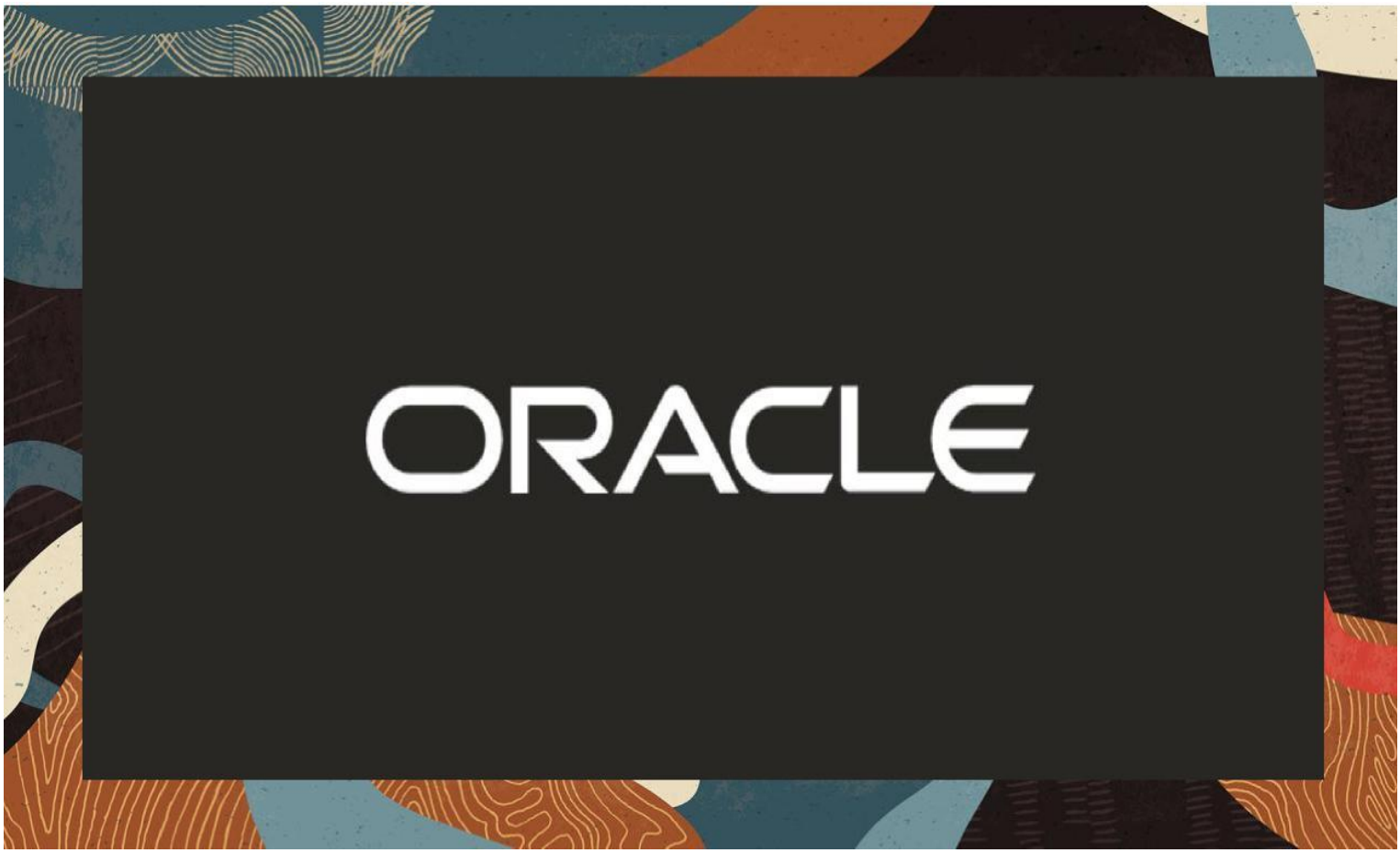

ORACLE

Deploying Oracle SBC in Amazon Web Services (AWS) Public Cloud

Technical Application Note

ORACLE
COMMUNICATIONS

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Ora

Contents

1 Intended Audience 5
2 Document Overview 5
3 Related Documentation 5
3.1 Oracle SBC 5
3.2 AWS 5
3.3 Software Used 5
3.4 Revision History 5
4 Requirements 6
5 Create and deploy on AWS 6
5.1 Prerequisites to Deploying an EC2 instance 6
5.2 Generate an EC2 AMI from the Oracle SBC Image 6
5.2.1 Installing Oracle Linux Machine 6
5.3 EC2 Deployment Procedure 17
5.3.1 Configure an IAM Role (Only Needed if deploying ORACLE SBC in HA) 17
6 Initial Access To SBC 28
6.1 Set the User and Administrative Passwords on AWS deployed ORACLE SBC 28
6.2 Interface Mapping 29
7 Appendix A 30
7.1 Deploying SBC behind the NAT 30

1 Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, and end users of the Oracle Session Border Controller. It assumes that the reader is familiar with basic operations of the Oracle Session Border Controller and Amazon Web Services (AWS) Cloud Deployments.

2 Document Overview

You can deploy the Oracle Session Border Controller on Amazon's Elastic Computing (EC2) infrastructure in either standalone or High Availability (HA) mode. AWS provides multiple ways of managing your environment(s). This document focuses on the web console. The console provides navigation via a web-page pane with links to specified functions on the left side of console pages. These procedures also assume you have reviewed AWS documentation, and can access console pages and navigation

3 Related Documentation

3.1 Oracle SBC

- Oracle® Communications Session Border Controller Platform Preparation and Installation Guide
- Oracle® Enterprise Session Border Controller Web GUI User Guide
- Oracle® Enterprise Session Border Controller ACLI Configuration Guide
- Oracle® Enterprise Session Border Controller Release Notes

3.2 AWS

- Introduction to AWS
- Getting started with AWS

3.3 Software Used

Software version
SBC 8.5

3.4 Revision History

Version	Date Revised	Description of Changes
1.0	01/13/2020	Initial publication
1.1	02/06/2020	Added lot more Screenshots, revision history table

4 Requirements

1) A subscription for AWS
2) Access to Oracle Enterprise SBC kvm image.

   The KVM release package can be downloaded through the My Oracle Support portal, under the Patches and Upgrades tab, or can be obtained by reaching out to your Oracle Account representatives.

5 Create and deploy on AWS

5.1 Prerequisites to Deploying an EC2 instance

- You have identified and are deploying to the correct AWS Region. This is typically a default component of your EC2 Account
- You have identified and are deploying to the correct AWS Availability Zone. By deploying 2 (HA) instances during deployment at the same time, you are ensuring that both instances reside in the same Availability Zone.
- An Amazon Virtual Private Cloud (VPC) is configured.
- A security policy is configured.
- You have determined the number of management and media interfaces you want for each instance.
- All subnets are configured. Each Oracle SBC management and media interface requires its own unique subnet.

Note: Your EC2 workspace may present dialogs and fields that differ from this procedure. For full information on deploying EC2 instances, see the Amazon EC2 documentation.

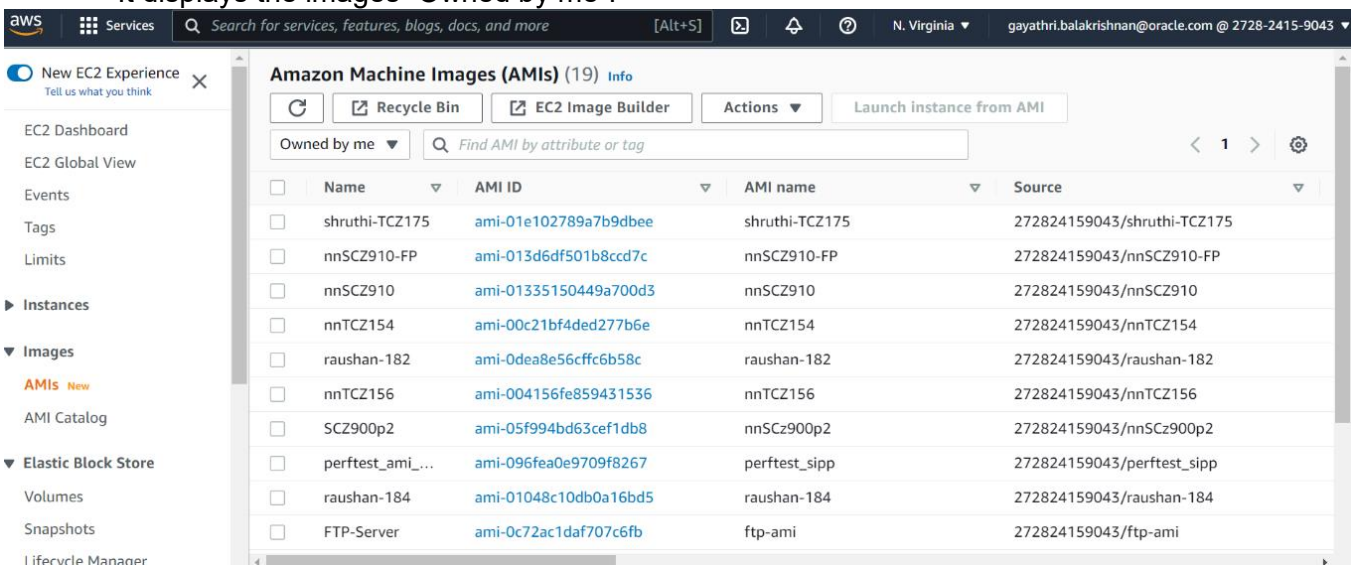
5.2 Generate an EC2 AMI from the Oracle SBC Image

You need to perform this procedure to convert the Oracle SBC image into an AMI, from which you can create Oracle SBC machines.
This procedure requires that you, from the EC2 system, create an Oracle linux machine, attach a new disk to it, and put the ORACLE SBC image on your machine. Next, use the linux command line to convert the image from qemu to raw format, then perform a data definition (dd) procedure to write the disk image. Finally, you create a snapshot of the disk and convert the snapshot to an AMI image. You can create Oracle SBCs from this AMI.

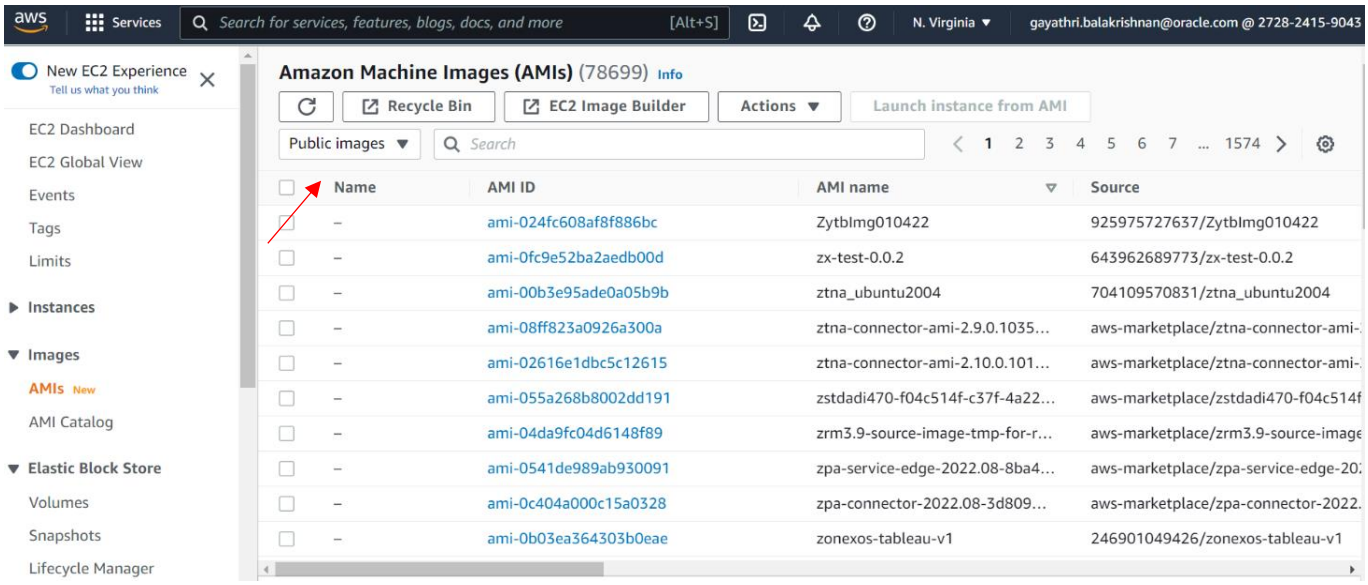
5.2.1 Installing Oracle Linux Machine

Oracle Linux AMI's are available in AWS as public images. Please find the link to download here (https://www.oracle.com/linux/)
Here we go through the steps to locate the Oracle-provided Oracle Linux AMIs in AWS and launch an Oracle Linux instance using Amazon EC2 console.

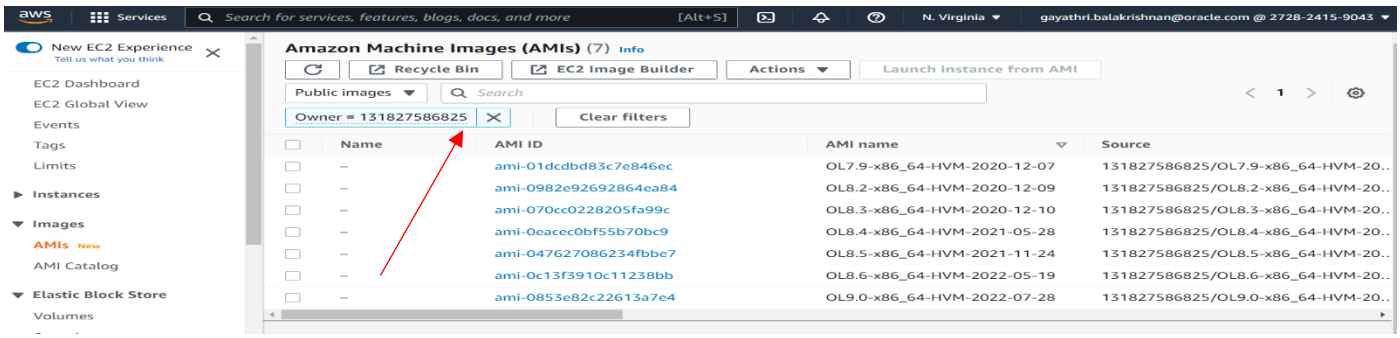
1. Login to the console. Scroll down to Images ->AMI.
It displays the images “Owned by me”.



2. Now change the option to Public Images

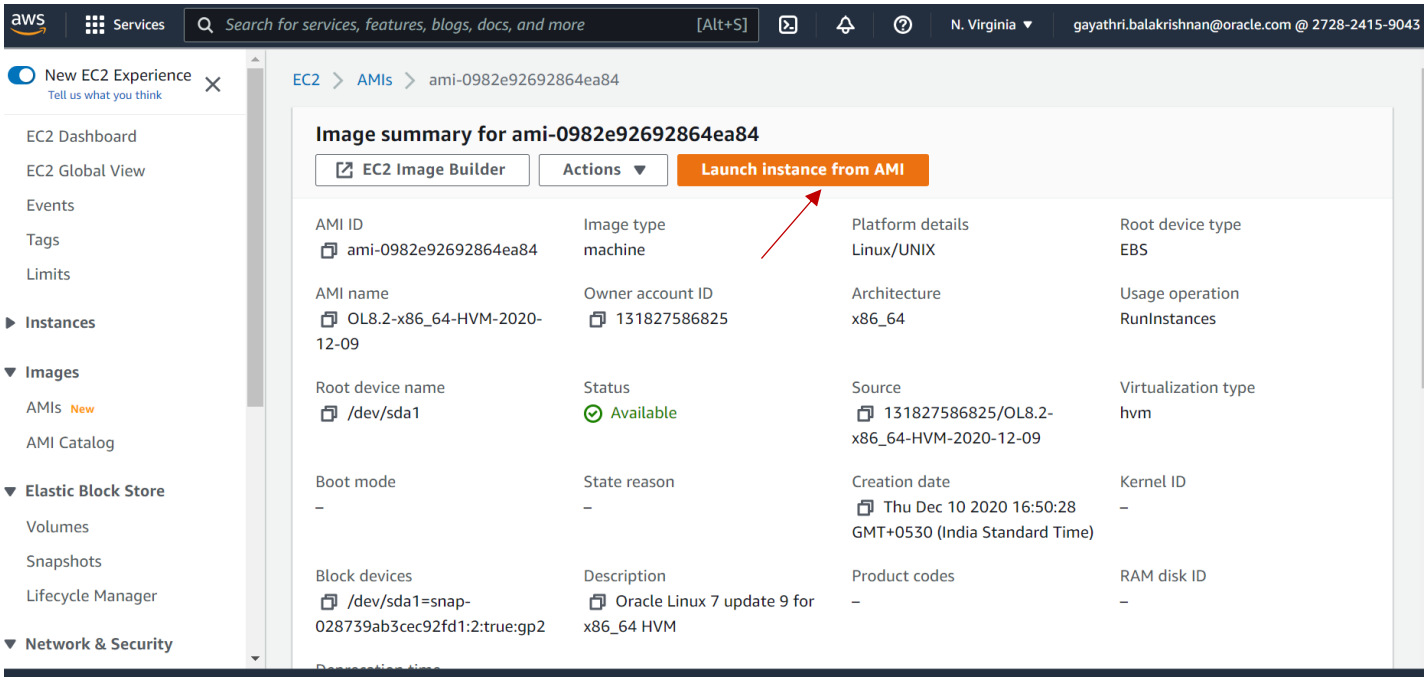


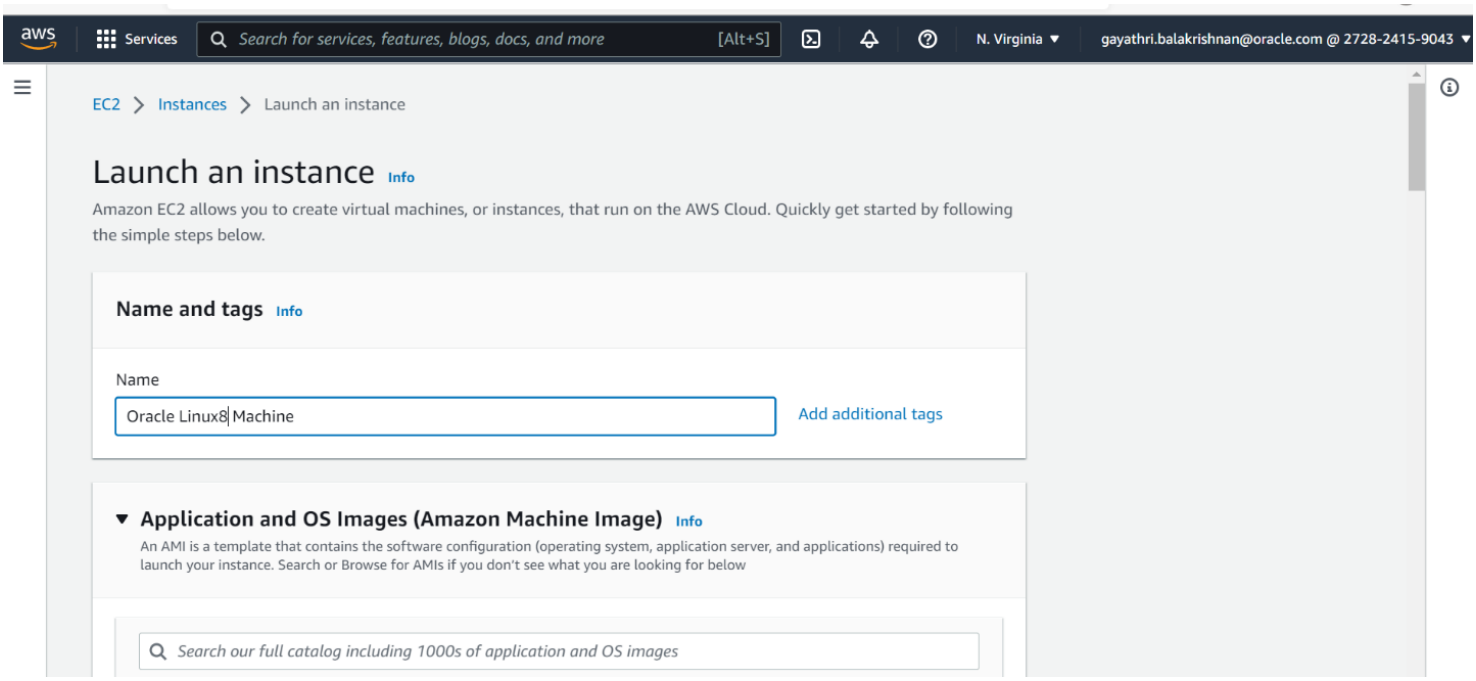
3. The Oracle provided Oracle Linux AMI’s are present if we search using the Owner Id filter where the value is owner ID =**131827586825** .



Oracle Linux AMI starting from 6.9 to the latest patches in various releases are available..We have used OL 8.2 in our setup.

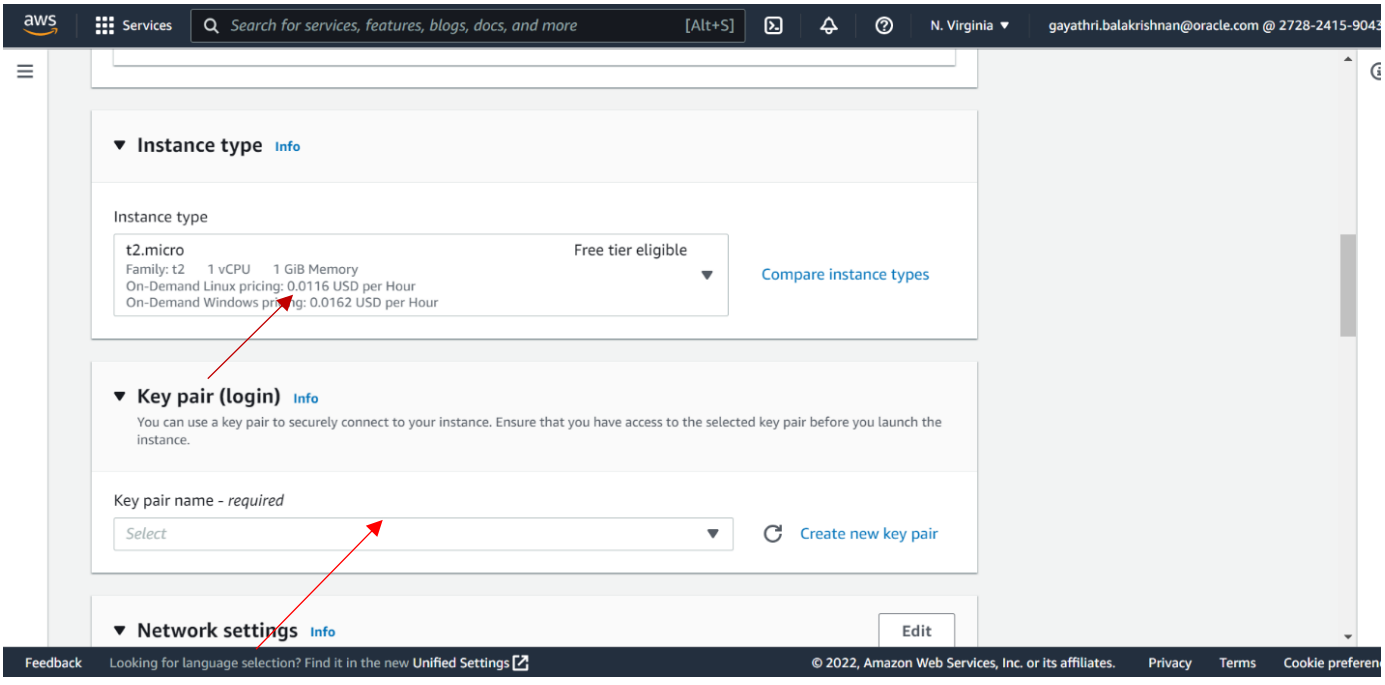
4. Click on the chosen AMI and Launch Instance from AMI as shown



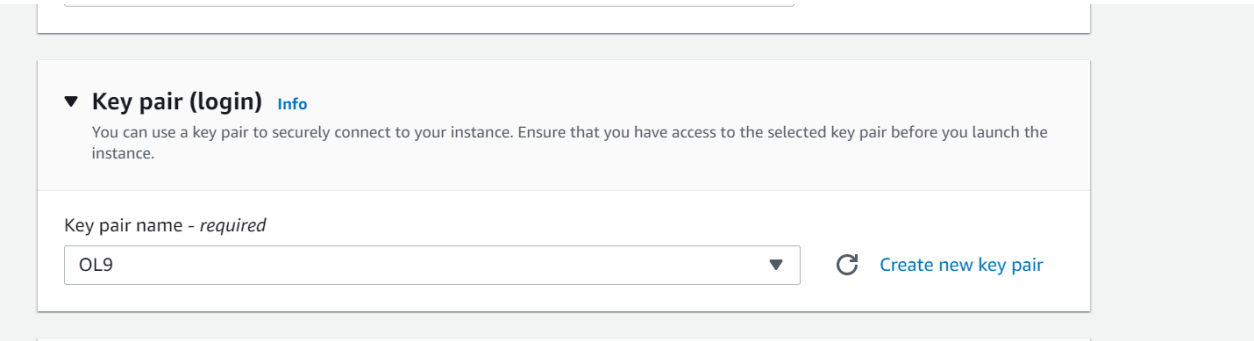


Launch the instance with type as t2.micro.

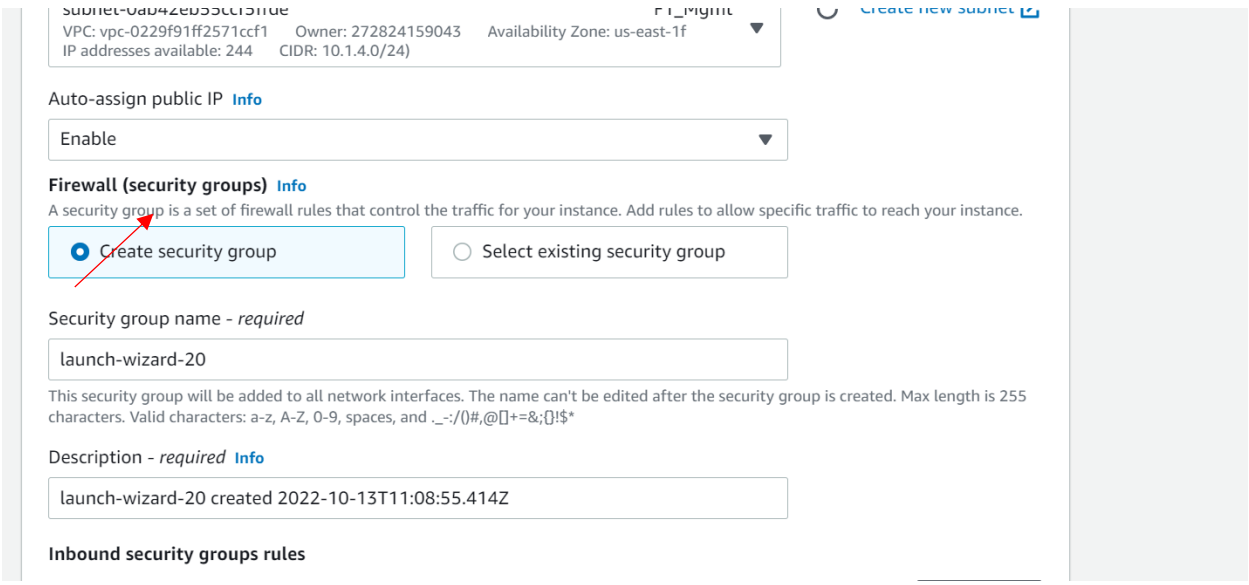
The instance requires a keypair.You can enter a key if you already have one or choose to



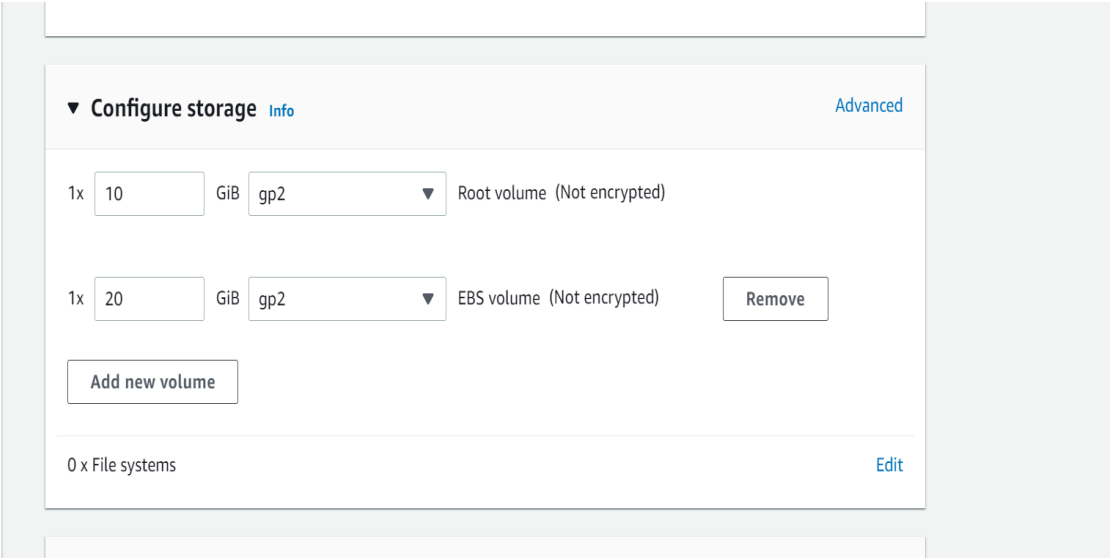
Create a new key pair



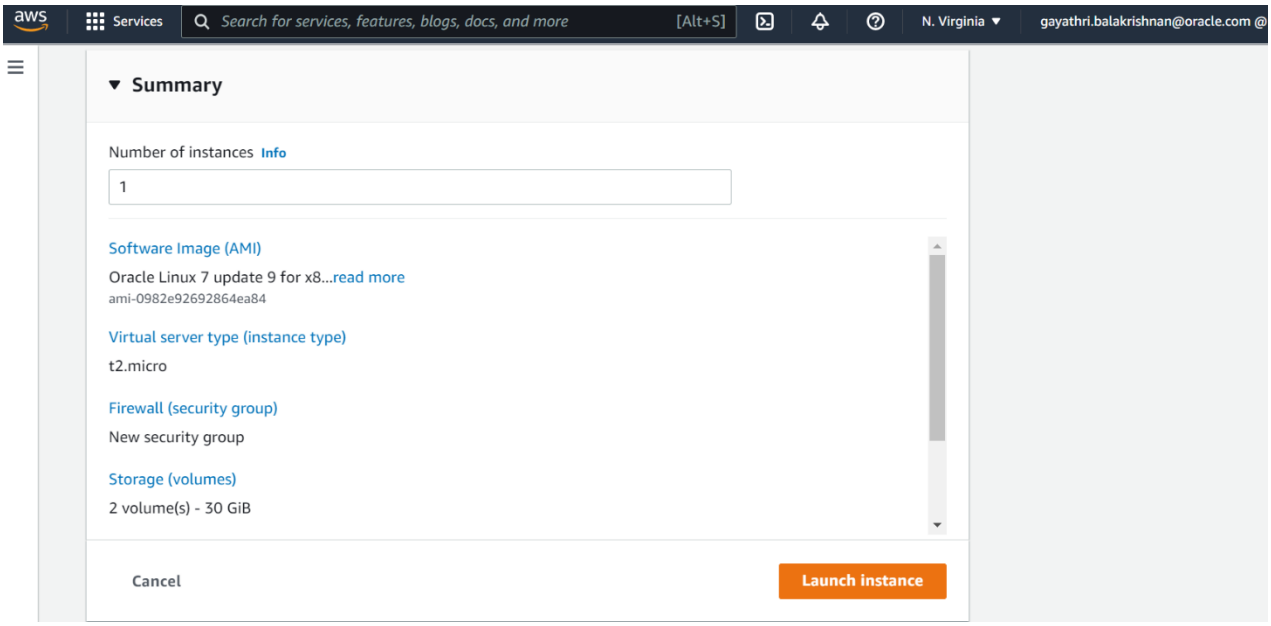
Click on the Network Settings and click Edit.Enable the Auto -assign public IP .



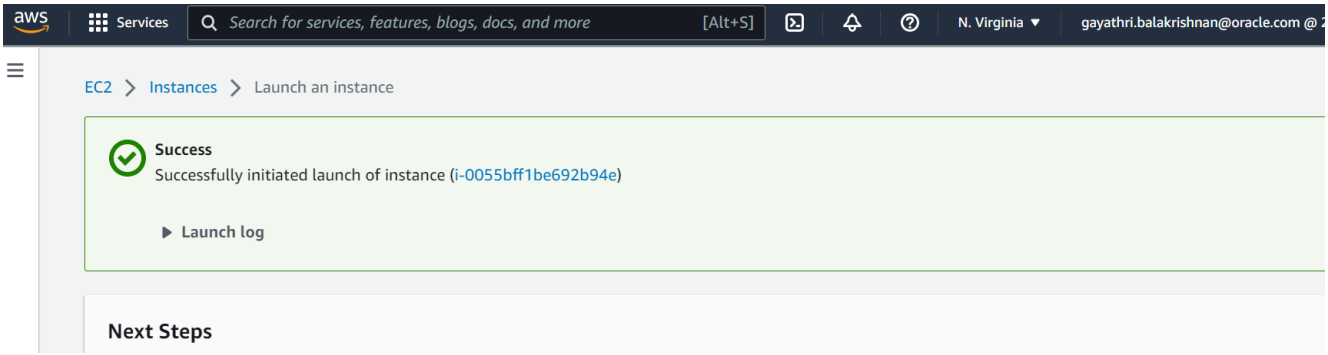
Scroll Down to Configure Storage and configure the volumes as shown below



Now review the summary and launch the instance



The instance is launched successfully as shown.



For more information on how to launch and Oracle Linux image in AWS please refer https://community.oracle.com/tech/apps-infra/discussion/4417739/launch-an-oracle-linux-instance-in-aws

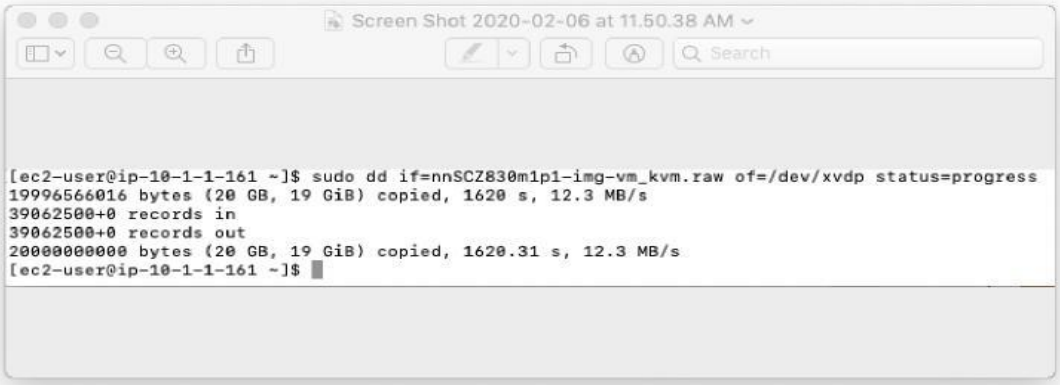
- Download your ORACLE SBC image via Oracle support. The correct image name is appended with -img-vm_kvm.tgz.
- Copy the KVM release image to the target VM using Winscp.
- ssh into the target VM. ssh -i "vSBC.pem" ec2-user@public_ip_addr
- Install the following packages on the Oracle Linux machine.
- KVM image conversion utility.-sudo yum install qemu-img
- Unzip
- Tar

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
[ec2-user@ip-10-1-4-188 ~]$ sudo su
[root@ip-10-1-4-188 ec2-user]#
[root@ip-10-1-4-188 ec2-user]#
[root@ip-10-1-4-188 ec2-user]#
[root@ip-10-1-4-188 ec2-user]#
[root@ip-10-1-4-188 ec2-user]# sudo yum install qemu-img
Last metadata expiration check: 0:18:39 ago on Tue 11 Oct 2022 03:49:25 PM GMT.
Dependencies resolved.
================================================================================
 Package              Architecture          Version                                  Repository                  Size
================================================================================
Installing:
 qemu-img             x86_64                15:6.2.0-11.module+el8.6.0+20743+999ad699.5  ol8_appstream           2.2 M
Installing dependencies:
 libaio               x86_64                0.3.112-1.el8                            ol8_baseos_latest           33 k

Transaction Summary
================================================================================
Install  2 Packages

Total download size: 2.2 M
Installed size: 8.3 M
Is this ok [y/N]: y
Downloading Packages:
(1/2): libaio-0.3.112-1.el8.x86_64.rpm                  208 kB/s |  33 kB     00:00
(2/2): qemu-img-6.2.0-11.module+el8.6.0+20743+999ad699.5.x86_64.rpm  9.2 MB/s | 2.2 MB     00:00
--------------------------------------------------------------------------------
Total                                                   9.2 MB/s | 2.2 MB     00:00
Oracle Linux 8 BaseOS Latest (x86_64)                   3.0 MB/s | 3.1 kB     00:00
Importing GPG key 0xAD986DA3:
 Userid     : "Oracle OSS group (Open Source Software group) <build@oss.oracle.com>"
 Fingerprint: 76FD 3DB1 3AB6 7410 B89D B10E 8256 2EA9 AD98 6DA3
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
Is this ok [y/N]: y
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
```

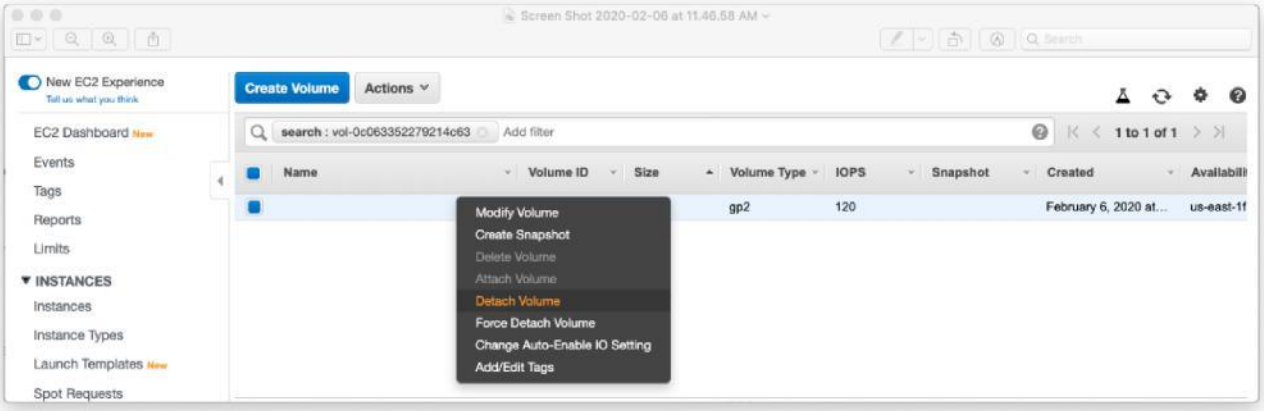
```
[root@ip-10-1-4-188 ec2-user]# sudo yum install unzip
Last metadata expiration check: 0:19:02 ago on Tue 11 Oct 2022 03:49:25 PM GMT.
Dependencies resolved.
================================================================================
 Package              Architecture          Version                  Repos
================================================================================
Installing:
 unzip                x86_64                6.0-46.0.1.el8           ol8_b

Transaction Summary
================================================================================
Install  1 Package

Total download size: 196 k
Installed size: 414 k
Is this ok [y/N]: y
Downloading Packages:
unzip-6.0-46.0.1.el8.x86_64.rpm
--------------------------------------------------------------------------------
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
  Installing       : unzip-6.0-46.0.1.el8.x86_64
  Running scriptlet: unzip-6.0-46.0.1.el8.x86_64
  Verifying        : unzip-6.0-46.0.1.el8.x86_64

Installed:
  unzip-6.0-46.0.1.el8.x86_64

Complete!
```

```
tar-1.30-5.el8.x86_64.rpm                                                
```

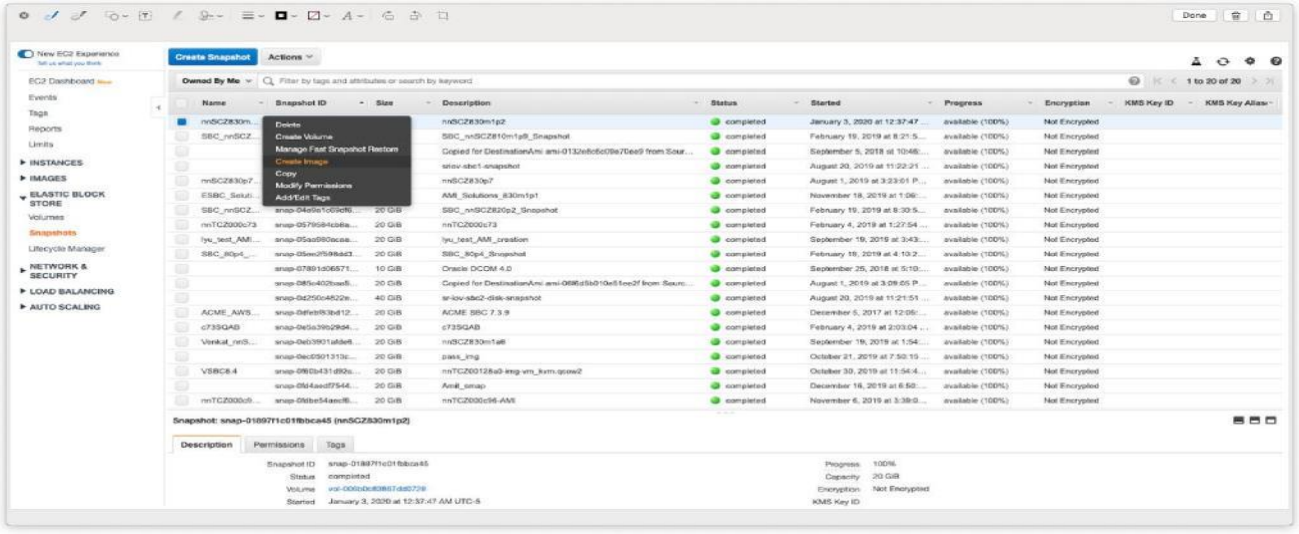
You may or may not be able to use the status=progress flag within this command. This is
dependent on the version of the dd command. In addition, note that using the status=progress flag causes the process to take longer.



- From the EC2/Elastic Block Store/Volumes tab, right-click the 20GB volume and click Detach Volume from the VM.

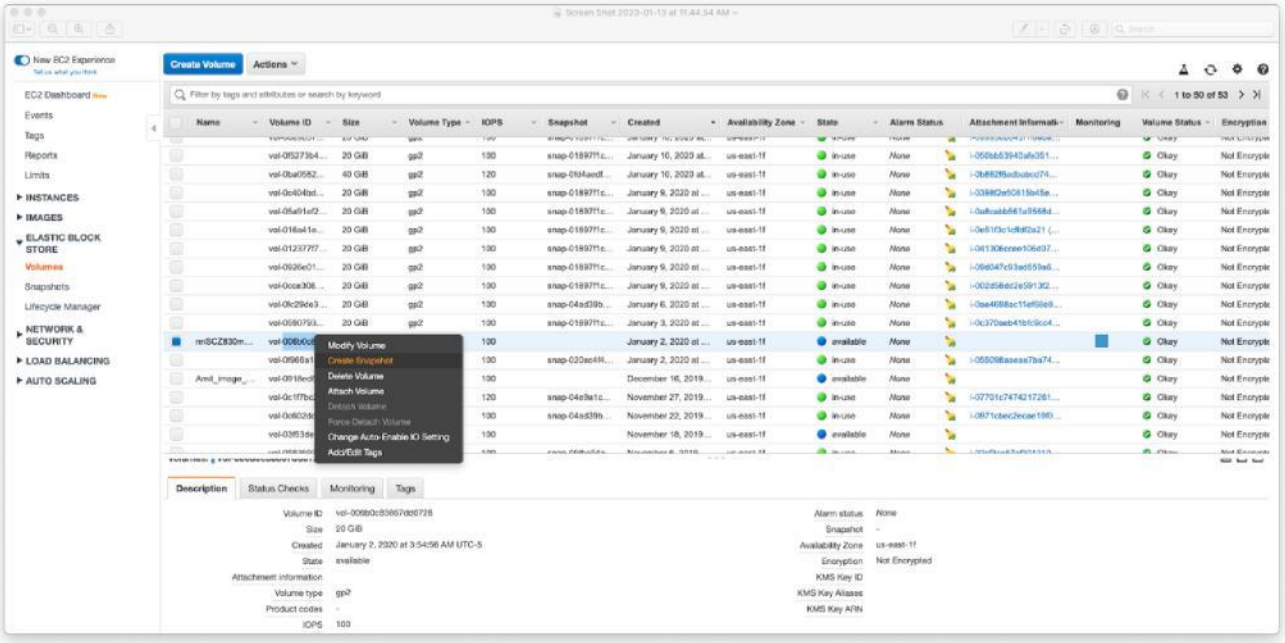


From the same tab, right click the 20GB volume again, click Create Snapshot and wait for the snapshot to complete.

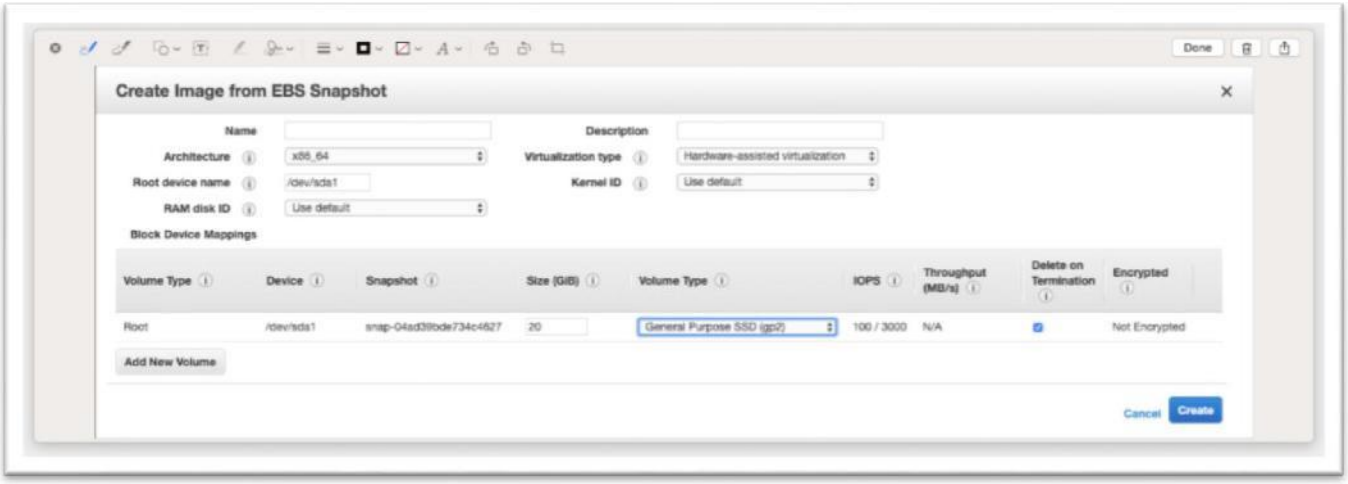


C2/Elastic Block Store/Snapshots tab, right-click the snapshot, and click Create Image to generate an AMI.

The “Create Image” from EBS Snapshot Dialog provides for multiple configurations, Use below parameters



- Name your Image
- Select “x86_64” from the Architecture drop-down.
- Select “Use default” from the RAM disk ID drop-down.
- Select “Hardware-assisted virtualization” from the Virtualization type drop-down.
- Select “Use default” from the Kernel ID drop-down.
- Select “General Purpose SSD” (gp2) from the Volume Type drop-down.

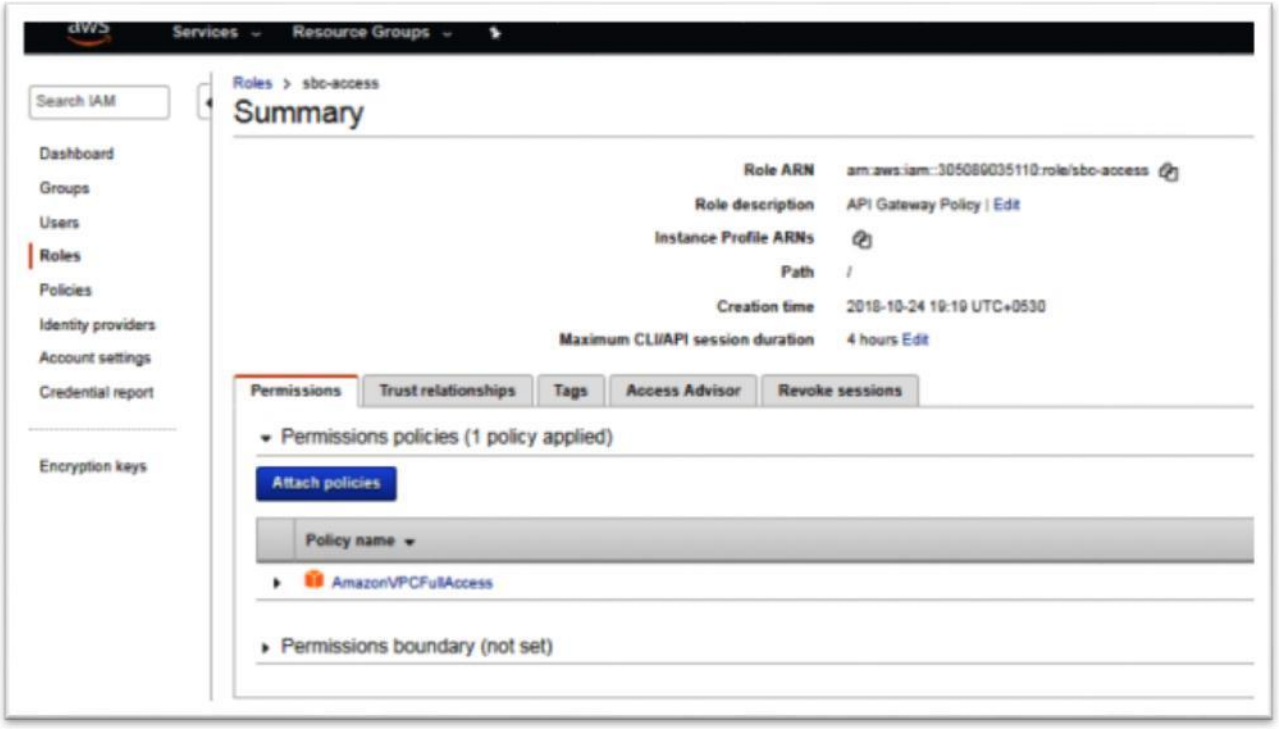


Note: You can use this created AMI to launch any number of new VM instances.

5.3 EC2 Deployment Procedure

5.3.1 Configure an IAM Role (Only Needed if deploying ORACLE SBC in HA)

Create an IAM role to use by HA ORACLE SBC instances deployed for High Availability. Attach the

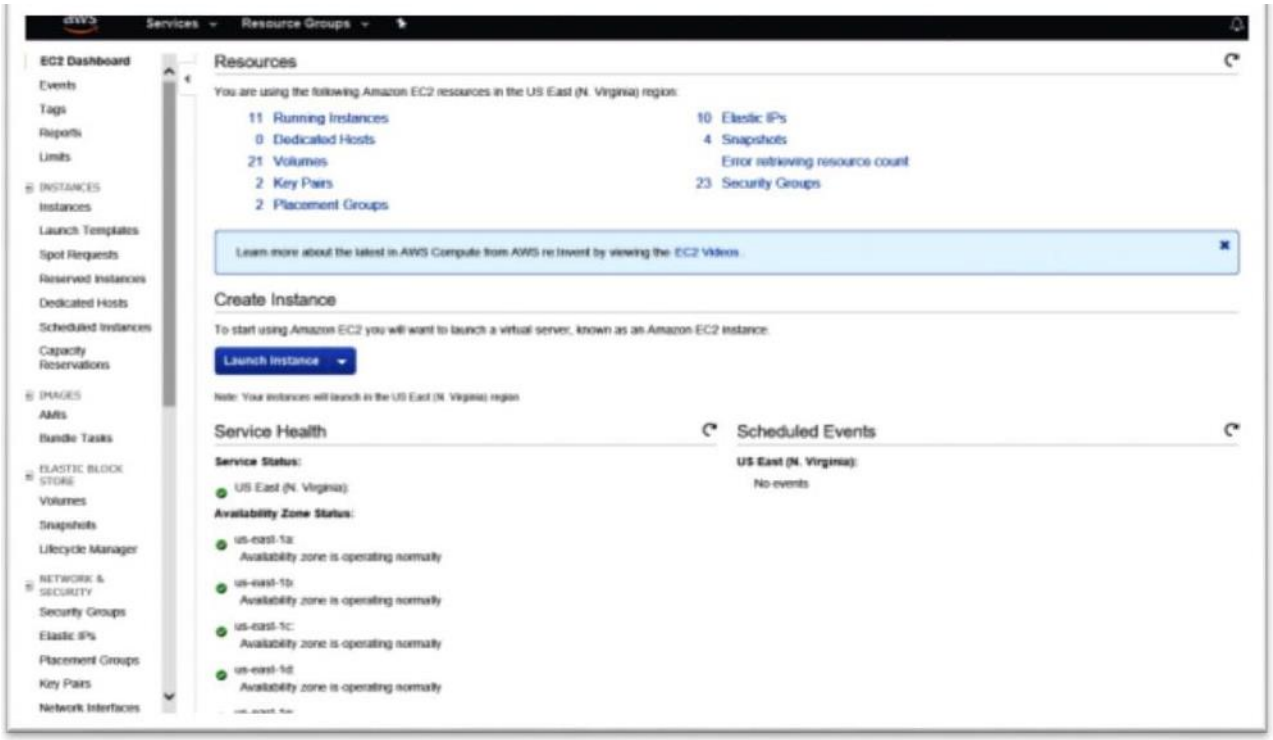


policy “AmazonVPCFullAccess” to this IAM role.

5.3.2 Launch your EC2 Instance

This is the main instance configuration procedure. It includes a multi-dialog wizard that presents configuration options in the preferred sequence. The result of this is an installed, operational standalone ORACLE SBC or HA ORACLE SBC instances with no networking.

- Login to the AWS management console and click the EC2 link to open the EC2 Dashboard.
- Review and confirm your deployment's Region and Availability Zone.
- On the EC2 Dashboard, click Launch Instance.

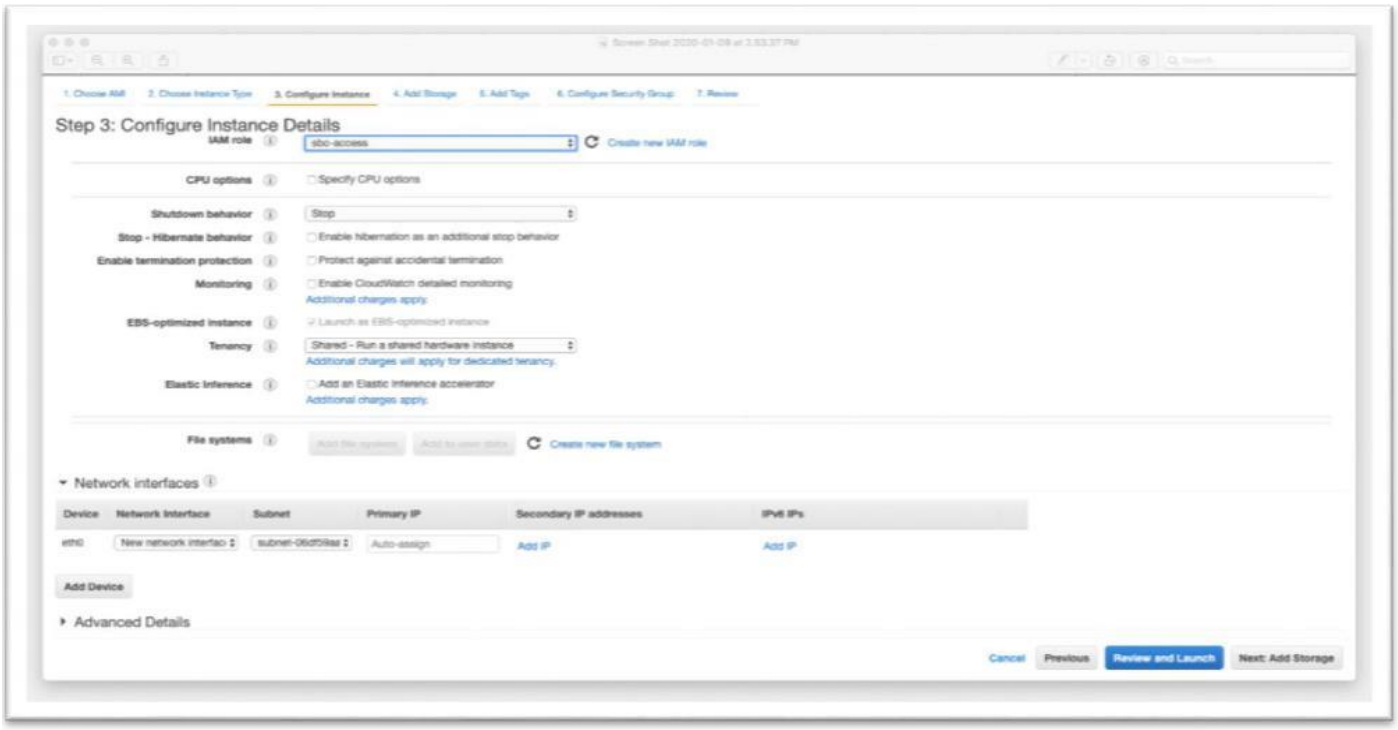


- Navigate to the “My AMIs” link to choose the image for your instance and click Select.
- Chose the desired instance type. The c4.2xlarge is an example instance type that includes 8 vCPU. Validated instance types include:

Instance Type	vCPU
c4.xlarge	4
c4.2xlarge	8
c4.4xlarge	16
c4.8xlarge	36
m4. xlarge	4
m4.2xlarge	8
m4.4xlarge	16

- Click “Next: Configure Instance Details”. The AWS instance deployment sequence displays the Configure Instance Details dialog.
- Configure the following instance details; leave the others at their defaults:

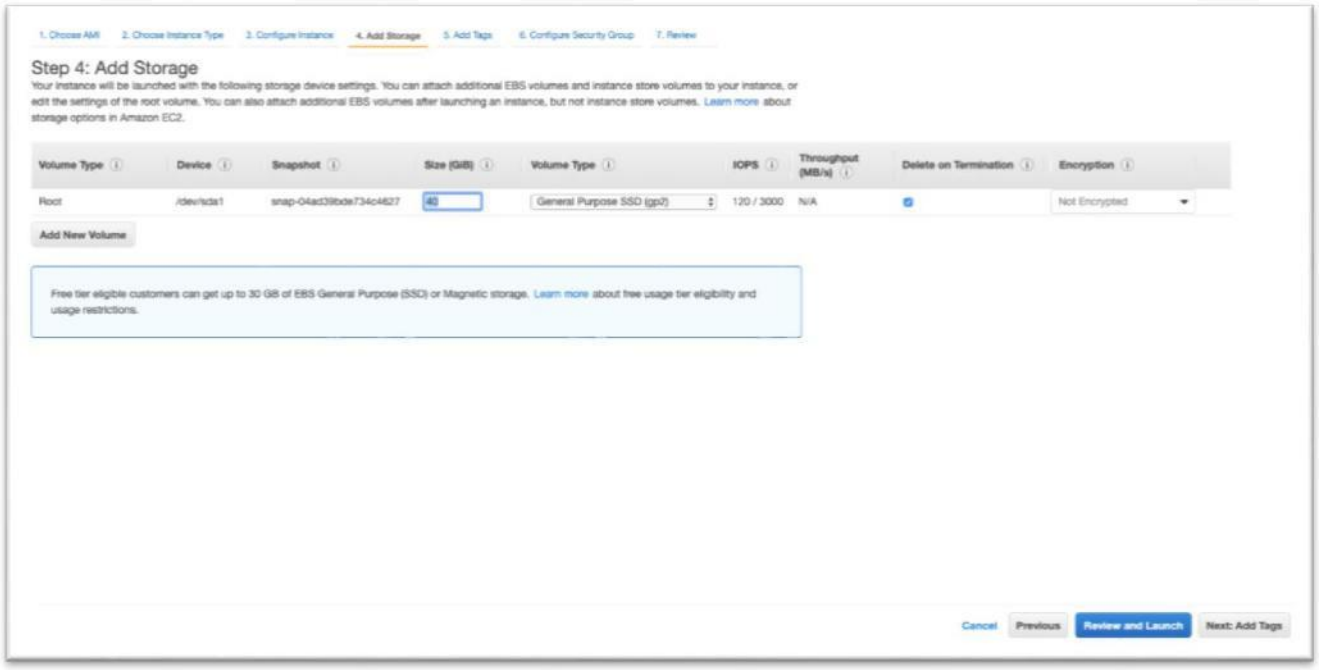
a. Specify the number of Instances. (Specify 1 for standalone and Specify 2 for an HA setup)
b. Select the correct Network for wancom0
c. Select the correct Subnet for wancom0
d. Establish a public IP for wancom0, either by using the Auto assign Public IP control or by configuring an elastic IP after deployment
e. HA specific: Select the appropriate IAM role. (Choose the IAM role you configured above.)
f. Scroll down to the “Network interfaces” configuration fields.
g. Ensure you are configuring the Device named eth0.
h. Select “New network interface” from the Network Interfaces dropdown list for wancom0 (eth0).



i. Select the correct Subnet from the dropdown list for wancom0 (eth0).
j. Ensure the “Primary IP” field is set to “Auto-assign”.
k. Click the “Add Device” button to add wancom0 (eth0) to your instance.

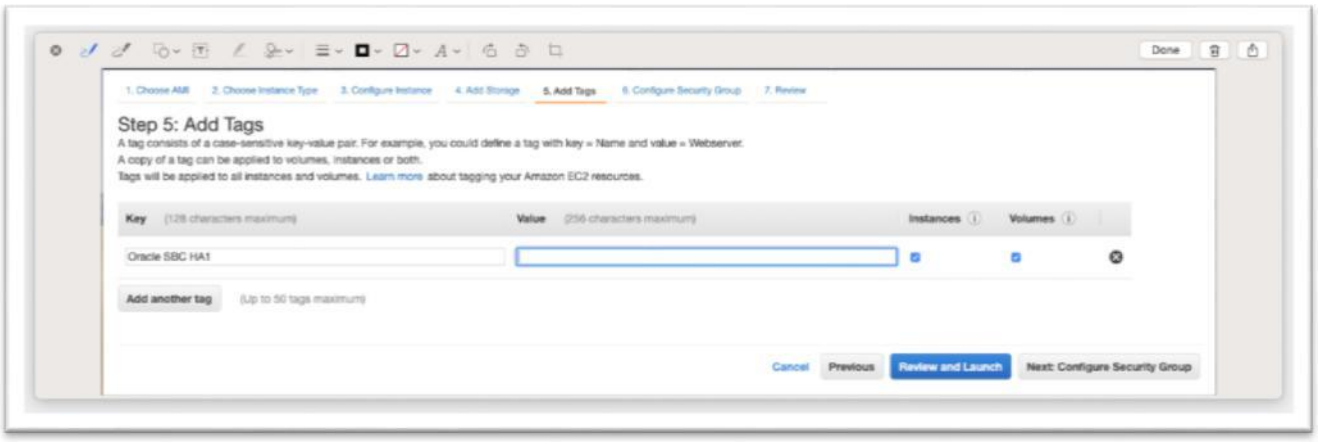
- Scroll to the bottom of the Configure Instance Details dialog and click “Next: Add Storage”.

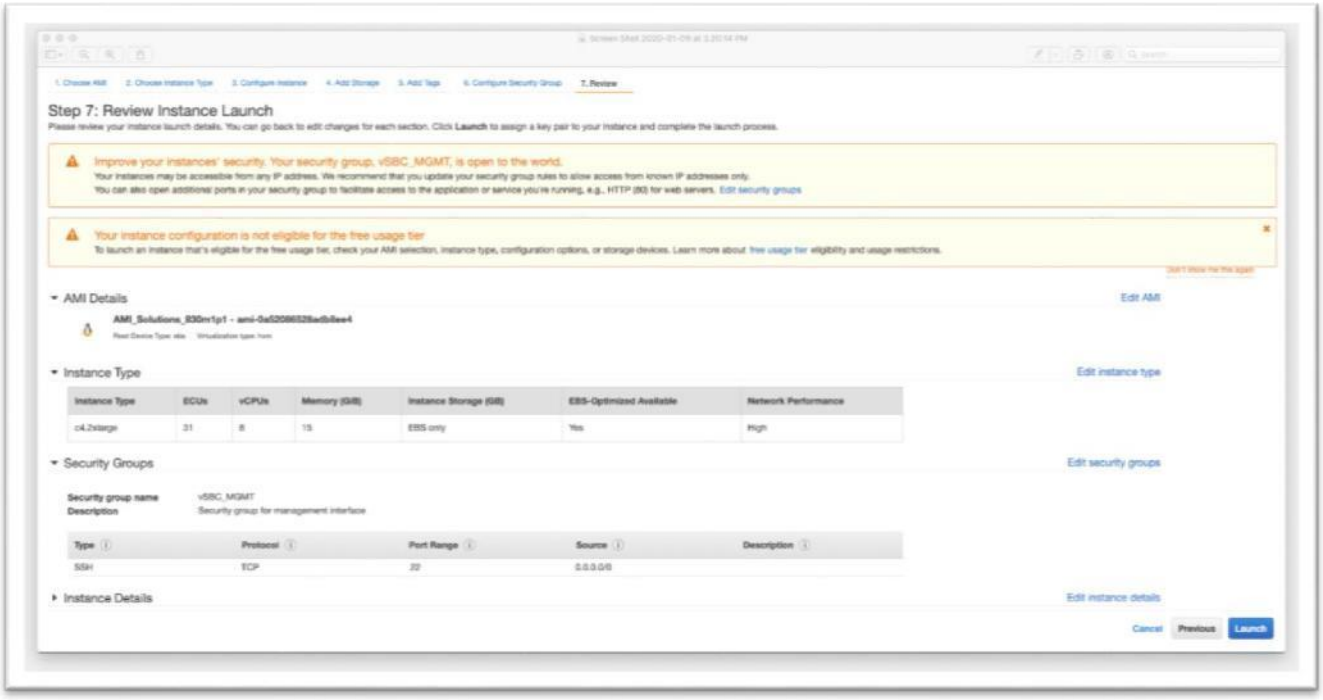
- Choose your desired ORACLE SBC storage size in GiB. The default storage size is 40 GiB.



- Click “Next: Add Tags”.
- Enter any desired name to identify the instance. Ensure the name allows you to uniquely identify this instance during later deployment procedures and operation.

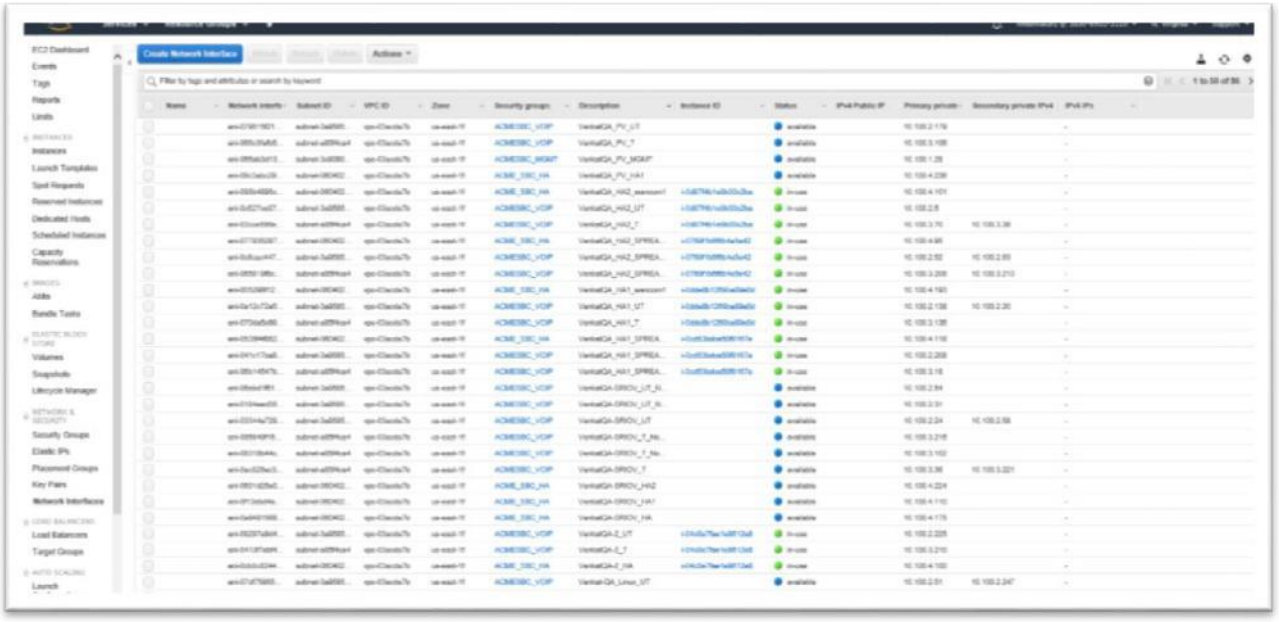
- Click “Next: Configure Security Group”.
- You can either create a new security group or select an existing security group to set appropriate firewall rules. Refer to EC2 security group documentation for configuration instructions.
- Click the Review and Launch button. EC2 displays a summary of your instance.





- Click Launch. EC2 creates your instances.
- Return to the EC2 Dashboard and click the Running instances link.

5.3.3 Create Network Interfaces for ORACLE SBC Instances



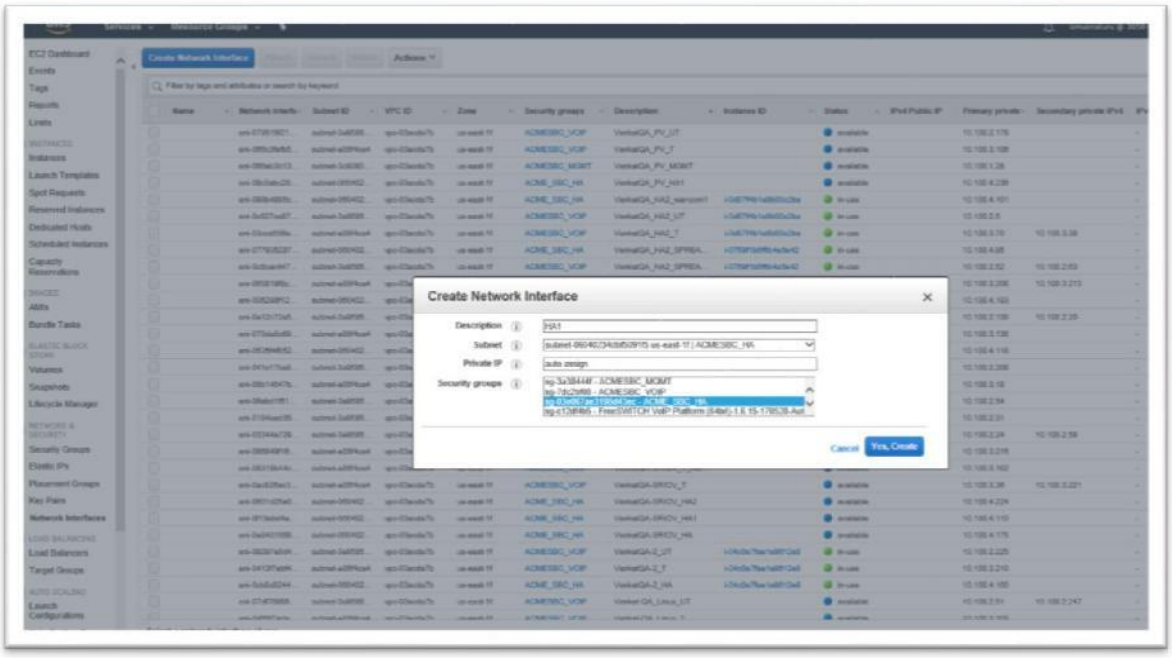
- From the EC2 Dashboard, click Network Interfaces under Network & Security on the left panel.

- Click Create Network Interfaces button.
- Create HA and/or Media interfaces by selecting the appropriate subnet and security group popup.

Example configurations on an instance named HA1 include: a.

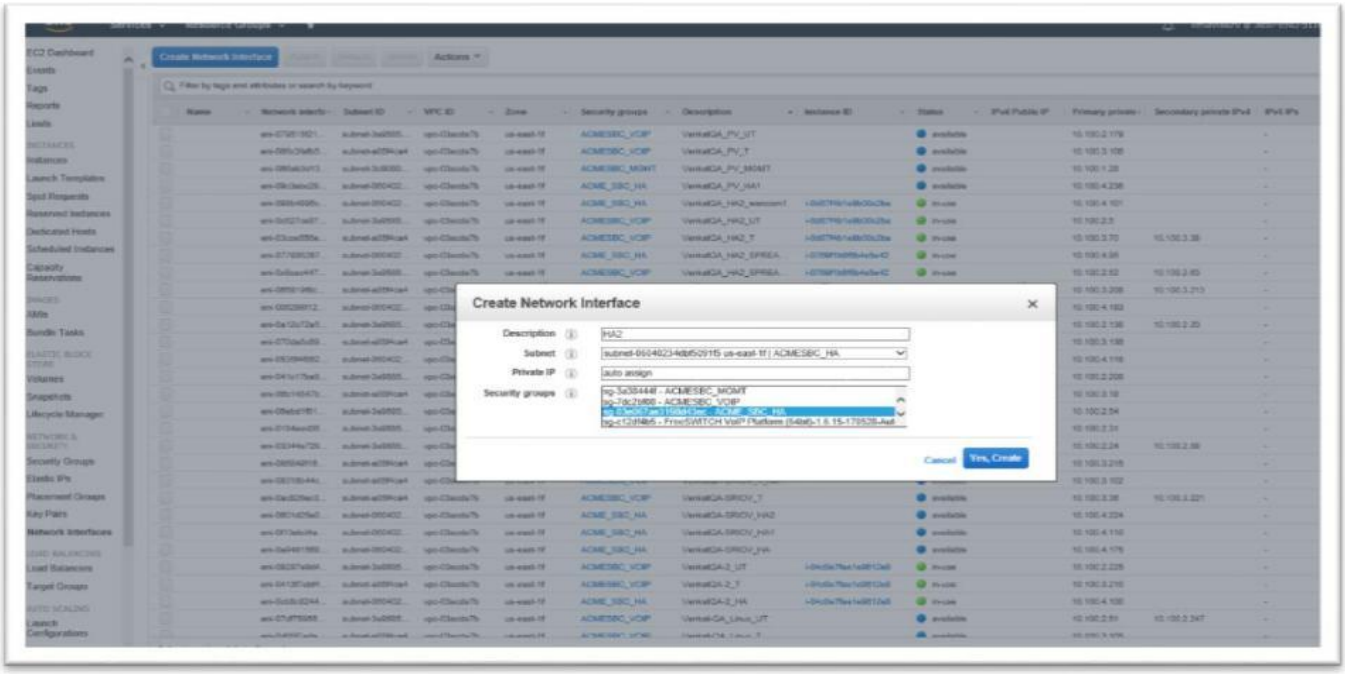
Wancom1 interface for instance-1 HA1 (Only if you have HA pair)

- For Description, type in name that you can clearly recognize later.
- For Subnet, choose the subnet you created for HA management from the drop-down.
- For Private IP, retain the auto assign setting, based on the following criteria. If you use auto assign, EC2 applies the first available IP from the subnet to that interface. If you need more precise IP management, the custom option is recommended.
- For Security groups, choose the Security group you created for this management from the drop-down.



b. Wancom1 interface for instance-2 HA2 (Only if you have HA pair): repeat above steps

l. s0p0 media interface for instance-1 (HA1)



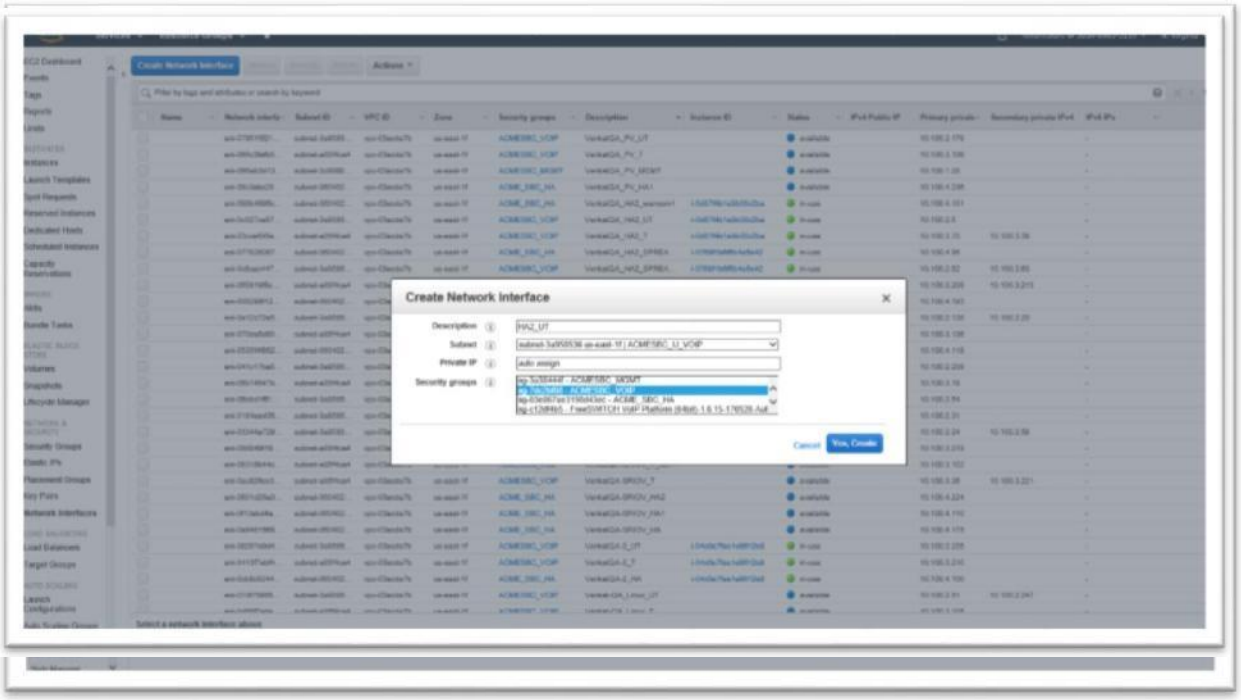
– For Description, type in name that you can clearly recognize later.

– For Subnet, choose the subnet you created for HA management from the drop-down.

– For Private IP, retain the auto assign setting, based on the following criteria. If you use auto assign, EC2 applies the first available IP from the subnet to that interface. If you need more precise IP management, the custom option is recommended.

– For Security groups, choose the Security group you created for the media from the drop-down.

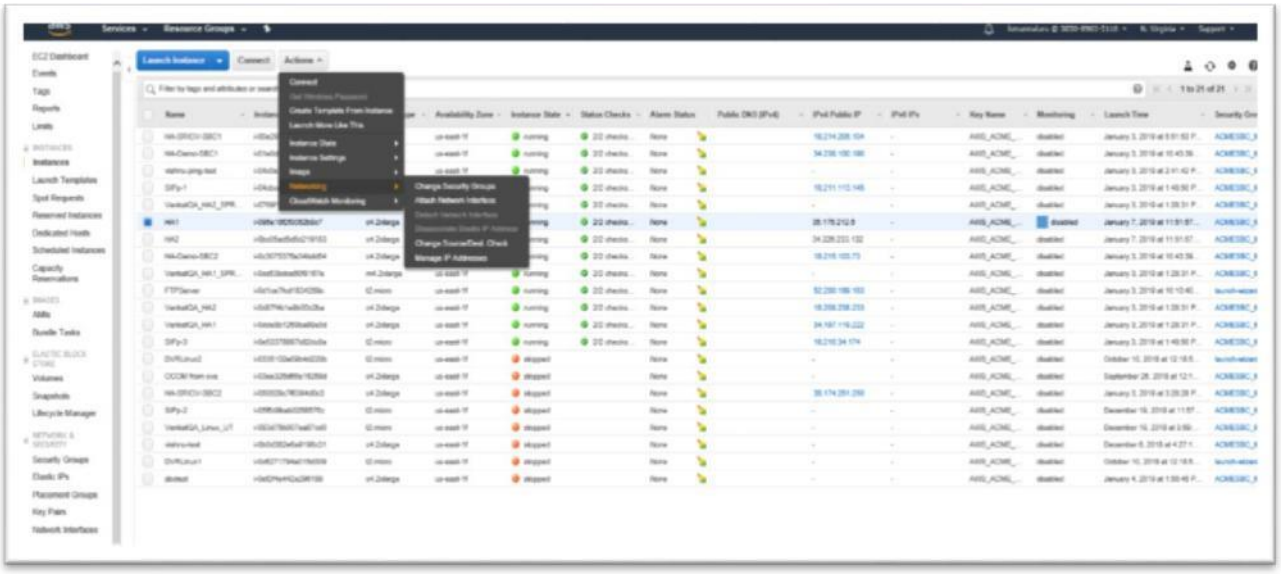
d. s0p0 media interface for instance-2 (HA2): Only if you have HA repeat above steps for second instance



Perform these steps for each management and media interfaces on your instance.

5.3.4 Attach Network Interfaces for ORACLE SBC Instances

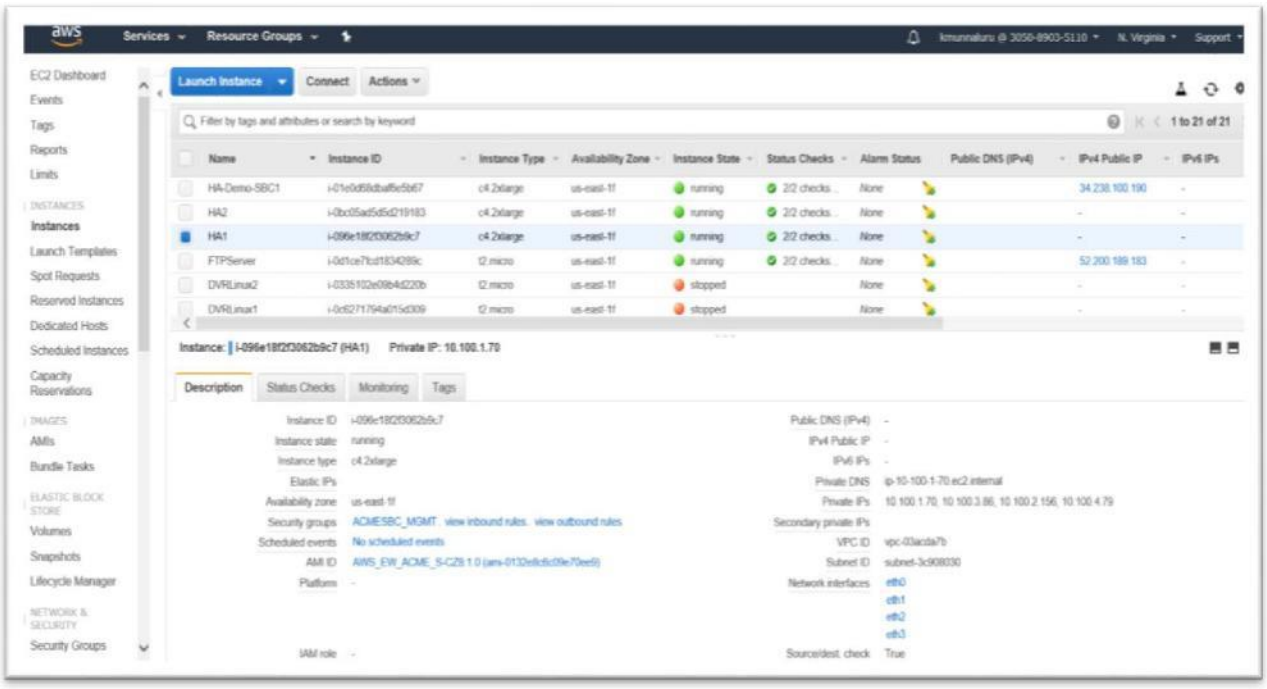
- Go to EC2 Dashboard, click Running Instances.
- Select your first instance. Ensure that it is highlighted.
- Open the Actions drop down and select Networking, Attach Network Interface.
- From the Attach Network Interface pop-up, select your first network interface name.
- Repeat these steps for all the created network interfaces.
- Repeat these steps for all your instances.

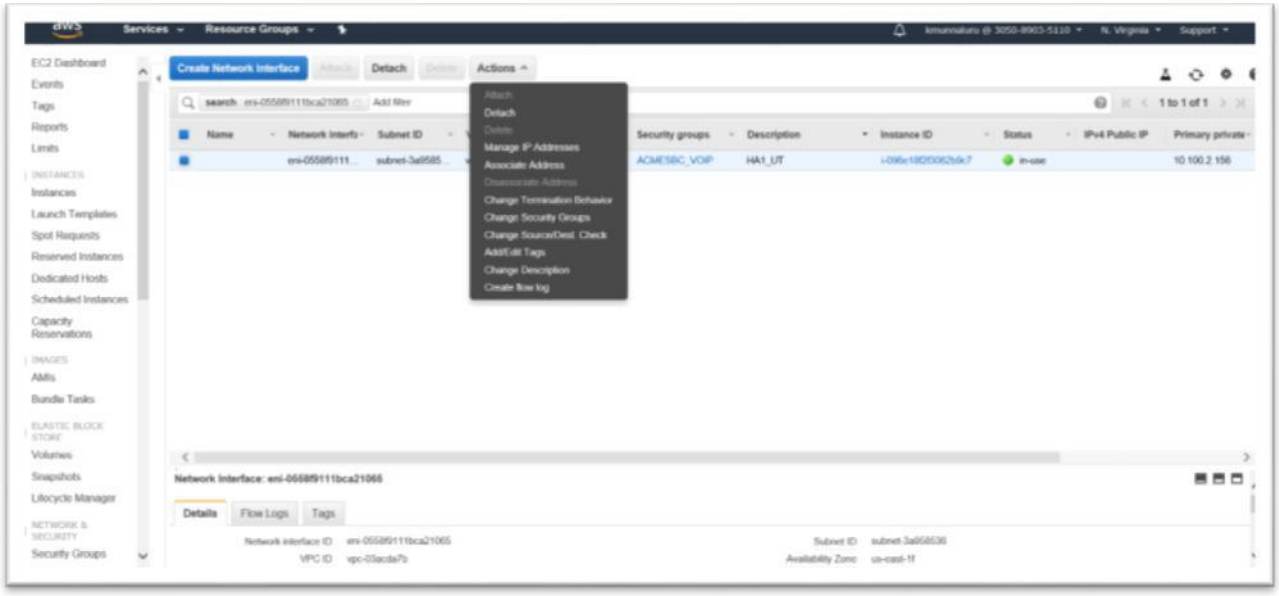


5.3.5 Configure secondary private IPs (Virtual IPs) for all media interfaces

This procedure, which creates virtual addressing, applies only to HA deployments. Perform these steps only on the Primary instance of the HA pair.

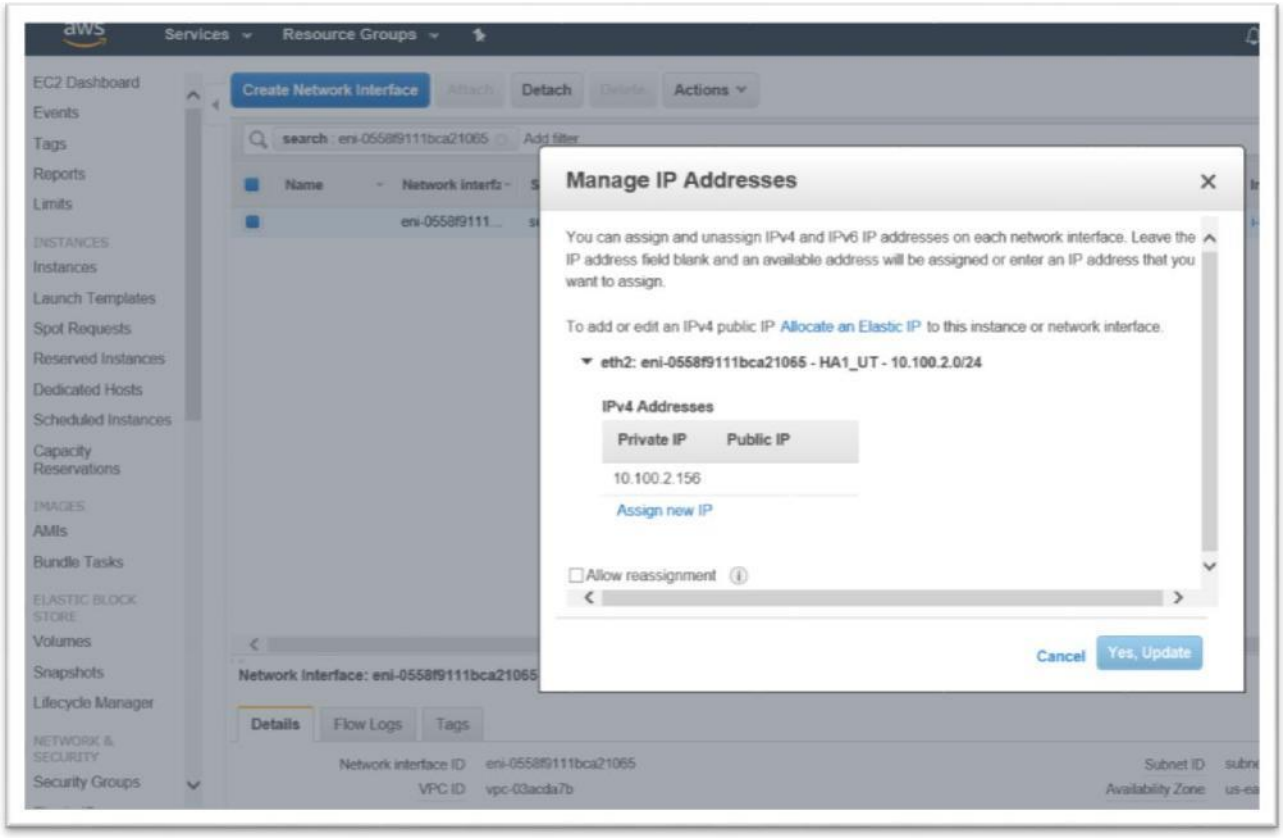
a. Go to EC2 Dashboard, click Running Instances.
b. Select the newly created instance (eg: HA1).
c. From the bottom panel, select Description -> Network Interfaces
d. Click one of the media interfaces i.e eth2/eth3 which then shows up network interface details in a pop-up.
e. Click “Interface ID” from the pop-up window. This takes you to the network interface that is mapped to this media interface.
f. Go to “Actions” tab and then click on “Manage IP Addresses” option, which will open “Manage IP Addresses” pop-up
g. Click on “Assign new IP” option, which assigns new secondary private IP address to the network-interface selected
h. Click on “Yes, Update” button.





Repeat the above steps for all the other media interfaces of HA1

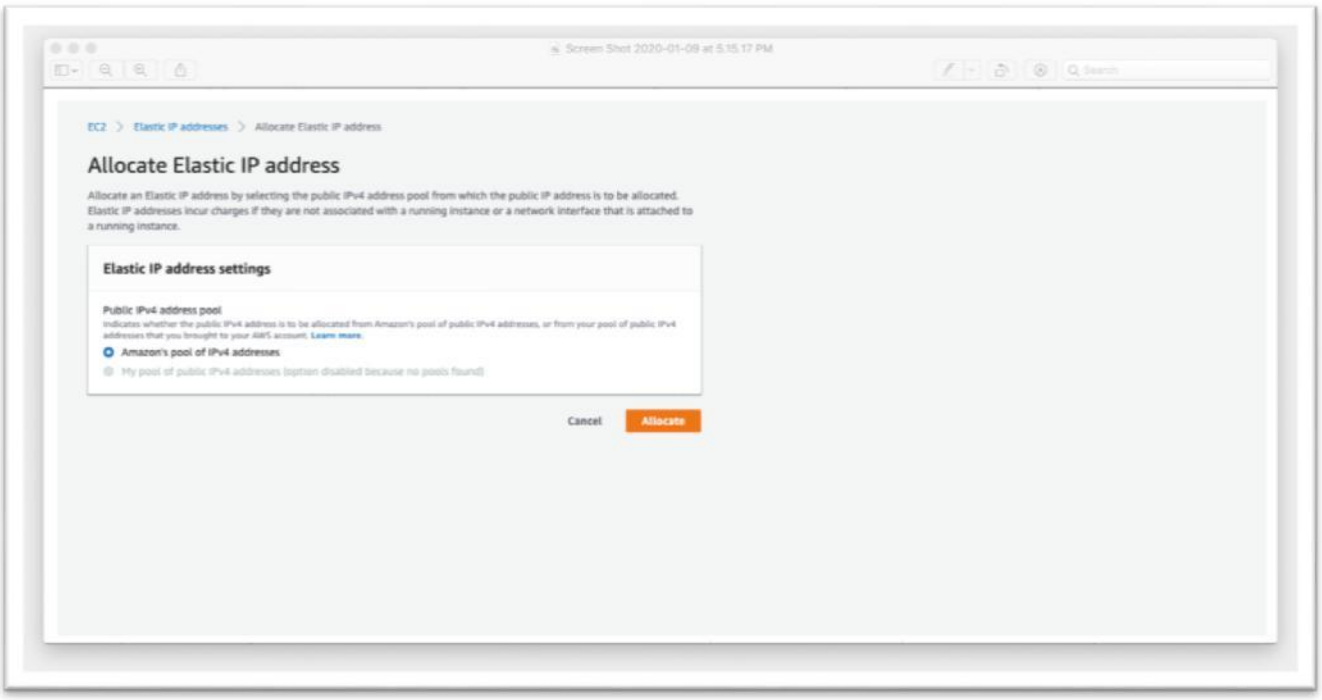
instance.



5.3.6 Configure Elastic IP Addressing

This procedure,makes virtual addresses persistent through HA switchovers and needs to be followed when deploying ORACLE SBC instance in HA pair.
This procedure can also be followed in the case where you need public ip addresses for your media interfaces.

a) Under Network and Security in the left column, click Elastic IPs.
b) Click Allocate New Address -> Yes, Allocate -> Close.
c) Select the newly allocated IP address and click Actions -> Associate Address.
d) Click on the test box next to instance and select your instance from the drop-down menu.
e) Click “Associate”.


Screen Shot 2020-01-09 at 5.15.17 PM
EC2 > Elastic IP addresses > Allocate Elastic IP address
Allocate Elastic IP address
Allocate an Elastic IP address by selecting the public IPv4 address pool from which the public IP address is to be allocated. Elastic IP addresses incur charges if they are not associated with a running instance or a network interface that is attached to a running instance.
Elastic IP address settings
Public IPv4 address pool
Indicates whether the public IPv4 address is to be allocated from Amazon's pool of public IPv4 addresses, or from your pool of public IPv4 addresses that you brought to your AWS account. Learn more.
Amazon's pool of IPv4 addresses
My pool of public IPv4 addresses (option disabled because no pools found)
Cancel
Allocate

6 Initial Access To SBC

6.1 Set the User and Administrative Passwords on AWS deployed ORACLE SBC

Once the Oracle SBC is deployed on AWS perform the password procedures which are required before any further ORACLE SBC operations. For HA deployments, perform these procedures on both ORACLE SBCs.

b) Under Instances in the left column, click Instances and click the newly created ORACLE SBC.
c) Under the Description tab, note the Public DNS address.
d) When the EC2 instance has finished initializing, SSH to the public DNS address.
The username is “user” and the initial SSH password is “acme”.
e) Set the user password by logging in for the first time.

```
$ ssh user@somewhere.compute-1.amazonaws.com
user@somewhere.compute-1.amazonaws.com's password:
*ALERT*

**********************************************************************
user password has not been set. Please set password now.
**********************************************************************
** Only alphabetic (upper or lower case), numeric and punctuation
** characters are allowed in the password.
** Password must be 8 - 64 characters,
** and have 3 of the 4 following character classes :
** - lower case alpha
** - upper case alpha
** - numerals
** - punctuation
**********************************************************************
Enter New Password:
Confirm New Password:

>
```

f) Set the administrative password by typing enable at the command prompt. (the initial enable password is “packet”.)

```
> enable
Password:
*ALERT*
**********************************************************************
admin password has not been set. Please set password now.
**********************************************************************
** Only alphabetic (upper or lower case), numeric and punctuation
** characters are allowed in the password.

** Password must be 8 - 64 characters,
** and have 3 of the 4 following character classes :
```

```
** - lower case alpha
** - upper case alpha
** - numerals
** - punctuation
*****************************************************************
Enter New Password:
Confirm New Password:
```

f. Reboot the virtual machine.

```
# reboot
```

6.2 Interface Mapping

After a reboot, SSH to the EC2 instance, verify the network interfaces have expected MAC addresses.

– `$ ssh user@somewhere.compute-1.amazonaws.com`

– Switch to the administrative user.

```
> enable
```

– Use the “show interfaces mapping” command to verify the network interfaces have expected MAC addresses.

```
# show interfaces mapping
Interface Mapping Info

Eth-IF MAC-Addr                Label
wancom0 06:DF:71:BA:D8:77      #generic
wancom1 06:A6:08:58:92:C9      #generic
s0p0    06:D4:E6:E8:B8:FB      #generic
s1p0    06:EA:08:51:4D:DF      #generic
wancom2 FF:FF:FF:FF:FF:FF      #dummy
spare FF:FF:FF:FF:FF:FF        #dummy
s0p1    FF:FF:FF:FF:FF:FF      #dummy
s1p1    FF:FF:FF:FF:FF:FF      #dummy
s0p2    FF:FF:FF:FF:FF:FF      #dummy
s1p2    FF:FF:FF:FF:FF:FF      #dummy
s0p3    FF:FF:FF:FF:FF:FF      #dummy
s1p3    FF:FF:FF:FF:FF:FF      #dummy
```

– Execute the “interfaces-mapping swap” command, if necessary, in order to correct any issues with your interface to MAC address mapping. See below for example command

```
# interface-mapping swap s0p0 wancom1
```

Refer to Oracle Communications Sessions Border Controller Configuration Guide after you have completed this deployment for administrative and service configuration, including product setup, entitlement setup and HA configuration.

7 Appendix A

7.1 Deploying SBC behind the NAT

The SPL configuration is a must for ORACLE SBC deployed in Cloud Environments.

The Oracle Communication once deployed in AWS public cloud environment, you need to configure SPL NAT plugin in order for proper signaling and voice path between deployed ORACLE SBC and PSTN.

The plug-in modifies the information in SIP messages to hide the end point located inside the private network of AWS deployed ORACLE SBC. Configure the Support for SBC behind the NAT SPL plugin for each SIP interface on the SBC. Here there are two interfaces, one on the side facing AWS and the other on the PSTN side. One public-private address pair required for each SIP interface that uses the SPL plug-in as follows.

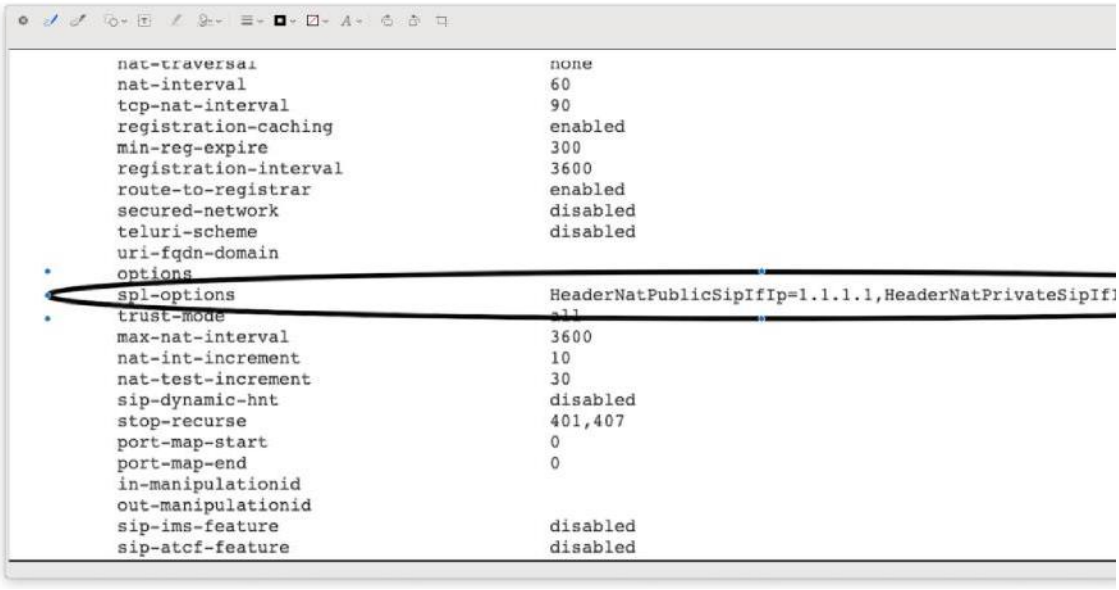
- The private IP address must be the same as the SIP interface IP address.
- The public IP address must be the elastic ip address configured in AWS for particular network interface

Here is an example configuration with SBC behind NAT SPL config. The SPL is applied to M00 interface.

To configure SBC behind NAT SPL plug-in using the GUI, Go to session-router -> sip-interface -> spl-options and input the following value, save and activate>

HeaderNatPublicSiplfIp=<Reserved Public IP of the M00 interface>,HeaderNatPrivate IfIp=<Private IP of the M00 interface>
eg: HeaderNatPublicSipIfIp=1.1.1.1,HeaderNatPrivateSipIfIp=2.2.2.2

Here the HeaderNatPublicSipIfIp is the reserved public interface ip and HeaderNatPrivateSipIfIp is the private ip.



```
nat-traversal                   none
nat-interval                    60
tcp-nat-interval                90
registration-caching            enabled
min-reg-expire                  300
registration-interval           3600
route-to-registrar              enabled
secured-network                 disabled
teluri-scheme                   disabled
uri-fqdn-domain
options
spl-options                     HeaderNatPublicSipIfIp=1.1.1.1,HeaderNatPrivateSipIfI
trust-mode                      all
max-nat-interval                3600
nat-int-increment               10
nat-test-increment              30
sip-dynamic-hnt                 disabled
stop-recurse                    401,407
port-map-start                  0
port-map-end                    0
in-manipulationid
out-manipulationid
sip-ims-feature                 disabled
sip-atcf-feature                disabled
```

SPL option HeaderNatPublicSiplfIp=<Public IP of the M00 interface>,HeaderNatPrivateSiplfIp=<Private IP of the M00 interface>

Click on “Done”. Save and activate the config.

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Copyright © 2019, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615