FortiADC - OCI Deployment Guide

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 3, 2021
FortiADC OCI Deployment Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-05-13	Third release with 6.1.1 content.
2019-10-02	Second release with Marketplace support and Template 4.0.
2019-05-29	First release 5.2.4

Introduction

Oracle Cloud Infrastructure Compute provides bare metal compute capacity that delivers performance, flexibility, and control without compromise. It is powered by Oracle's next generation, internet-scale infrastructure designed to help you develop and run your most demanding applications and workloads in the cloud.

This guide is for users to deploy FortiADC-VM on Oracle Cloud Infrastructure.

For FortiADC 5.2.4 (and subsequent versions), limitations on memory and disk size are removed, for any license. However, the number of vCPU's you can deploy is still limited, in accordance with the guidelines of the relevant license.

Deploying FortiADC-VM on Oracle Cloud Infrastructure

1. Create a virtual cloud network.

Log into your Oracle Cloud Infrastructure account. Navigate by way of the sidebar to **Compute**. Make sure that under List Scope (on the sidebar) you are in the right compartment.

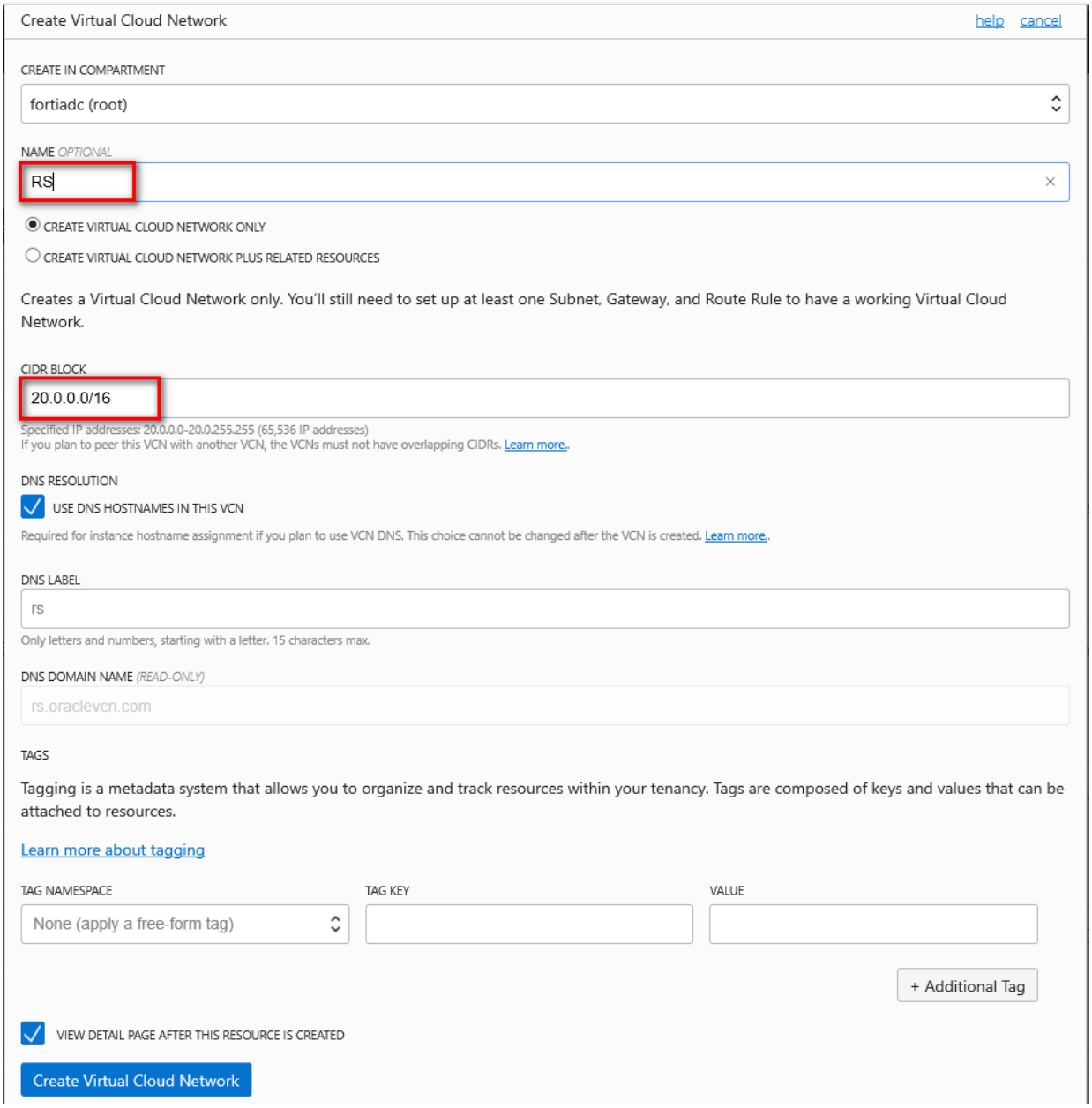
Navigate to **Networking > Virtual Cloud Networks > Create Virtual Cloud Network** (the blue tab).

In the **name** field, enter the VCN name.

Select between the following two options:

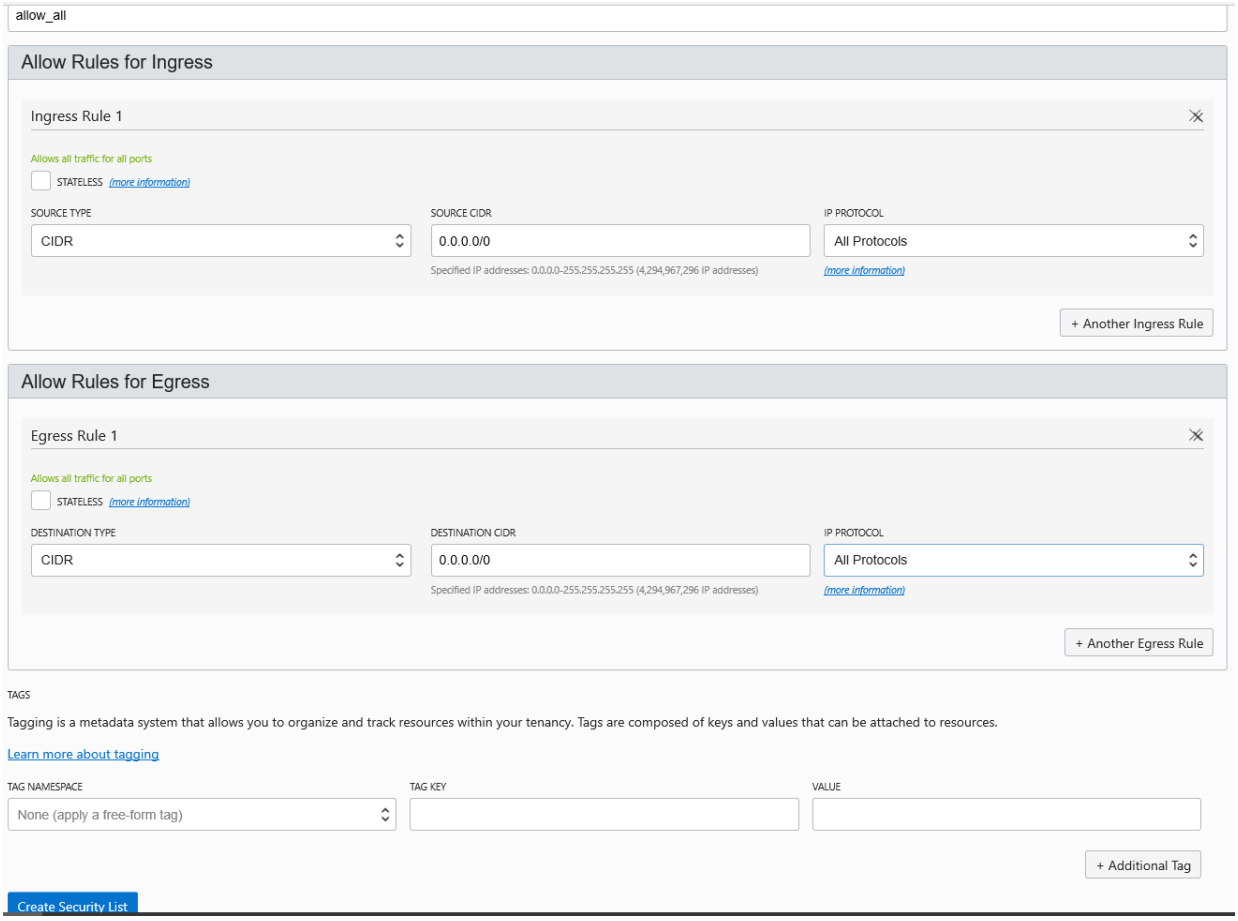
- CREATE VIRTUAL CLOUD NETWORK ONLY—allows you to create each resource separately by specifying your own inputs.
- CREATE VIRTUAL CLOUD NETWORK PLUS RELATED RESOURCES—allows you to create the Internet gateway, routing table, and subnet all together using Oracle default settings.

In this example, the first choice is used.



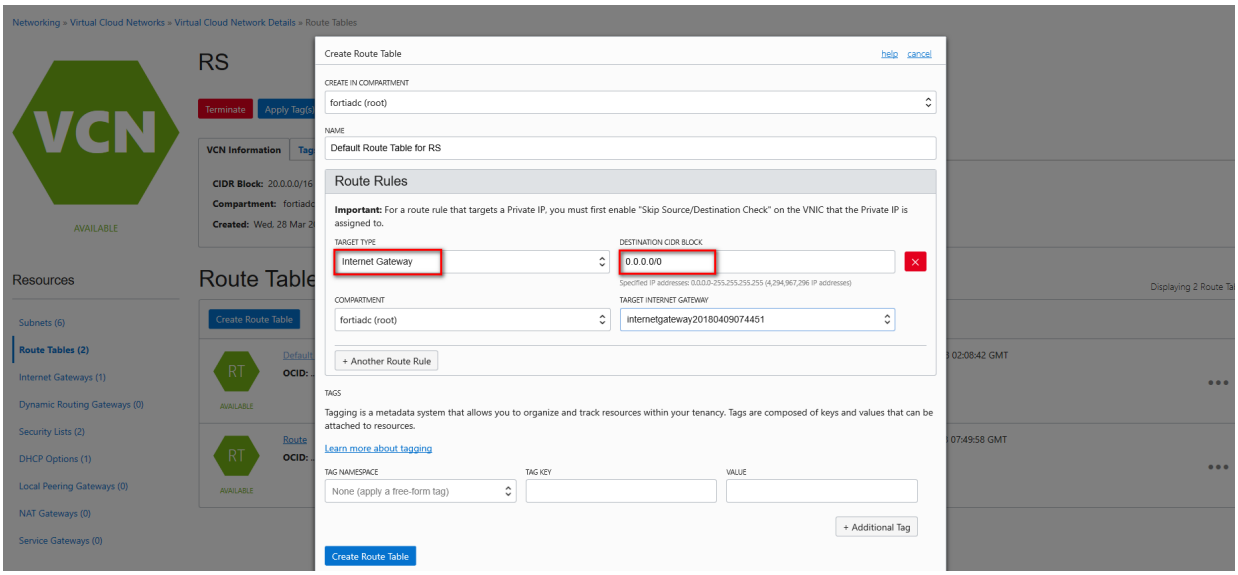
2. Create a security list.

Navigate to **Networking > Virtual Cloud Networks**. Click into the individual Virtual Cloud Network you have just created, then go to **Security Lists**. Click **Create Security List**, then add or edit the rule according to the actual network environment. The following is an example of a configuration that allows all traffic. However, the user must create rules according to their own network requirements.

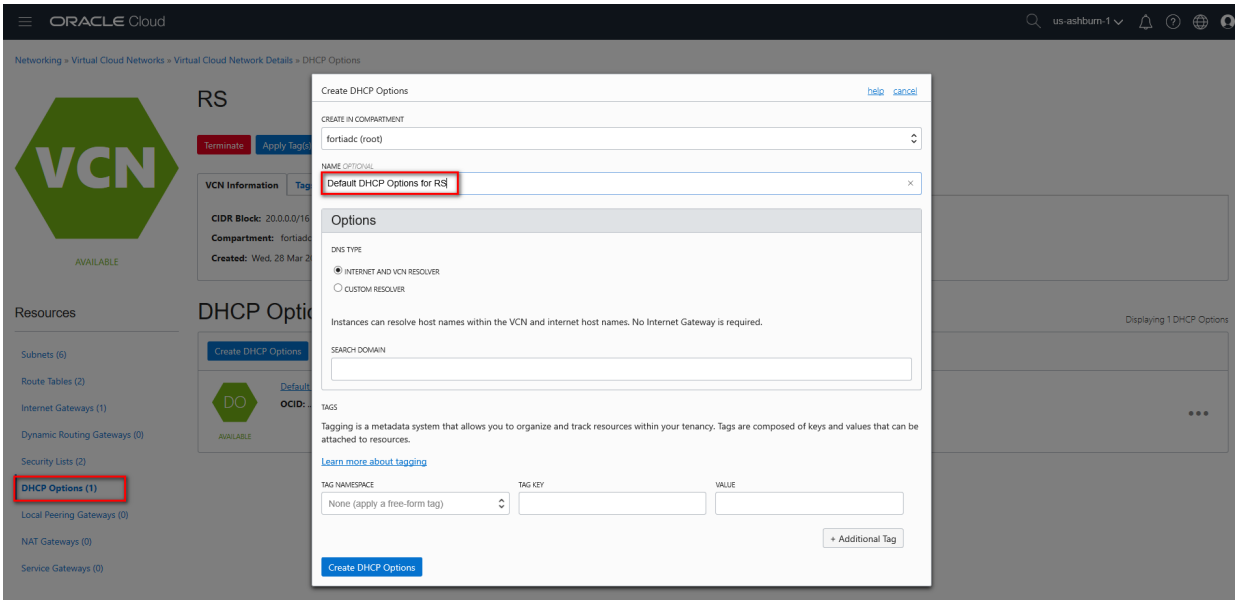


3. Create a route table and DHCP options for the internal network.

Navigate to **Networking > Virtual Cloud Networks**. Click into your individual Virtual Cloud Network and go to **Route Tables**. Click **Create Route Table**. You can configure route rules according to the actual network environment.



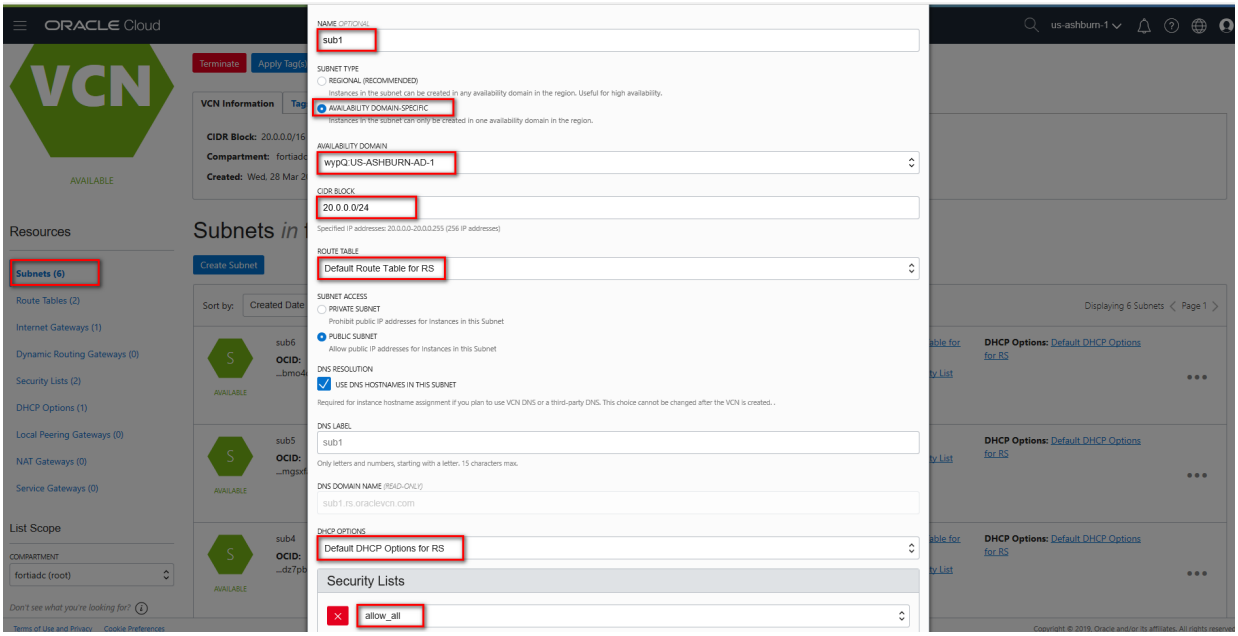
Click **Create DHCP Options**. Write a name.



4. Create internal network subnet.

Create internal network subnet In the NAME field, enter the Subnet name. For SUBNET TYPE, select AVAILABILITY DOMAIN-SPECIFIC.

Set the AVAILABILITY DOMAIN, configure the CIDR BLOCK，select ROUTE TABLE. Go down and select DHCP OPTIONS and Security Lists.



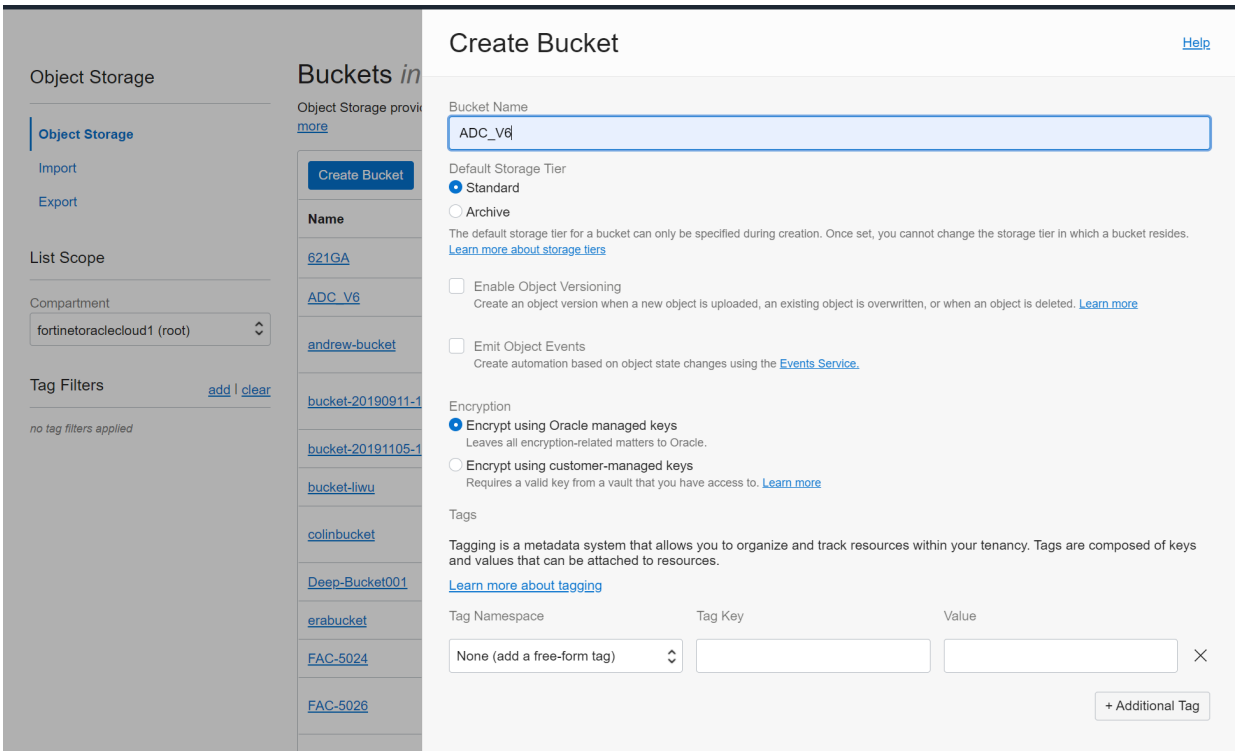
5. Upload the image.

Starting from 5.2.4 we suggest configuring the ADC instance from Marketplace. If the user has gone this route, the user does not need to worry about step 5, "Upload the image," and may proceed to step 6, "Create the FortiADC instance."

We also suggest using Paravirtualized Mode over Emulated Mode for better performance.

Download VM Images from https://support.fortinet.com. Decompress FAD_OCI-V500-buildXXXX-FORTINET.out.oci.gz to get the qcow image.

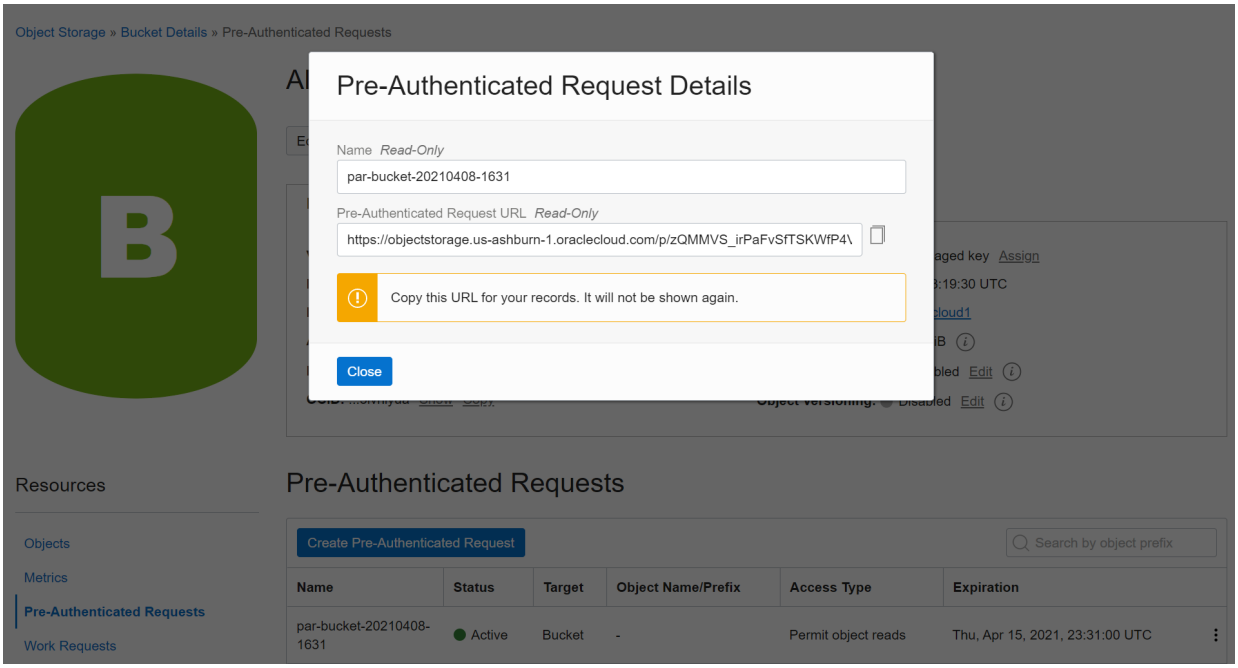
Navigate to **Object Storage > Object Storage**. Click **Create Bucket**. Enter BUCKET NAME and click **Create Bucket.**



Select the bucket, then **upload** the qcow image.

Once uploaded, the following screen appears. Click **Create Pre-Authenticated Requests** from the left or right menu.

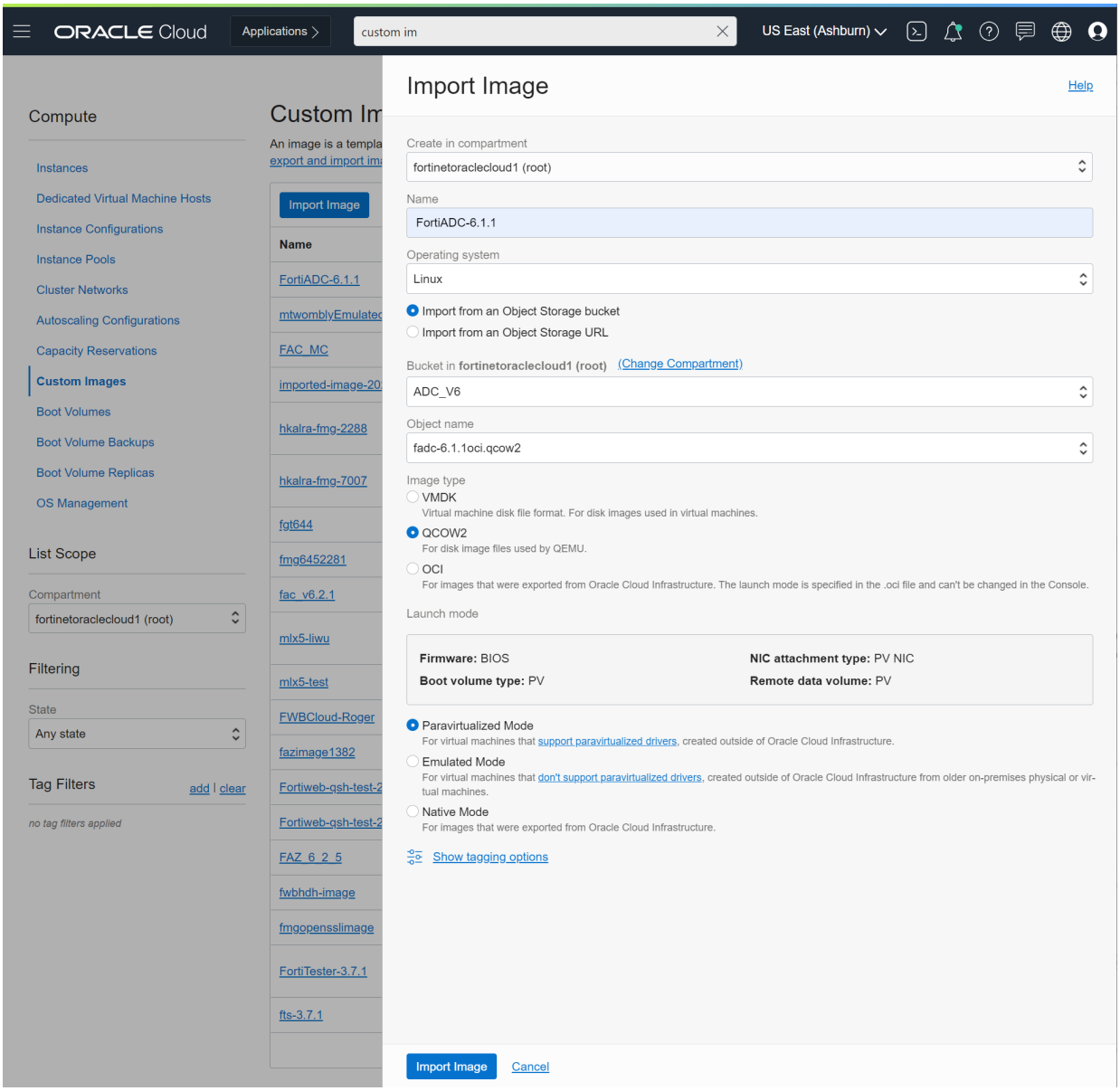
Copy the request URL manually for next step (or just click Copy).



Navigate to **Compute > Custom Images**. Click **Import Image**. Complete the fields. If you choose **Import from an Object Storage bucket**, simply choose the bucket you created and the object you just uploaded. Or, you can select **Import from an Object Storage URL** and paste the URL you copied from **Pre-Authenticated Request**.

Under IMAGE TYPE, select QCOW2. Under LAUNCH MODE, select PARAVIRTUALIZED MODE.

You have now imported the image. Wait until the Importing… state changes to **Succeeded**. After the change, navigate to the image.



6. Create the FortiADC instance.

Starting from 5.2.4 we suggest configuring the ADC instance from Marketplace, which is newly supported.

FortiADC license requirements

If you are working with FortiADC pre-5.2.2, the trial license only supports 2 vCPU's and 8G memory. When you are selecting an instance shape, be careful not to exceed these limitations. The trial license limitations match the shape **VM.Standard.E2.1,** with 1 OCPU and 8G memory.

The FortiADC license applies to VCPU and not OCPU, which is an Oracle Cloud object.

The FortADC virtual machine uses 2G bootdisk size by default. However, the OCI allocated "boot volume size" (the same meaning a "bootdisk size") has to be larger than 46.6G, which is its minimum. Thus we use the default bootdisk size (46.6G) when configuring the FortiADC bootdisk.

The FortiADC requires at minimum 1 vCPU and 4G memory. In actual practice, though, it's suggested that you use at least 2 vCPU and 8G memory.

How to create the FortiADC instance: Marketplace and Custom images

There are two options for creating the FortiADC instance: Marketplace and Custom images.

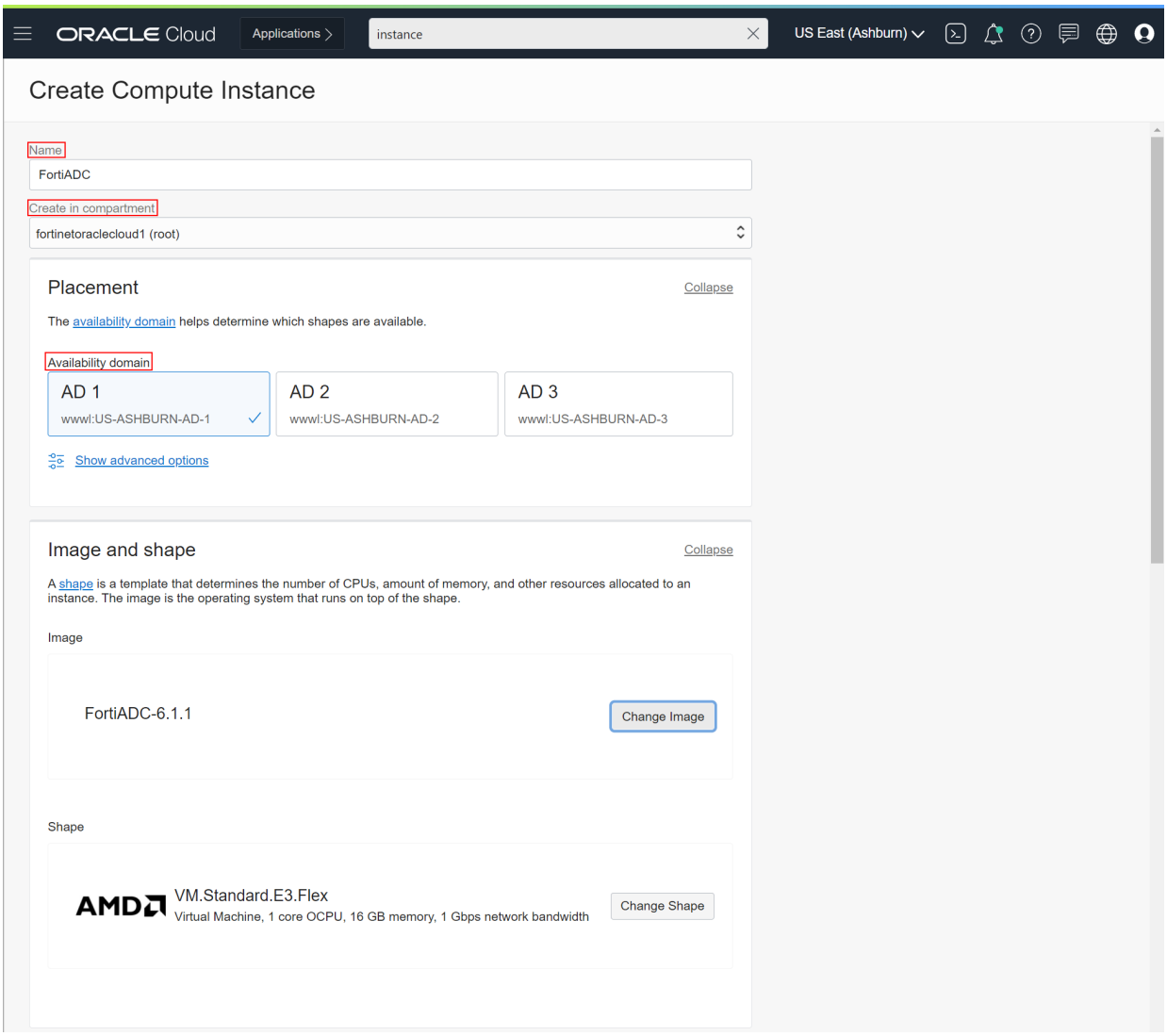
1. Marketplace

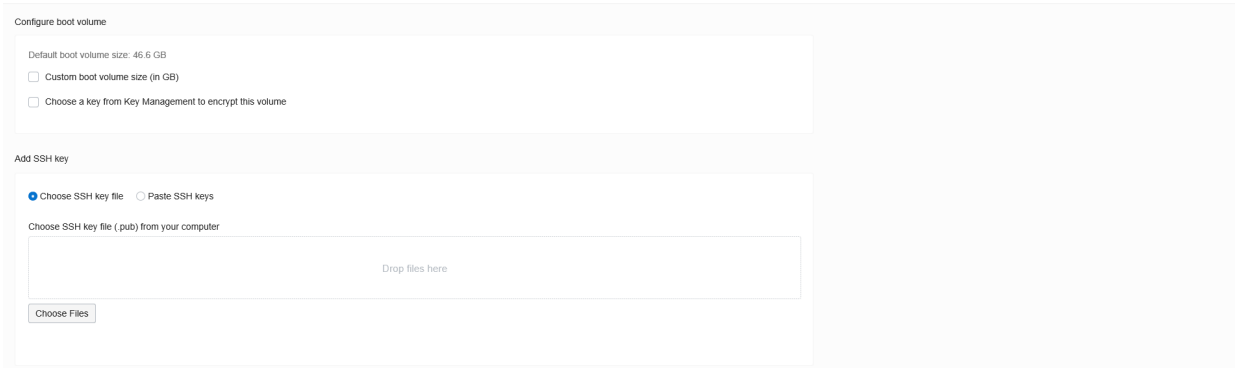
Go to **Marketplace > find the FortiADC > Launch Instance.** Choose the version (Paravirtualized Mode, the default, is suggested). Select compartment. **Accept terms of agreement > Launch Instance**.

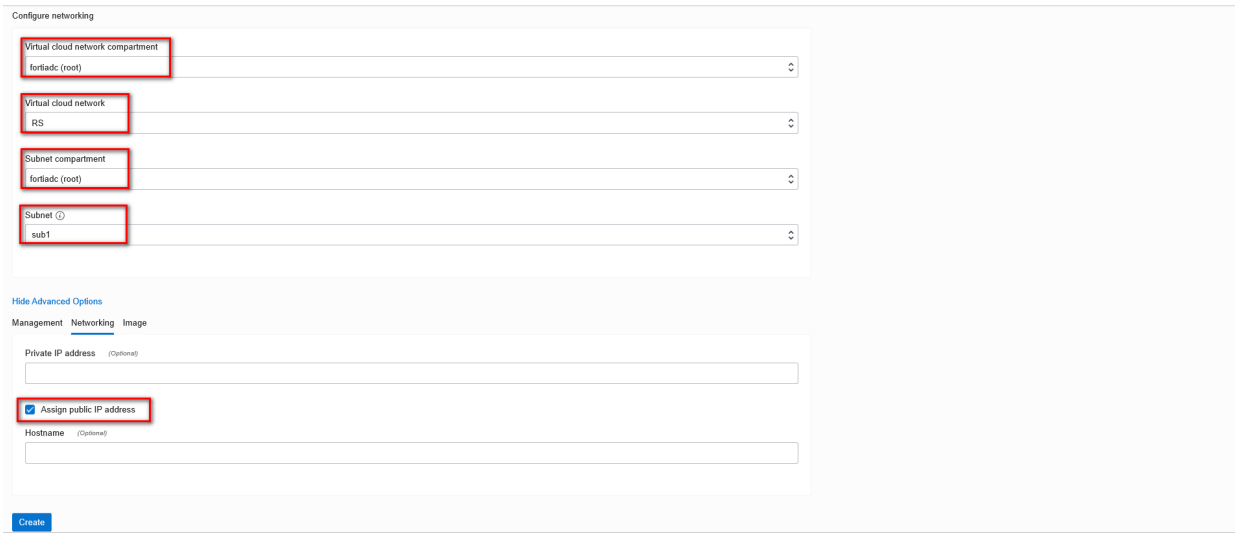
2. Custom images

Navigate to **Compute > Instances**. Click **Create Instance.** Enter NAME, select the desired DOMAIN, Under IMAGE SOURCE, select CUSTOM IMAGES, then select the image you imported earlier. Under SHAPE TYPE, select VIRTUAL MACHINE. In the SHAPE FIELD, select one of the following supported instance shapes. For **Networking**, select the desired VIRTUAL CLOUD NETWORK and SUBNET.

Ensure **Assign public IP address** is selected so you can access the FortiADC over the Internet. Then click **Create,** on the very bottom.


ORACLE Cloud
Applications
instance
US East (Ashburn)
Create Compute Instance
Name
FortiADC
Create in compartment
fortinetoraclecloud1 (root)
Placement
Collapse
The availability domain helps determine which shapes are available.
Availability domain
AD 1
wwwl:US-ASHBURN-AD-1
AD 2
wwwl:US-ASHBURN-AD-2
AD 3
wwwl:US-ASHBURN-AD-3
Show advanced options
Image and shape
Collapse
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
FortiADC-6.1.1
Change Image
Shape
AMD
VM.Standard.E3.Flex
Virtual Machine, 1 core OCPU, 16 GB memory, 1 Gbps network bandwidth
Change Shape


Configure boot volume
Default boot volume size: 46.6 GB
Custom boot volume size (in GB)
Choose a key from Key Management to encrypt this volume
Add SSH key
Choose SSH key file
Paste SSH keys
Choose SSH key file (.pub) from your computer
Drop files here
Choose Files

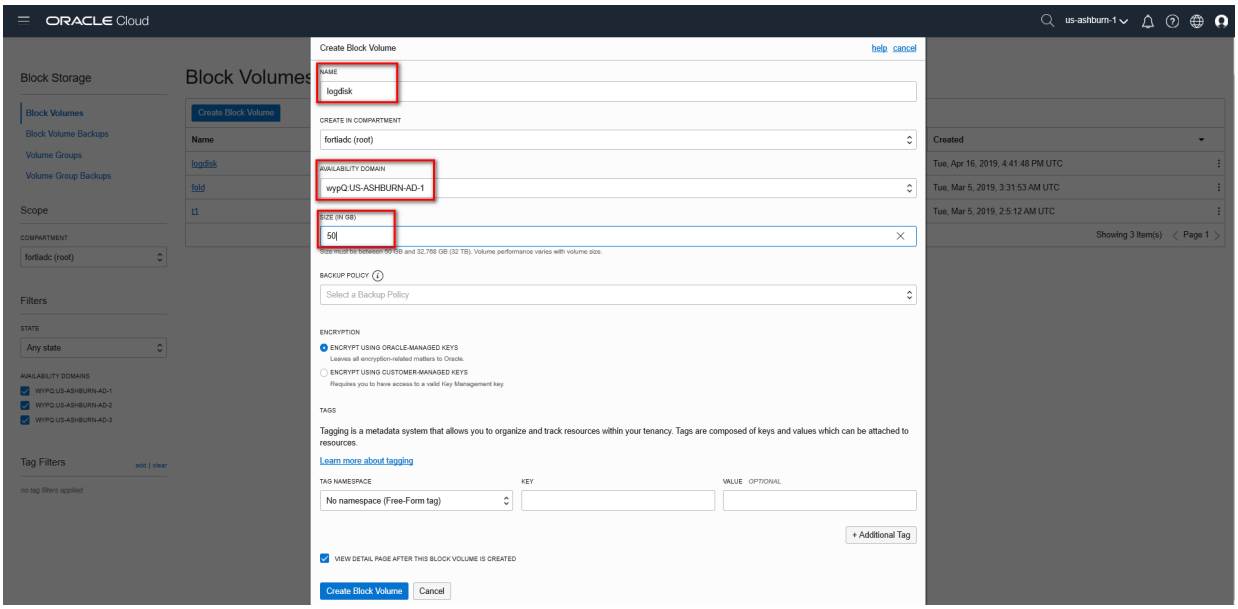


7. Attach a storage to FortiADC.

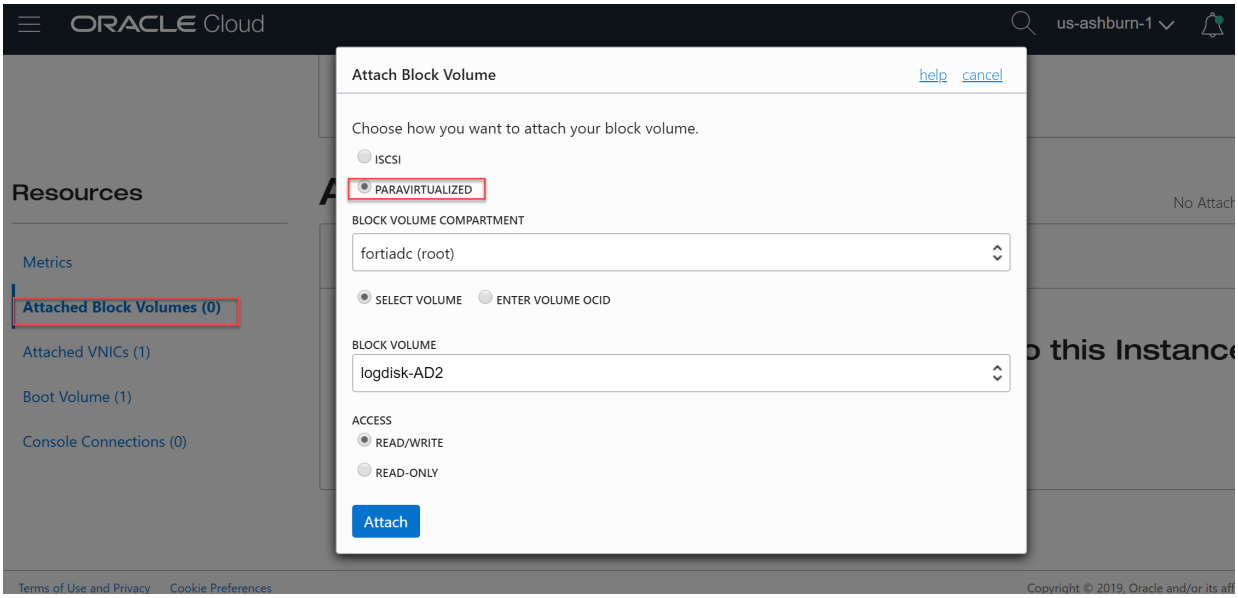
The instance was launched without a log disk. To add log disk, Navigate to Block Storage > **Block Volumes**. Click **Create Block Volume.** Set NAME, select DOMAIN, set SIZE and then click **Create Block Volume**.

The FortADC virtual machine uses 30G logdisk by default. However, the OCI allocated disk size has to be larger than 50G, which is its minimum. As shown in this example, configure the FortiADC logdisk to be 50G (the ADC does not limit its size).

It is recommended that users attach a logdisk, otherwise some functions will not work properly, such as HA and upload image, etc.



Return to the FortiADC instance. Click **Attach Block Volumes**, select PARAVIRTUALIZED and select BLOCK VOLUME. Click **Attach**.



After attaching the block volume, ensure you **reboot** the FortiADC instance. You can use “execute reboot”.

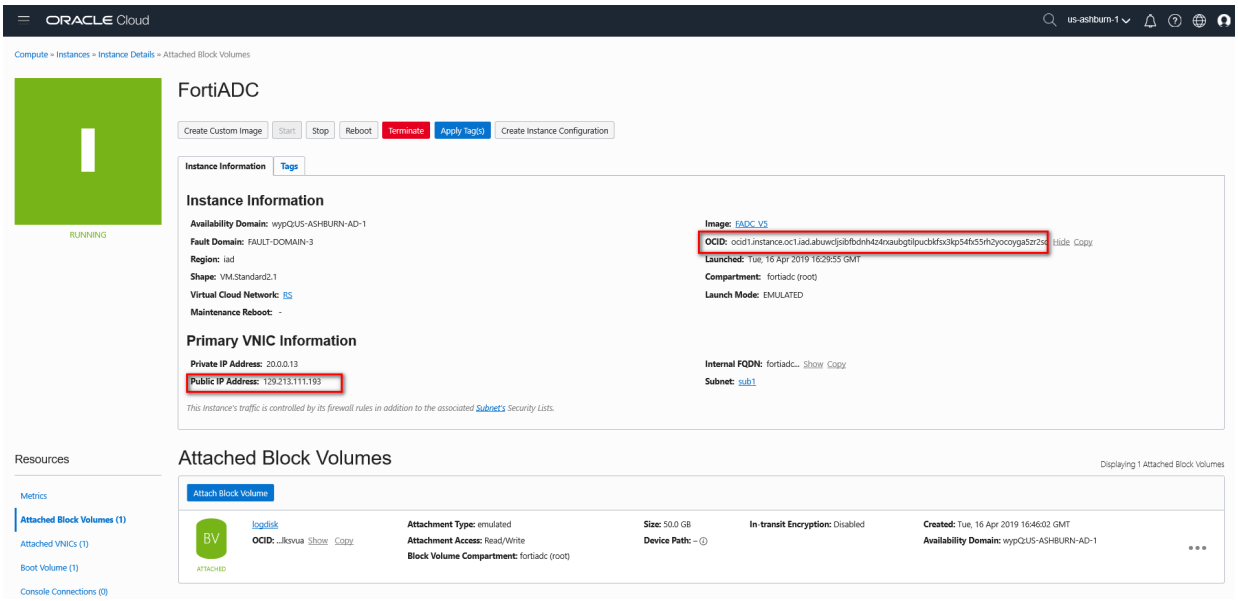
If the instance was configured in **Emulated Mode**, when attaching the log disk, you will see the following dialogue box. Ensure that Emulated Mode is selected.

8. Access the FortiADC.

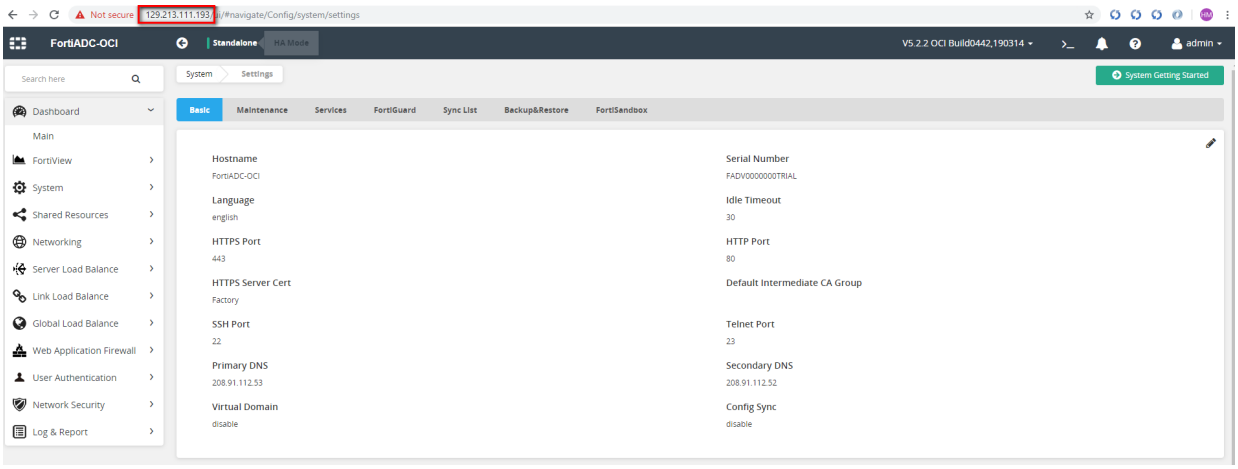
In the FortiADC instance, find the public IP address. In a browser, you can now use this public IP to log into FortiADC through the following ways:

- http://<public_IP_address>
- https://<public_IP_address>
- SSH

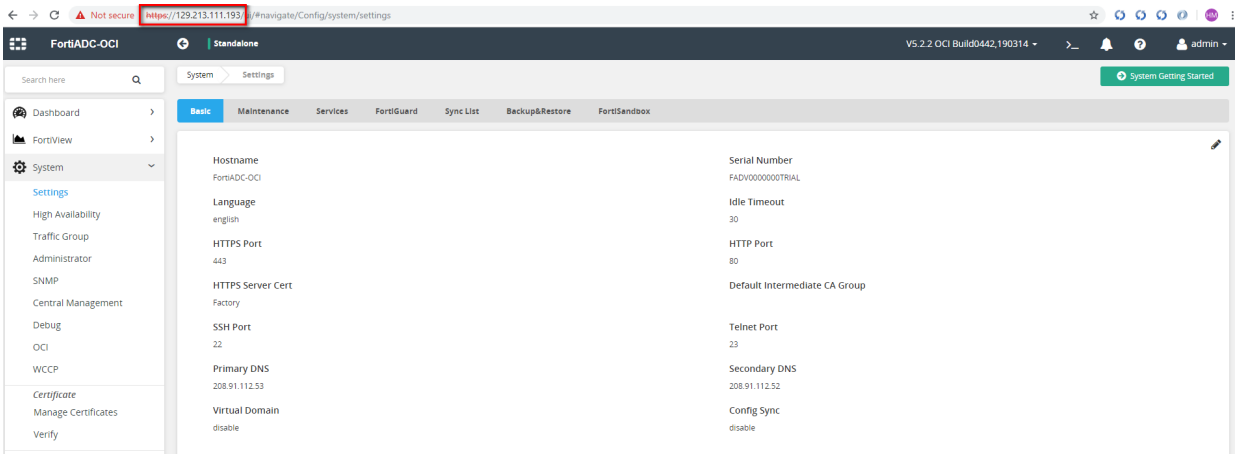
The default username is admin. The default password is the OCID.



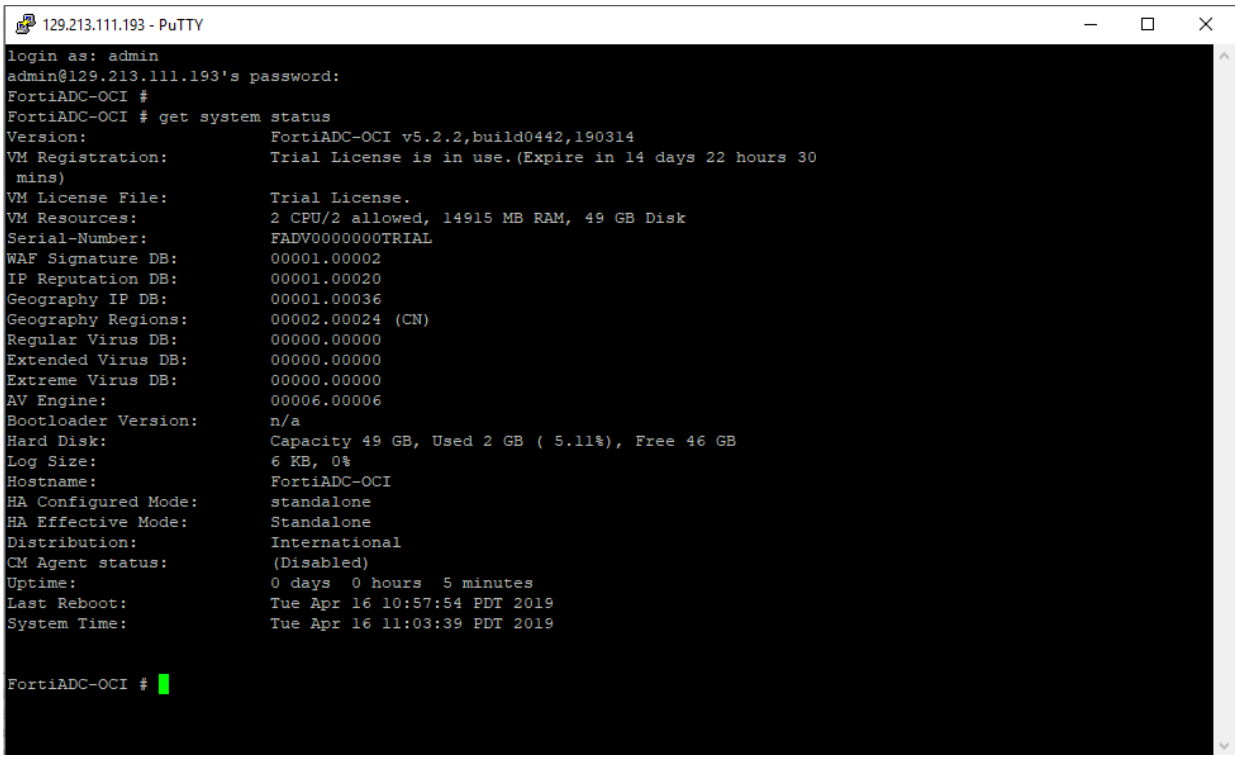
Log into FortiADC by way of HTTP.



Log into FortiADC by way of HTTPS.

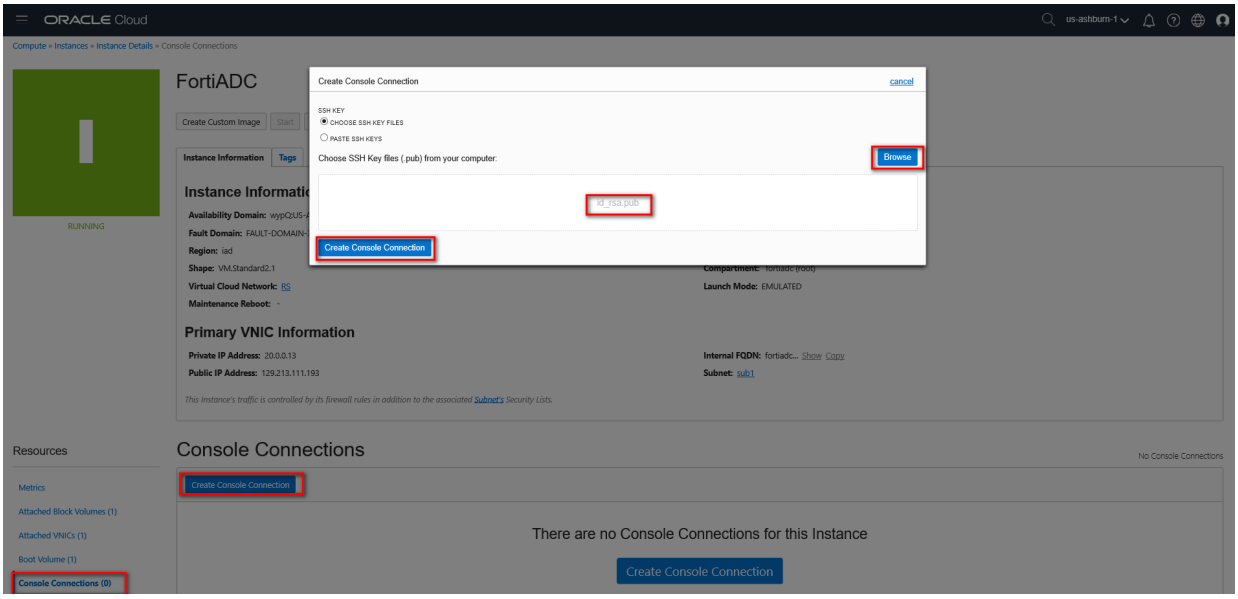


Log into FortiADC by way of SSH.

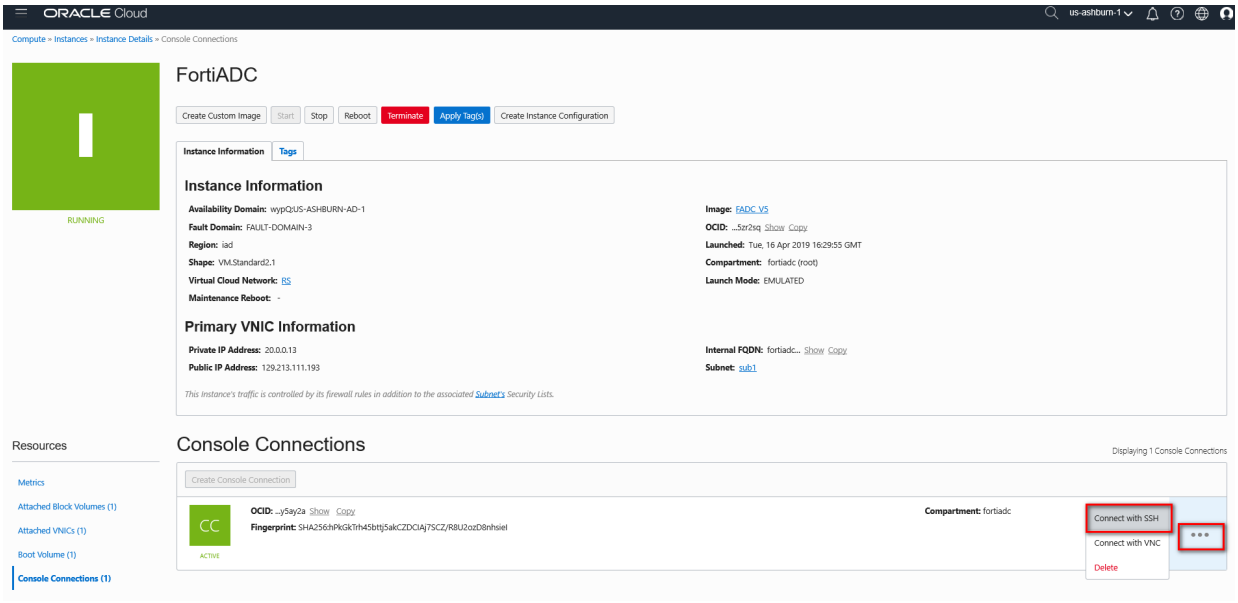


9. Create Console Connection.

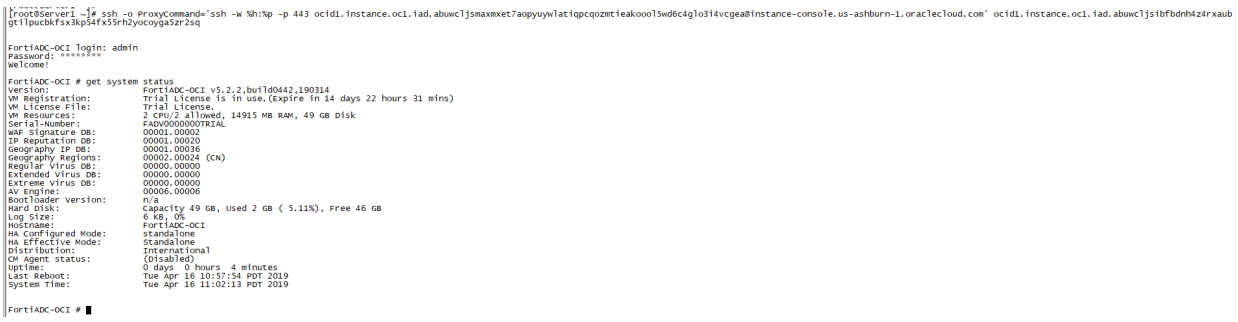
Navigate to **Instance** page. Click **Console Connections** and click **Create Console Connection**. **Upload** your host SSH public key. If you don't have a public key, please use ssh-keygen to generate one.



Click **Connectwith SSH** and copy the ssh command.



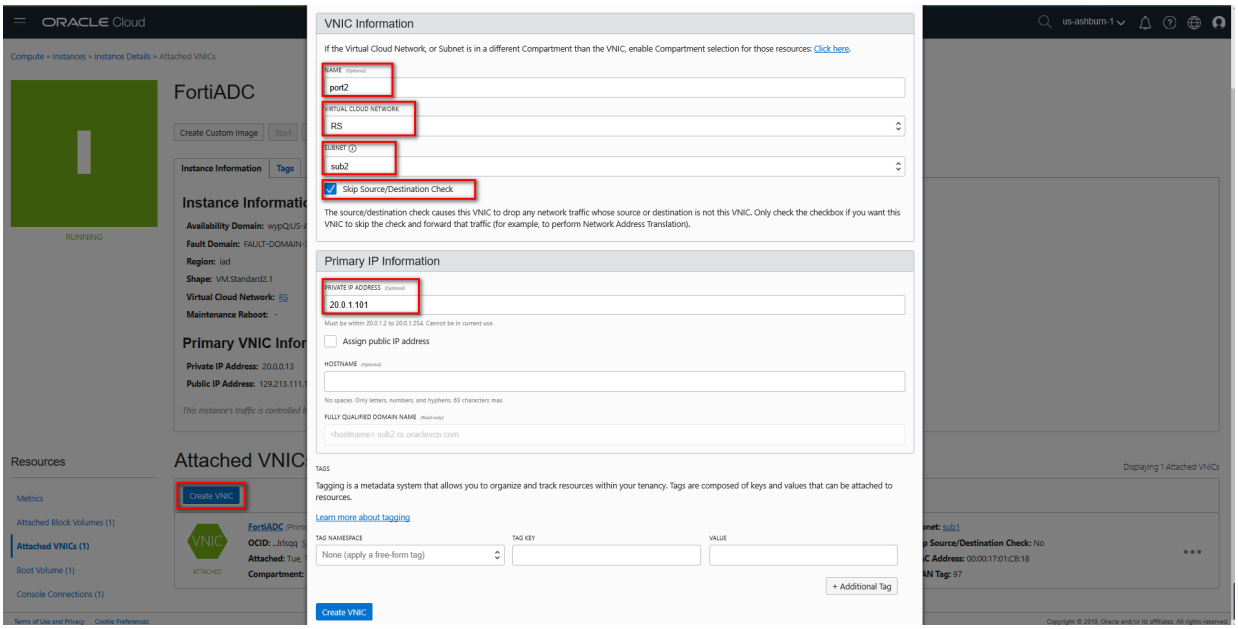
Run the copied command under Linux console. Press **Enter** to refresh the output.

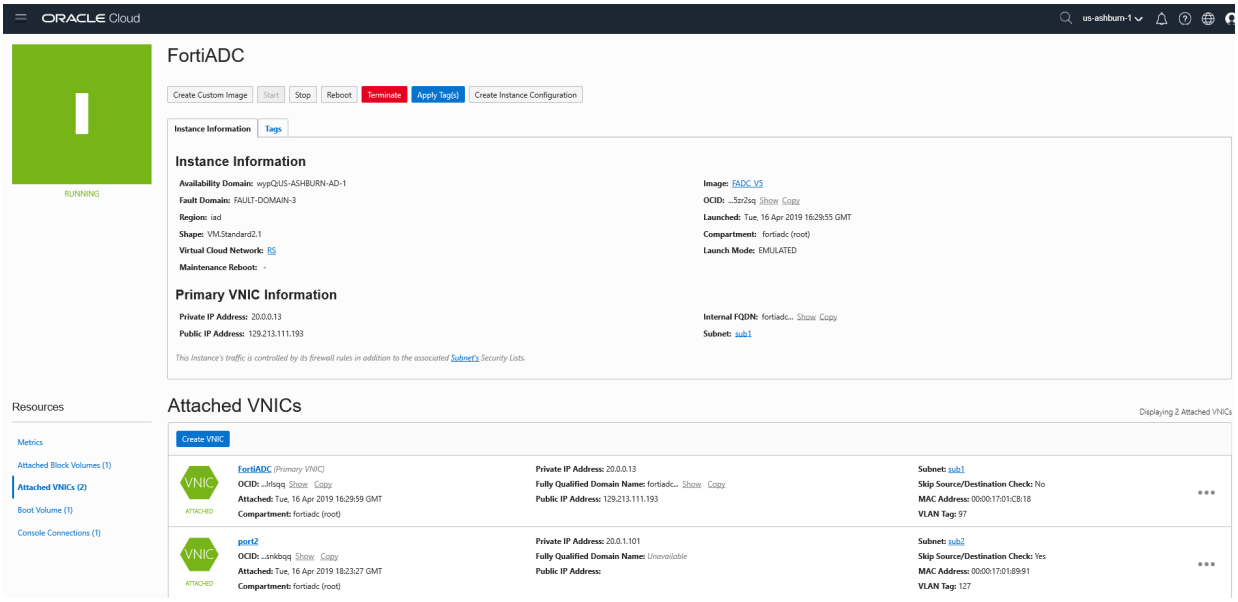


10. Create the second vNIC.

In the FortiADC instance, click **Attached VNICs > Create VNIC.** Create the virtual network interface by specifying the name, then specify the **Virtual Cloud Network**, and the internal subnet created earlier. Ensure **Skip Source/Destination Check** is selected. Enter an IP address and click **Create VNIC.**

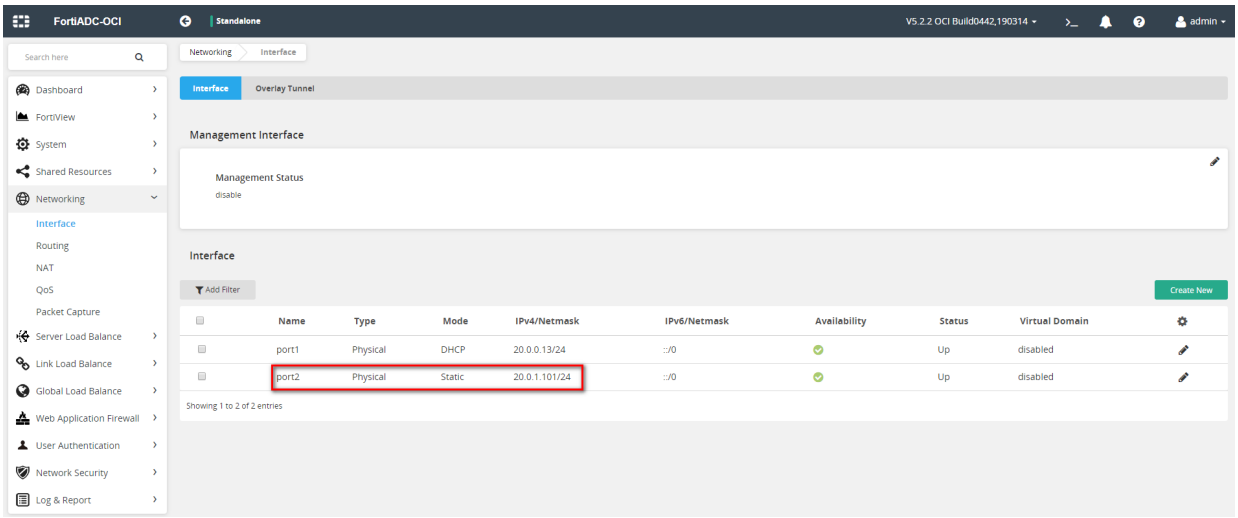
The FortADC virtual machine supports a maximum 10 ports. Users can add interfaces according to their network requirements. It's suggested that you use at least 2 ports.





11. Configure the second vNIC on the FortiADC.

After attaching the second vNIC to the FortiADC, ensure you **reboot** the FortiADC, then log into the FortiADC. Log into the GUI console and navigate to **Network > Interfaces**. You now see two ports, but the second port is not configured with an IP address. Manually configure the same IP address specified on OCI.



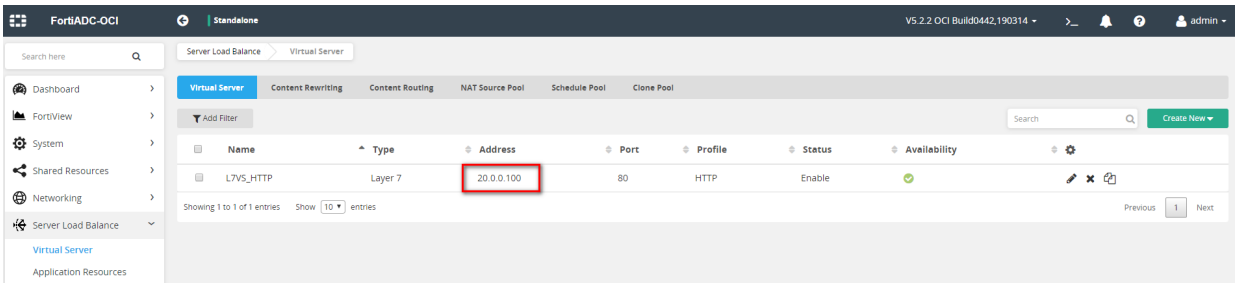
12. To assign a new secondary private IP to a VNIC

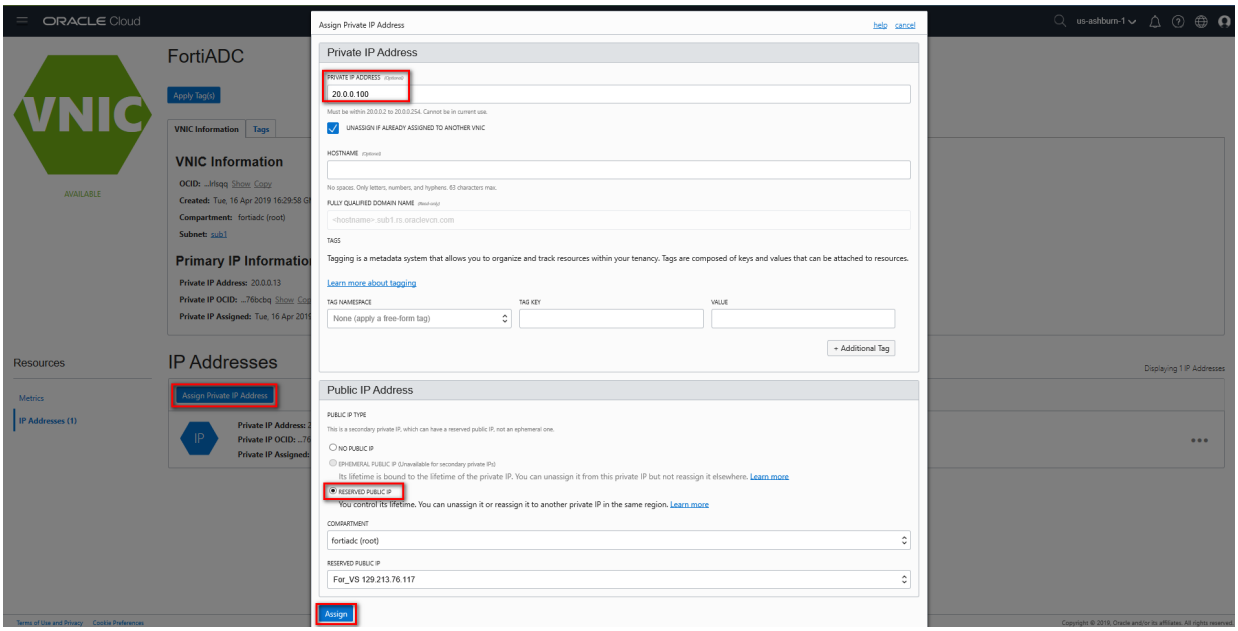
After configuring the VS on the FortiADC, you must assign the VS IP to the VNIC on OCI.

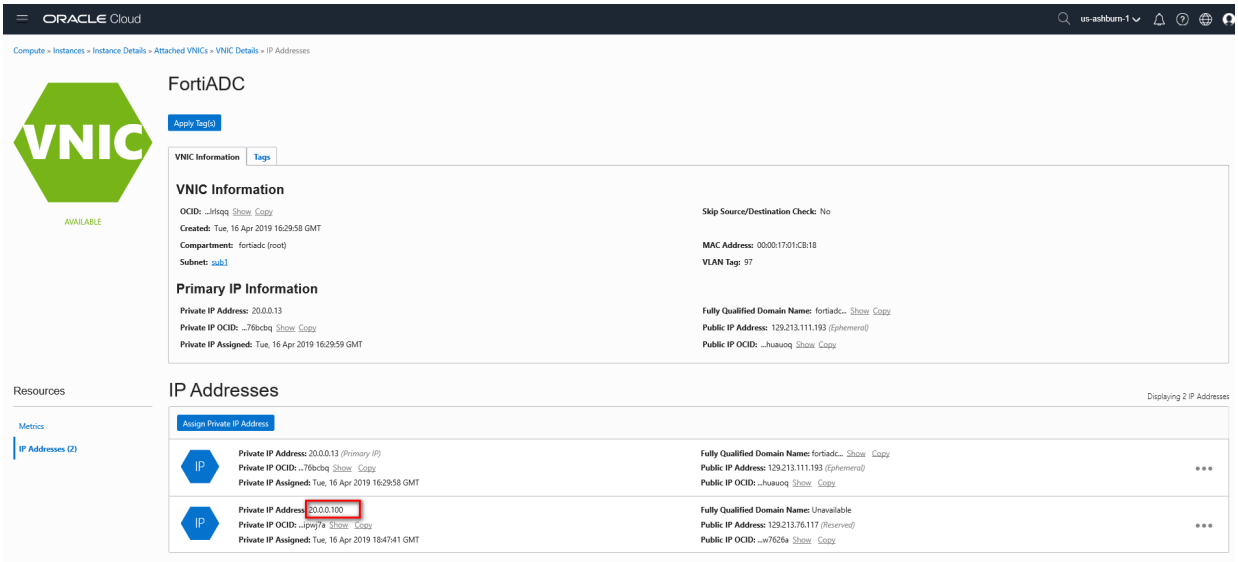
In addition, if you configure “Secondary IP Address”, “Floating IP”, L4VS “NAT Source Pool”, SNAT “Translation to IP Address”, or DNAT “External Address Range” etc, you must assign these IP to the VNIC on OCI also.

Open the navigation menu. Under Compute, click **Instances**. Click the instance to view its details. Click **Attached VNICs,** and then click the VNIC you're interested in. Click **Assign IP Address.**

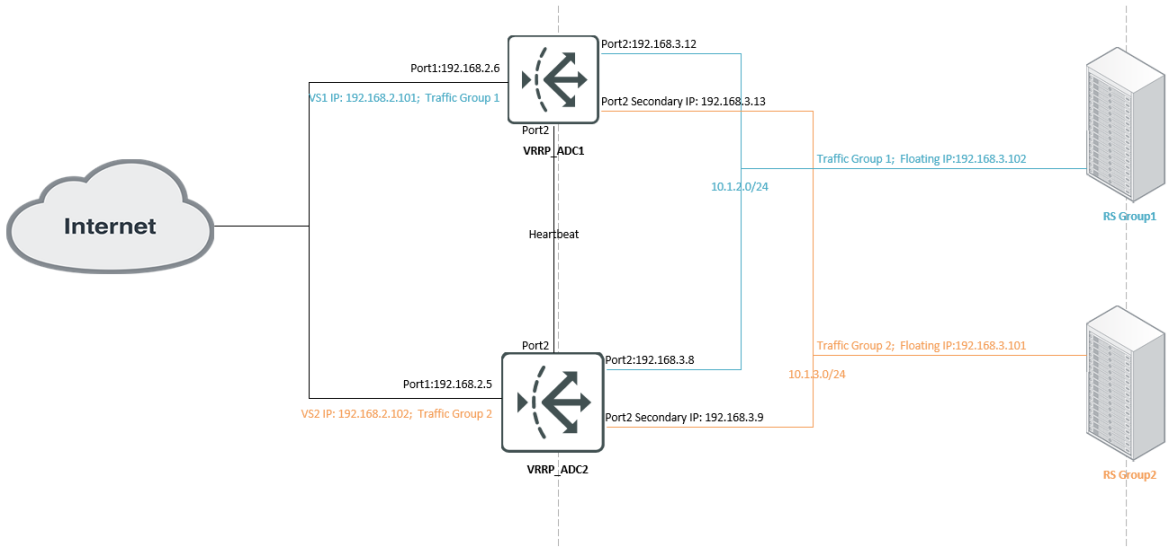
If necessary, you can assign a public IP, after then user can access the VS through the public IP.




ORACLE Cloud
Assign Private IP Address
help cancel
Private IP Address
PRIVATE IP ADDRESS (Optional)
20.0.0.100
UNASSIGN IF ALREADY ASSIGNED TO ANOTHER VNIC
HOSTNAME (Optional)
TAGS
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
None (apply a free-form tag)
TAG KEY
VALUE
+ Additional Tag
Public IP Address
PUBLIC IP TYPE
NO PUBLIC IP
EPHEMERAL PUBLIC IP
RESERVED PUBLIC IP
You control its lifetime. You can unassign it or reassign it to another private IP in the same region. Learn more
COMPARTMENT
fortiadc (root)
RESERVED PUBLIC IP
For_VS 129.213.76.117
Assign
FortiADC
Apply Tag(s)
VNIC Information
Tags
VNIC Information
Primary IP Information
Resources
IP Addresses
Assign Private IP Address
Metrics
IP Addresses (1)


ORACLE Cloud
us-ashburn-1
Compute » Instances » Instance Details » Attached VNICs » VNIC Details » IP Addresses
FortiADC
Apply Tag(s)
VNIC Information
Tags
VNIC Information
OCID: ...lrlsqq Show Copy
Created: Tue, 16 Apr 2019 16:29:58 GMT
Compartment: fortiadc (root)
Subnet: sub1
Skip Source/Destination Check: No
MAC Address: 00:00:17:01:CB:18
VLAN Tag: 97
Primary IP Information
Private IP Address: 20.0.0.13
Private IP OCID: ...76bcbq Show Copy
Private IP Assigned: Tue, 16 Apr 2019 16:29:59 GMT
Fully Qualified Domain Name: fortiadc... Show Copy
Public IP Address: 129.213.111.193 (Ephemeral)
Public IP OCID: ...huauoq Show Copy
Resources
IP Addresses
Displaying 2 IP Addresses
Assign Private IP Address
Metrics
IP Addresses (2)
Private IP Address: 20.0.0.13 (Primary IP)
Private IP OCID: ...76bcbq Show Copy
Private IP Assigned: Tue, 16 Apr 2019 16:29:58 GMT
Fully Qualified Domain Name: fortiadc... Show Copy
Public IP Address: 129.213.111.193 (Ephemeral)
Public IP OCID: ...huauoq Show Copy
Private IP Address: 20.0.0.100
Private IP OCID: ...ipwj7a Show Copy
Private IP Assigned: Tue, 16 Apr 2019 18:47:41 GMT
Fully Qualified Domain Name: Unavailable
Public IP Address: 129.213.76.117 (Reserved)
Public IP OCID: ...w7626a Show Copy

Example: Set VS on OCI in HA-VRRP mode



Configure HA on ADC1

```
config system ha
   set mode active-active-vrrp
   set hbdev port2
   set datadev port2
   set group-id 31
   set local-node-id 1
   set group-name oci_group
   set config-priority 200
   set override enable
   set l7-persistence-pickup enable
   set l4-persistence-pickup enable
   set l4-session-pickup enable
   set hb-type unicast
   set local-address 192.168.3.12
   set peer-address 192.168.3.8
   end
```

Configure HA on ADC2

```
config system ha
   set mode active-active-vrrp
   set hbdev port2
   set datadev port2
   set group-id 31
   set group-name oci_group
   set override enable
   set l7-persistence-pickup enable
   set l4-persistence-pickup enable
   set l4-session-pickup enable
   set hb-type unicast
   set local-address 192.168.3.8
```

```
   set peer-address 192.168.3.12
   end
```

Configure Traffic-Group on ADC

```
config system traffic-group
   edit "0_1"
   set failover-order 0 1
   set preempt enable
next
   edit "1_0"
   set failover-order 1 0
   set preempt enable
next
end
```

Configure VS on ADC

```
config load-balance real-server
   edit "RS1"
   set ip 192.168.3.2
   next
   edit "RS2"
   set ip 192.168.3.3
   next
   end
   config load-balance pool
   edit "Pool_1"
   set real-server-ssl-profile NONE
   config pool_member
   edit 1
   set pool_member_cookie rs1
   set real-server RS1
   next
   end
   next
   edit "Pool_2"
   set real-server-ssl-profile NONE
config pool_member
   edit 1
   set pool_member_cookie rs1
   set real-server RS2
   next
   end
   next
   end
config load-balance virtual-server
edit "L7_HTTP_Public_IP"
   set type l7-load-balance
   set interface port1
   set ip 192.168.2.102
   set port 8003
   set load-balance-profile HTTP
   set load-balance-method LB_METHOD_ROUND_ROBIN
   set load-balance-pool Pool_1
   set traffic-log enable
   set traffic-group 0_1
```

```
   set fortiview enable
next
   edit "L7_HTTP_Public_IP_Secondary"
   set type l7-load-balance
      set interface port1
      set ip 192.168.2.101
      set port 8003
      set load-balance-profile HTTP
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool Pool_2
      set traffic-log enable
      set traffic-group 1_0
      set fortiview enable
next
end
```

FortiADC OCI setting

FortiADC has introduced OCI Connector in 6.1.1, which you can use to retrieve the HA member's IP addresses upon failover. Create an OCI Connector on the primary node in the HA group, and specify the required information to authorize FortiADC to get the information of the HA members. Remember to enable **OCI HA status** in the OCI connector configuration so that the system will know this connector is used for OCI HA.

Refer to OCI Connector in *FortiADC Handbook* for more information on how to create an OCI Connector.

If you already have the corresponding settings before 6.1.1, they still work after the system is upgraded to 6.1.1, but the settings can't be edited anymore.

From 5.2.5 and 5.3.1, OCI region type has been added to the GUI. OCI Region and OCI Region Type do not need to be selected, as FortiADC will do it automatically.

oci-privatekey

1. Generate private key & public key

Generate the private key:

```
openssl genrsa -out ~/.oci/oci_api_key.pem 2048
```

Generate the public key:

```
openssl rsa -pubout -in ~/.oci/oci_api_key.pem -out ~/.oci/oci_api_key_public.pem
```

For more details about **generating an API key**, please refer to this page in the OCI: https://docs.cloud.oracle.com/iaas/Content/API/Concepts/apisigningkey.htm.

2. Upload public key to OCI

Navigate to Identity > Users > User Details > API Keys, click **Add Public Key**, then **upload** public key to OCI.

3. Set private key to ADC

Configure on OCI

1. Ensure that the VS IP and Secondary IP are assigned to the VNIC on OCI. Please refer to step 13 of this guide.

In this example, you should assign:

- VS IP 192.168.2.101 to.....ADC1 VNIC1
- VS IP 192.168.2.102 to.....ADC2 VNIC1
- Secondary IP 192.168.3.13 to ADC1 VNIC2
- Secondary IP 192.168.3.9 to .....ADC2 VNIC2.

2. **Create** Reserved Public IP and bind with VS IP. User can access the VS through the public IP.

In this example, you should allocate Public IP for VS1 IP 192.168.2.101 and VS2 IP 192.168.2.102.

Configure IAM role on OCI

1. In OCI, go to **Compute > Instances**, and select the desired FortiADC-VM instance.

2. On the **Instance Details** page, take note of the instance's OCID.

3. Open the OPC menu and go to **Identity > Dynamic Groups**. Create a dynamic group with rules that allow instances that match the FortiADC-VM's instance OCID. Use the syntax "ALL {instance.id ='instanceID'}" when creating the rule. If you have multiple instances to include in the dynamic group, create multiple rules for this dynamic group.

4. Go to **Identity > Policies**. Create a policy that allows the dynamic group to manage the environment. This allows the instance referenced in the dynamic group to query metadata and move resources around if the OCI connector is used for HA. In the STATEMENT field, use the syntax "Allow dynamic-group <group-name> to manage all-resources in TENANCY".

Important notes

1. In L4_VS DNAT mode or L7_VS mode enabled "client-address", you need to enable “Skip Source/Destination Check” on OCI_ADC interface, which connects to RS. You also need to ensure that ADC is the gateway for RS. Note: Floating IP is better in HA-VRRP mode.

2. Does not support HA-AP and HA-AA mode.

3. Only supports HA-VRRP group with two ADCs currently.

4. If you configure “VS IP”, “Secondary IP Address”, “Floating IP”, L4VS “NAT Source Pool”, SNAT “Translation to IP Address”, or DNAT “External Address Range” etc. You must assign these IP to the VNIC on OCI.

5. FortiADC trial license can support 2 VCPU on OCI, for the 15 days that trial license is valid. You can execute “get system status” to check the number of VCPU. Starting from 5.2.2, the ADC license does not limit the memory and hard disk size; only the number of VCPUs is limited.

6. It's suggested that you not delete the VNIC on OCI. If you have to delete VNIC for some reason, then when you create a new VNIC, please “set retrieve_physical_hwaddr enable” on the new port.

```
config system interface
   edit portXX
```

```
    set retrieve_physical_hwaddr enable
  end
```