Lab 1. Launch an Instance Using Console

Objectives:

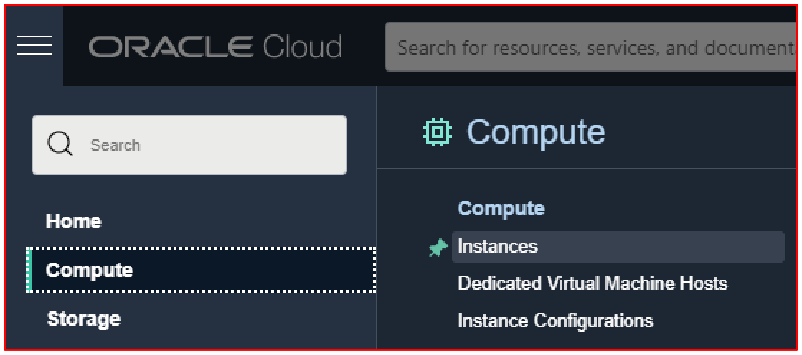
- Create a Linux Compute instance in OCI
- Connect to it using ***ssh*** from your VM Terminal over the internet.
- Connect to the instance using Putty
- Install a Web Server and Access it using the Public IP of the Instance.

Pre-Requisites

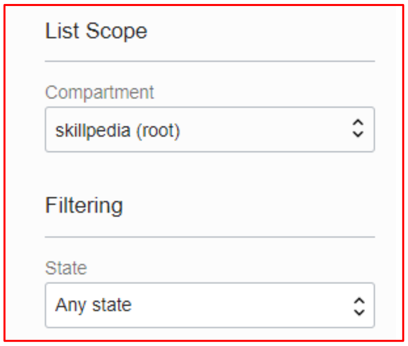
- To sign in to the Console, you need the following:
  - Tenant, User name and Password
  - URL for the Console: https://console.us-ashburn-1.oraclecloud.com/
  - Oracle Cloud Infrastructure supports the latest versions of Google Chrome, Firefox or Internet Explorer 11

Sequence 1. Create a Linux Instance

1. Login to the Linux VM and launch Firefox browser. You are doing this practice from within the VM because you have the SSH Key inside the VM, you will be able to upload the SSH Key from within the VM.
2. Login to the OCI Console as a privileged user and from the Menu on Top left, Click **Compute - > Instances**



3. Choose the Region from the *Regions* Menu on the Top Right in your OCI Console Browser. Now, on the Left panel, choose a compartment in which you have requisite privileges granted.



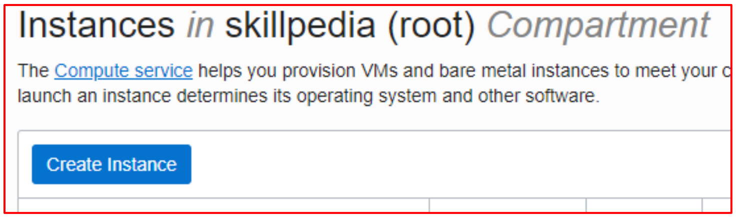
List Scope

Compartment: skillpedia (root)

Filtering

State: Any state

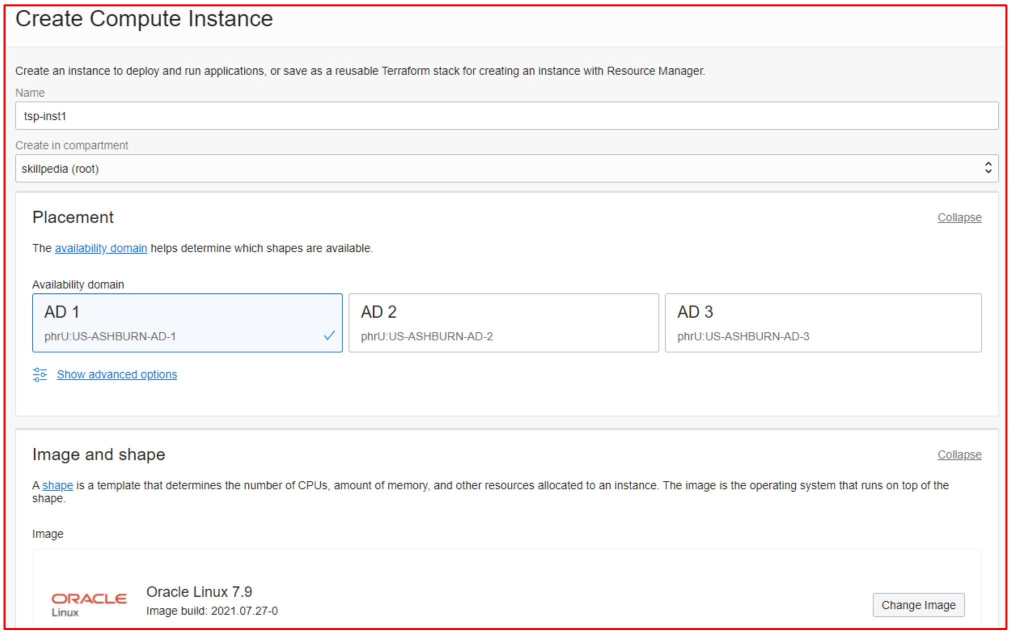
4. Click Create Instance.



Instances *in* skillpedia (root) *Compartment*

The Compute service helps you provision VMs and bare metal instances to meet your c
launch an instance determines its operating system and other software.

5. Enter the following details for the Instance specification
   - **Name** – tsp-inst1
   - **Image** – Choose the default – Oracle Linux 7.9
   - **Availability Domain** – Choose AD1



Create Compute Instance

Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating an instance with Resource Manager.

Name: tsp-inst1

Create in compartment: skillpedia (root)

Placement

The availability domain helps determine which shapes are available.

Availability domain

AD 1	AD 2	AD 3
phrU:US-ASHBURN-AD-1 ✓	phrU:US-ASHBURN-AD-2	phrU:US-ASHBURN-AD-3

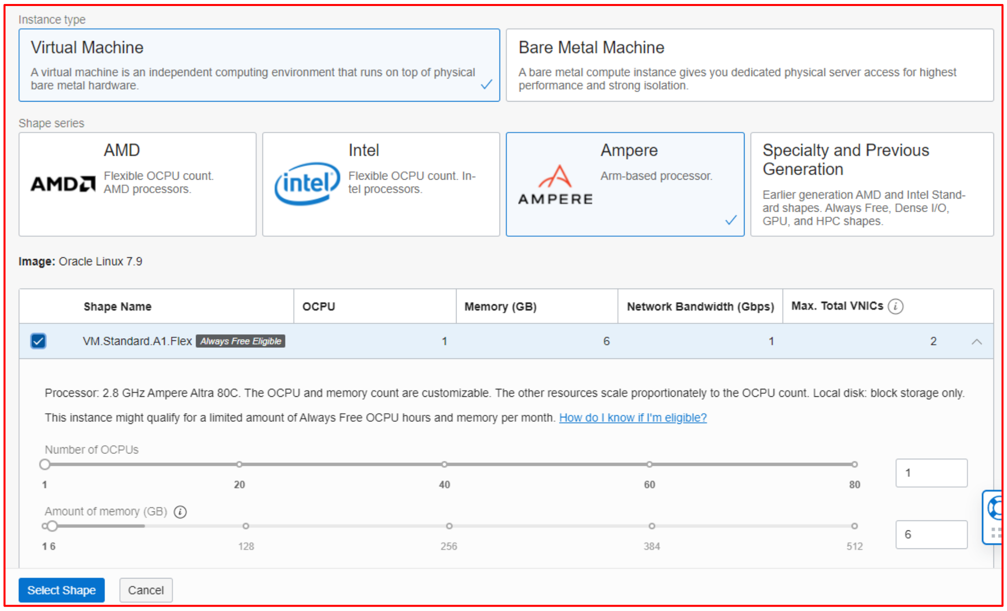
Image and shape

A shape is a template that determines the number of CPUs, amount of memory, and other resources allocated to an instance. The image is the operating system that runs on top of the shape.

Image

Oracle Linux 7.9
Image build: 2021.07.27-0

6. Click on “Change Shape” to explore shape and type options for an instance. For example, for the current instance select:
   - **Instance Type** – Virtual Machine
   - **Shape** – Under Shape Series, select “*Ampere*” to show Image(s). Now select **VM.Standard.A1.Flex** *Always Free Eligible.*



Instance type

Virtual Machine ✓
A virtual machine is an independent computing environment that runs on top of physical bare metal hardware.

Bare Metal Machine
A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Shape series

AMD Flexible OCPU count. AMD processors.

Intel Flexible OCPU count. Intel processors.

Ampere ✓ Arm-based processor.

Specialty and Previous Generation Earlier generation AMD and Intel Standard shapes. Always Free, Dense I/O, GPU, and HPC shapes.

Image: Oracle Linux 7.9

Shape Name	OCPU	Memory (GB)	Network Bandwidth (Gbps)	Max. Total VNICs ⓘ
☑ VM.Standard.A1.Flex *Always Free Eligible*	1	6	1	2

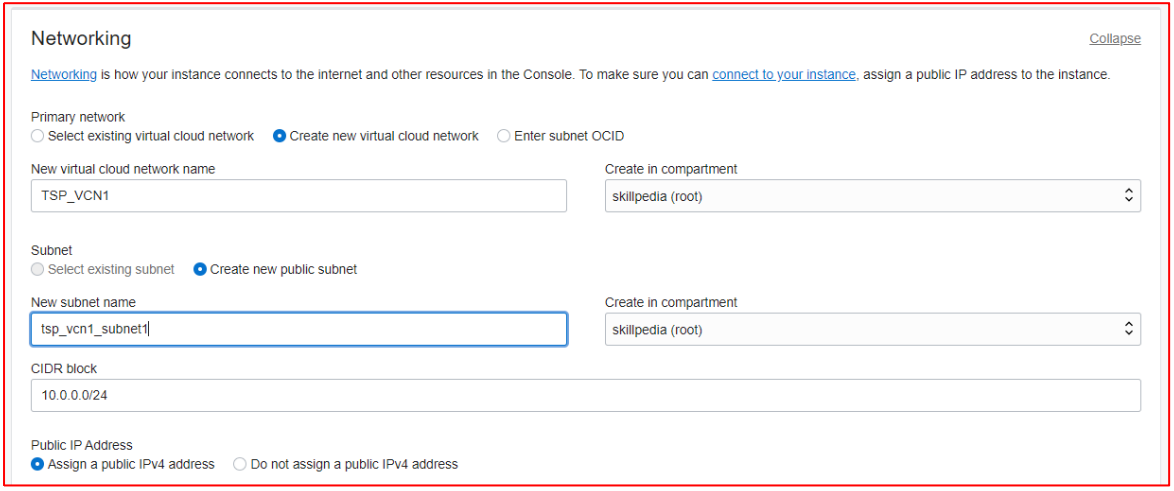
Processor: 2.8 GHz Ampere Altra 80C. The OCPU and memory count are customizable. The other resources scale proportionately to the OCPU count. Local disk: block storage only.

This instance might qualify for a limited amount of Always Free OCPU hours and memory per month. How do I know if I'm eligible?

Number of OCPUs: 1

Amount of memory (GB) ⓘ: 6

7. Scroll down to the Configure Networking Section and select the radio button "*Create new virtual cloud network*" enter following details.
   - VCN Name - tsp_vcn1
   - New subnet name : tsp_vcn1_subnet1
   - VCN CIDR Block – 10.0.0.0/16 (Keep Default)
   - Public Subnet CIDR Block – 10.0.0.0/24 (Keep Default)
   - Private Subnet CIDR Block – 10.0.1.0/24
   - Assign Public IPV4 Address (Keep Default)



Networking

Networking is how your instance connects to the internet and other resources in the Console. To make sure you can connect to your instance, assign a public IP address to the instance.

Primary network
○ Select existing virtual cloud network ● Create new virtual cloud network ○ Enter subnet OCID

New virtual cloud network name: TSP_VCN1

Create in compartment: skillpedia (root)

Subnet
○ Select existing subnet ● Create new public subnet

New subnet name: tsp_vcn1_subnet1

Create in compartment: skillpedia (root)

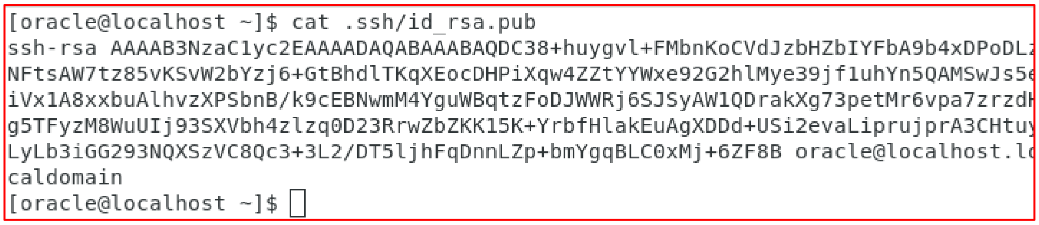
CIDR block: 10.0.0.0/24

Public IP Address
● Assign a public IPv4 address ○ Do not assign a public IPv4 address

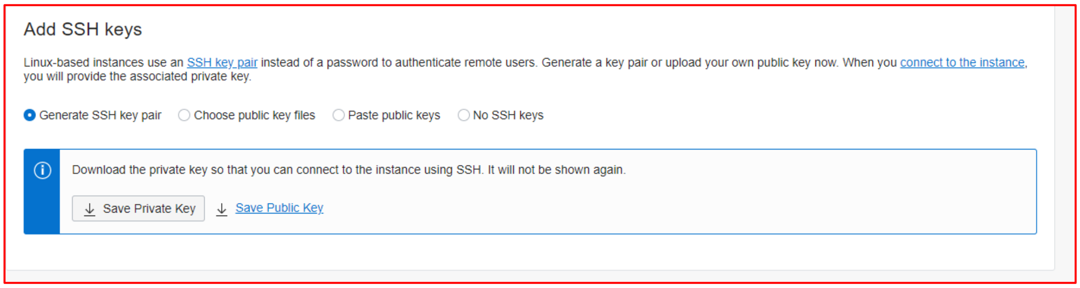
8. Accept the defaults for the Configure Boot Volume section.
9. Scroll down to the Add SSH Key Section.

Create by Clicking on "***Save Private Key***" under default option "Generate SSH key pair". You may choose this if you want to connect to this instance from Putty/Linux Terminal. Download Private and Public Keys.

OR
Provide the Public Key that you created on ***server*** VM with the Radio button for **Paste SSH Keys**. Copy Paste the contents of **id_rsa.pub** file



```
[oracle@localhost ~]$ cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDC38+huygvl+FMbnKoCVdJzbHZbIYFbA9b4xDPoDL
NFtsAW7tz85vKSvW2bYzj6+GtBhdlTKqXEocDHPiXqw4ZZtYYWxe92G2hlMye39jf1uhYn5QAMSwJs5
iVx1A8xxbuAlhvzXPSbnB/k9cEBNwmM4YguWBqtzFoDJWWRj6SJSyAW1QDrakXg73petMr6vpa7zrzd
g5TFyzM8WuUIj93SXVbh4zlzq0D23RrwZbZKK15K+YrbfHlakEuAgXDDd+USi2evaLiprujprA3CHtu
LyLb3iGG293NQXSzVC8Qc3+3L2/DT5ljhFqDnnLZp+bmYgqBLC0xMj+6ZF8B oracle@localhost.l
caldomain
[oracle@localhost ~]$ 
```



Add SSH keys

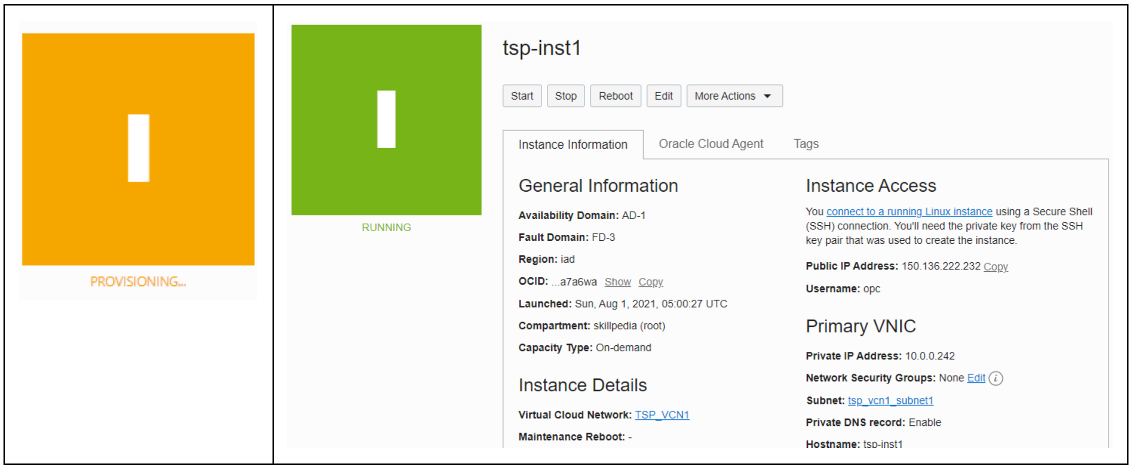
Linux-based instances use an SSH key pair instead of a password to authenticate remote users. Generate a key pair or upload your own public key now. When you connect to the instance, you will provide the associated private key.

● Generate SSH key pair ○ Choose public key files ○ Paste public keys ○ No SSH keys

Download the private key so that you can connect to the instance using SSH. It will not be shown again.

You can explore the Show Advanced options, don't make any changes.

10. Verify if you have taken care of all details, click ***Create***. Your instance will be in Provisioning State and will be available in a few minutes.



tsp-inst1

General Information

Availability Domain: AD-1

Fault Domain: FD-3

Region: iad

OCID: ...a7a6wa Show Copy

Launched: Sun, Aug 1, 2021, 05:00:27 UTC

Compartment: skillpedia (root)

Capacity Type: On-demand

Instance Details

Virtual Cloud Network: TSP_VCN1

Maintenance Reboot: -

Instance Access

You connect to a running Linux instance using a Secure Shell (SSH) connection. You'll need the private key from the SSH key pair that was used to create the instance.

Public IP Address: 150.136.222.232 Copy

Username: opc

Primary VNIC

Private IP Address: 10.0.0.242

Network Security Groups: None Edit

Subnet: tsp_vcn1_subnet1

Private DNS record: Enable

Hostname: tsp-inst1

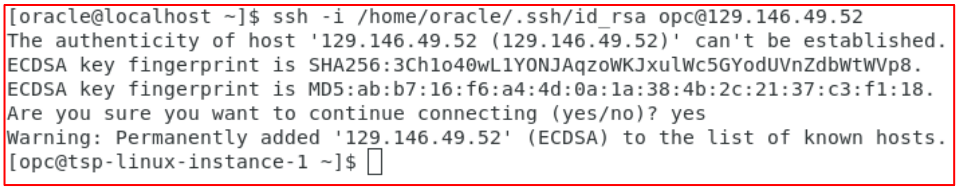
Wait until its status of your instance changes to Running as shown.

11. In the Instance page, you can identify the Public IP address of the Linux Instance. Take note of it. You will access your instance with ***ssh*** from Linux Instance, by providing private key. Note that ping command will not show connectivity since the ICMP ingress rule from internet is not added by default. You can add ingress rule for ICMP protocol.

Sequence 2. Login to the Instance using Private Key (If you pasted public key of your Linux VM from terminal)

1. Start your VM, ***server***. Open the terminal in your virtual machine, ***server***. From your VM terminal, issue the following command

   ```
   # ssh -i <path_to_private_key> opc@<public_ip_address_of_instance>
   ```



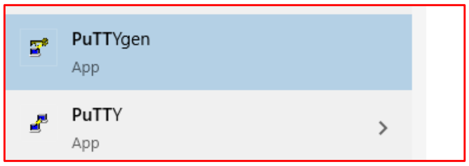
```
[oracle@localhost ~]$ ssh -i /home/oracle/.ssh/id_rsa opc@129.146.49.52
The authenticity of host '129.146.49.52 (129.146.49.52)' can't be established.
ECDSA key fingerprint is SHA256:3Ch1o40wL1YONJAqzoWKJxulWc5GYodUVnZdbWtWVp8.
ECDSA key fingerprint is MD5:ab:b7:16:f6:a4:4d:0a:1a:38:4b:2c:21:37:c3:f1:18.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '129.146.49.52' (ECDSA) to the list of known hosts.
[opc@tsp-linux-instance-1 ~]$ 
```

2. You will be logged into your Linux Compute Instance.

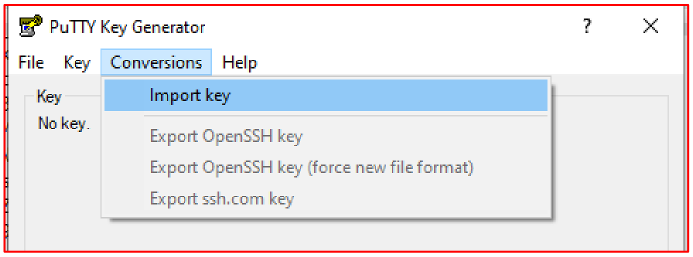
Sequence 3. Login to the Instance using Putty

To use putty to connect any of the VM, you first have to convert the Private Key of that machine to PPK format.

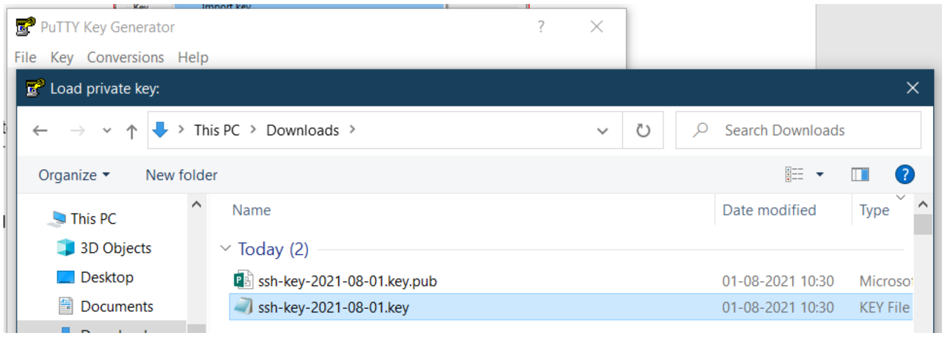
1. Start Puttygen Program to convert the Private key to PPK format.



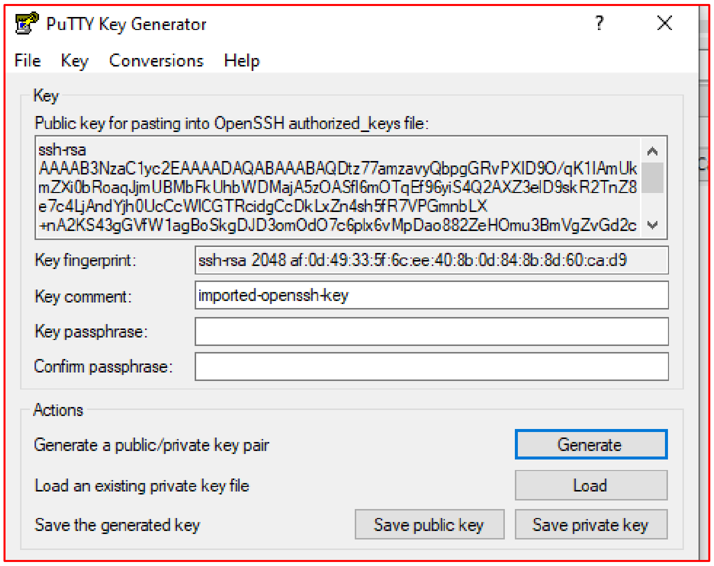
2. Open ***Conversions -> Import Key***



3. Provide the path of your key Downloaded private key (E.g. ssh-key-2021-08-01.key).



4. It will import the Private Key to Puttygen



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDtz77amzavyQbpgGRvPXID9O/qK1IAmUk
mZXi0bRoaqJjmUBMbFkUhbWDMajA5zOASfl6mOTqEf96yiS4Q2AXZ3elD9skR2TnZ8
e7c4LjAndYjh0UcCcWICGTRcidgCcDkLxZn4sh5fR7VPGmnbLX
+nA2KS43gGVfW1agBoSkgDJD3omOdO7c6plx6vMpDao882ZeHOmu3BmVgZvGd2c
```

Key fingerprint: ssh-rsa 2048 af:0d:49:33:5f:6c:ee:40:8b:0d:84:8b:8d:60:ca:d9

Key comment: imported-openssh-key

Key passphrase:

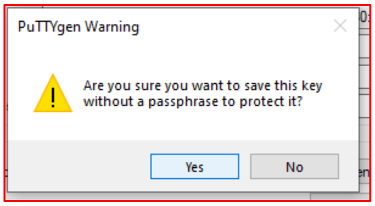
Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

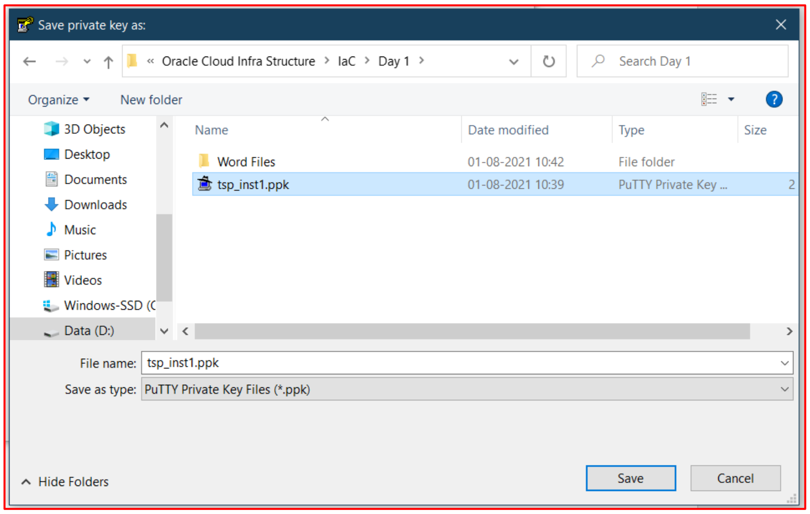
Save the generated key

5. Click on ***Save Private Key*** and Confirm the ***Puttygen*** waring on saving this key without passphrase.



Are you sure you want to save this key without a passphrase to protect it?

6. Specify a location and accept the default name. Save the PPK format Key on your Host machine.

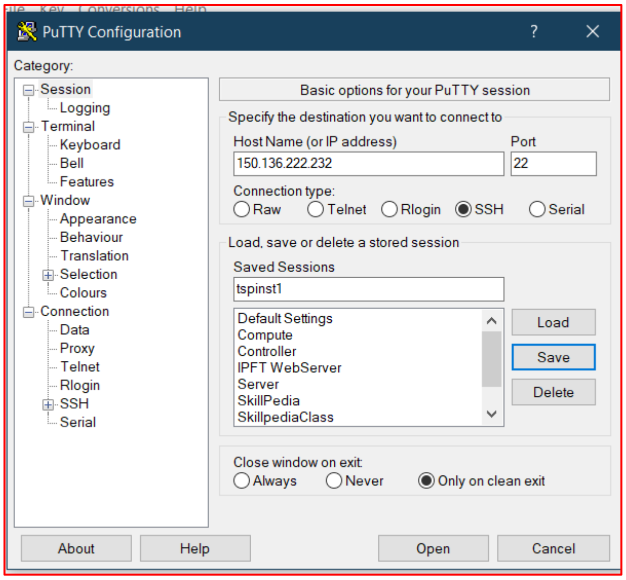


Name	Date modified	Type	Size
Word Files	01-08-2021 10:42	File folder	
tsp_inst1.ppk	01-08-2021 10:39	PuTTY Private Key ...	2

File name: tsp_inst1.ppk

Save as type: PuTTY Private Key Files (*.ppk)

7. You can now use this PPK format key to connect to your tsp_inst1 VM. Launch Putty from your windows machine. Enter the Public IP address of ***your instance***.



Specify the destination you want to connect to

Host Name (or IP address): 150.136.222.232

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

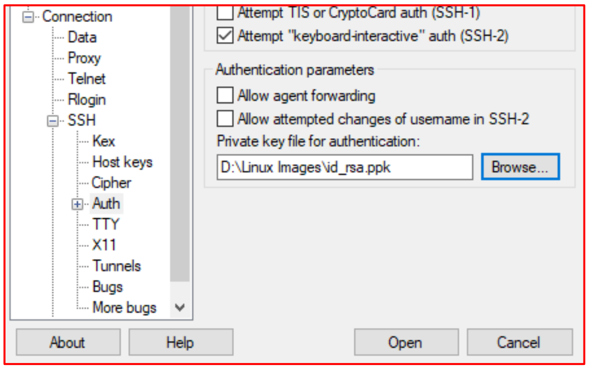
Load, save or delete a stored session

Saved Sessions: tspinst1

Default Settings
Compute
Controller
IPFT WebServer
Server
SkillPedia
SkillpediaClass

Close window on exit: ○ Always ○ Never ● Only on clean exit

8. Expand ***SSH*** under ***Connection*** from Left part of the window and select ***Auth***. Now on the right part of the window, ***browse*** to the PPK format Key on your system



□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

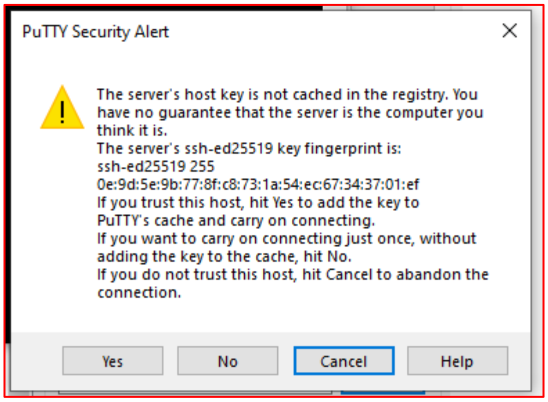
Authentication parameters

□ Allow agent forwarding

□ Allow attempted changes of username in SSH-2

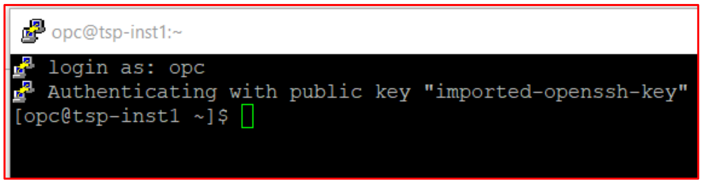
Private key file for authentication: D:\Linux Images\id_rsa.ppk

9. Click on ***Open*** to Connect. You will see a Security alert. Click on ***YES*** to accept.



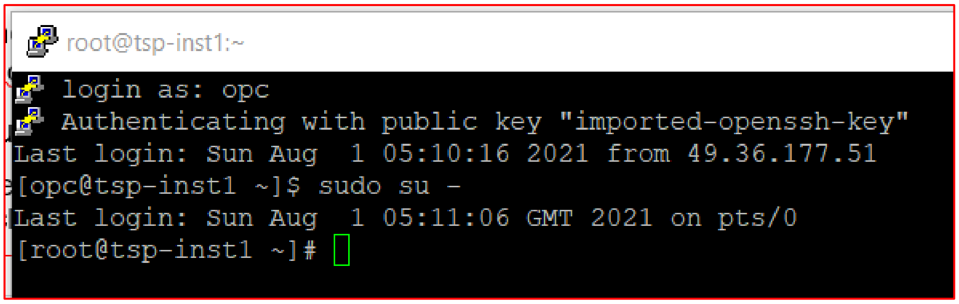
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255
0e:9d:5e:9b:77:8f:c8:73:1a:54:ec:67:34:37:01:ef
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

10. Enter the user name "***opc***" and press enter key.



```
opc@tsp-inst1:~
login as: opc
Authenticating with public key "imported-openssh-key"
[opc@tsp-inst1 ~]$
```

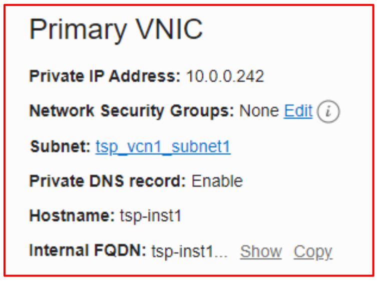
11. You are now logged into the ***tsp-inst1*** from putty using Key based authentication. To login as root, use the command “sudo su –“



```
root@tsp-inst1:~
login as: opc
Authenticating with public key "imported-openssh-key"
Last login: Sun Aug  1 05:10:16 2021 from 49.36.177.51
[opc@tsp-inst1 ~]$ sudo su -
Last login: Sun Aug  1 05:11:06 GMT 2021 on pts/0
[root@tsp-inst1 ~]#
```

Sequence 4. Change Security List and open Ports for Connectivity

1. From the Instance Page, click on Subnet “tsp_vcn1_subnet1”.



Primary VNIC

Private IP Address: 10.0.0.242

Network Security Groups: None Edit

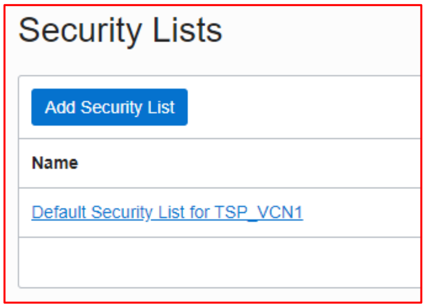
Subnet: tsp_vcn1_subnet1

Private DNS record: Enable

Hostname: tsp-inst1

Internal FQDN: tsp-inst1... Show Copy

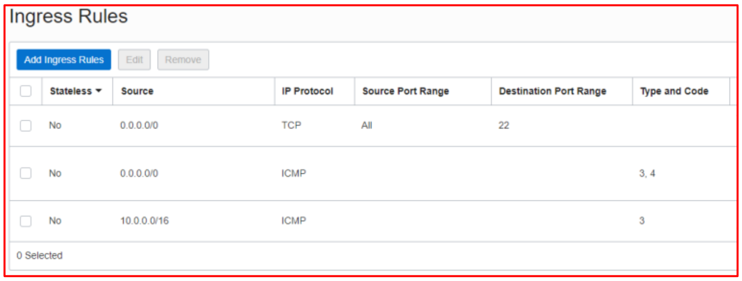
2. Cick on “Default Security List for TSP_VCN1”, that appears at the center of the screen.



Security Lists

Name
Default Security List for TSP_VCN1

3. Click on “Add Ingress Rules”



Ingress Rules

□	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code
□	No	0.0.0.0/0	TCP	All	22	
□	No	0.0.0.0/0	ICMP			3, 4
□	No	10.0.0.0/16	ICMP			3

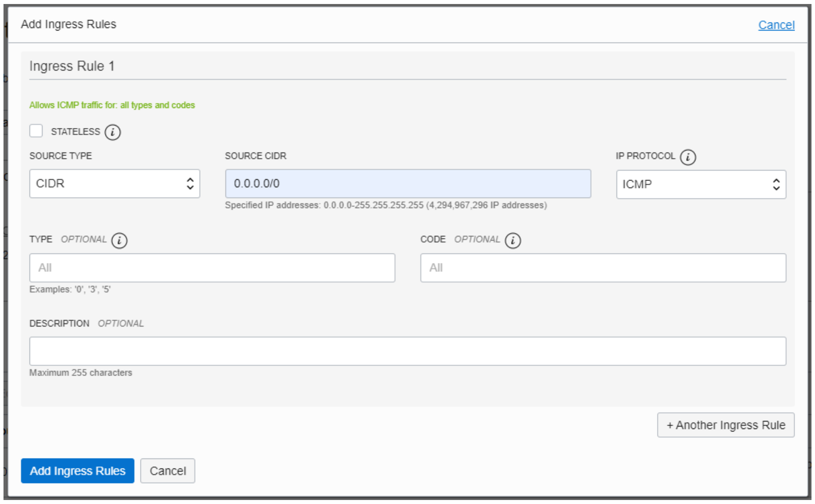
0 Selected

4. Add an Ingress Rule to allow ping command

   Source CIDR : 0.0.0.0/0

   IP Protocol : ICMP

   Keep rest of the details and Click on “Add Ingress Rules” as given in the screen shot.



Add Ingress Rules

Ingress Rule 1

Allows ICMP traffic for: all types and codes

□ STATELESS

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: ICMP

TYPE OPTIONAL: All

Examples: '0', '3', '5'

CODE OPTIONAL: All

DESCRIPTION OPTIONAL

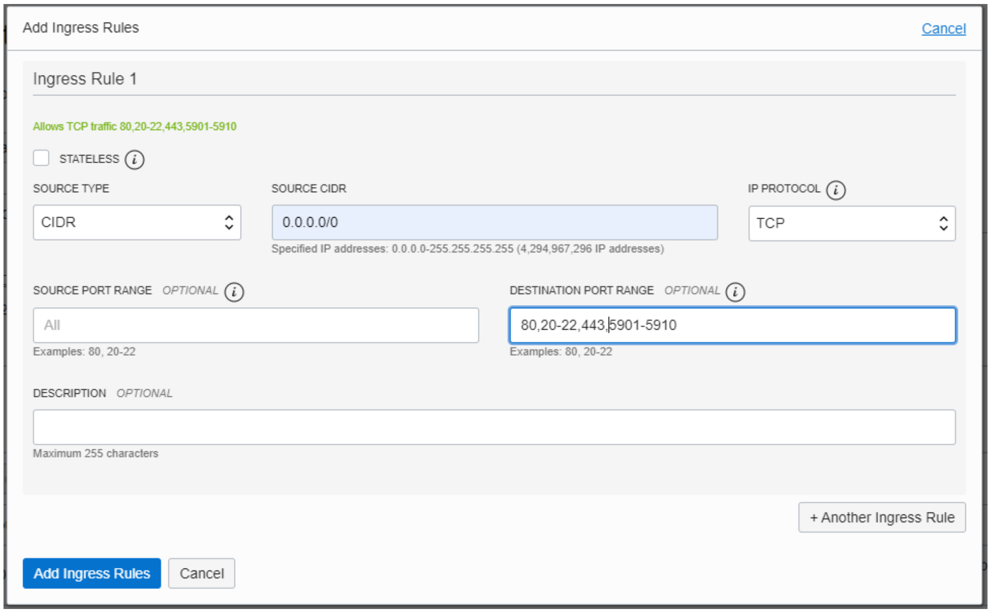
Maximum 255 characters

5. Add an Ingress Rule to allow https and other services

   Source CIDR : *0.0.0.0/0*

   IP Protocol : *TCP*

   DESTINATION PORT RANGE : *80,20-22,443,5901-5910*



Add Ingress Rules

Ingress Rule 1

Allows TCP traffic 80,20-22,443,5901-5910

□ STATELESS

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: TCP

SOURCE PORT RANGE OPTIONAL: All

Examples: 80, 20-22

DESTINATION PORT RANGE OPTIONAL: 80,20-22,443,5901-5910

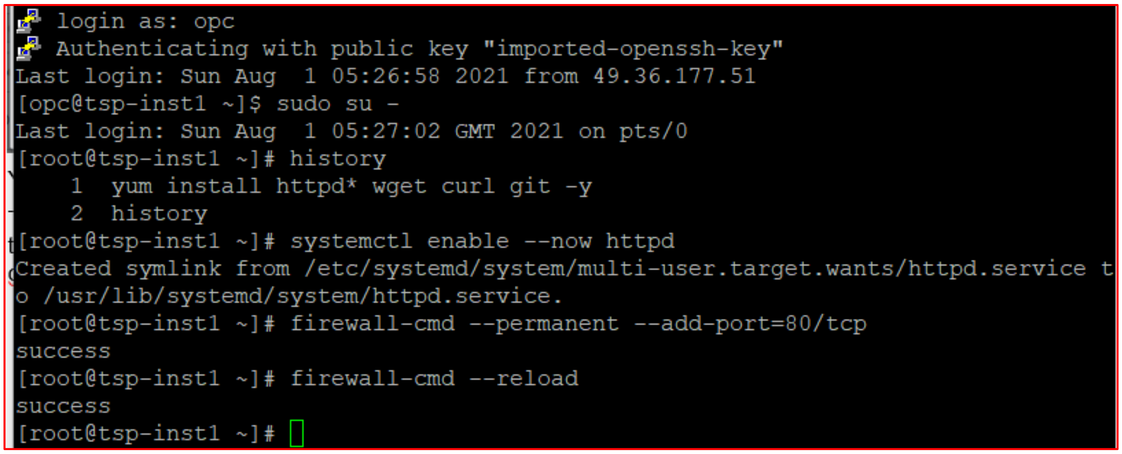
Examples: 80, 20-22

DESCRIPTION OPTIONAL

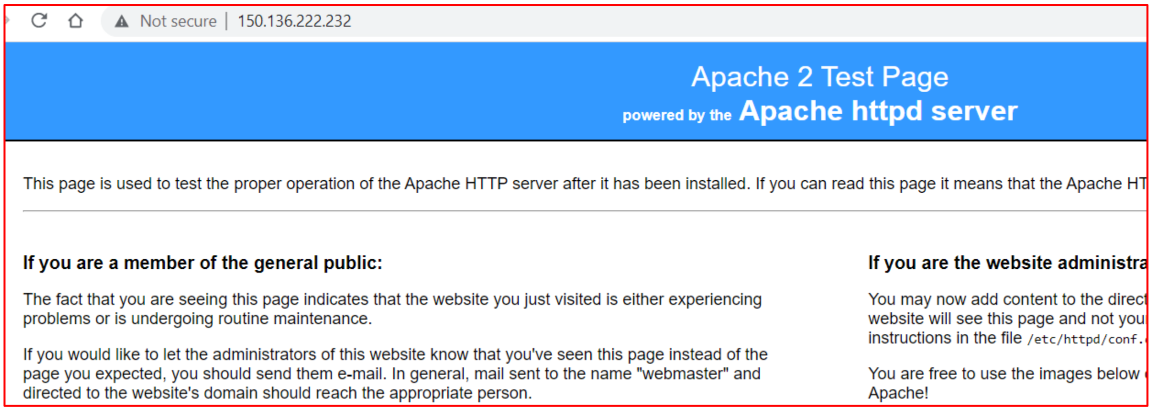
Maximum 255 characters

6. You have successfully launched an Instance and configured Security Lists for various services.

7. Try Installing a Web Server and Access it using Public IP Address of the Instance. Note that you have to open post 80 from the instance also using “firewall-cmd --permanent --add-port=80/tcp; firewall-cmd --reload” as given in screen shots.



```
login as: opc
Authenticating with public key "imported-openssh-key"
Last login: Sun Aug  1 05:26:58 2021 from 49.36.177.51
[opc@tsp-inst1 ~]$ sudo su -
Last login: Sun Aug  1 05:27:02 GMT 2021 on pts/0
[root@tsp-inst1 ~]# history
    1  yum install httpd* wget curl git -y
    2  history
[root@tsp-inst1 ~]# systemctl enable --now httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service t
o /usr/lib/systemd/system/httpd.service.
[root@tsp-inst1 ~]# firewall-cmd --permanent --add-port=80/tcp
success
[root@tsp-inst1 ~]# firewall-cmd --reload
success
[root@tsp-inst1 ~]# 
```



150.136.222.232

Apache 2 Test Page

powered by the **Apache httpd server**

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that the Apache HT

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

If you are the website administra

You may now add content to the direct website will see this page and not you instructions in the file `/etc/httpd/conf.`

You are free to use the images below Apache!