Lab 1: VCN Basics

Introduction

The cloud paradigm changes the way applications are developed, architected, and operated. Improved agility, speed of development, and increased automation in operations allow enterprises to truly benefit from cloud infrastructure.

Security is one of the main concerns when assessing migration and operating an application in the cloud. However, nowadays applications can benefit from several additional layers of security when deployed in the cloud. It is up to the cloud architect to leverage the many features offered by most IaaS providers to ensure that an application remains highly available, robust, and secure while offering a good experience to end-users.

The instructions in the lab go through the necessary steps of implementing **two VM**, one in a Public Subnet accessible from the Internet, and the second one in a Private Subnet. Both subnets are part of a VCN and for security, they are using NSG.

Objective

This lab walks you to the steps needed to the below resources

1. VCN
2. Public subnet
3. Private subnet
4. VM's in each subnet
5. Gateway
6. Routing Rules
7. NSG's

We will conncet to the VM in public subnet via the Internet Gateway and from that VM then to the VM in the private subnet

Pre-Requisite

To perform the lab you will need the access to the following:

1. Web Browser
2. OCI Tenenacy with the right permissions
3. Putty and putty-gen for Windows user or Terminal for Mac users

Best practise and Consideration

Keep in mind that this is a lab, so choose appropriate VM shapes. Use a Naming Convention for your resources to easily identify them. As a suggestion, you can start with your signum followed by the resource type. Please find below some examples:

> **VCN:** *caandrei-vcn-192.168.23.0/24* **Subnet:** *caandrei-net-192.168.23.0/28* **Route table:** *caandrei-rt-192.168.23.0/28* **Security list:** *caandrei-sl-192.168.23.0/28*

Architecture Overview

The scenario deployed will show the access to a private VM via a bastion host. In the lab we will use relaxed security and will permit ssh access to the bastion from everywhere (0.0.0.0/0). In a production environment, this will be restricted to the authorized Public IP addresses.

Section

> ## Generate the public/private key

> ### MAC/LINUX

1. Generate ssh-keys for your machine if you don’t have one. As long as an id_rsa and id_rsa.pub key pair is present they can be reused. By default these are stored in ~/.ssh folder. Enter the following command if you are using MAC or Linux Desktop:

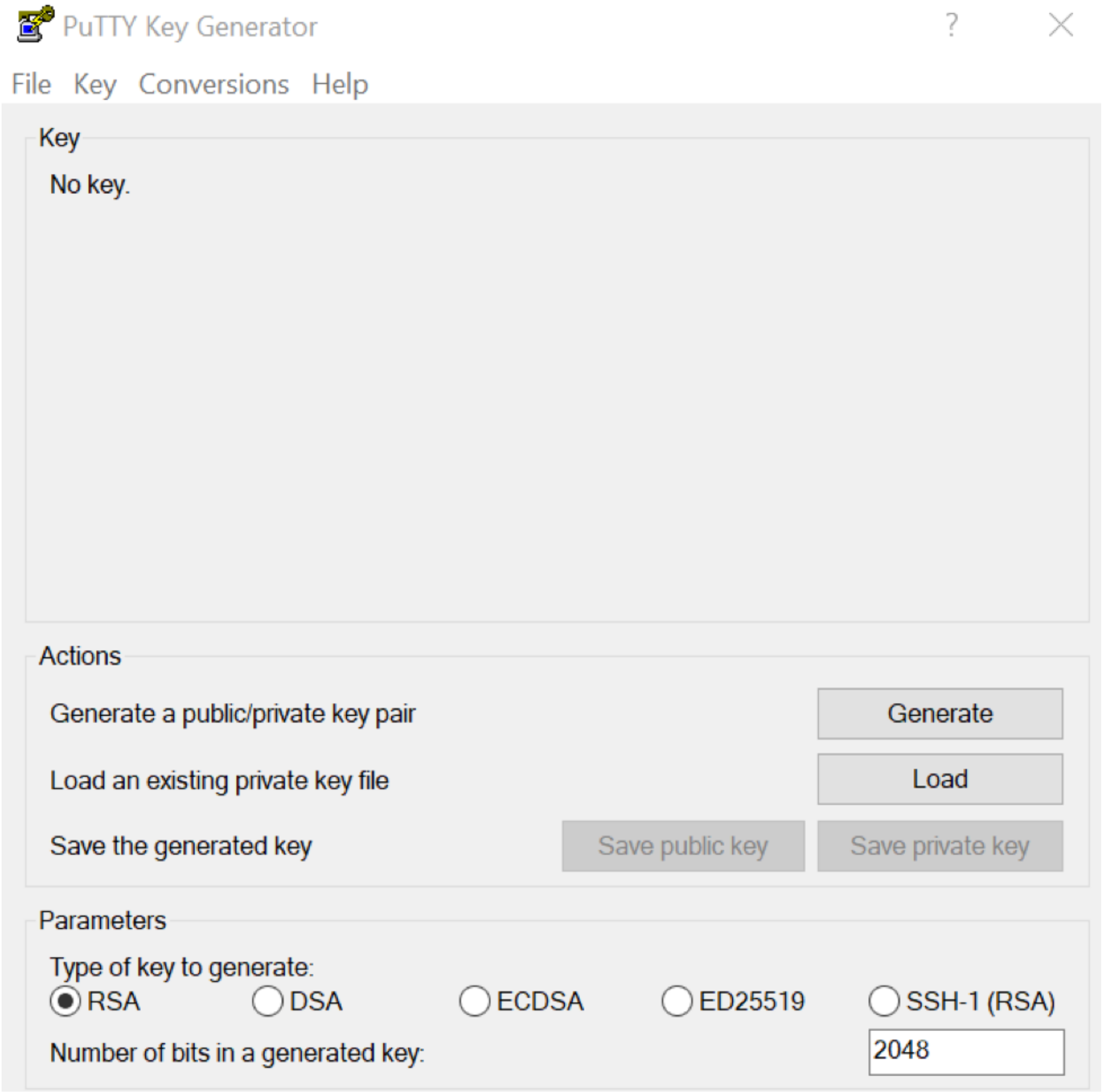
```
ssh-keygen
```

2. Make sure permissions are restricted, sometimes ssh will fail if private keys have permissive permissions.

```
chmod 0700 ~/.ssh
chmod 0600 ~/.ssh/id_rsa
chmod 0644 ~/.ssh/id_rsa.pub
```

> ### FOR WINDOWS

Open puttygen (or a similar tool), make sure that the key is RSA and the length of the key is 2048 and hit generate:



No key.

Generate a public/private key pair

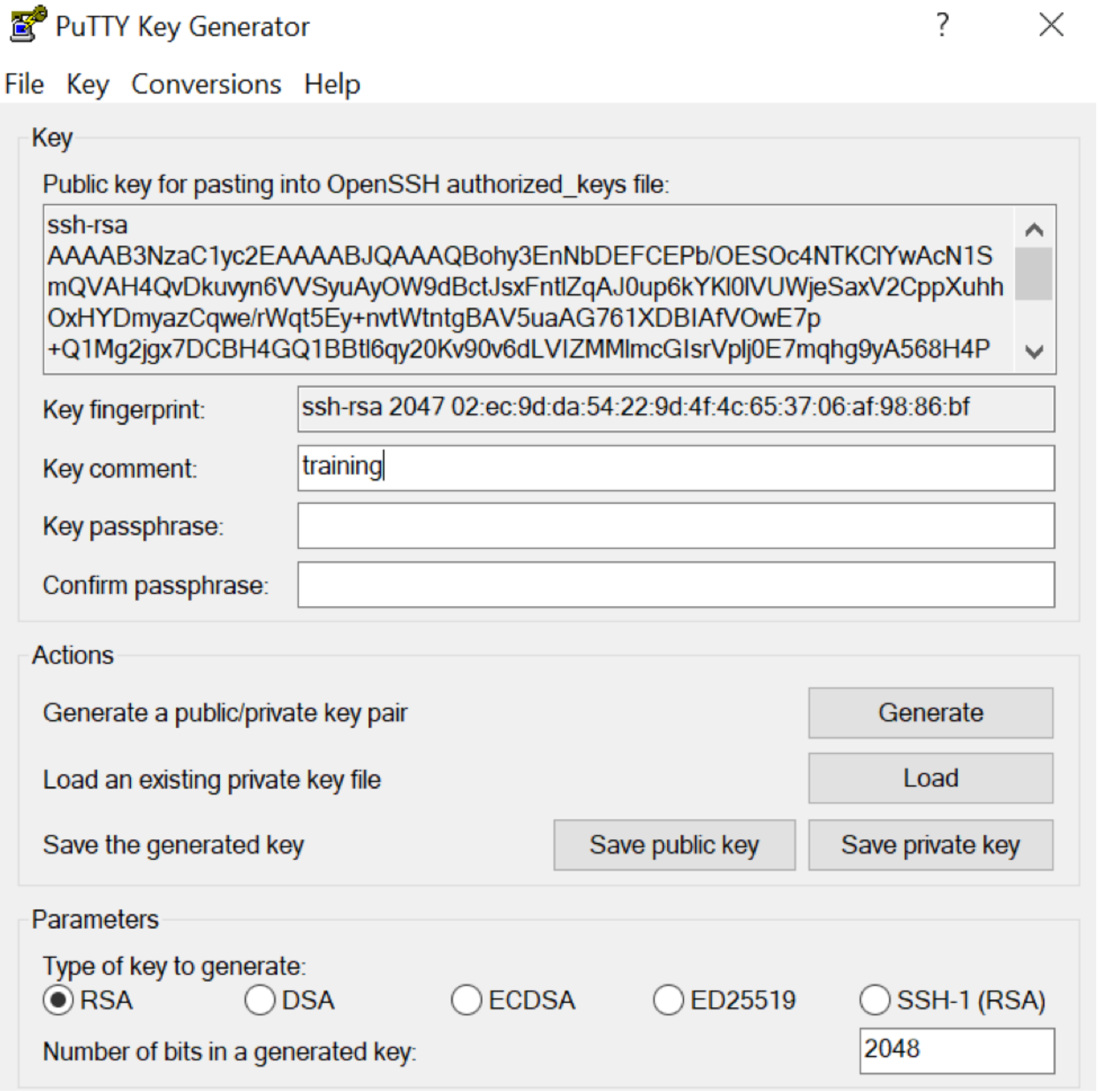
Load an existing private key file

Save the generated key

Type of key to generate:
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

Wait for the process to finish and save the private key (putty format and openssh format).



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQBohy3EnNbDEFCEPb/OESOc4NTKClYwAcN1S
mQVAH4QvDkuvyn6VVSyuAyOW9dBctJsxFntlZqAJ0up6kYKl0lVUWjeSaxV2CppXuhh
OxHYDmyazCqwe/rWqt5Ey+nvtWtntgBAV5uaAG761XDBIAfVOwE7p
+Q1Mg2jgx7DCBH4GQ1BBtl6qy20Kv90v6dLVIZMMlmcGIsrVplj0E7mqhg9yA568H4P
```

Key fingerprint: ssh-rsa 2047 02:ec:9d:da:54:22:9d:4f:4c:65:37:06:af:98:86:bf

Key comment: training

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:

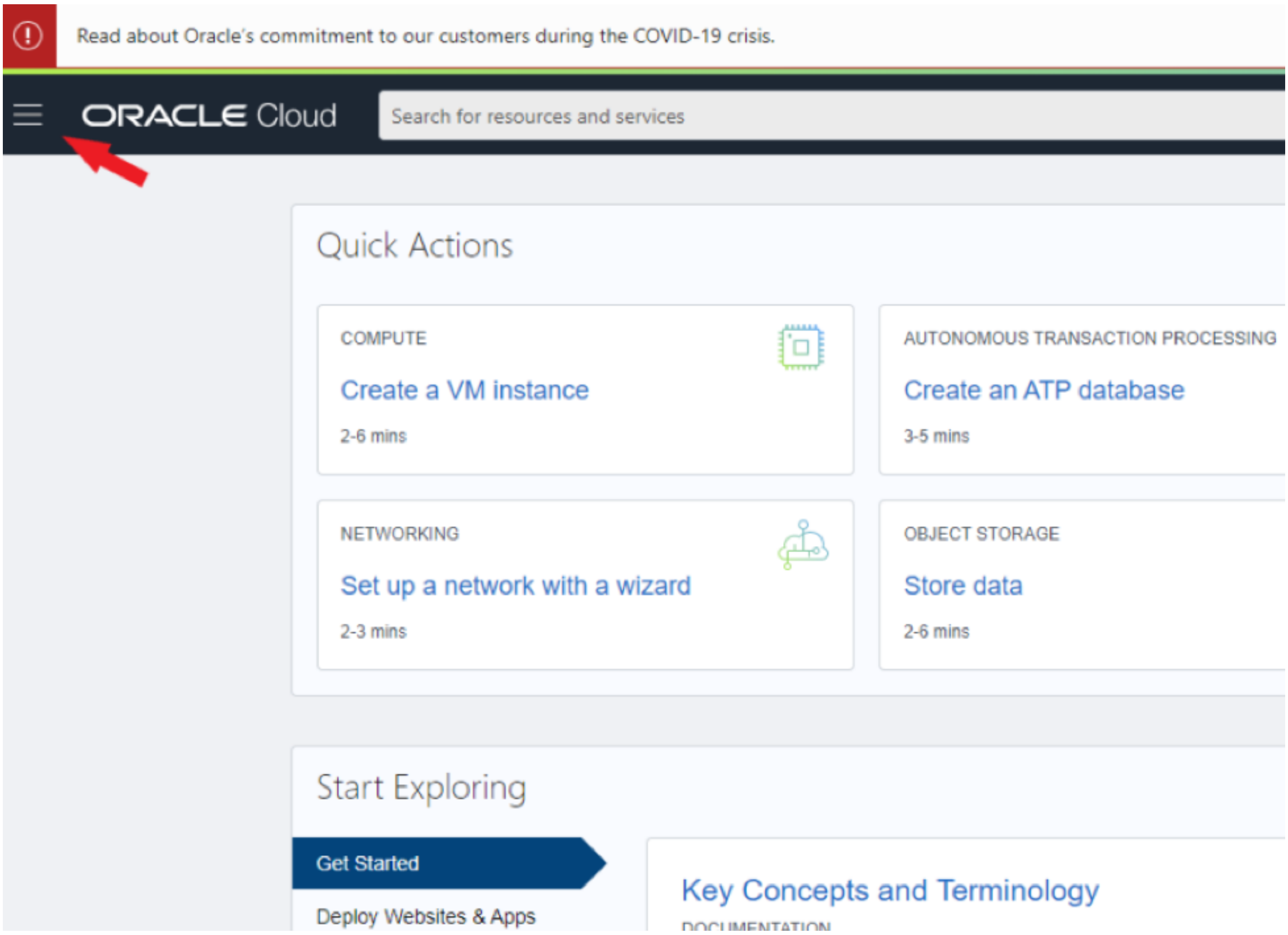
● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

To save the private key in the putty format (.ppk) click on the “Save private key” button. To save the private key to openssh format, navigate to conversions and select “Export OpenSSH key”. Keep this application open, we will use it later in the lab.

Create the network resources

Open your browser and navigate to the OCI webUI. Once you login navigate to the Networking section



Read about Oracle's commitment to our customers during the COVID-19 crisis.

Quick Actions

COMPUTE
Create a VM instance
2-6 mins

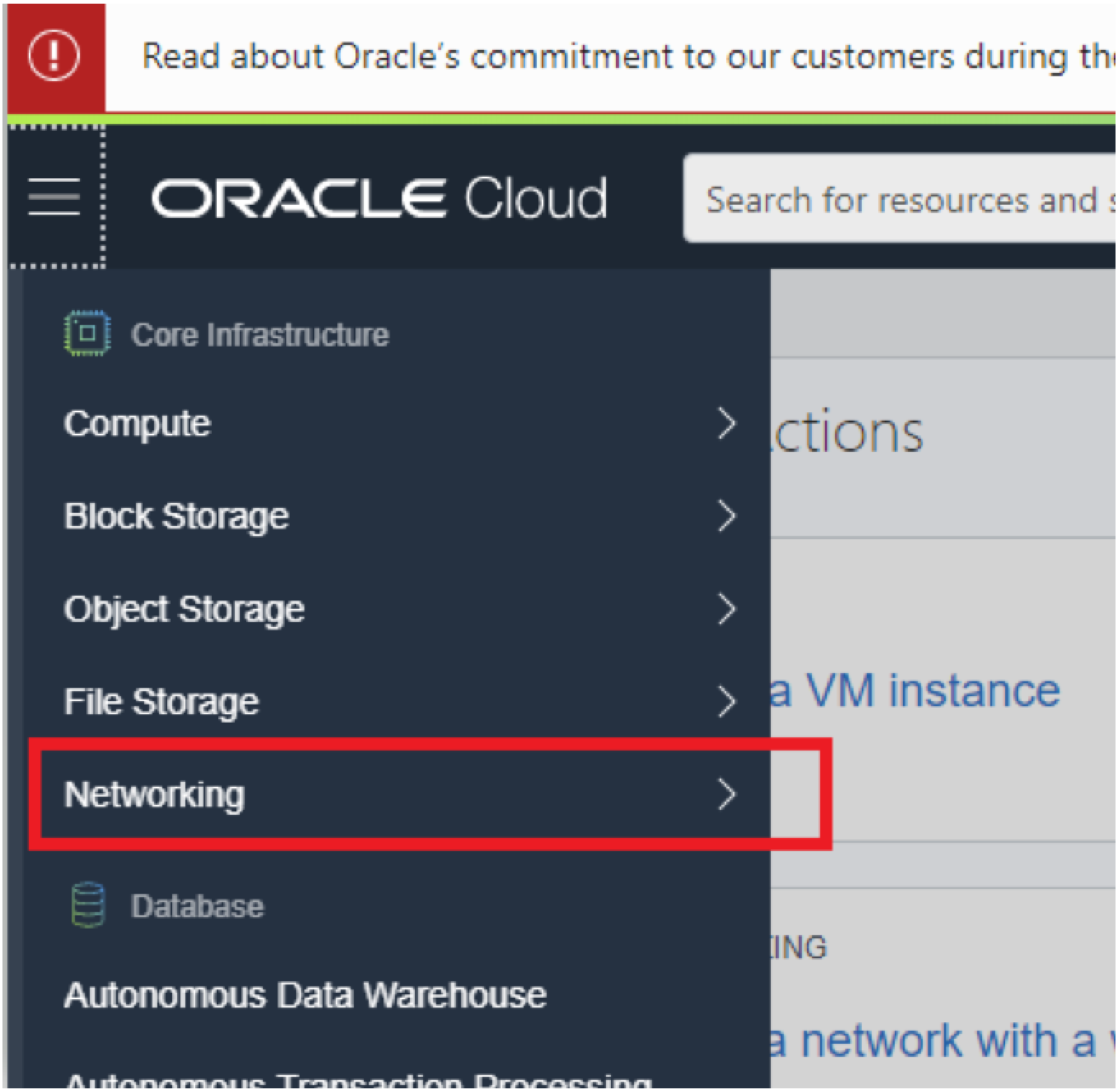
AUTONOMOUS TRANSACTION PROCESSING
Create an ATP database
3-5 mins

NETWORKING
Set up a network with a wizard
2-3 mins

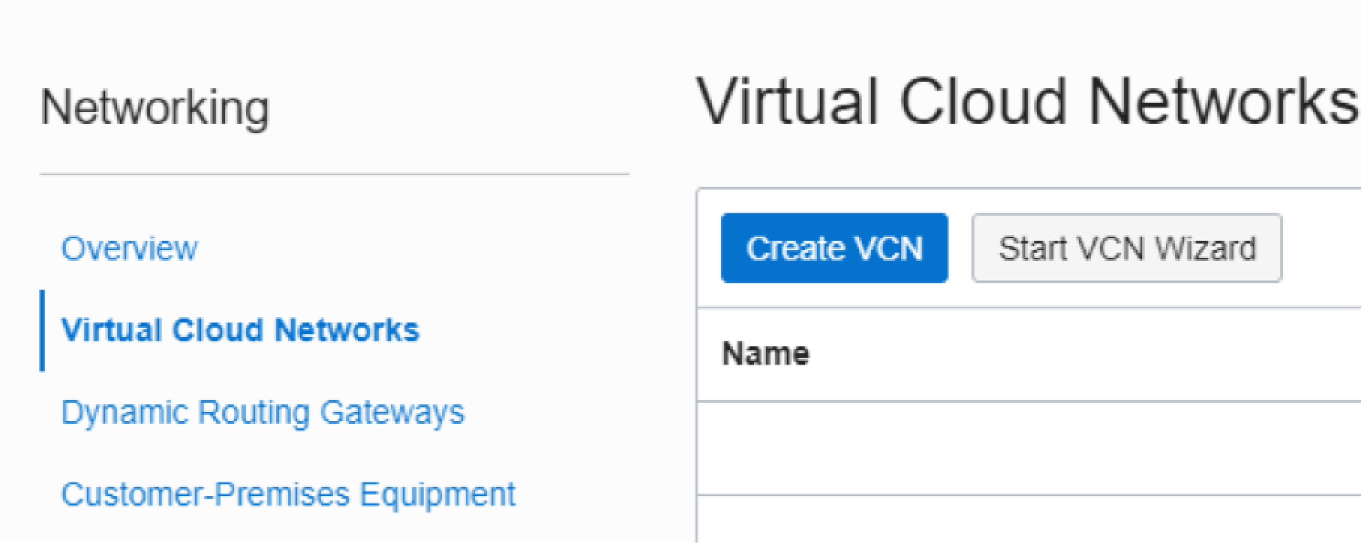
OBJECT STORAGE
Store data
2-6 mins

Start Exploring

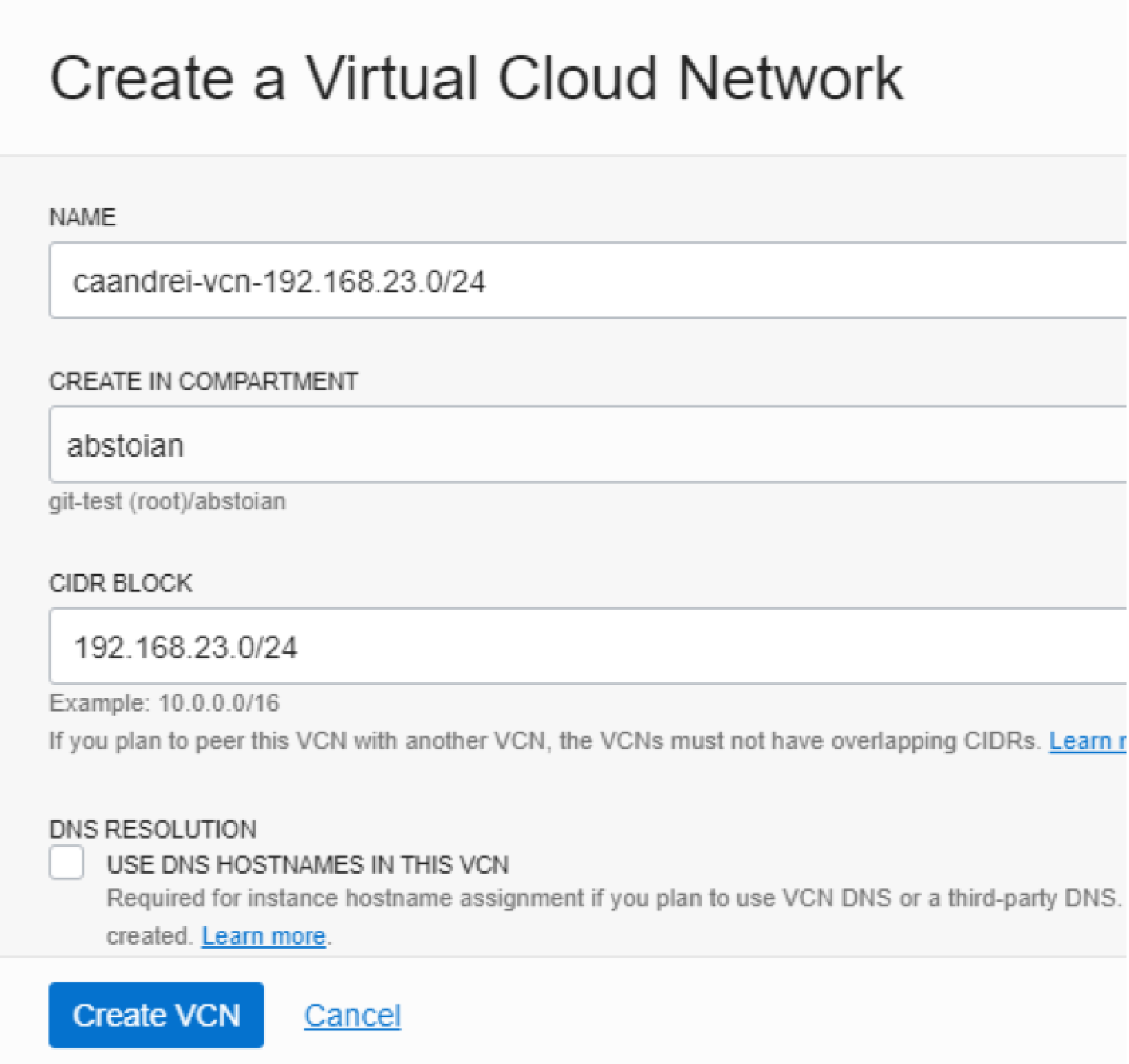
Key Concepts and Terminology
DOCUMENTATION


Read about Oracle's commitment to our customers during th
ORACLE Cloud
Search for resources and s
Core Infrastructure
Compute
Block Storage
Object Storage
File Storage
Networking
Database
Autonomous Data Warehouse
Autonomous Transaction Processing
ctions
a VM instance
ING
a network with a

Navigate to the VCN section and select Create VCN



Put the name, select compartment and the CIDR Block. I disabled the DNS resolution inside the VCN



Create a Virtual Cloud Network

NAME

caandrei-vcn-192.168.23.0/24

CREATE IN COMPARTMENT

abstoian

git-test (root)/abstoian

CIDR BLOCK

192.168.23.0/24

Example: 10.0.0.0/16

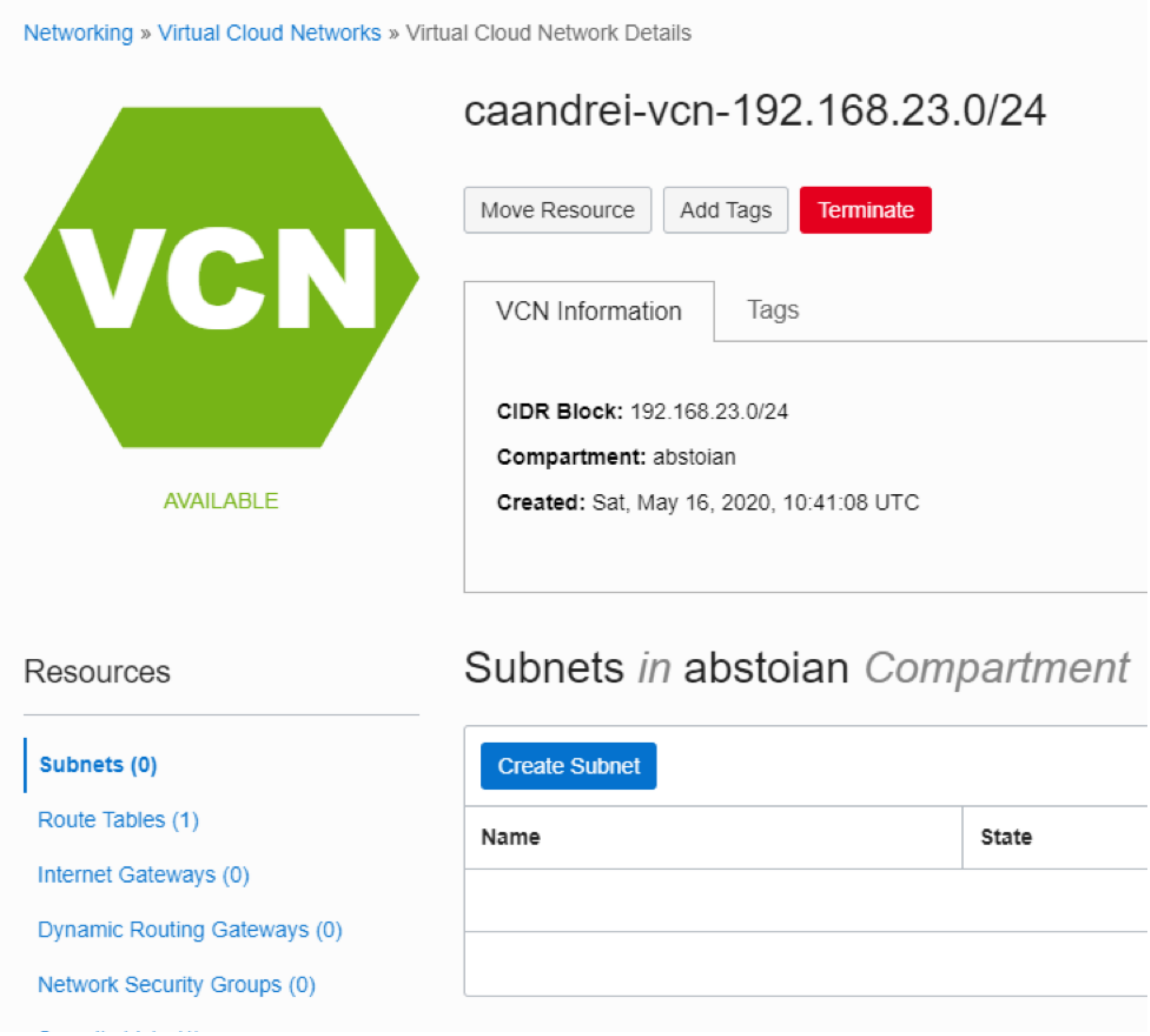
If you plan to peer this VCN with another VCN, the VCNs must not have overlapping CIDRs. Learn r

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. created. Learn more.

Click on the “Create Subnet” button



Networking » Virtual Cloud Networks » Virtual Cloud Network Details

caandrei-vcn-192.168.23.0/24

CIDR Block: 192.168.23.0/24

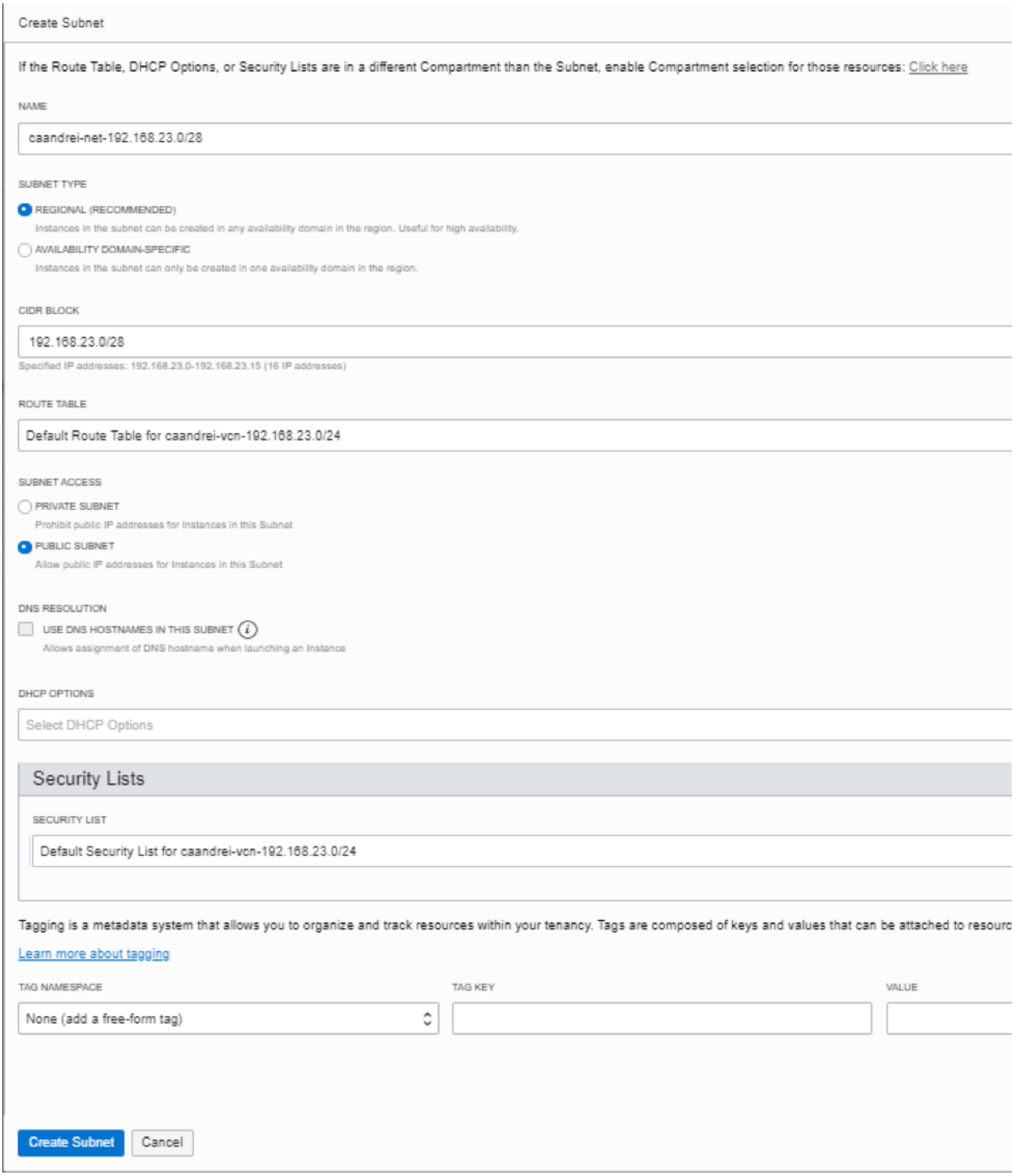
Compartment: abstoian

Created: Sat, May 16, 2020, 10:41:08 UTC

Subnets *in* abstoian *Compartment*

Name	State

Click the “Create Subnet” button and we will configure the Public Subnet. Fill the name, select “Regional”, fill the “CIDR Block”. I will use for now the Default route table and the Default Security List.



Create Subnet

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, enable Compartment selection for those resources: Click here

NAME

caandrei-net-192.168.23.0/28

SUBNET TYPE

● REGIONAL (RECOMMENDED)

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

○ AVAILABILITY DOMAIN-SPECIFIC

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

CIDR BLOCK

192.168.23.0/28

Specified IP addresses: 192.168.23.0-192.168.23.15 (16 IP addresses)

ROUTE TABLE

Default Route Table for caandrei-vcn-192.168.23.0/24

SUBNET ACCESS

○ PRIVATE SUBNET

Prohibit public IP addresses for Instances in this Subnet

● PUBLIC SUBNET

Allow public IP addresses for Instances in this Subnet

DNS RESOLUTION

□ USE DNS HOSTNAMES IN THIS SUBNET

Allows assignment of DNS hostname when launching an Instance

DHCP OPTIONS

Select DHCP Options

Security Lists

SECURITY LIST

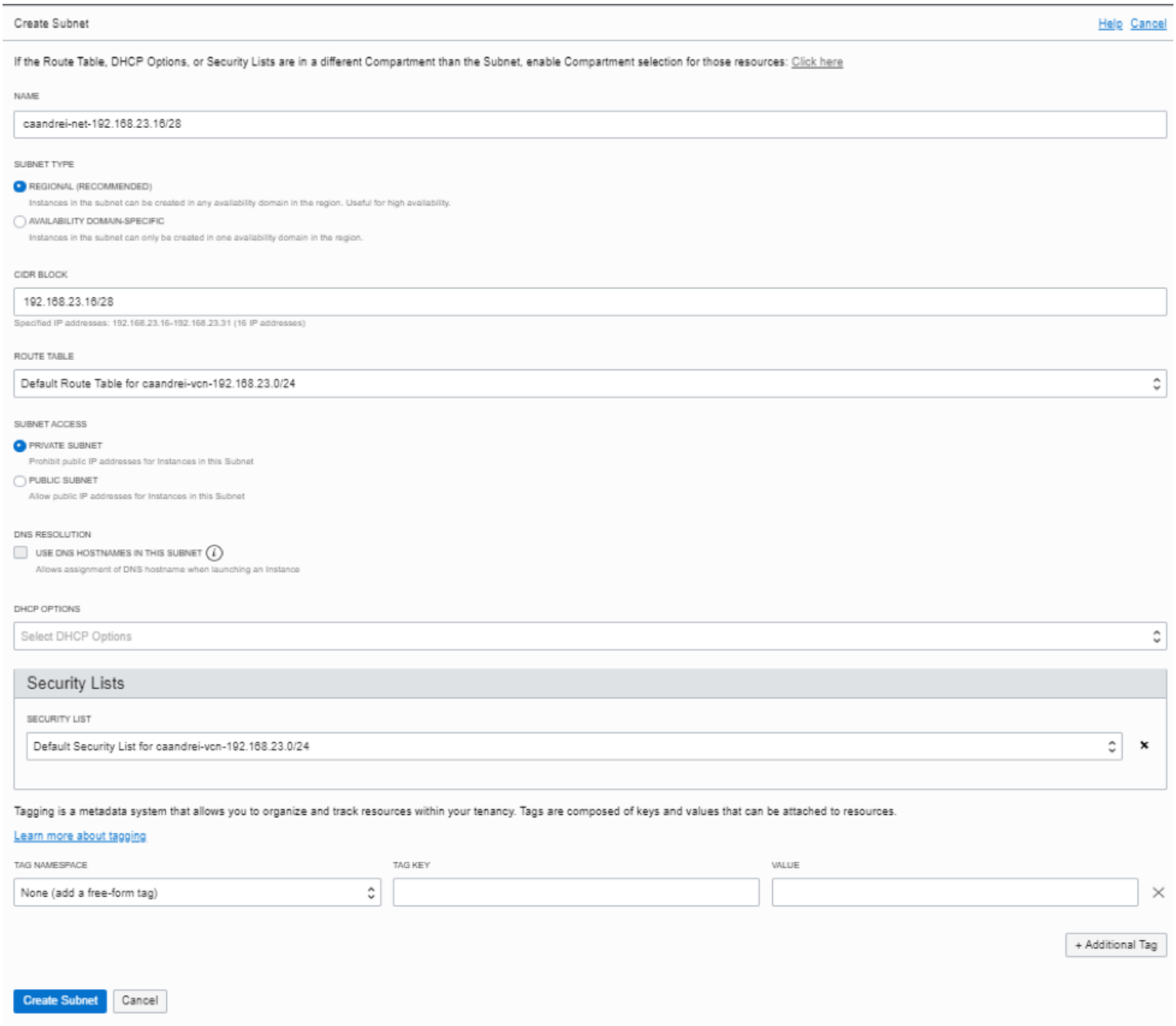
Default Security List for caandrei-vcn-192.168.23.0/24

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resourc

Learn more about tagging

TAG NAMESPACE	TAG KEY	VALUE
None (add a free-form tag)		

Perform the same Steps to create the Private Subnet



Create Subnet

If the Route Table, DHCP Options, or Security Lists are in a different Compartment than the Subnet, enable Compartment selection for those resources: Click here

NAME

caandrei-net-192.168.23.16/28

SUBNET TYPE

● REGIONAL (RECOMMENDED)

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

○ AVAILABILITY DOMAIN-SPECIFIC

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

CIDR BLOCK

192.168.23.16/28

Specified IP addresses: 192.168.23.16-192.168.23.31 (16 IP addresses)

ROUTE TABLE

Default Route Table for caandrei-vcn-192.168.23.0/24

SUBNET ACCESS

● PRIVATE SUBNET

Prohibit public IP addresses for Instances in this Subnet

○ PUBLIC SUBNET

Allow public IP addresses for Instances in this Subnet

DNS RESOLUTION

□ USE DNS HOSTNAMES IN THIS SUBNET

Allows assignment of DNS hostname when launching an Instance

DHCP OPTIONS

Select DHCP Options

Security Lists

SECURITY LIST

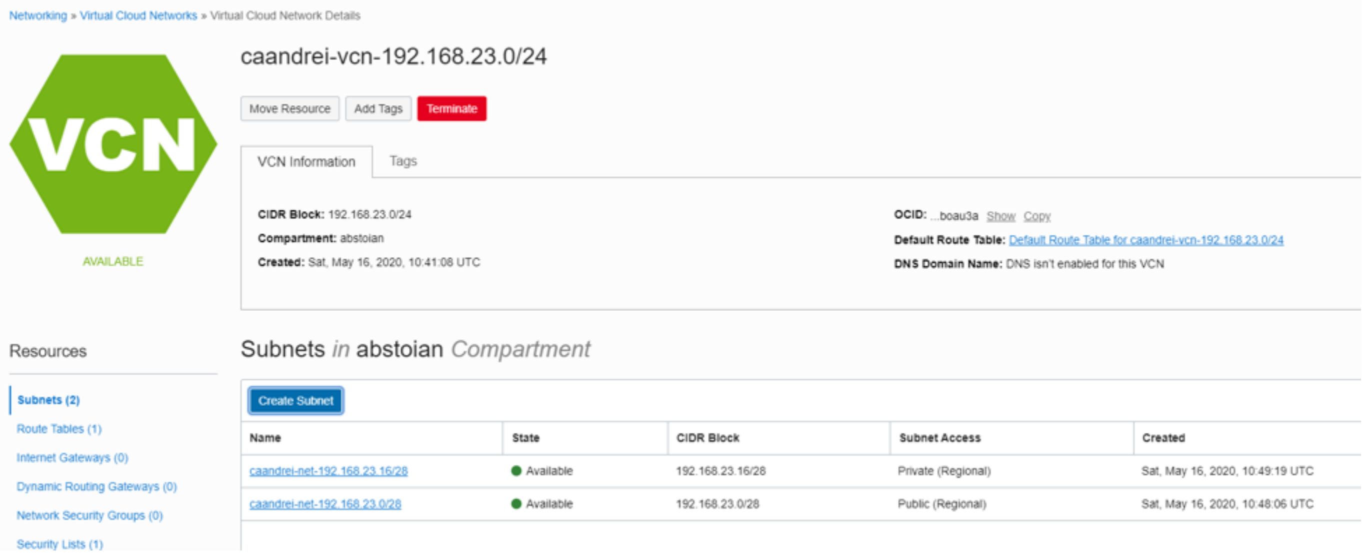
Default Security List for caandrei-vcn-192.168.23.0/24

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.

Learn more about tagging

TAG NAMESPACE	TAG KEY	VALUE
None (add a free-form tag)		

The resulting 2 subnets will look like this



Networking » Virtual Cloud Networks » Virtual Cloud Network Details

caandrei-vcn-192.168.23.0/24

CIDR Block: 192.168.23.0/24

Compartment: abstoian

Created: Sat, May 16, 2020, 10:41:08 UTC

OCID: ...boau3a Show Copy

Default Route Table: Default Route Table for caandrei-vcn-192.168.23.0/24

DNS Domain Name: DNS isn't enabled for this VCN

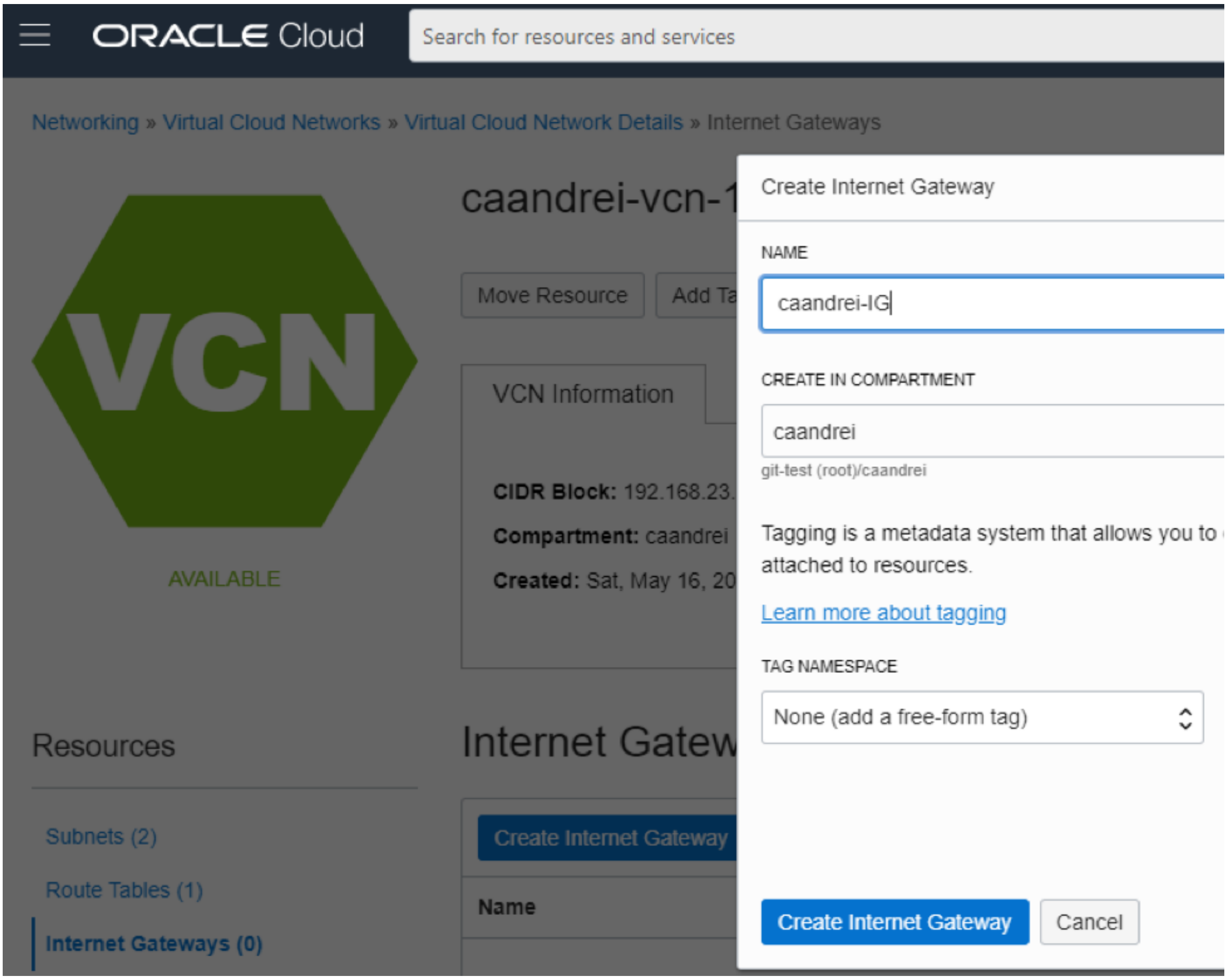
Resources

- Subnets (2)
- Route Tables (1)
- Internet Gateways (0)
- Dynamic Routing Gateways (0)
- Network Security Groups (0)
- Security Lists (1)

Subnets *in* abstoian *Compartment*

Name	State	CIDR Block	Subnet Access	Created
caandrei-net-192.168.23.16/28	● Available	192.168.23.16/28	Private (Regional)	Sat, May 16, 2020, 10:49:19 UTC
caandrei-net-192.168.23.0/28	● Available	192.168.23.0/28	Public (Regional)	Sat, May 16, 2020, 10:48:06 UTC

Navigate to the Internet Gateway section and create a new item



Create Internet Gateway

NAME

caandrei-IG

CREATE IN COMPARTMENT

caandrei

git-test (root)/caandrei

Tagging is a metadata system that allows you to attached to resources.

TAG NAMESPACE

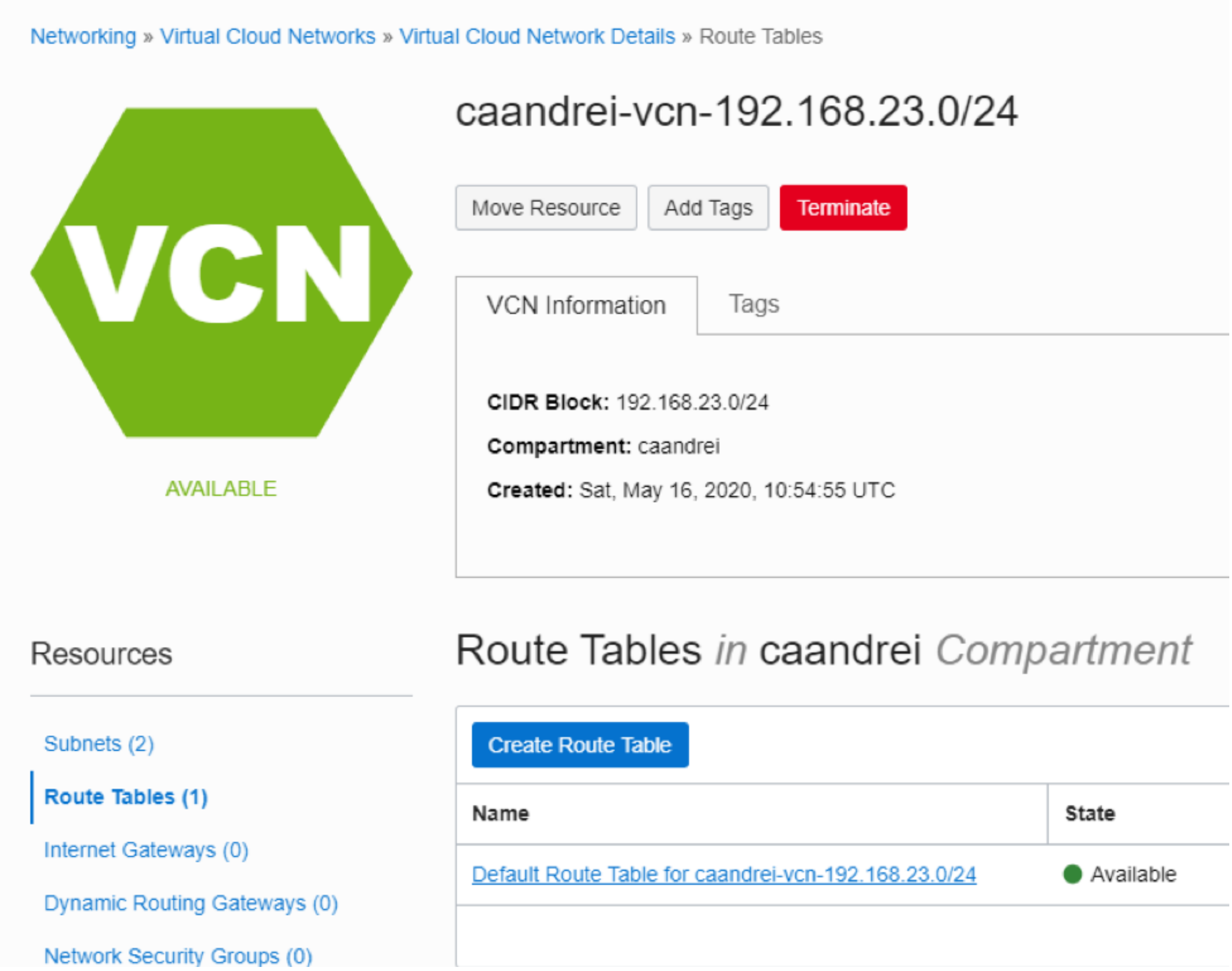
None (add a free-form tag)

CIDR Block: 192.168.23.

Compartment: caandrei

Created: Sat, May 16, 20

At this point, we want to create a routing table for each subnet. Navigate at the “route Tables” section and click the “Create Route Table” button



Networking » Virtual Cloud Networks » Virtual Cloud Network Details » Route Tables

caandrei-vcn-192.168.23.0/24

CIDR Block: 192.168.23.0/24

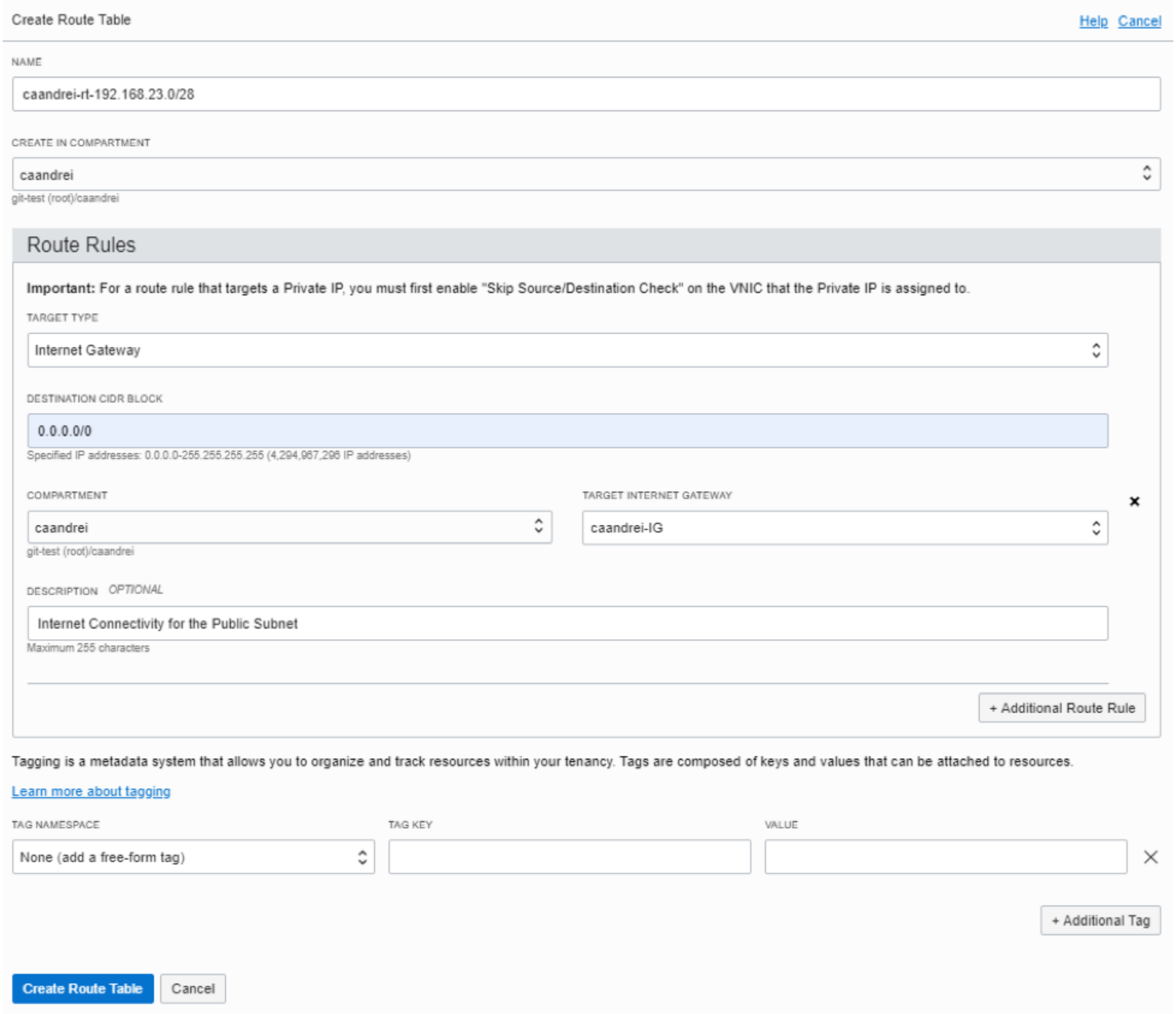
Compartment: caandrei

Created: Sat, May 16, 2020, 10:54:55 UTC

Route Tables *in* caandrei *Compartment*

Name	State
Default Route Table for caandrei-vcn-192.168.23.0/24	● Available

We will create the route table for the Public Subnet



Create Route Table

NAME

caandrei-rt-192.168.23.0/28

CREATE IN COMPARTMENT

caandrei

git-test (root)/caandrei

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.

TARGET TYPE

Internet 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)

COMPARTMENT

caandrei

git-test (root)/caandrei

TARGET INTERNET GATEWAY

caandrei-IG

DESCRIPTION *OPTIONAL*

Internet Connectivity for the Public Subnet

Maximum 255 characters

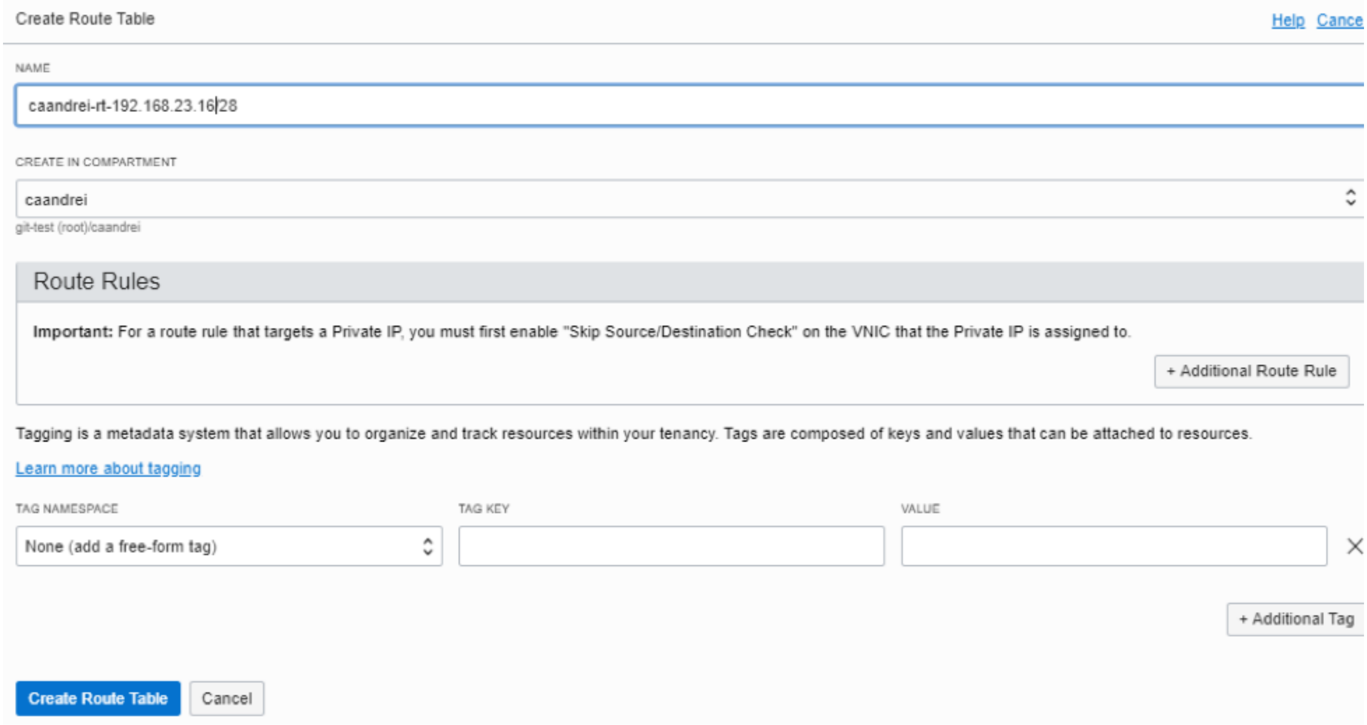
Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.

Learn more about tagging

TAG NAMESPACE	TAG KEY	VALUE
None (add a free-form tag)		

Notice that we created a default route that uses the Internet Gateway.

Create a route table for the private subnet. This table will be empty, and it will be used in a future lab.



Create Route Table

NAME: caandrei-rt-192.168.23.16|28

CREATE IN COMPARTMENT: caandrei

git-test (root)/caandrei

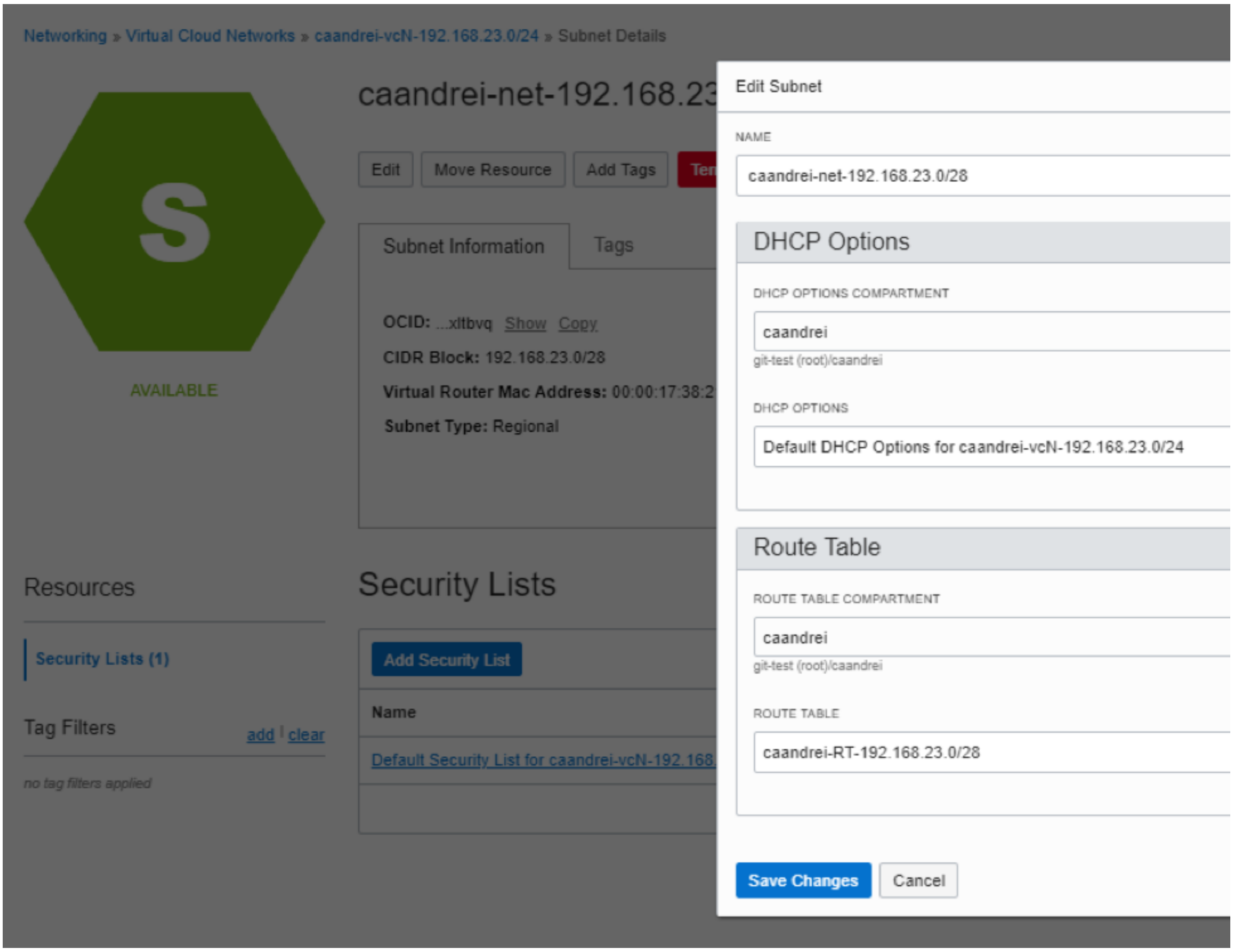
Route Rules

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.

Tagging is a metadata system that allows you to organize and track resources within your tenancy. Tags are composed of keys and values that can be attached to resources.

TAG NAMESPACE	TAG KEY	VALUE
None (add a free-form tag)		

Edit each Subnet and associate the correct route table. For example, below is a screenshot for the public subnet



Networking » Virtual Cloud Networks » caandrei-vcN-192.168.23.0/24 » Subnet Details
caandrei-net-192.168.23
S
AVAILABLE
Edit
Move Resource
Add Tags
Ter
Subnet Information
Tags

OCID: ...xltbvq Show Copy

CIDR Block: 192.168.23.0/28

Virtual Router Mac Address: 00:00:17:38:2

Subnet Type: Regional

Edit Subnet

NAME: caandrei-net-192.168.23.0/28

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

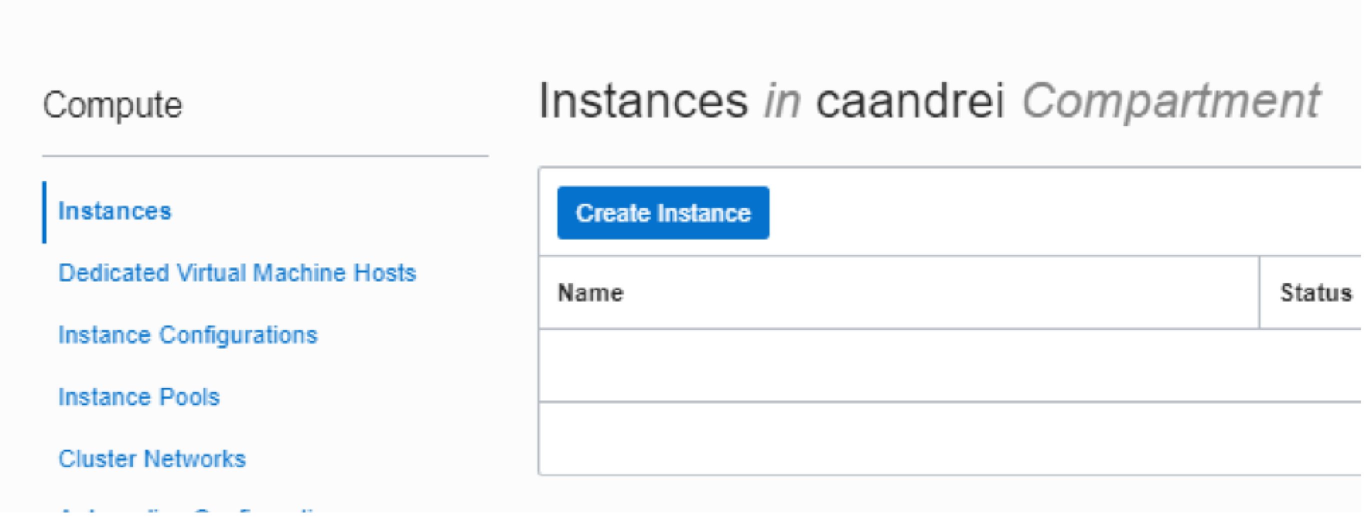
ROUTE TABLE COMPARTMENT: caandrei

git-test (root)/caandrei

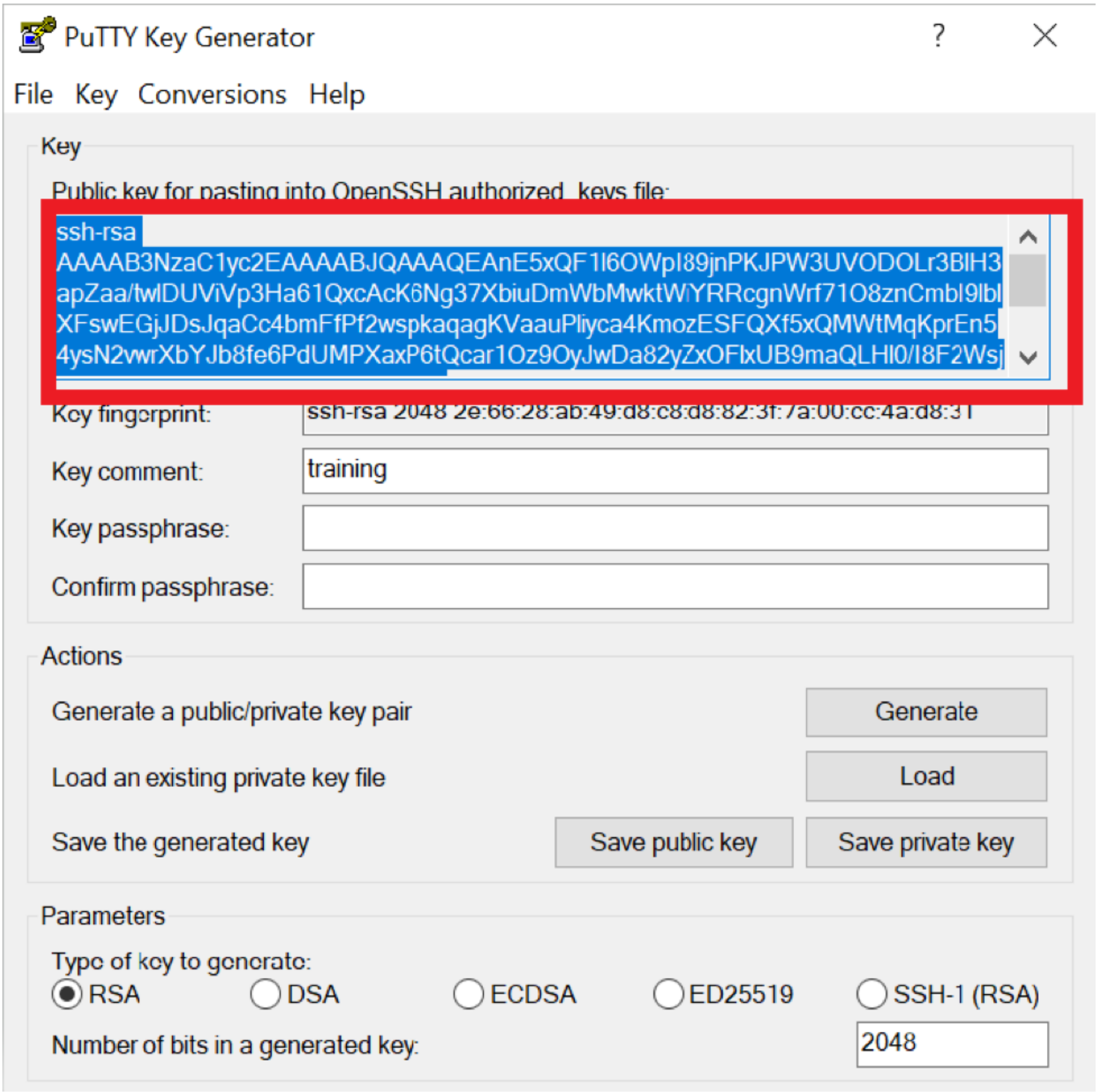
ROUTE TABLE: caandrei-RT-192.168.23.0/28

Create the Public VM

Navigate to the Compute > Instances section and click on the “Create Instance: Button



Fill in the Name, choose a VM shape (considering that we are doing a test, provision a small shape). Now we reach the Networking details: select the VCN, select the subnet (the difference between the public VM and the private VM is the subnet in which they will be provisioned). For the Public VM choose “Assign a Public IP Address”. In the puttygen that we used earlier, copy the public key and paste it in the Key section of the OCI webUI



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAnE5xQF1l6OWpl89jnPKJPW3UVODOLr3BIH3
apZaa/twIDUViVp3Ha61QxcAcK6Ng37XbiuDmWbMwktWiYRRcgnWrf71O8znCmbl9lbl
XFswEGjJDsJqaCc4bmFfPf2wspkaqagKVaauPliyca4KmozESFQXf5xQMWtMqKprEn5
4ysN2vwrXbYJb8fe6PdUMPXaxP6tQcar1Oz9OyJwDa82yZxOFlxUB9maQLHI0/I8F2Wsj
```

Key fingerprint: ssh-rsa 2048 2e:66:28:ab:49:d8:c8:d8:82:3f:7a:00:cc:4a:d8:31

Key comment: training

Key passphrase:

Confirm passphrase:

Generate a public/private key pair — Generate

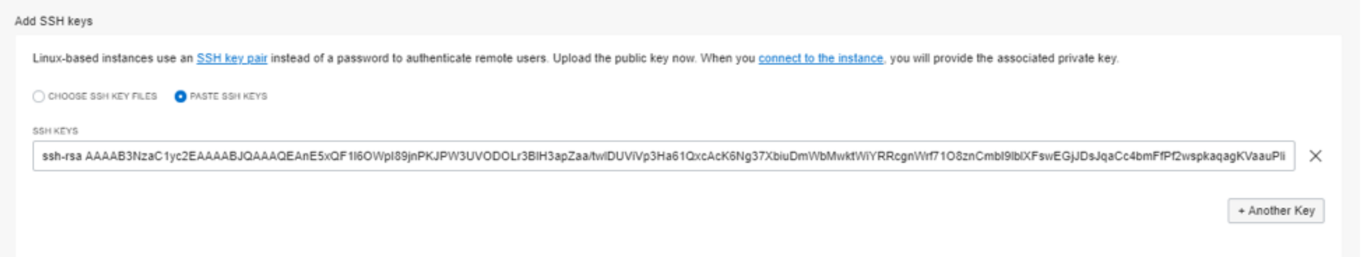
Load an existing private key file — Load

Save the generated key — Save public key — Save private key

Type of key to generate:

● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048



Add SSH keys

Linux-based instances use an SSH key pair instead of a password to authenticate remote users. Upload the public key now. When you connect to the instance, you will provide the associated private key.

○ CHOOSE SSH KEY FILES ● PASTE SSH KEYS

SSH KEYS

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAnE5xQF1l6OWpl89jnPKJPW3UVODOLr3BIH3apZaa/twIDUViVp3Ha61QxcAcK6Ng37XbiuDmWbMwktWiYRRcgnWrf71O8znCmbl9lbIXFswEGjJDsJqaCc4bmFfPf2wspkaqagKVaauPli
```

At this point, we have all the mandatory information and we are ready to click the “Create” button

Create the Private VM

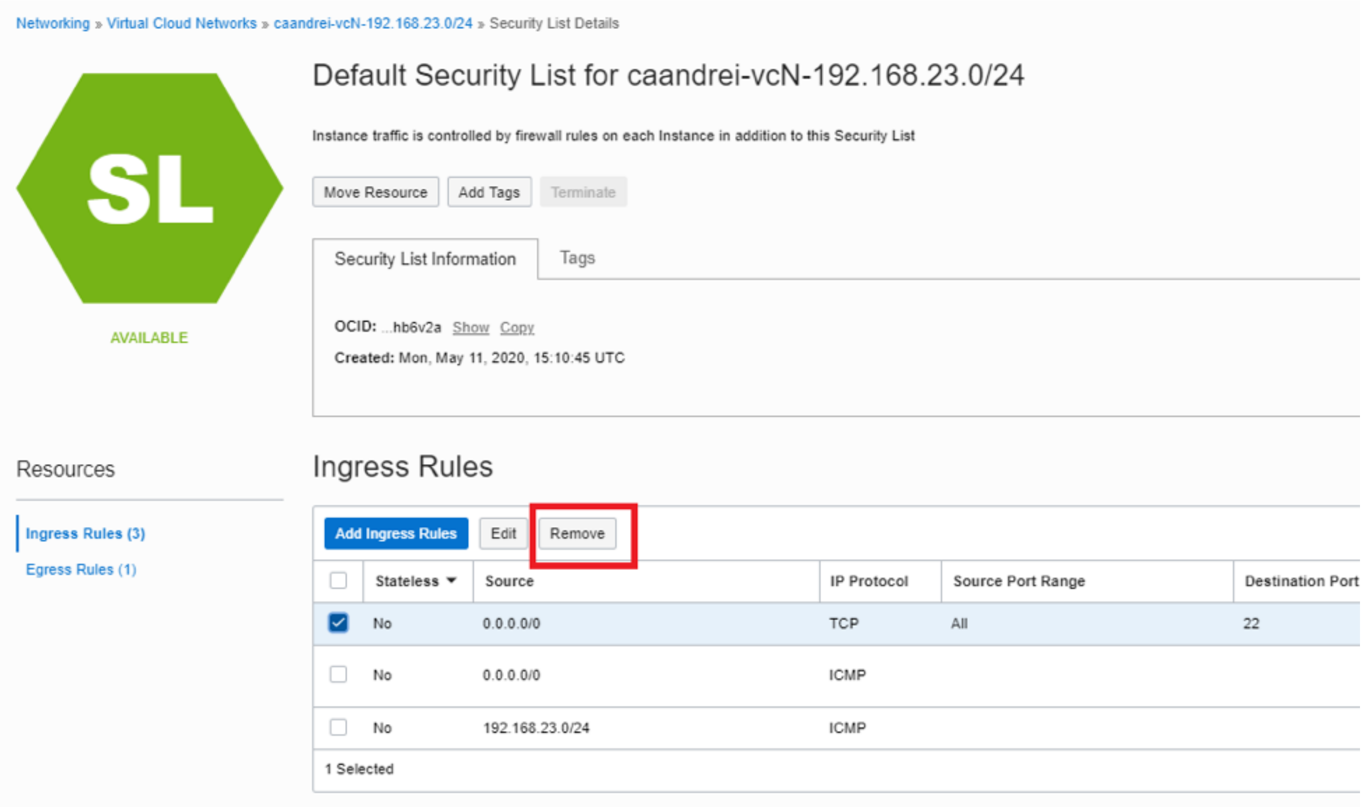
Follow the same steps and create also the Private VM

Adjust the security to permit connectivity

At this step, we will adjust the security to permit ssh connection from the Internet for the Public VM and from that VM we will connect to the private VM.

Navigate to the Networking>Virtual Cloud Networks>{Your VCN}>Security Lists and click on the Default security List

Remove the ssh access



Networking » Virtual Cloud Networks » caandrei-vcN-192.168.23.0/24 » Security List Details

Default Security List for caandrei-vcN-192.168.23.0/24

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

OCID: ...hb6v2a Show Copy

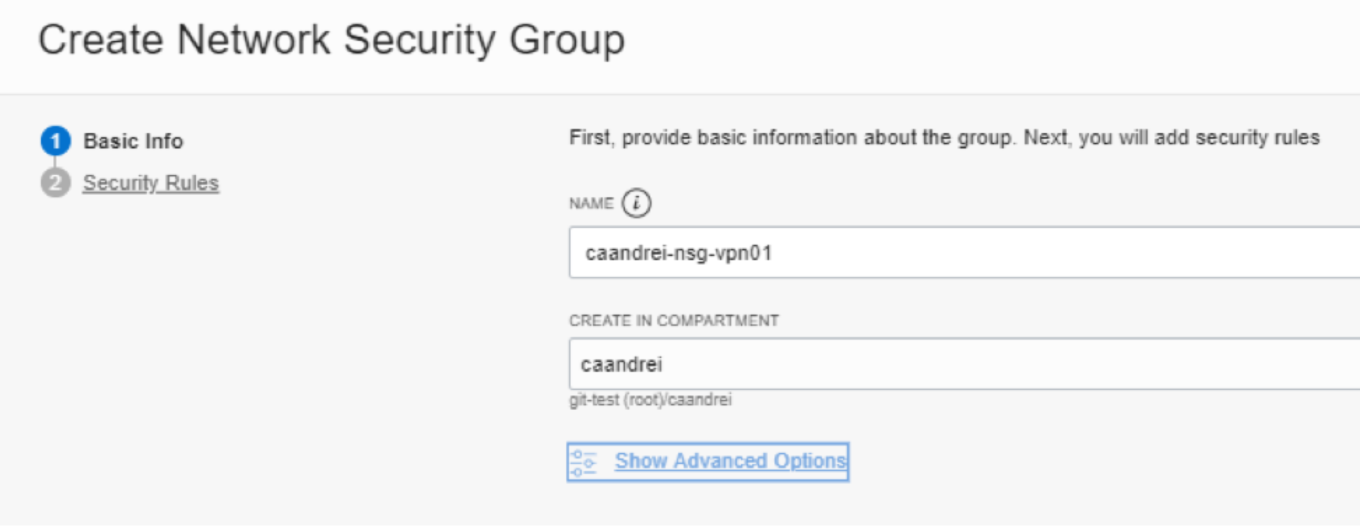
Created: Mon, May 11, 2020, 15:10:45 UTC

Ingress Rules

□	Stateless	Source	IP Protocol	Source Port Range	Destination Port
☑	No	0.0.0.0/0	TCP	All	22
□	No	0.0.0.0/0	ICMP		
□	No	192.168.23.0/24	ICMP		

1 Selected

Navigate to the Networking>Virtual Cloud Networks>{Your VCN}>Network Security Groups and create a NSG for the public VM: Fill in the Name and click next



Create Network Security Group

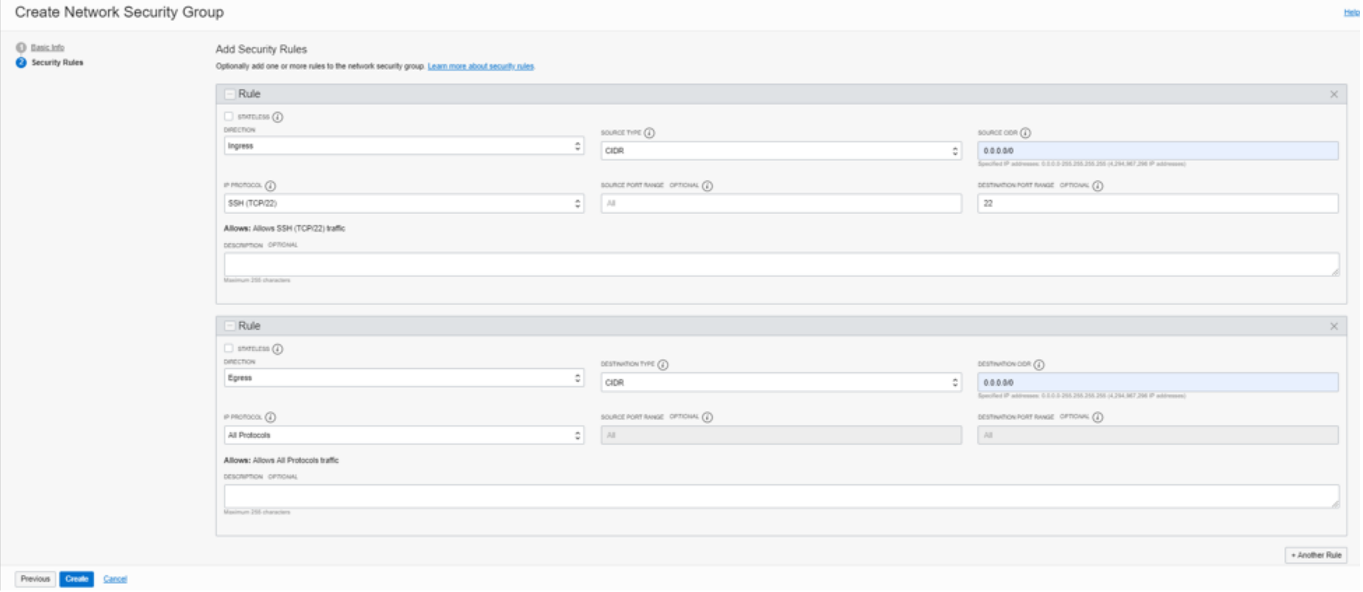
First, provide basic information about the group. Next, you will add security rules

NAME: caandrei-nsg-vpn01

CREATE IN COMPARTMENT: caandrei

git-test (root)/caandrei

Add the following rules and click **Create**



Create Network Security Group

Help

1 Basic Info
2 Security Rules

Add Security Rules

Optionally add one or more rules to the network security group. Learn more about security rules.

Rule

□ STATELESS

DIRECTION: Ingress

SOURCE TYPE: CIDR

SOURCE CIDR: 0.0.0.0/0

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

IP PROTOCOL: SSH (TCP/22)

SOURCE PORT RANGE OPTIONAL: All

DESTINATION PORT RANGE OPTIONAL: 22

Allows: Allows SSH (TCP/22) traffic

DESCRIPTION OPTIONAL

Maximum 255 characters

Rule

□ STATELESS

DIRECTION: Egress

DESTINATION TYPE: CIDR

DESTINATION CIDR: 0.0.0.0/0

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

IP PROTOCOL: All Protocols

SOURCE PORT RANGE OPTIONAL: All

DESTINATION PORT RANGE OPTIONAL: All

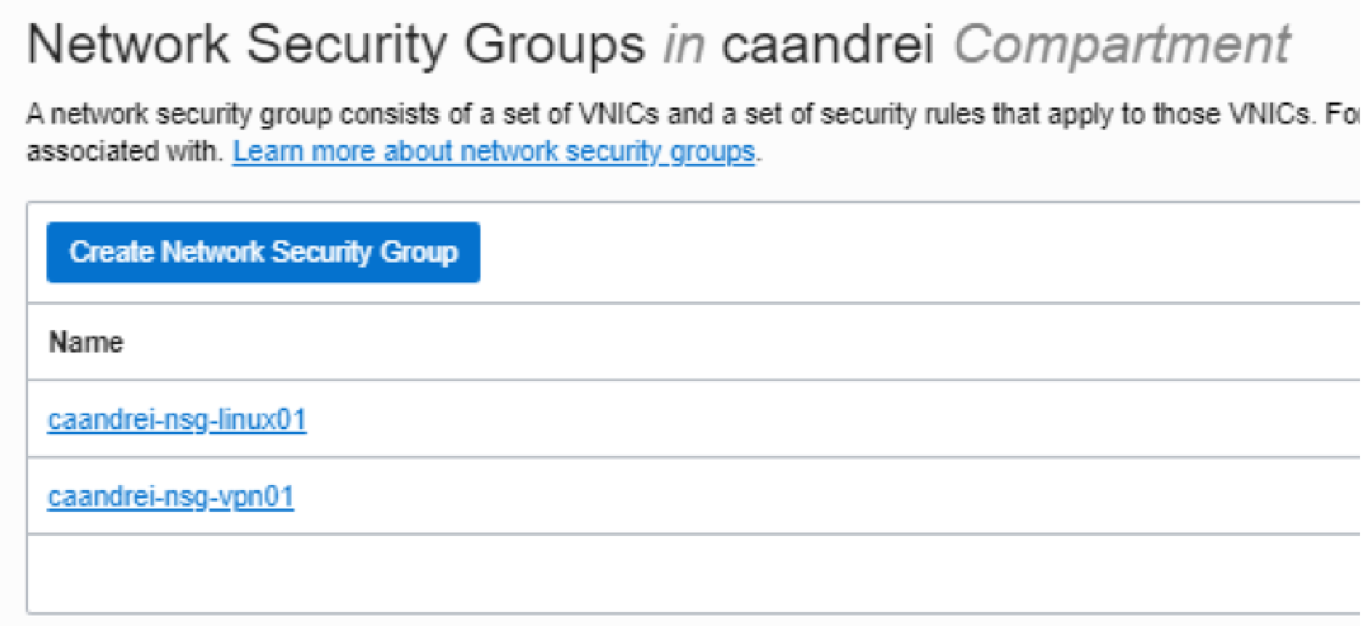
Allows: Allows All Protocols traffic

DESCRIPTION OPTIONAL

Maximum 255 characters

At this point, the public VM is reachable via SSH from the Internet and it is allowed to initiate any connection.

Create a second NSG for the private vm with the same rules. After the creation you will have two NSGs

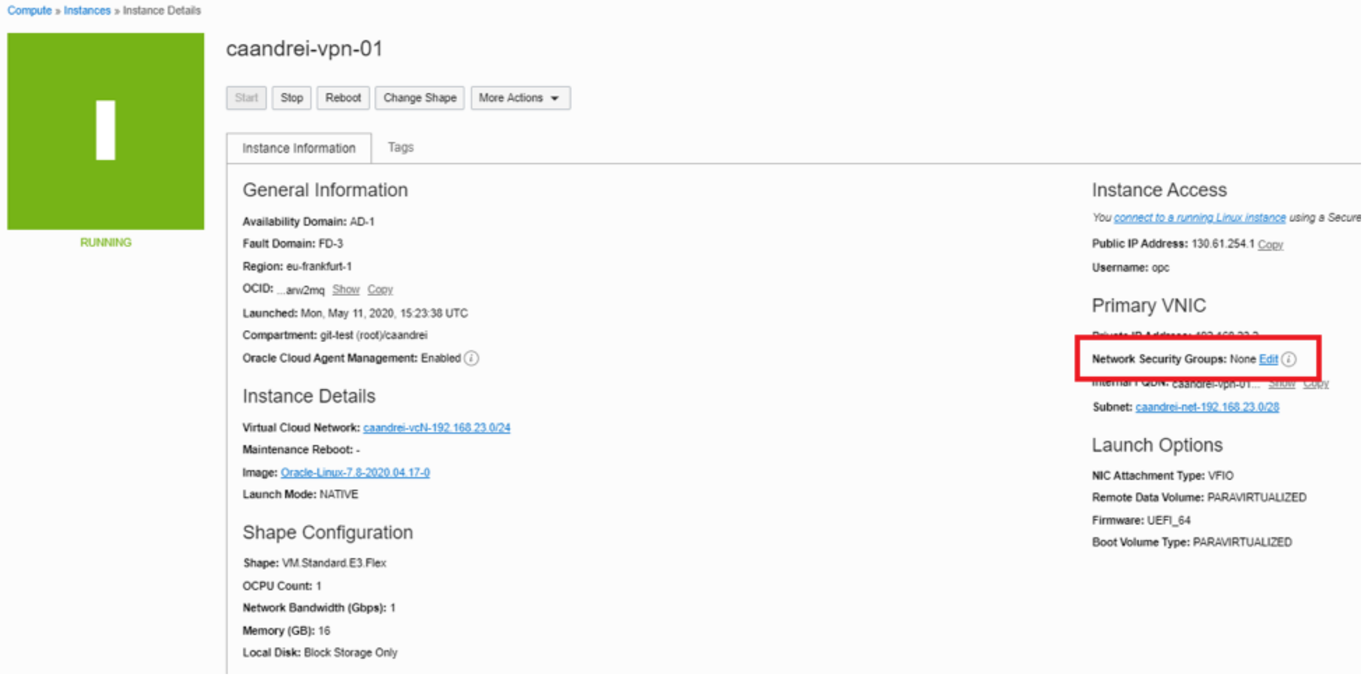


Network Security Groups *in* caandrei *Compartment*

A network security group consists of a set of VNICs and a set of security rules that apply to those VNICs. Fo
associated with. Learn more about network security groups.

Name
caandrei-nsg-linux01
caandrei-nsg-vpn01

To use them, we need to associate them with the VMs. Navigate to Compute > Instances > {Public VM} and edit the NSG section



Compute » Instances » Instance Details

caandrei-vpn-01

General Information

Availability Domain: AD-1

Fault Domain: FD-3

Region: eu-frankfurt-1

OCID: ...arv2mq Show Copy

Launched: Mon, May 11, 2020, 15:23:38 UTC

Compartment: git-test (root)/caandrei

Oracle Cloud Agent Management: Enabled

Instance Details

Virtual Cloud Network: caandrei-vcN-192.168.23.0/24

Maintenance Reboot: -

Image: Oracle-Linux-7.8-2020.04.17-0

Launch Mode: NATIVE

Shape Configuration

Shape: VM.Standard.E3.Flex

OCPU Count: 1

Network Bandwidth (Gbps): 1

Memory (GB): 16

Local Disk: Block Storage Only

Instance Access

You connect to a running Linux instance using a Secure

Public IP Address: 130.61.254.1 Copy

Username: opc

Primary VNIC

Private IP Address: 192.168.23.2

Network Security Groups: None Edit

Internal FQDN: caandrei-vpn-01... Show Copy

Subnet: caandrei-net-192.168.23.0/28

Launch Options

NIC Attachment Type: VFIO

Remote Data Volume: PARAVIRTUALIZED

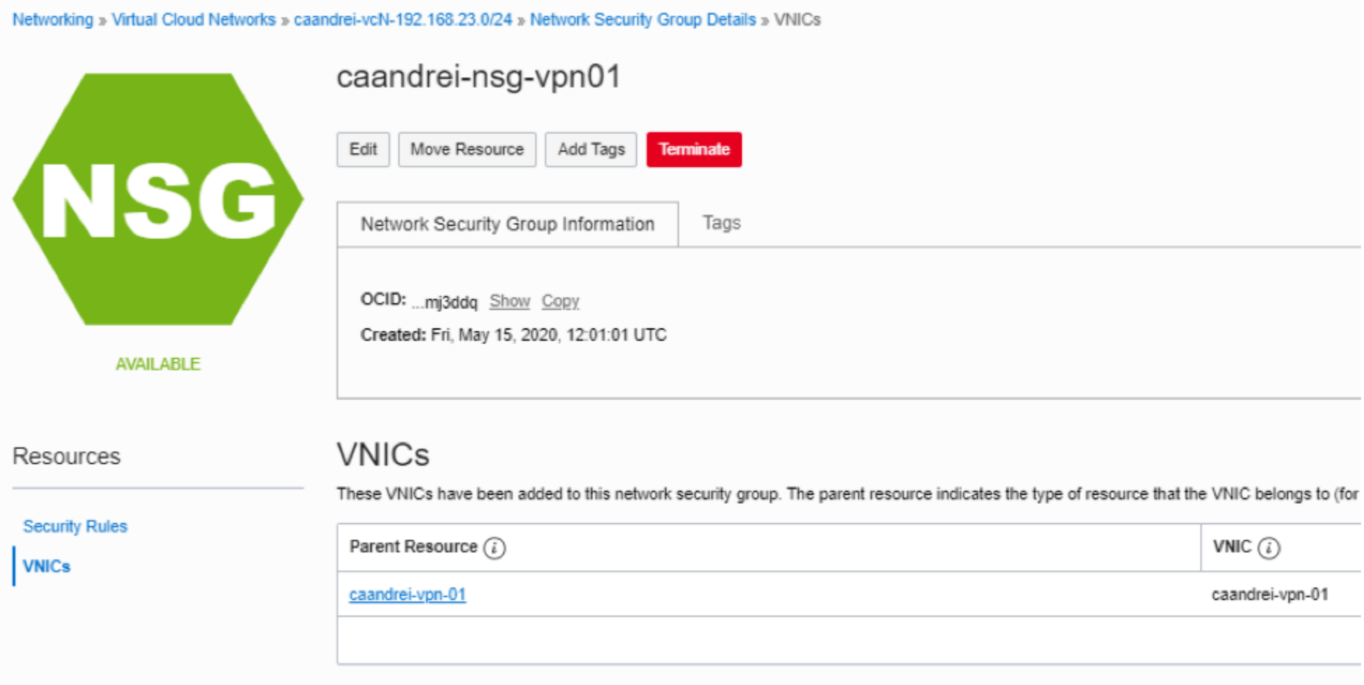
Firmware: UEFI_64

Boot Volume Type: PARAVIRTUALIZED

Add the configured NSG for the public VM.

Repeat the step for the private instance.

Navigate to the Networking>Virtual Cloud Networks>{Your VCN}>Network Security Groups, click on each NSG and check the VNIC section



Networking » Virtual Cloud Networks » caandrei-vcN-192.168.23.0/24 » Network Security Group Details » VNICs

caandrei-nsg-vpn01

OCID: ...mj3ddq Show Copy

Created: Fri, May 15, 2020, 12:01:01 UTC

VNICs

These VNICs have been added to this network security group. The parent resource indicates the type of resource that the VNIC belongs to (for

Parent Resource	VNIC
caandrei-vpn-01	caandrei-vpn-01

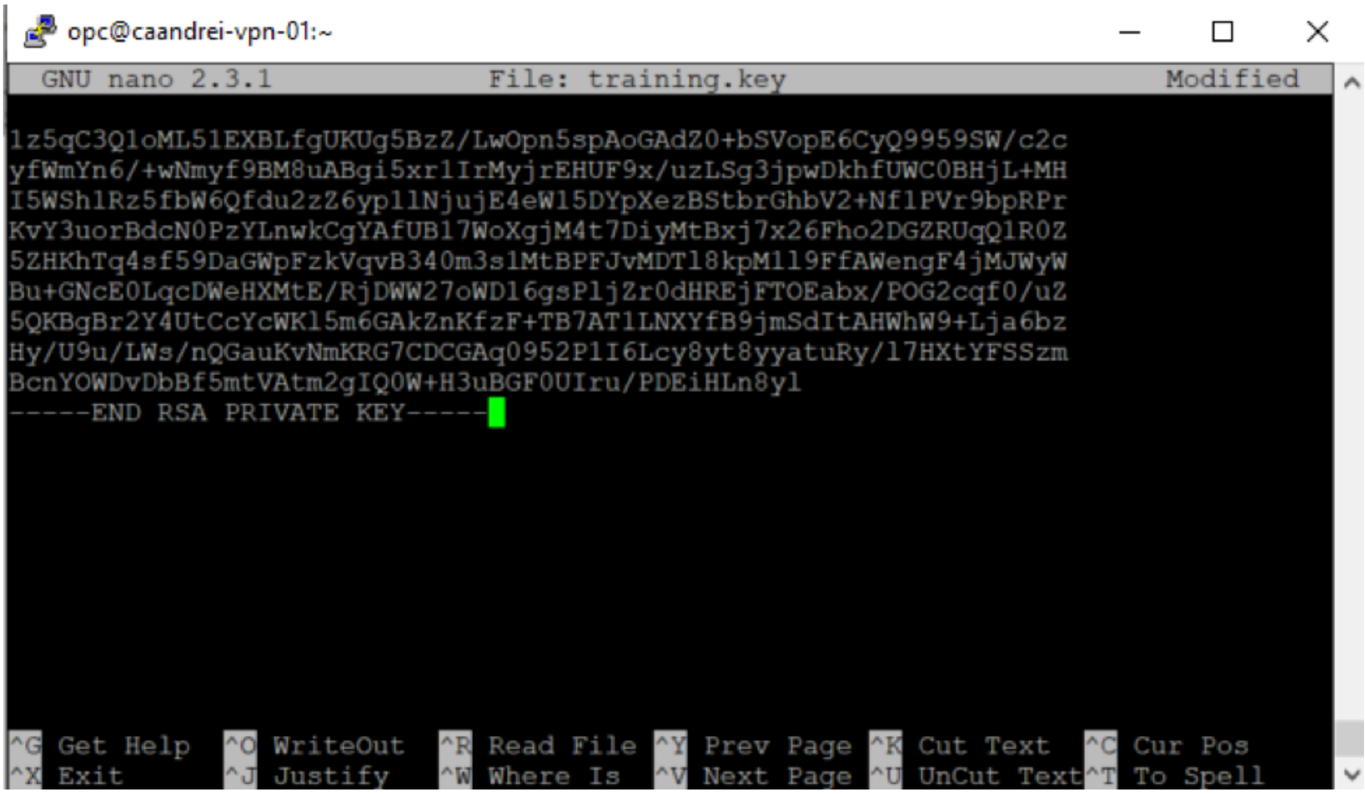
Please notice that the NSG is associated with the VM

Test the Connectivity

Connect to the Public IP address of the public VM and create a file called training.key using your favorite Linux editor (I used nano in the screenshot):

```
nano training.key
```

Paste the private key (the one generated at the beginning of the lab) information



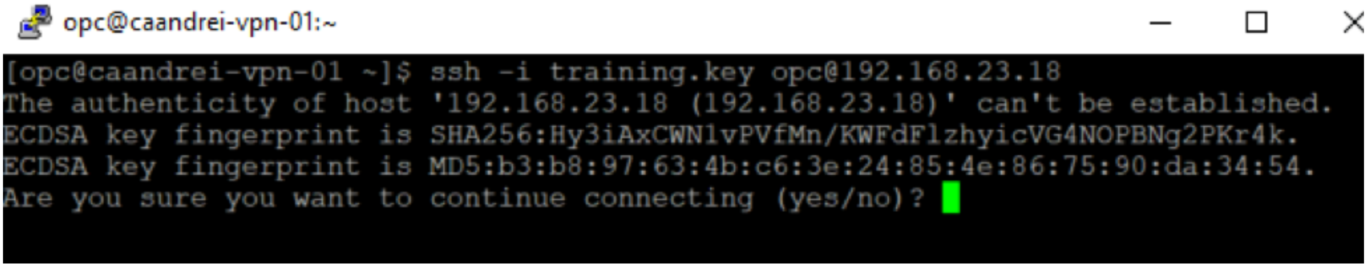
```
  GNU nano 2.3.1              File: training.key                    Modified

1z5qC3Q1oML51EXBLfgUKUg5BzZ/LwOpn5spAoGAdZ0+bSVopE6CyQ9959SW/c2c
yfWmYn6/+wNmyf9BM8uABgi5xr1IrMyjrEHUF9x/uzLSg3jpwDkhfUWC0BHjL+MH
I5WSh1Rz5fbW6Qfdu2zZ6yp11NjujE4eW15DYpXezBStbrGhbV2+Nf1PVr9bpRPr
KvY3uorBdcN0PzYLnwkCgYAfUB17WoXgjM4t7DiyMtBxj7x26Fho2DGZRUqQ1R0Z
5ZHKhTq4sf59DaGWpFzkVqvB340m3s1MtBPFJvMDT18kpM119FfAWengF4jMJWyW
Bu+GNcE0LqcDWeHXMtE/RjDWW27oWD16gsP1jZr0dHREjFTOEabx/POG2cqf0/uZ
5QKBgBr2Y4UtCcYcWK15m6GAkZnKfzF+TB7AT1LNXYfB9jmSdItAHWhW9+Lja6bz
Hy/U9u/LWs/nQGauKvNmKRG7CDCGAq0952P1I6Lcy8yt8yyatuRy/17HXtYFSSzm
BcnYOWDvDbBf5mtVAtm2gIQ0W+H3uBGF0UIru/PDEiHLn8y1
-----END RSA PRIVATE KEY-----

^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

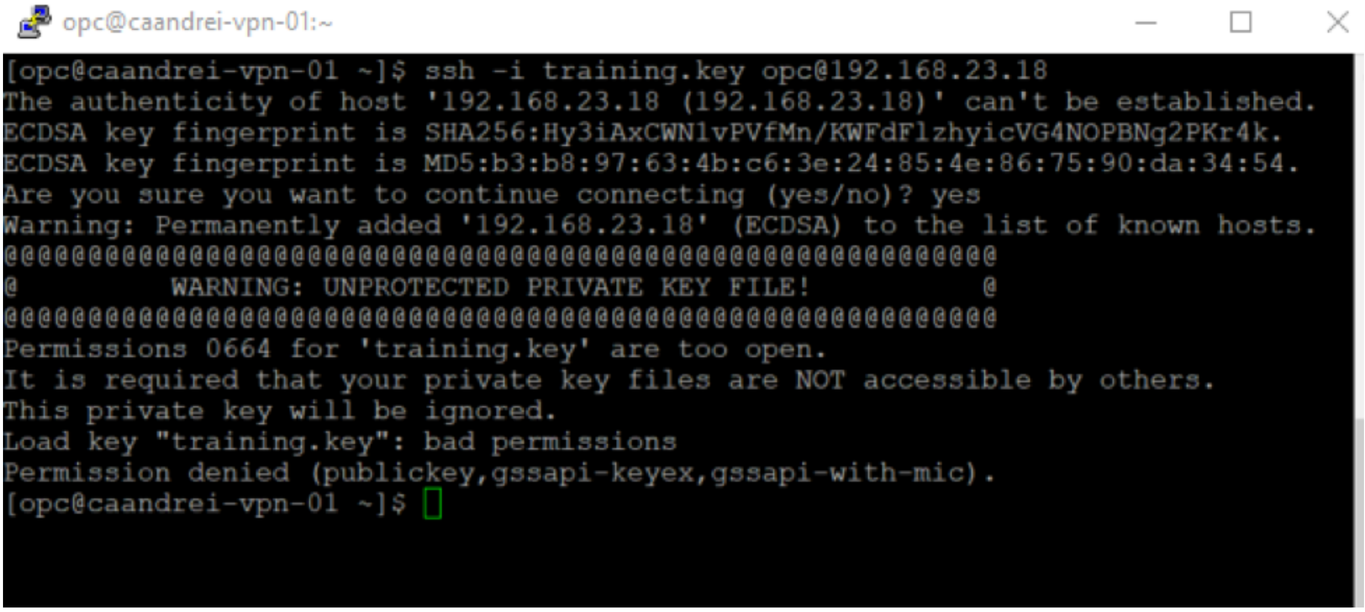
Hit **CTRL+X** to close the file. It will ask you if you want to save it, Press **Y** then press ENTER

Connect to the private VM



```
[opc@caandrei-vpn-01 ~]$ ssh -i training.key opc@192.168.23.18
The authenticity of host '192.168.23.18 (192.168.23.18)' can't be established.
ECDSA key fingerprint is SHA256:Hy3iAxCWN1vPVfMn/KWFdFlzhyicVG4NOPBNg2PKr4k.
ECDSA key fingerprint is MD5:b3:b8:97:63:4b:c6:3e:24:85:4e:86:75:90:da:34:54.
Are you sure you want to continue connecting (yes/no)?
```

Accept the fingerprint. Notice that we are getting an error (file permissions for the key are too open

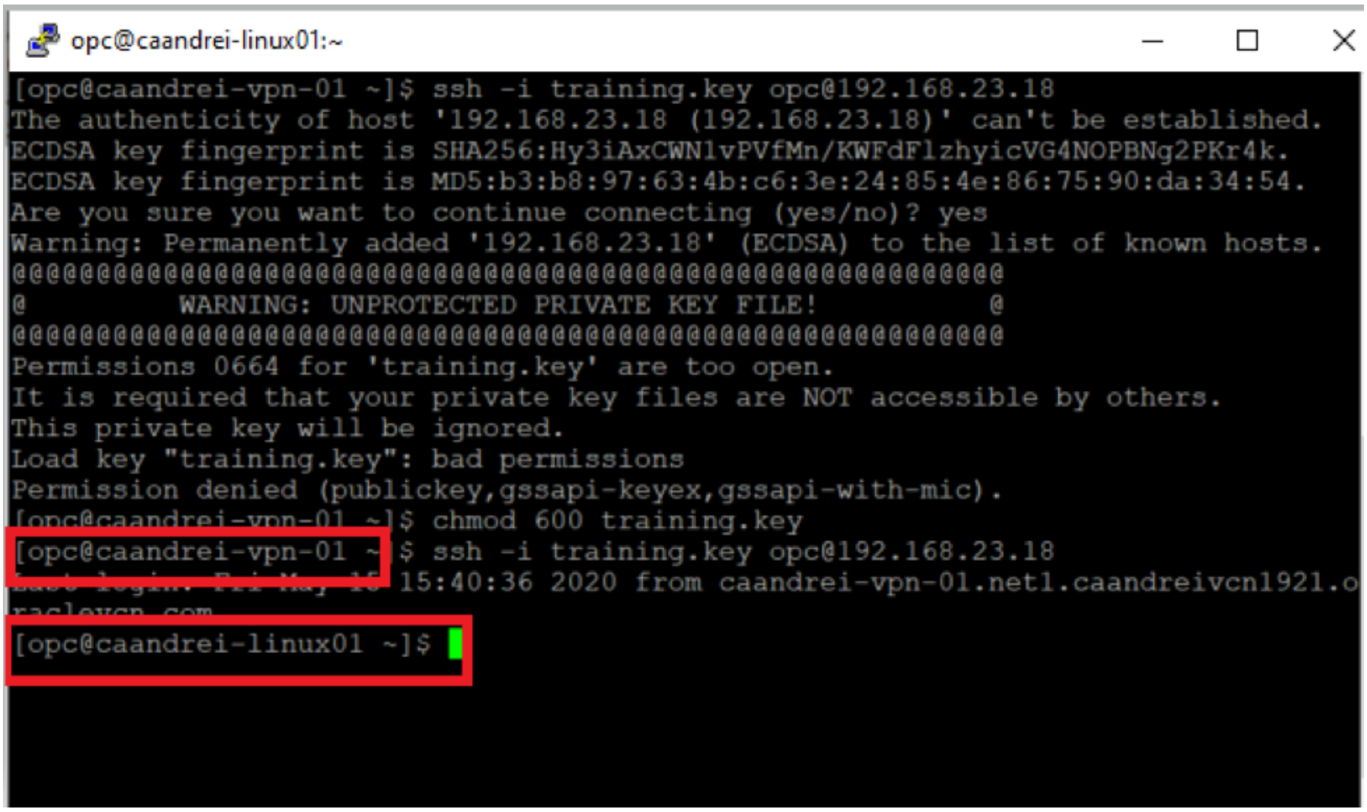


```
[opc@caandrei-vpn-01 ~]$ ssh -i training.key opc@192.168.23.18
The authenticity of host '192.168.23.18 (192.168.23.18)' can't be established.
ECDSA key fingerprint is SHA256:Hy3iAxCWN1vPVfMn/KWFdFlzhyicVG4NOPBNg2PKr4k.
ECDSA key fingerprint is MD5:b3:b8:97:63:4b:c6:3e:24:85:4e:86:75:90:da:34:54.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.23.18' (ECDSA) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0664 for 'training.key' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "training.key": bad permissions
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[opc@caandrei-vpn-01 ~]$
```

Adjust the security for the key:

```
chmod 600 training.key
```

Connect again



```
[opc@caandrei-vpn-01 ~]$ ssh -i training.key opc@192.168.23.18
The authenticity of host '192.168.23.18 (192.168.23.18)' can't be established.
ECDSA key fingerprint is SHA256:Hy3iAxCWN1vPVfMn/KWFdFlzhyicVG4NOPBNg2PKr4k.
ECDSA key fingerprint is MD5:b3:b8:97:63:4b:c6:3e:24:85:4e:86:75:90:da:34:54.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.23.18' (ECDSA) to the list of known hosts.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0664 for 'training.key' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "training.key": bad permissions
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[opc@caandrei-vpn-01 ~]$ chmod 600 training.key
[opc@caandrei-vpn-01 ~]$ ssh -i training.key opc@192.168.23.18
Last login: Fri May 15 15:40:36 2020 from caandrei-vpn-01.net1.caandreivcn1921.o
raclevcn.com
[opc@caandrei-linux01 ~]$
```

Notice the change in the hostname prompt. Now you are connected to the private VM

Conclusion

By Completing this lab you should have learned:

- Create a VCN
- Create Subnets
- Create routing tables
- Adjust Network Security to have connectivity to a VM.
- Create a VM in either private or public subnet