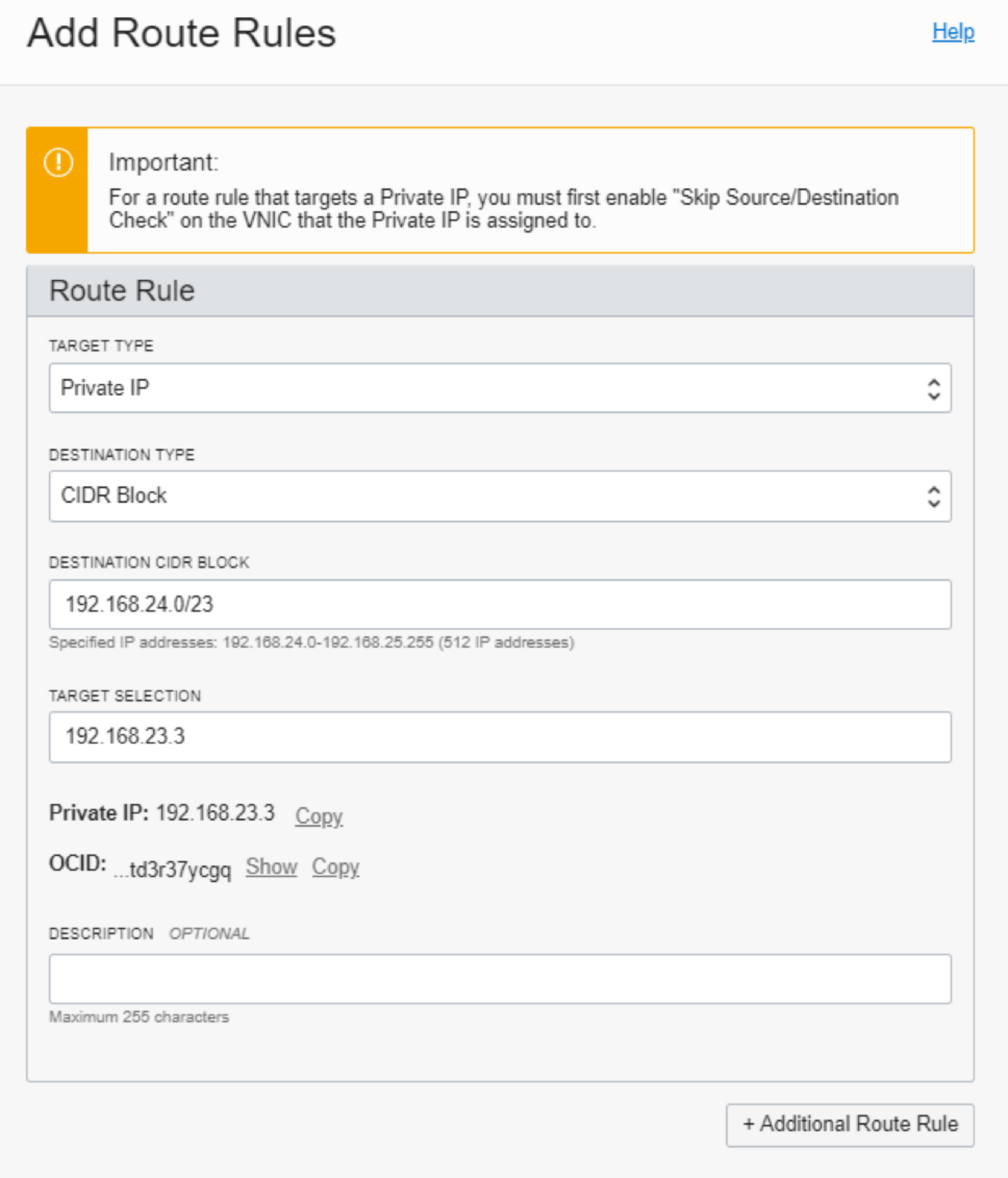


```
caandrei-vpn-01# sh ip route bgp
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

B>* 192.168.24.0/24 [20/0] via 10.10.10.6, vti2, 01:41:15
B>* 192.168.25.0/24 [20/0] via 10.10.10.6, vti2, 00:08:19
```

Observe that we are receiving the spoke vcn routes

Navigate to the Libreswan VCN and create a routing table for the private subnet. Add a route entry for the CIDR space that is behind the DRG:



Add Route Rules

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: Private IP

DESTINATION TYPE: CIDR Block

DESTINATION CIDR BLOCK: 192.168.24.0/23

Specified IP addresses: 192.168.24.0-192.168.25.255 (512 IP addresses)

TARGET SELECTION: 192.168.23.3

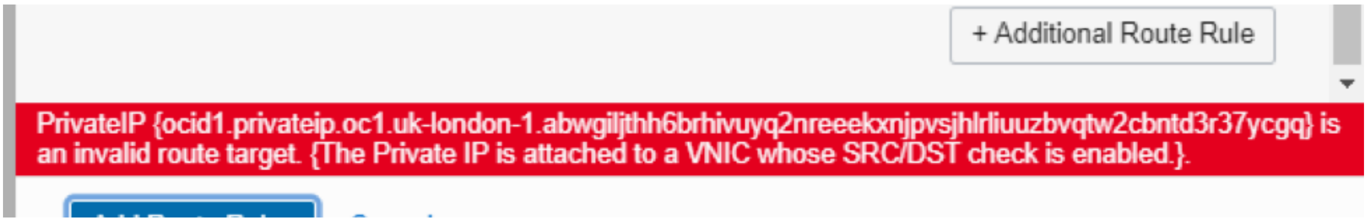
Private IP: 192.168.23.3 Copy

OCID: ...td3r37ycgq Show Copy

DESCRIPTION *OPTIONAL*

Maximum 255 characters

Notice the error message

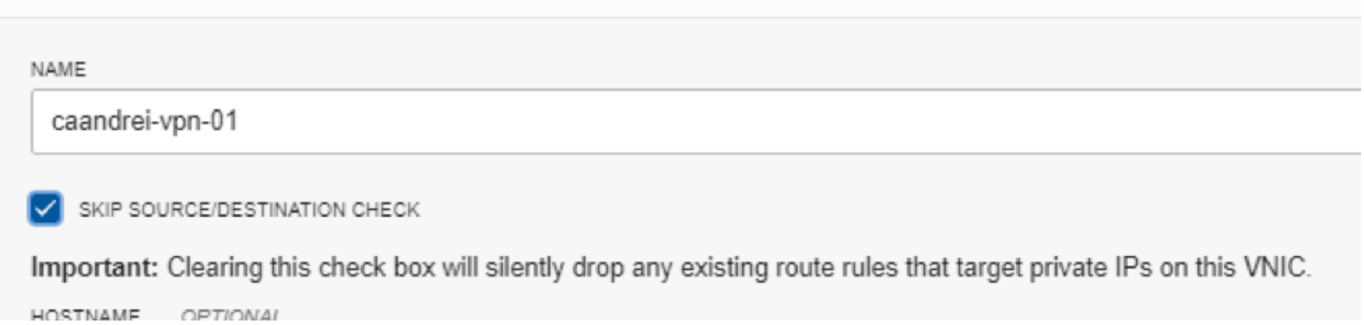


PrivateIP {ocid1.privateip.oc1.uk-london-1.abwgiljthh6brhivuyq2nreeekxnjpvsjhlrliuuzbvqtw2cbntd3r37ycgq} is an invalid route target. {The Private IP is attached to a VNIC whose SRC/DST check is enabled.}

We need to change the VNIC of the Libreswan VM.

Navigate to Compute > Instances > Libreswan VM. Navigate to the Attached VNICs.

Edit the VNIC and check "Skip source/destination check"



NAME

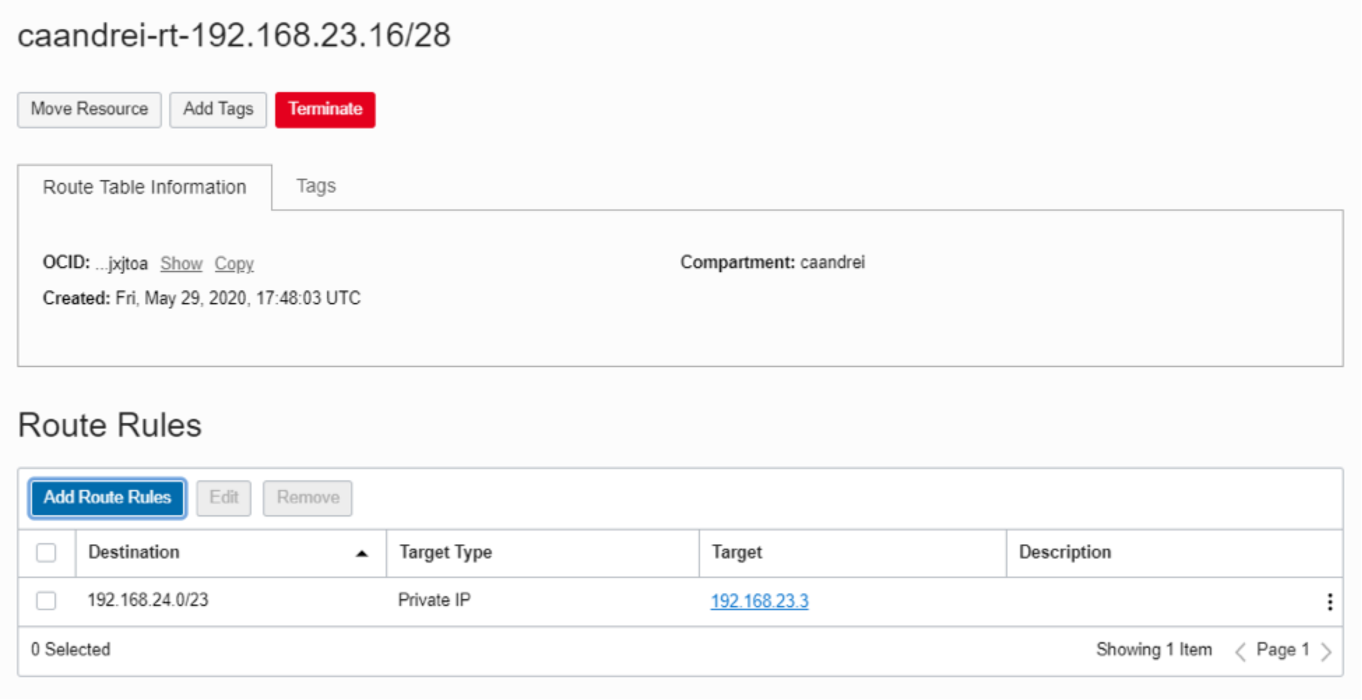
caandrei-vpn-01

☑ SKIP SOURCE/DESTINATION CHECK

Important: Clearing this check box will silently drop any existing route rules that target private IPs on this VNIC.

HOSTNAME OPTIONAL

Navigate back to the route table and re-add the routing rule



caandrei-rt-192.168.23.16/28

OCID: ...jxjtoa Show Copy

Compartment: caandrei

Created: Fri, May 29, 2020, 17:48:03 UTC

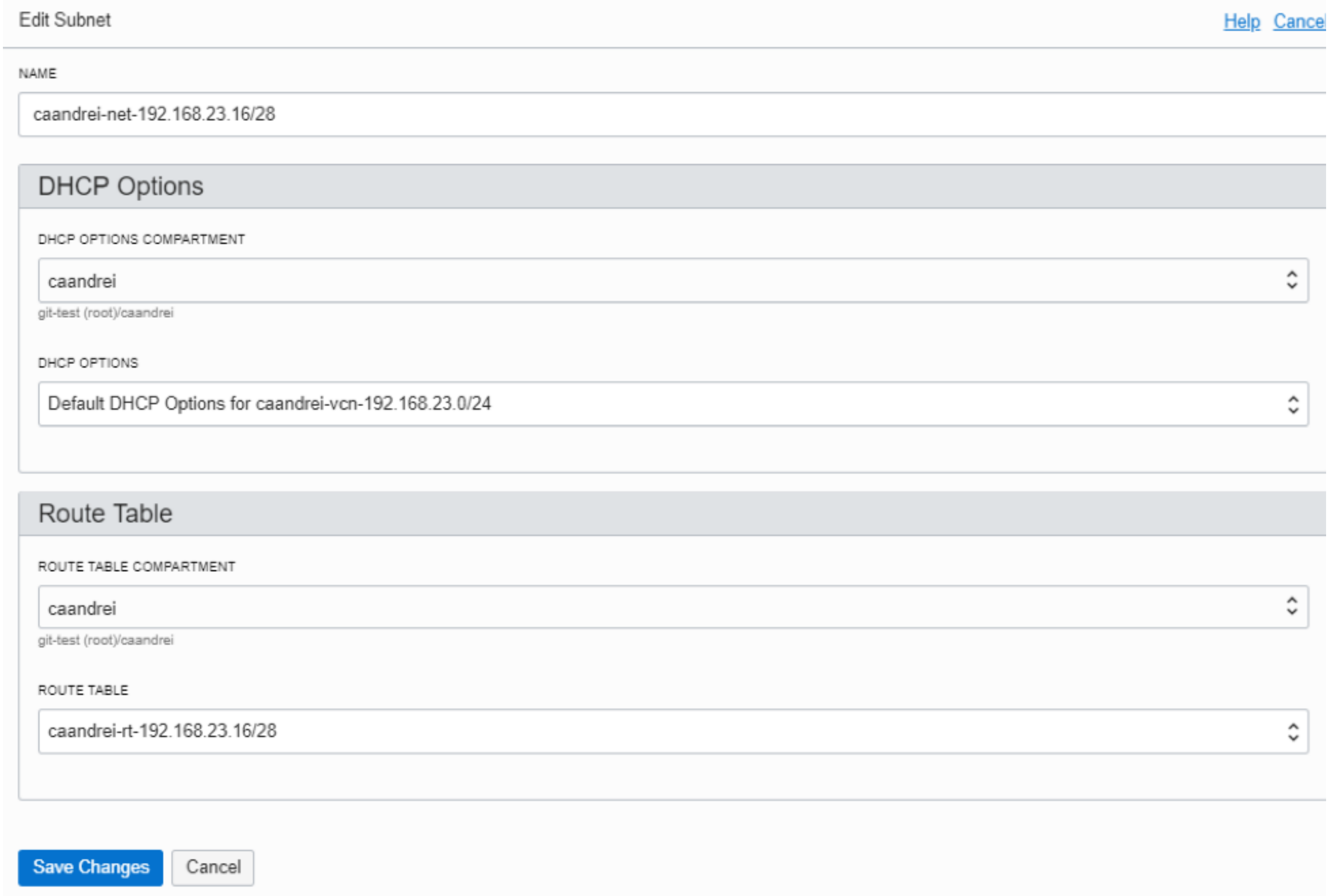
Route Rules

□	Destination	Target Type	Target	Description
□	192.168.24.0/23	Private IP	192.168.23.3	

0 Selected Showing 1 Item Page 1

Navigate to Networking > Virtual Cloud Network > caandrei-vcn-192.168.23.0/24

Click on the private subnet and edit the subnet and select the routing table



Edit Subnet

NAME

caandrei-net-192.168.23.16/28

DHCP Options

DHCP OPTIONS COMPARTMENT

caandrei

git-test (root)/caandrei

DHCP OPTIONS

Default DHCP Options for caandrei-vcn-192.168.23.0/24

Route Table

ROUTE TABLE COMPARTMENT

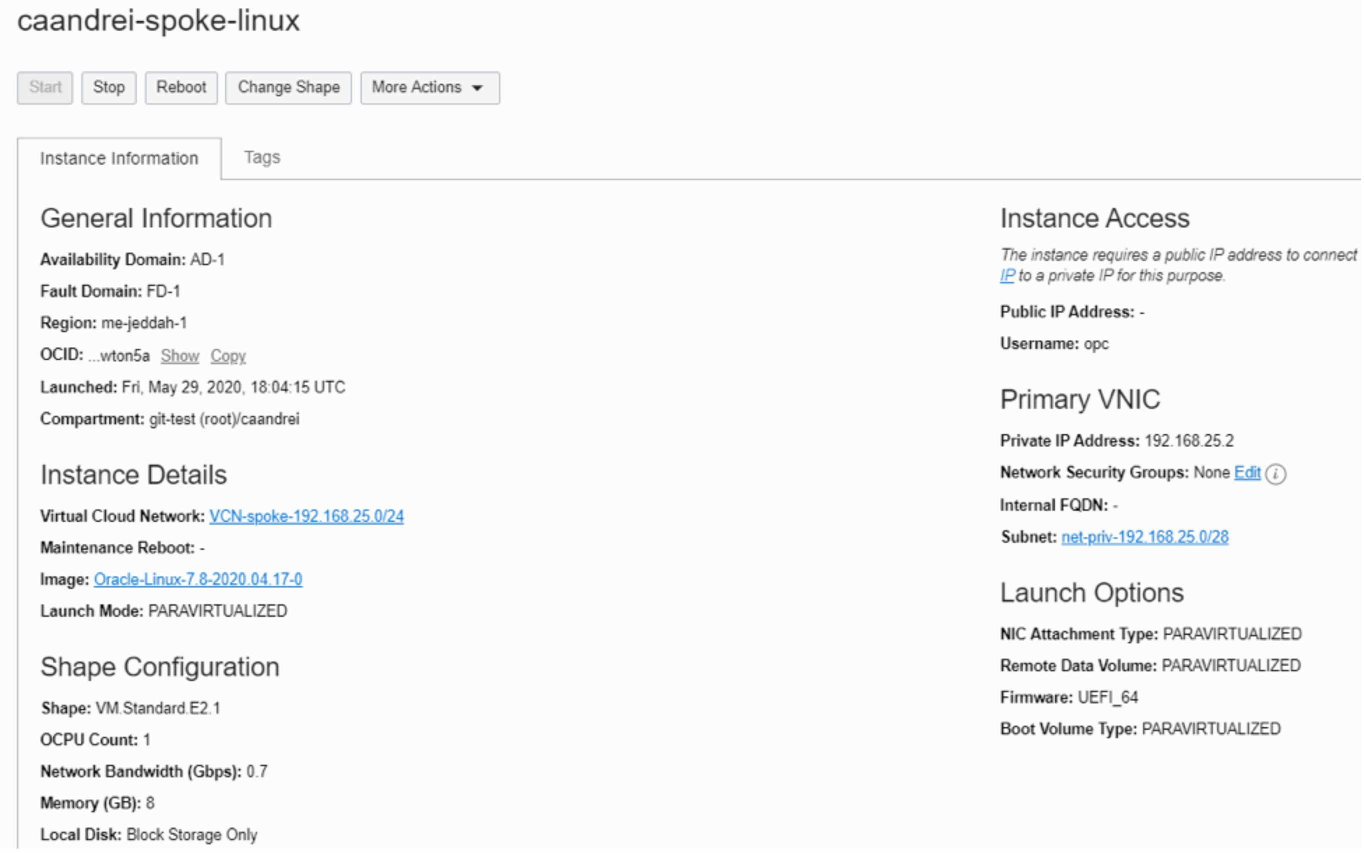
caandrei

git-test (root)/caandrei

ROUTE TABLE

caandrei-rt-192.168.23.16/28

Navigate to the region where the DRG is and create a compute VM in the spoke VCN.



caandrei-spoke-linux

General Information

Availability Domain: AD-1

Fault Domain: FD-1

Region: me-jeddah-1

OCID: ...wton5a Show Copy

Launched: Fri, May 29, 2020, 18:04:15 UTC

Compartment: git-test (root)/caandrei

Instance Details

Virtual Cloud Network: VCN-spoke-192.168.25.0/24

Maintenance Reboot: -

Image: Oracle-Linux-7.8-2020.04.17-0

Launch Mode: PARAVIRTUALIZED

Shape Configuration

Shape: VM.Standard.E2.1

OCPU Count: 1

Network Bandwidth (Gbps): 0.7

Memory (GB): 8

Local Disk: Block Storage Only

Instance Access

The instance requires a public IP address to connect
IP to a private IP for this purpose.

Public IP Address: -

Username: opc

Primary VNIC

Private IP Address: 192.168.25.2

Network Security Groups: None Edit

Internal FQDN: -

Subnet: net-priv-192.168.25.0/28

Launch Options

NIC Attachment Type: PARAVIRTUALIZED

Remote Data Volume: PARAVIRTUALIZED

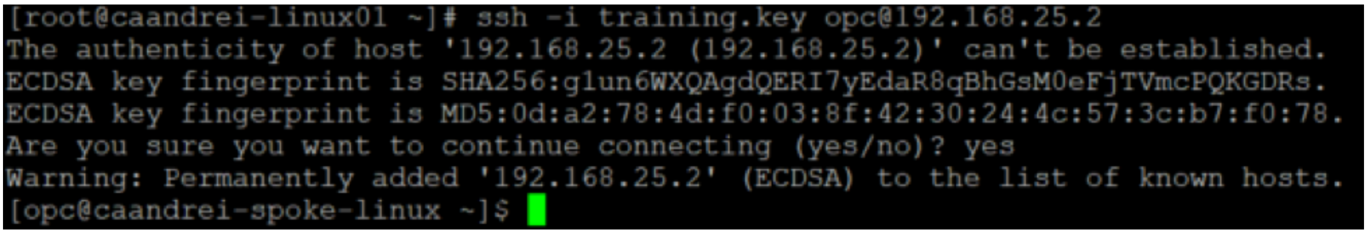
Firmware: UEFI_64

Boot Volume Type: PARAVIRTUALIZED

Test the connectivity

Connect to the private VM that is behind the Libreswan. Create the private key (use the same steps from lab1)

Connect from the Private VM to the spoke VM



```
[root@caandrei-linux01 ~]# ssh -i training.key opc@192.168.25.2
The authenticity of host '192.168.25.2 (192.168.25.2)' can't be established.
ECDSA key fingerprint is SHA256:g1un6WXQAgdQERI7yEdaR8qBhGsM0eFjTVmcPQKGDRs.
ECDSA key fingerprint is MD5:0d:a2:78:4d:f0:03:8f:42:30:24:4c:57:3c:b7:f0:78.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.25.2' (ECDSA) to the list of known hosts.
[opc@caandrei-spoke-linux ~]$
```

Observe that we connected to the spoke VCN