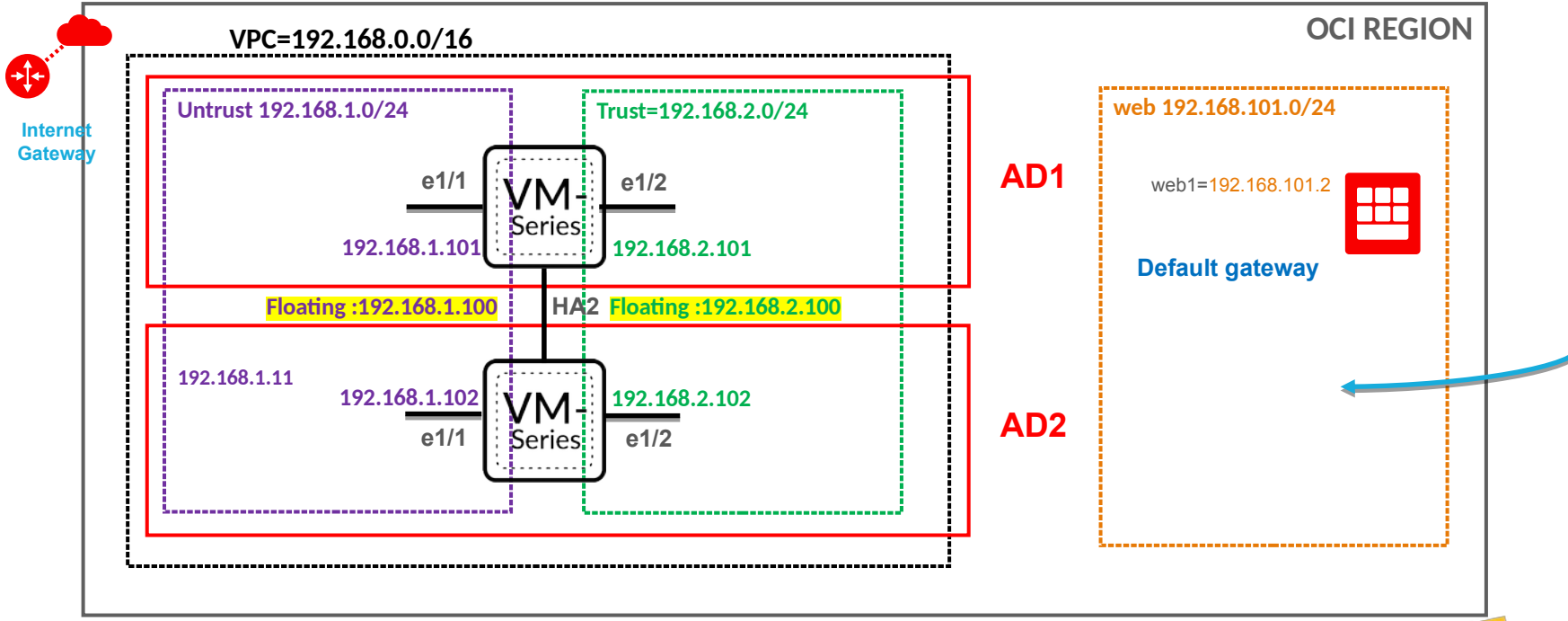
paloalto® NETWORKS in ORACLE® CLOUD

VM-Series on Oracle Cloud High Availability deployment guide – Terraform Version

Patrick Glynn – Public Cloud CE

Mar 2020

- **Topology:** This is the setup that will be built.



Important Notes:

- This document details the setup of the environment using Terraform.
- This setup build an active/standby pair of VM-Series in OCI.
- This solution is appropriate for inspecting Outbound traffic for a single VCN. Inspecting subnet-to-subnet traffic within a VCN is not possible due to OCI routing rules.
- If you have a Transit VCN design, this setup can be deployed in the Hub VCN to inspect Outbound traffic from Spokes or inspect East-West traffic between Spokes.
- In this setup, VM-Series (with code >= 9.1.1) will have a plugin installed by default that will make an API call to OCI and move the IP Configuration from active firewall to passive firewall when the active firewall becomes unavailable.
- Firewalls can sit in different OCI Availability Domains.

Terraform Notes:

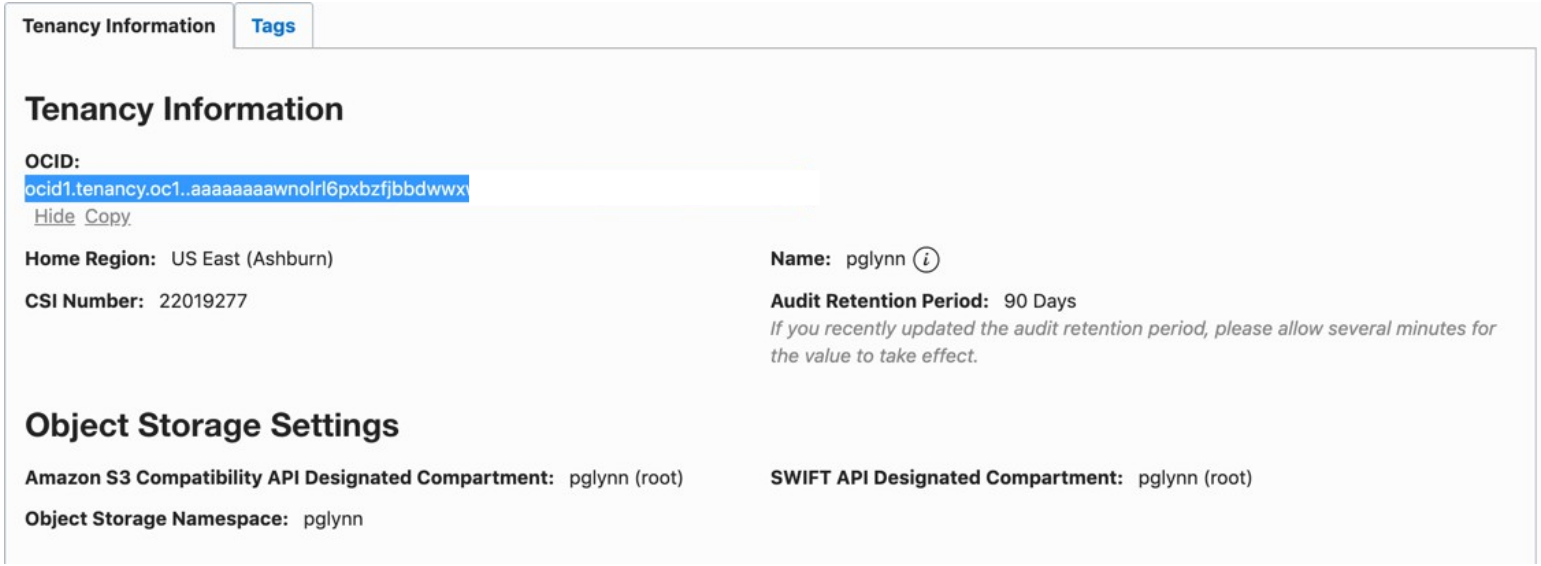
- The IP addressing specified in the terraform.tfvars file matches that in the manual build documentation. This can be changed as desired but the FW configs will need to be updated.
- The TF has been tested in the Ashburn region but should run in any region where the VM-series image is available.

Gathering the information and modifying terraform.tfvars

Although the IP addressing scheme may be used as-is, it is necessary to setup your environment to be able to use Terraform with Oracle cloud. The subsequent slides step through the configuration of the relevant variables in the terraform.tfvars file and preparing for deployment.

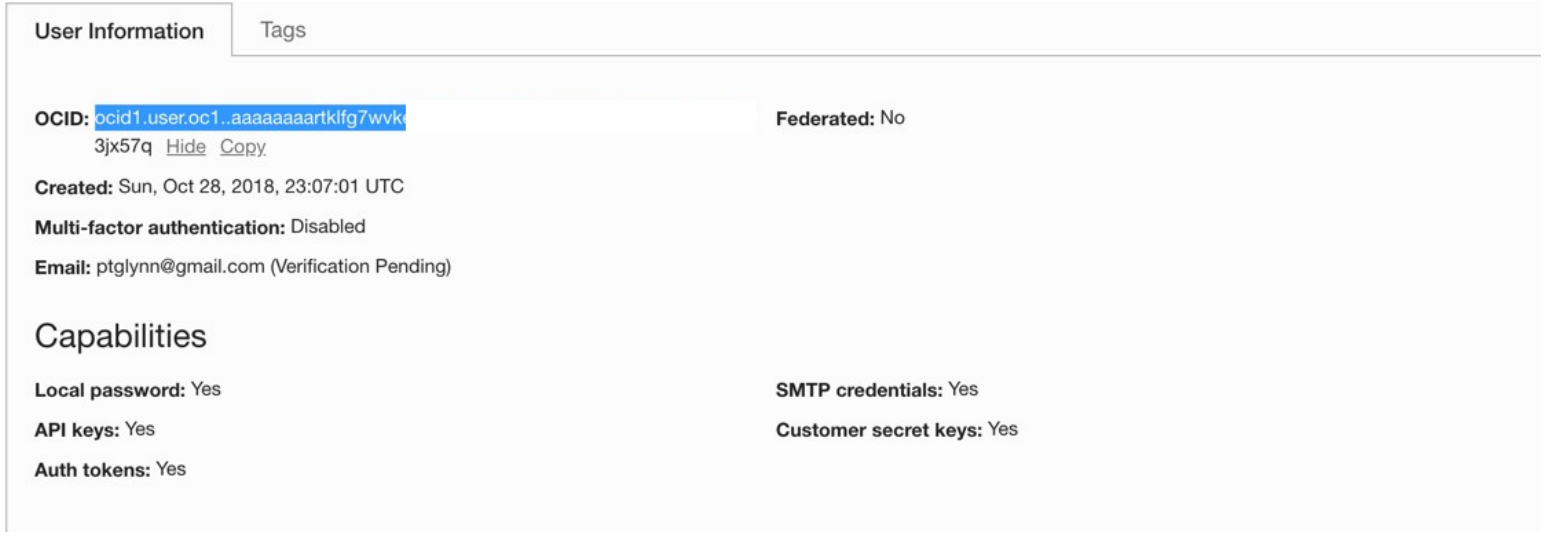
Variable: tenancy_ocid

The tenancy OCID may be retrieved from **Administration > Tenancy details**:



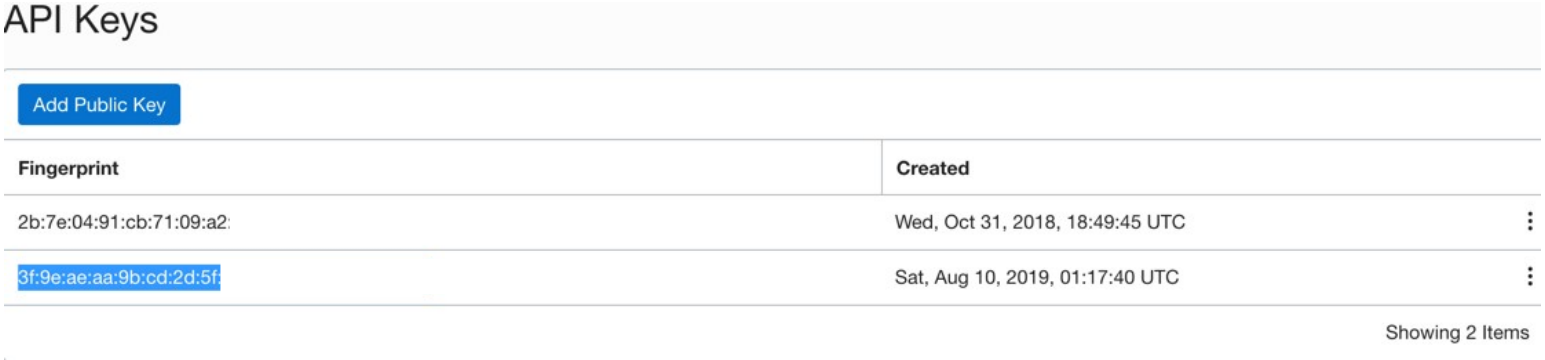
Variable: user_ocid

The user OCID may be retrieved from **Identity > Users** and then clicking on the desired user:



Variable: fingerprint

Add a PEM-formatted public SSH key to the user account and note the associated fingerprint:



Variable: private_key_path

Determine the absolute path to the PEM-formatted private ssh key:

```
bash-4.3# pwd
/root/.oci
bash-4.3# ls -altr
total 12
-rw-------    1 root     root           451 Aug 10  2019 oci_api_key_public.pem
-rw-------    1 root     root          1675 Aug 10  2019 oci_api_key.pem
-rw-------    1 root     root           296 Aug 10  2019 config
drwxr-xr-x    5 root     root           160 Aug 10  2019 .
drwxr-xr-x  129 root     root          4128 Mar  5 20:27 ..
```

Variable: parent_compartment_ocid

This is the OCID of the parent (root) compartment located under **Identity > Compartments**:

Variable: ssh_authorized_key

This is the public SSH key for the user and must be formatted “ssh-rsa <public_key> <username>”.

Variable: fw_mgmt_src_ip

This is the public IP address/subnet that will be permitted to connect to the management interface of the firewalls.

Variable: region

This is the properly-formatted OCI region into which the infrastructure will be deployed. Examples include:

- me-jeddah-1
- sa-saopaulo-1
- uk-gov-london-1
- uk-london-1
- us-ashburn-1
- us-langley-1
- us-luke-1
- us-phoenix-1

Deployment

Once the terraform.tfvars has been modified, it is ready for deployment:

```
oci_core_vnic_attachment.firewall1_ha2: Creation complete after 14s (ID: ocid1.vnicattachment.oc1.iad
anuwcljtaj...ptf4dpn37aefgybwh32sffiihctsgdvtd7ftia)
oci_core_instance.web1: Still creating... (20s elapsed)
oci_core_instance.web1: Still creating... (30s elapsed)
oci_core_instance.web1: Still creating... (40s elapsed)
oci_core_instance.web1: Still creating... (50s elapsed)
oci_core_instance.web1: Still creating... (1m0s elapsed)
oci_core_instance.web1: Still creating... (1m10s elapsed)
oci_core_instance.web1: Still creating... (1m20s elapsed)
oci_core_instance.web1: Creation complete after 1m26s (ID: ocid1.instance.oc1.iad.anuwcljtajvtbmac...
qi6cgfcby37coop25ha24vbjffvs55wbqeayq)

Apply complete! Resources: 28 added, 0 changed, 0 destroyed.
bash-4.3#
```

FW Configuration

The fw-config folder contains basic firewall configurations (username: admin, password: Pal0Alt0@123) for HA and supports SSH connections to the web1 host as well as outbound internet connectivity.