



ORACLE

Deploying Oracle SBC with
High availability in Oracle Cloud
Infrastructure

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 Oracle.

Revision History

Version	Description of Changes	Date Revision Completed
1.0	Deploying Oracle SBC with HA in Oracle cloud	15-11-2019
2.0	Added Oracle SBC marketplace deployment	13-05-2020
3.0	Refreshed the app note with new screenshots and SBC version	10-09-2024

Table of Contents

1. INTRODUCTION	4
2. DOCUMENT OVERVIEW	4
3. RELATED DOCUMENTATION	4
3.1 ORACLE SBC	4
3.2 ORACLE CLOUD INFRASTRUCTURE	4
4. REQUIREMENTS	4
5. CREATE AND DEPLOY ON OCI	5
5.1 PREREQUISITES	5
5.2 SELECTING A REGION	5
5.3 SETTING UP/PICKING A COMPARTMENT	5
5.4 CREATING DYNAMIC GROUPS AND POLICY	6
5.5 SETTING UP NETWORKING	7
5.6 SUBNETS	15
6. CREATING A SBC INSTANCE	18
6.1 ASSIGNING VNIC'S TO THE INSTANCES	24
6.2 ASSIGN RESERVED PUBLIC IP'S TO MEDIA INTERFACES	27
6.3 ASSIGNING UTILITY ADDRESSES FROM OCI	28
7. CONFIGURING SBC FOR HA IN OCI	29
7.1 CONFIGURE SBC USING WEB GUI	32
7.2 INTERFACE MAPPING	34
7.3 CONFIGURE SYSTEM-CONFIG	35
7.4 CONFIGURE PHYSICAL INTERFACE VALUES	36
7.5 CONFIGURE NETWORK INTERFACE VALUES	38
7.6 CONFIGURE REDUNDANCY	41
7.7 ACQUIRING CONFIGURATION FROM THE PRIMARY SBC	43
7.8 SWITCHING OVER SBC	43
8. DEPLOYING SBC BEHIND THE OCI-NAT	45

1. Introduction

This document describes how to deploy the Oracle SBC with High availability configuration on OCI. This technical application note is intended for IT or telephony professionals. It assumes that the reader is familiar with basic operations of the Oracle Session Border Controller and OCI Cloud Deployments.

2. Document Overview

You can deploy the Oracle Communications Session Border Controller (OCSBC) on OCI via OCI Marketplace. OCI provides multiple ways of managing your environment(s), including via its web portal and CLI interfaces. This document focuses on the portal. This procedure also assume you have reviewed Oracle Cloud Infrastructure documentation and can access portal pages and navigation. This document also assumes that you are aware of the high availability configuration in Oracle SBC.

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 Configuration Guide](#)
- [Oracle® Enterprise Session Border Controller Release Notes](#)

3.2 Oracle Cloud Infrastructure

- [Oracle Cloud Infrastructure Documentation](#)
- [Managing Compartments](#)
- [OCI Security Best Practices](#)
- [Managing Dynamic Groups](#)
- [OCI Training](#)

4. Requirements

- 1) A subscription for Oracle Cloud Interface called Tenancy account. For more information, refer the documentation here <https://docs.oracle.com/en-us/iaas/Content/GSG/Concepts/settinguptenancy.htm>

Tip: You can utilize the search bar at the top of the OCI portal to quickly locate any element, resource or document during configuration and deployment of the Oracle SBC in OCI Cloud.

5. Create and deploy on OCI

5.1 Prerequisites

The following pre-requisites should be taken care, before deploying the oracle SBC on the OCI cloud.

- Selecting a Region
- Setting up or picking a compartment
- Creating dynamic groups and policies
- Setting up Networking
- Setting up Security lists.

5.2 Selecting a Region

Oracle Cloud Infrastructure is hosted in regions and availability domains. A region is a localized geographic area, and an availability domain is one or more data centers located within a region. A region is composed of one or more availability domains. Please select the following

- Accessible region
- Availability domain
- Fault domain

Note: For deploying the Oracle SBC in HA mode, the SBC's can be in

- Either the same availability region with different fault domains
- Different availability regions altogether

Choosing either of the above, depends entirely on the customer environment. In this deployment, we have deployed two SBC's in HA mode in same availability region with different fault domain.

5.3 Setting up/Picking a compartment

Compartments are the primary building blocks you use to organize your cloud resources. Compartments helps us organize and isolate your resources to make it easier to manage and secure access to them.

When your tenancy is provisioned, a root compartment is created for you. If you are looking to set up a new compartment, please refer the documentation here.

<https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingcompartments.htm>

Setting up a new compartment depends on the tenancy as well. For more information, please refer <https://docs.cloud.oracle.com/iaas/Content/GSG/Concepts/settinguptenancy.htm>

Similarly, resources can be deployed in the existing compartment as well. this compartment comes along with your tenancy account and can be chosen as shown below.

ORACLE Cloud Search resources, services, documentation, and Marketplace US East (Ashburn) ▾

Identity

Overview

Overview

Domains

Network Sources

Policies

Compartments

Federation

List scope

Compartment

vsbc

- oraclegbudevcorp (root)
 - CGBU_vSBC_CMP1
 - CGBU_vSBC_CMP2

no tag filters applied

Choose a compartment

Create compartments to organize your resources.

View and manage your resources: choose a compartment and resource type using

Oracle SBC can be deployed in both a new and an existing compartment. Here we have chosen the existing compartment. Also, both the SBC's are deployed in the same compartment.

5.4 Creating Dynamic Groups and policy

Dynamic Groups allow instances to have permissions that a user would have. This is required for HA deployments as the instances need to make calls to the OCI API for state transitions.

For creating dynamic groups, go to Identity->dynamic group.

Identity » Dynamic Groups » Dynamic Group Details

DG

CGBU_vSBC_sbc-access

Delete

OCID: `ocid1.dynamicgroup.oc1..aaaaaaa6pylpai3blzy5csm5xw2e5tzine24vtvqpguepm7g45r4rr7cla` [Show Copy](#)

Description: SBC instance access to OCI services

Created: Wed, 28 Nov 2018 17:07:47 GMT

Resources

Matching Rules Displaying 1 Matching Rules

Edit All Matching Rules *Instances that meet the criteria defined by any of these rules will be included in the group*

instance.compartment.id = `'ocid1.compartment.oc1...aaaaaaa6pylpai3blzy5csm5xw2e5tzine24vtvqpguepm7g45r4rr7cla'`

Create Policy

Create the following policy and assign it to the dynamic group.

The screenshot shows the 'Create Policy' interface. The 'NAME' field contains 'CGBU_vSBC_sbc_access_policy'. The 'DESCRIPTION' field contains 'Policy to allow SBC instances to work with vNICs'. Under 'Policy Versioning', 'KEEP POLICY CURRENT' is selected. The 'Policy Statements' section contains three statements: 'Allow dynamic-group CGBU_vSBC_sbc-access to use private-ips in compartment CGBU_vSBC_CMP1', 'Allow dynamic-group CGBU_vSBC_sbc-access to use vnics in compartment CGBU_vSBC_CMP1', and 'Allow dynamic-group CGBU_vSBC_sbc-access to use vnic-attachments in compartment CGBU_vSBC_CMP1'. The 'TAGS' section has a table with columns 'TAG NAMESPACE', 'TAG KEY', and 'VALUE'. The 'TAG NAMESPACE' dropdown is set to 'None (apply a free-form tag)'. There is an '+ Additional Tag' button at the bottom right.

Name: CGBU_vSBC_sbc_access_policy (this can be anything)

Policy Statements:

- Allow dynamic-group CGBU_vSBC_sbc-access to read all-resources in compartment CGBU_vSBC_CMP1
- Allow dynamic-group CGBU_vSBC_sbc-access to use private-ips in compartment CGBU_vSBC_CMP1
- Allow dynamic-group CGBU_vSBC_sbc-access to use vnics in compartment CGBU_vSBC_CMP1
- Allow dynamic-group CGBU_vSBC_sbc-access to use vnic-attachments in compartment CGBU_vSBC_CMP1

Note: The dynamic-group name, in this example CGBU_vSBC_sbc-access, shall match the name given to the Dynamic Group in the previous step.

5.5 Setting up Networking

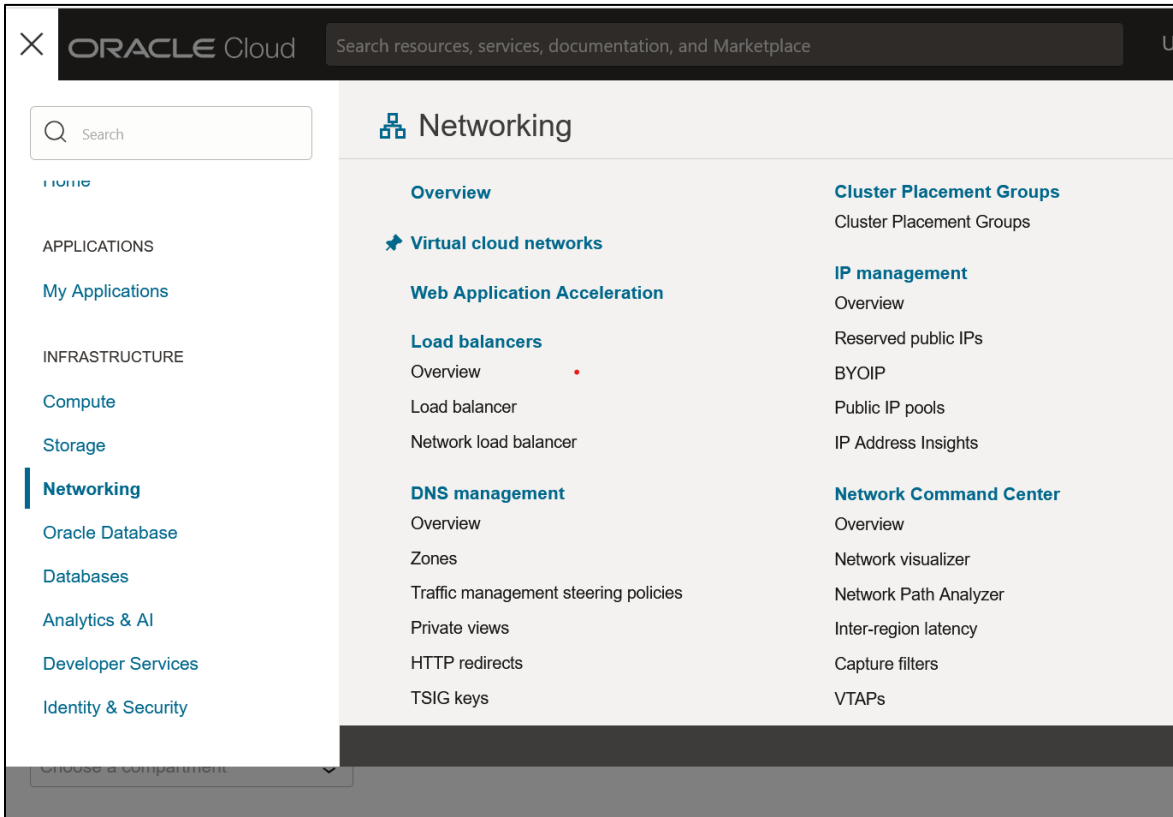
To setup networking on Oracle cloud, you have to create a Virtual Cloud Network (VCN) ,with all its resources.

5.5.1 Creating a Virtual cloud Network

Virtual cloud network is a private network that resides in Oracle data center and closely resembles a traditional network. A VCN resides in a single Oracle Cloud Infrastructure region and covers a single, contiguous IPv4 CIDR block of your choice. For more information on the virtual cloud networks, refer the following documentation

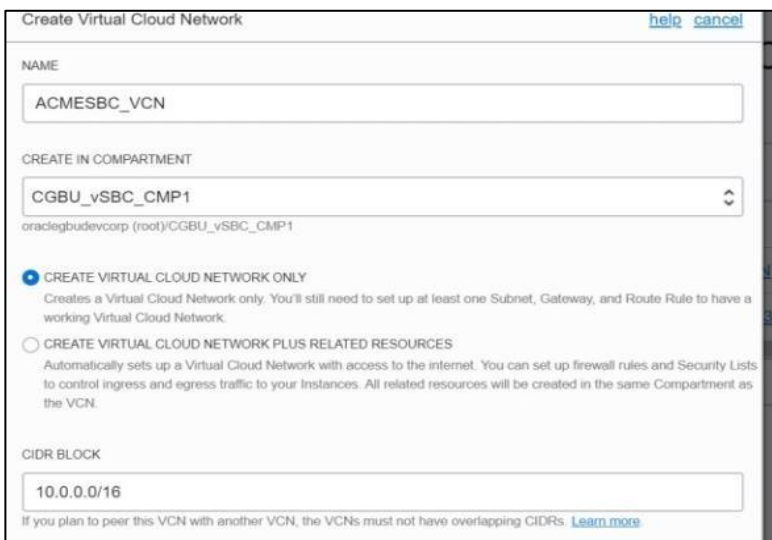
<https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/overview.htm>

To create a Virtual cloud Network (VCN), go to Networking->Virtual cloud Networks



Here we are creating the related resources, one by one after creating the VCN. **Here we have chosen a CIDR 10.0.0.0/16 for deploying the SBC.**

Note: Choosing the CIDR block, varies according to your deployment



Here is the list of resources that are mandatory for the Oracle SBC to be deployed on the OCI.

- Subnets
- Route Tables - default
- Internet Gateways - default
- Security Lists
- DHCP Options - default

The following resources are required only based on the customer deployment and are optional.

- Dynamic Routing Gateways
- Local Peering Gateways
- NAT Gateways
- Service Gateways

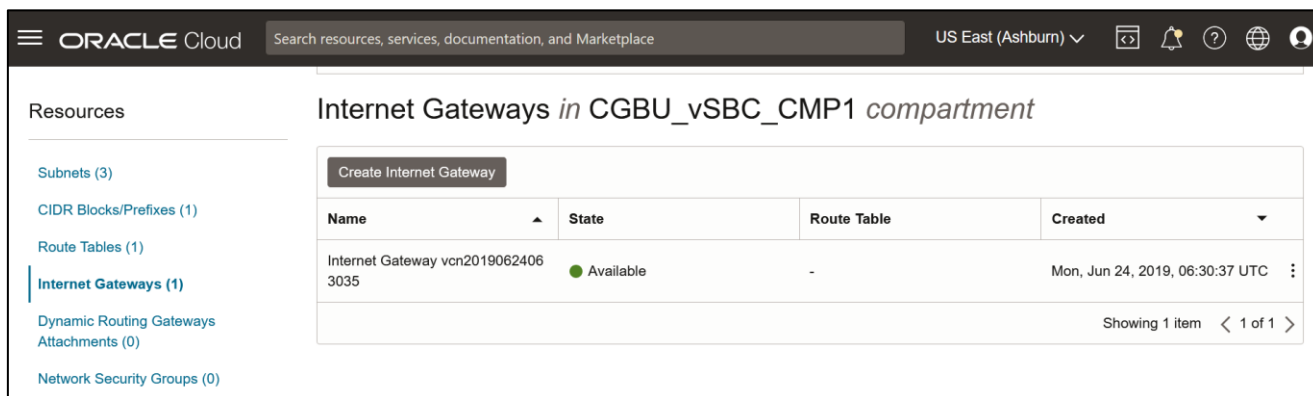
5.5.2 Internet Gateway

An internet gateway is an optional virtual router that connects the edge of the VCN with the internet. To use the gateway, the hosts on both ends of the connection must have public IP addresses for routing. Connections that originate in your VCN and are destined for a public IP address (either inside or outside the VCN) go through the internet gateway.

Connections that originate outside the VCN and are destined for a public IP address inside the VCN go through the internet gateway.

To create an internet gateway, follow the below steps.

- Select your VCN, click Internet Gateways
- Click Create Internet Gateway.
- Enter the following:
- Name
- Create in Compartment: The compartment where you want to create the internet gateway.
- Tags
- Click Create Internet Gateway.



The screenshot shows the Oracle Cloud console interface. At the top, there's a navigation bar with the Oracle Cloud logo, a search bar, and the region 'US East (Ashburn)'. Below the navigation bar, the page title is 'Internet Gateways in CGBU_vSBC_CMP1 compartment'. On the left side, there's a 'Resources' sidebar with links to Subnets (3), CIDR Blocks/Prefixes (1), Route Tables (1), Internet Gateways (1), Dynamic Routing Gateways Attachments (0), and Network Security Groups (0). The main content area features a 'Create Internet Gateway' button and a table with the following data:

Name	State	Route Table	Created
Internet Gateway vcn20190624063035	Available	-	Mon, Jun 24, 2019, 06:30:37 UTC

At the bottom right of the table, it says 'Showing 1 item < 1 of 1 >'.

5.5.3 Route Tables

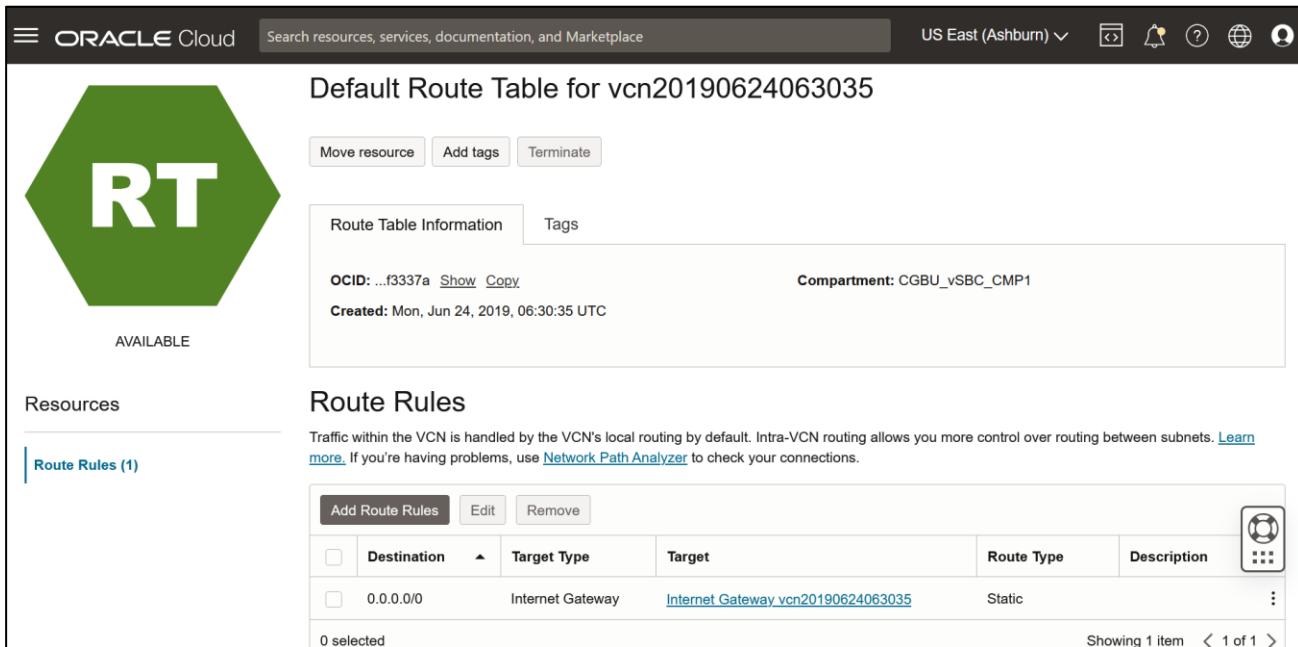
Each VCN automatically comes with a default route table that has no rules. If you don't specify otherwise, every subnet uses the VCN's default route table. When you add route rules to your VCN, you can simply add them to the default table if that suits your needs

Here, for Oracle SBC to work and connect to the outer world, we add the internet gateway to the route table to route it to the internet.

We have created 2 route tables for 3 subnets

- A route table with internet gateway added for management interface(wancom0)
- A route table with internet gateway added for media

For HA interface (wancom1 and wancom2) route tables are not required.



The screenshot displays the Oracle Cloud console interface for a Default Route Table. The title is "Default Route Table for vcn20190624063035". On the left, there is a green hexagonal icon with "RT" and the word "AVAILABLE" below it. The main content area shows "Route Table Information" with fields for "OCID: ...f3337a" and "Compartment: CGBU_vSBC_CMP1". Below this is the "Route Rules" section, which includes a table with one rule:

Destination	Target Type	Target	Route Type	Description
<input type="checkbox"/> 0.0.0.0/0	Internet Gateway	Internet Gateway vcn20190624063035	Static	

5.5.4 DHCP Options

The Networking service uses DHCP to automatically provide configuration information to instances when they boot up. Although DHCP lets you change some settings dynamically, others are static and never change. For example, when you launch an instance, either you or Oracle specifies the instance's private IP address. Each time the instance boots up or you restart the instance's DHCP client, DHCP passes that same private IP address to the instance. The address never changes during the instance's lifetime

To create DHCP options,

- Go to your VCN
- Under Resources, click DHCP Options.
- Click Create DHCP Options.
- Enter the following:
- Name:..
- Create in Compartment:
- DNS Type: for Oracle SBC, select Internet and VCN Resolver..
- Search Domain: Optional
- Tags:
- When you're done, click Create DHCP Options

Resources

DHCP Options in CGBU_vSBC_CMP1 Compartment

Create DHCP Options

Name	State	DNS Type	DNS Servers	Search Domain	Created
Default DHCP Options for vcn20190624063035	Available	Internet and VCN Resolver			Mon, Jun 24, 2019, 6:30:35 AM UTC

Showing 1 Item < Page 1 >

5.5.5 Creating Security Lists

A security list acts as a virtual firewall for an instance, with ingress and egress rules that specify the types of traffic allowed in and out. **Here for Oracle SBC, we configure security lists at the subnet level**, which means that all VNICs in a given subnet are subject to the same set of security lists. The security lists apply to a given VNIC whether it's communicating with another instance in the VCN or a host outside the VCN.

For Media, security lists stateless security lists are recommended.

For Oracle SBC, we create 3 security lists.

- Management security list
- Media security list
- HA security list

To create a security list, please follow the following steps

- Go to Networking and click Virtual Cloud Networks.
- Click on your VCN
- Under Resources, click Security Lists.
- Click Create Security List.
- Enter the following:
 - Name
 - Create in Compartment
- Add either an ingress rule or egress rule (for examples of rules, see Networking Scenarios):
- Click either Add Ingress Rule or Add Egress Rule.
- Choose whether it's a stateful or stateless rule (see Stateful Versus Stateless Rules). By default, rules are stateful unless you specify otherwise.
- Enter either the source CIDR (for ingress) or destination CIDR (for egress).
- Select the IP protocol (for example, TCP, UDP, ICMP, "All protocols", and so on).
- Enter further details depending on the protocol:
 - Repeat the preceding step for each rule you want to add to the list.
- Tags
- When you're done, click Create Security List.

5.5.5.1 Management security list

The security list for management ports can be stateful,

The following TCP/UDP protocols and/or ports should be opened for Oracle SBC ingress side. On the egress side, we have opened all ports as shown. These ports can be configured in security lists, according to customer's environment.

Protocol	Port
ICMP	n/a
SSH	22
NTP	123
SNMP	161
SNMP Trap	162
Diameter	3868
Radius	1812
TACACS	49
HTTP	80
HTTPS	443

Create Security List [help](#) [cancel](#)

A security list contains ingress and egress rules that specify the types of traffic allowed in and out of instances. [Learn more about Security Lists](#)

NAME

CREATE IN COMPARTMENT

oraclegbudevcorp (root)/CGBU_vSBC_CMP1

Allow Rules for Ingress

Ingress Rule 1 ✕

Allows ICMP traffic for: all types and codes

STATELESS (i)

SOURCE TYPE: CIDR ⇅

SOURCE CIDR: 0.0.0.0/0

IP PROTOCOL (i): ICMP ⇅

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

TYPE OPTIONAL (i): All

CODE OPTIONAL (i): All

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

Ingress Rule 2 ✕

Ingress Rule 2 ✕

Allows TCP traffic 22,3868,1812,443,80,49

STATELESS (i)

SOURCE TYPE: CIDR ⇅

SOURCE CIDR: 0.0.0.0/0

IP PROTOCOL (i): TCP ⇅

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

SOURCE PORT RANGE OPTIONAL (i): All

DESTINATION PORT RANGE OPTIONAL (i): 22,3868,1812,443,80,49

Examples: 80, 20-22

Ingress Rule 3 ✕

Ingress Rule 3 ✕

Allows UDP traffic 123,161,162

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 ⓘ: UDP

SOURCE PORT RANGE OPTIONAL ⓘ: All
Examples: 80, 20-22

DESTINATION PORT RANGE OPTIONAL ⓘ: 123,161,162
Examples: 80, 20-22

[+ Additional Ingress Rule](#)

Add Egress Rules [cancel](#)

Egress Rule 1

All traffic for all ports

STATELESS ⓘ

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

[+ Additional Egress Rule](#)

[Add Egress Rules](#) [Cancel](#)

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

[+ Additional Tag](#)

[Create Security List](#) [Cancel](#)

5.5.5.2 Media security list

It is recommended that the security lists for media ports be **stateless** to avoid performance penalties.

OCI and the SBC VM implement separate security rules. For some protocols to operate the media port configuration should mirror the security list below. **If a security list allows icmp, it is not necessary that the SBC VM also allows icmp.**

Protocol	Port
ICMP	N/a
SSH	22
IKE	500
SIP	5060
SIP	5061
H323	1719
H323 (sig)	1720

RTP	10000-12000(according to steering pool config)
-----	------------------------------------------------

5.5.5.3 HA Security List

For the HA configuration, we use private regional subnet. The following ports should be opened for Oracle SBC on ingress side. **Here we create a security list with 9090 port to support the redundancy configuration.** The source CIDR can be of the private subnet.

We also recommend customers using any one of the below methods for HA configuration security list.

- Set the Security List to allow all traffic sourced only from IPs in the wancom1 subnet.
- Set a Network Security Group with the 'Type' set to 'NSG' and apply that to the wancom1 VNICs.

This will lock it down so that only traffic sourced from the appropriate IP's from those VNIC's are allowed, while allowing traffic on all ports.

5.6 Subnets

Each subnet in a VCN consists of a contiguous range of IPv4 addresses that do not overlap with other subnets in the VCN.

Example: 172.16.1.0/24. The first two IPv4 addresses and the last in the subnet's CIDR are reserved by the Networking service. For more information please refer the documentation

<https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/managingVCNs.htm>

Each VCN can be divided into multiple subnets. The SBC has 3 types of vNICs: management (wancom0), HA (wancom1/wancom2) and Media (s0p0, s1p0 etc). To maintain traffic separation, each of the vNICs should be connected to a separate subnet within the VCN. Depending on whether access to these vNICs is required through Internet or not a public IP should be associated.

For any HA deployment we require the following subnets .The following subnets are mandatory

- wancom0
- wancom1
- Network interfaces (s0p0, s1p0) (according to your environment. Maximum up to 8) Here in this deployment, we have considered wancom2 as optional.

Please follow the below table to create subnets required for the deployment of Oracle SBC in HA mode.

Subnet Name	Type of subnet	Public subnet	Ephemeral Public IP	Reserved Public IP
wancom0	Regional	yes	yes	n/a
s0p0,s0p1	Regional	yes	no	yes
wancom1	Regional	no	n/a	no

To create a subnet,

- Open the navigation menu. In Core Infrastructure, go to Networking and click Virtual Cloud Networks.
- Click on the VCN created.
- Click Create Subnet.
- Enter the following:
- Create in Compartment
- Name

- **Subnet Type: Regional or AD-specific subnet:** Oracle recommends creating only regional subnets, which means that the subnet can contain resources in any of the region's availability domainser created in this subnet must also be in that availability domain.
- **CIDR Block:** A single, contiguous CIDR block for the subnet (for example, 172.16.0.0/24). Make sure it's within the cloud network's CIDR block and doesn't overlap with any other subnets. You cannot change this value later.
- **Route Table:** The route table created in the above section
- **Subnet Access:** Private or public subnet: This controls whether VNICs in the subnet can have public IP addresses.

Follow the above table and create a subnet for Oracle SBC.

- **DNS Resolution:** Use DNS Hostnames in this Subnet
- **DHCP Options:** Created in the section here
- **Security Lists:** Created in the section here.
- **Tags**
Click Create.

Create Subnet [help](#) [cancel](#)

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

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

Specified IP addresses: 10.0.10.0-10.0.10.255 (256 IP addresses)

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

DNS LABEL

Only letters and numbers, starting with a letter. 15 characters max.

DNS DOMAIN NAME *READ-ONLY*

DHCP OPTIONS

SECURITY LIST

ACMESBC-MGMT-SL

AGS

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)

6. Creating a SBC Instance

The SBC is now available as an easy to deploy instance in the OCI Marketplace listed as “Oracle Enterprise Virtual Session Border Controller”. This section walks through creating an SBC instance via OCI Marketplace.

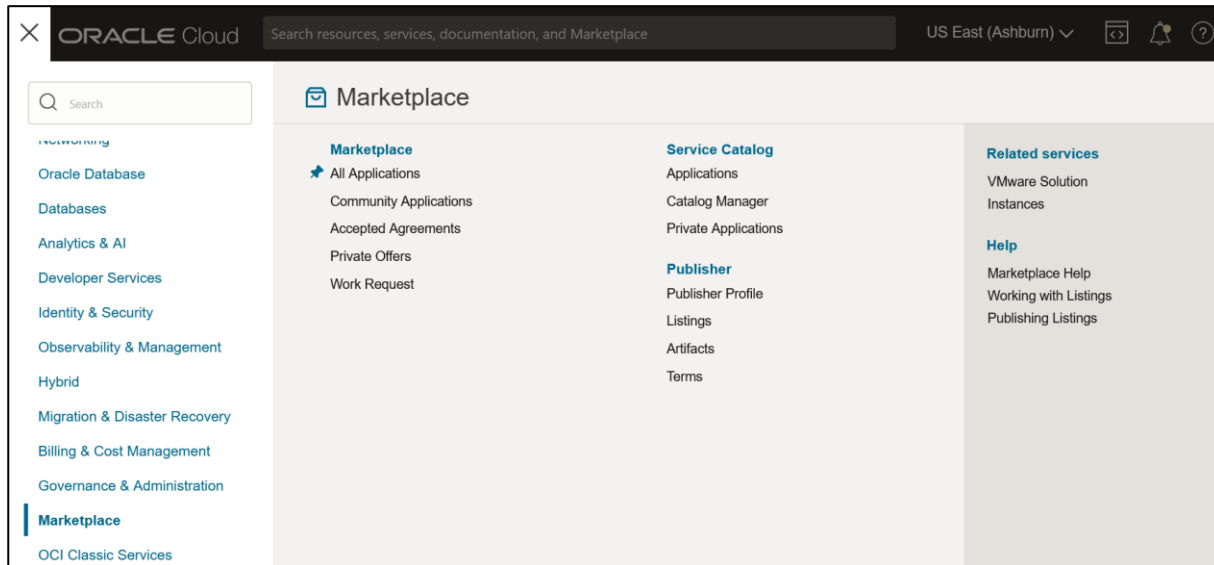
The supported VM shapes are listed as below:

Figure 1. Table 1 Supported VM shapes

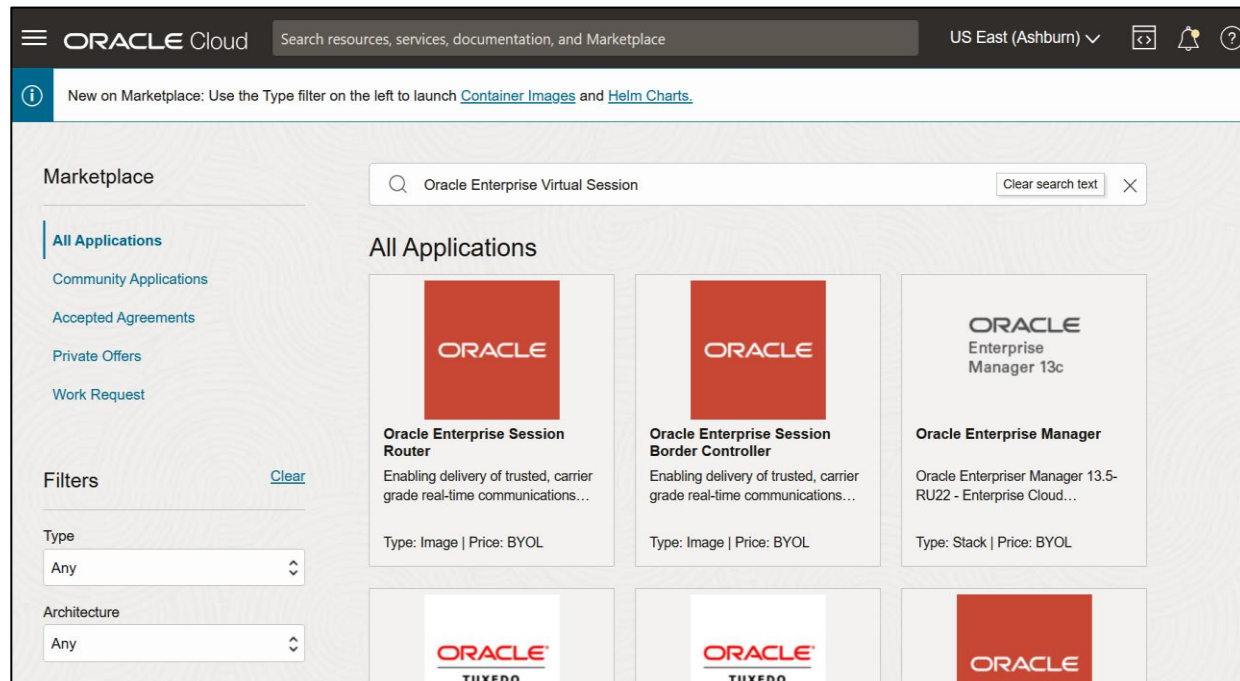
Shape	Supported	OCPUs/VCPUs	vNICs	Tx/Rx Queues	MAX Forwarding Cores	DOS Protection
VM.Standard1.1	N	1/2	2	2	0	N
VM.Standard1.2	Y	2/4	2	2	1	N
VM.Standard1.4	Y	4/8	4	2	2	Y
VM.Standard1.8	Y	8/16	8	2	2	Y
VM.Standard1.16	Y	16/32	16	2	2	Y
VM.Standard2.1	N	1/2	2	1	0	N
VM.Standard2.2	Y	2/4	2	1	1	N
VM.Standard2.4	Y	4/8	4	1	1	Y
VM.Standard 2.8	Y	8/16	8	1	1	Y
VM.Standard 2.16	Y	16/32	16	1	1	Y

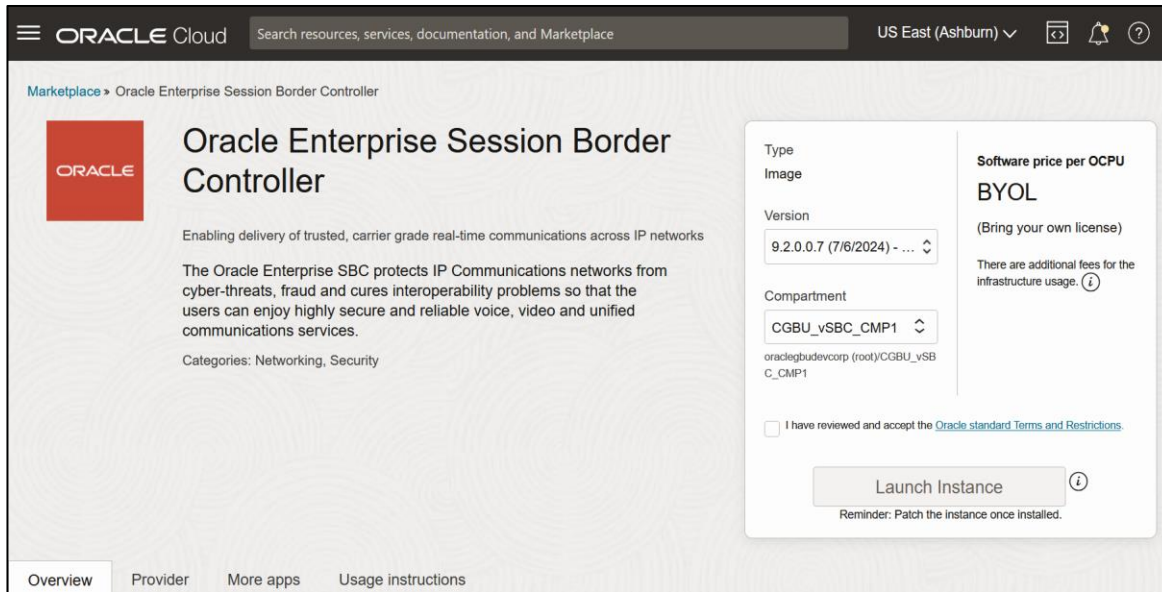
Following are the steps to create a SBC Instance.

- **Select Marketplace-> All Applications from the OCI portal.**
- **Search for “Oracle Enterprise Virtual Session Border Controller”**

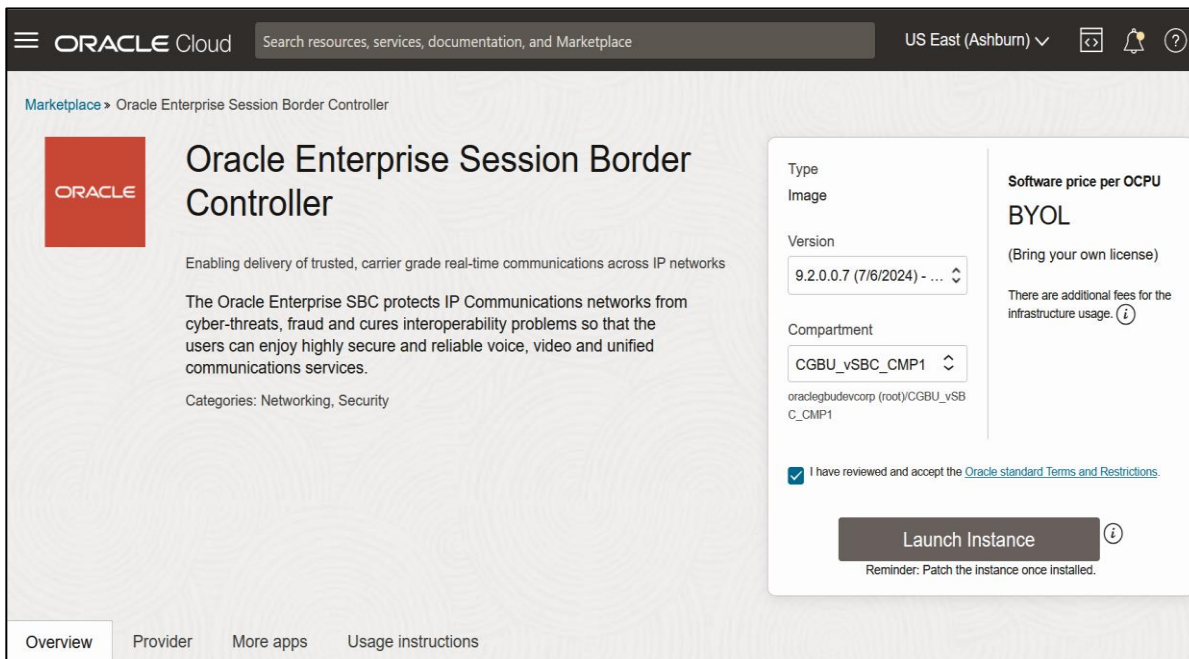


- **Search for “Oracle Enterprise Virtual Session” and select “Oracle Enterprise Session Border Controller”**

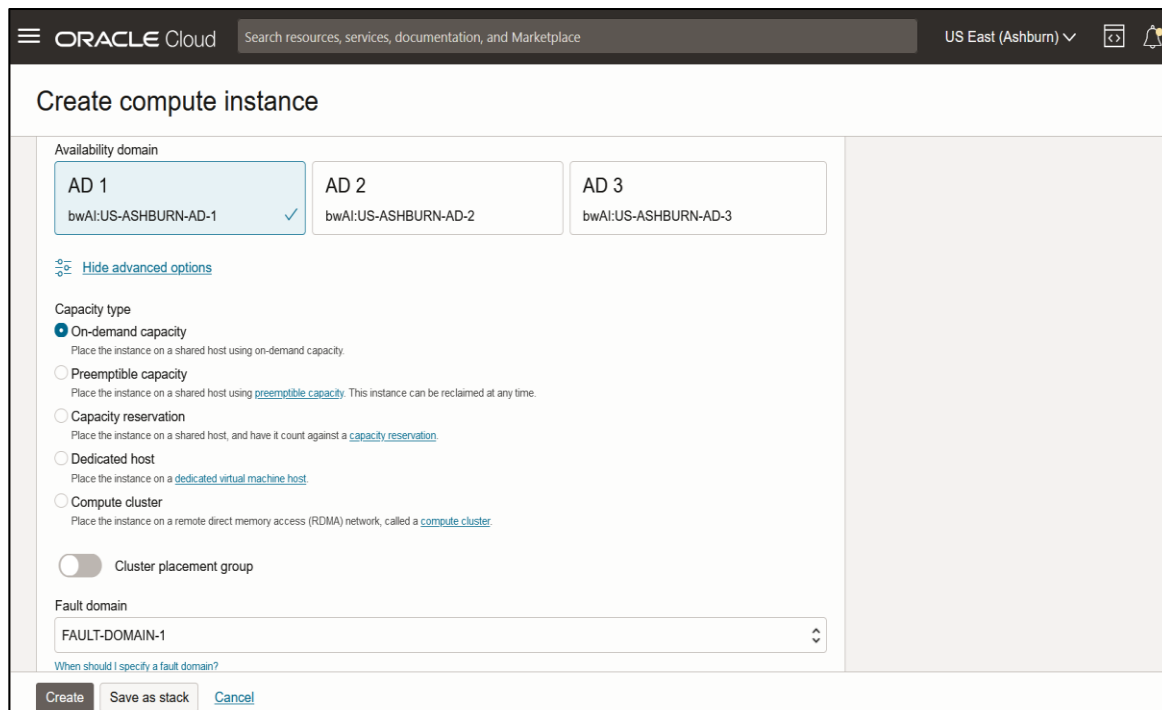
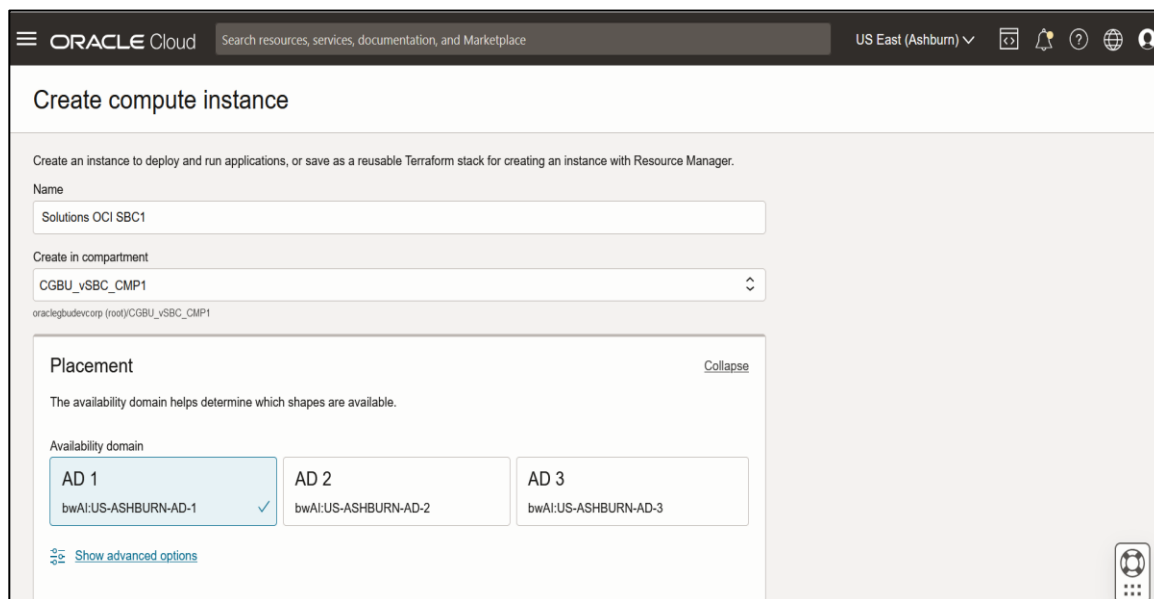




- **Select checkbox “I have reviewed and accept” and click “Launch Instance.”**
- **We can also select the appropriate SBC builds listed from the drop-down menu.**



- **Populate Name for your instance**
- **Select “Availability Domain” and the “Instance Type” and fault Domain.**



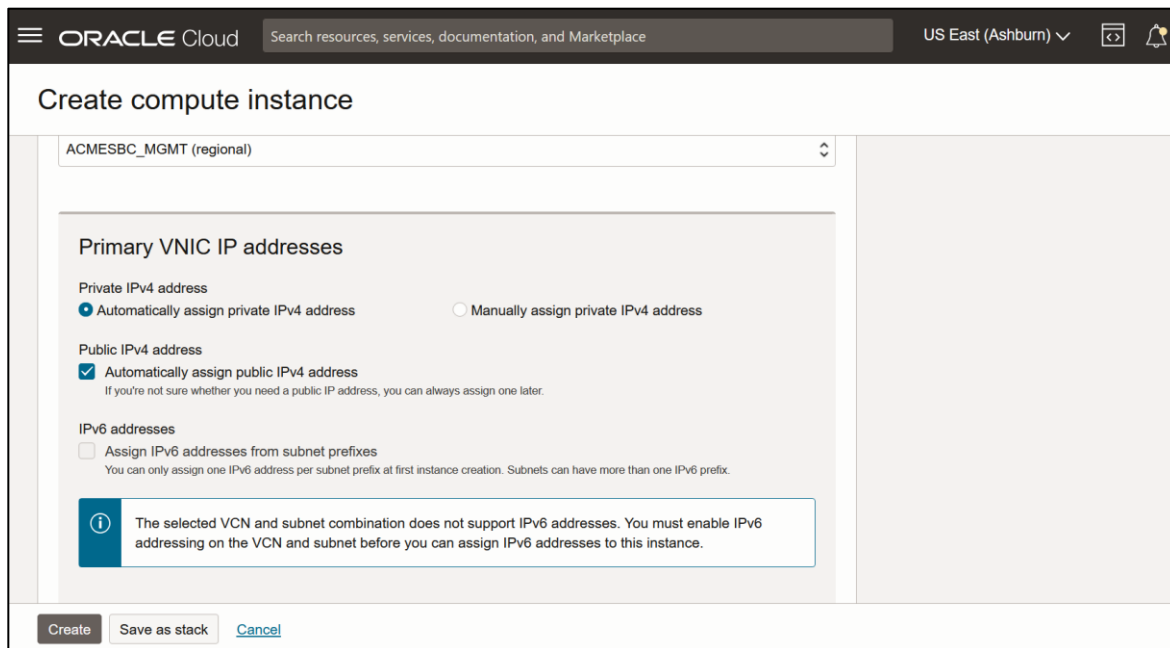
- Choose the appropriate shape.

The screenshot shows the Oracle Cloud console interface for creating a compute instance. At the top, the Oracle Cloud logo and a search bar are visible, along with the region 'US East (Ashburn)'. The main heading is 'Create compute instance'. Below this, a descriptive paragraph explains that a 'shape' is a template for CPU, memory, and other resources, and an 'image' is the operating system. The 'Image' section displays the 'Oracle Enterprise Session Border Controller' with a red Oracle logo and a 'Return to Marketplace' button. The 'Shape' section displays the 'VM.Standard.E4.Flex' shape with an AMD logo and a 'Change shape' button. At the bottom, there are three buttons: 'Create', 'Save as stack', and 'Cancel'.

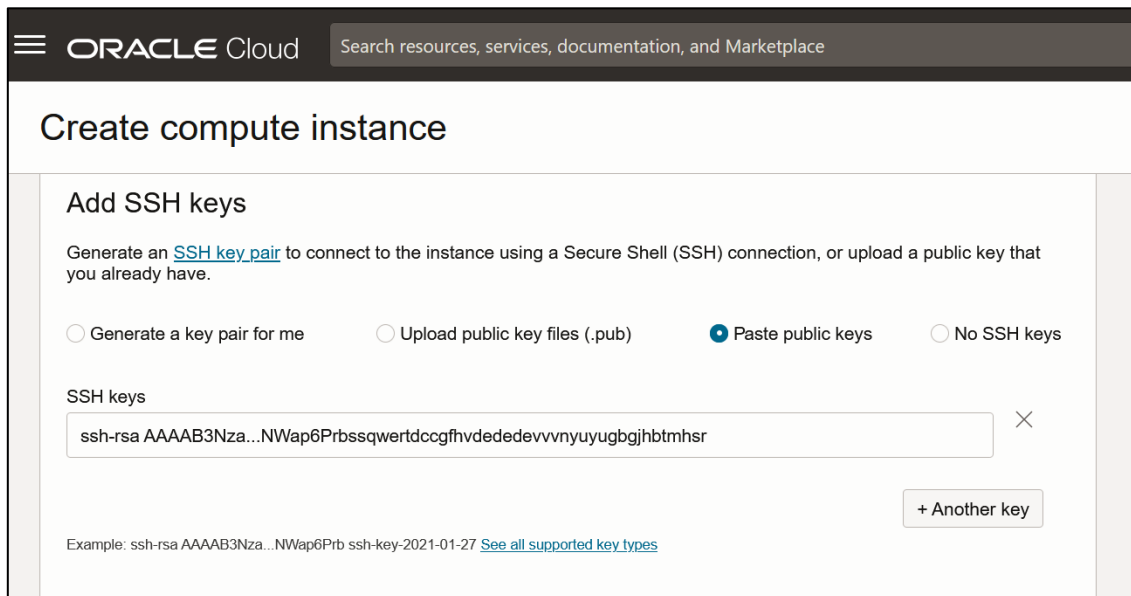
- Choose the corresponding VCN, compartment and subnets. Here choose the management subnet to access the Oracle SBC immediately after deployment.

This screenshot shows the network configuration step of the 'Create compute instance' process. The 'Primary network' section has three radio buttons: 'Select existing virtual cloud network' (which is selected), 'Create new virtual cloud network', and 'Enter subnet OCID'. Below this, a dropdown menu shows 'VCN in CGBU_vSBC_CMP1 (Change compartment)' with 'ACMESBC_VCN' selected. The 'Subnet' section includes a note about internet accessibility and two radio buttons: 'Select existing subnet' (selected) and 'Create new public subnet'. A second dropdown menu shows 'Subnet in CGBU_vSBC_CMP1 (Change compartment)' with 'ACMESBC_MGMT (regional)' selected. At the bottom, there is a section for 'Primary VNIC IP addresses' with a 'Private IPv4 address' field. The 'Create', 'Save as stack', and 'Cancel' buttons are at the very bottom.

- Click on Assign a public IP to the instance. (ephemeral),so that the Oracle SBC is accessible from the internet as well



Paste the public key in ssh keys



- **Select Custom Boot Size Volume. Choose the size of the boot volume as 80GB.**

ORACLE Cloud Search resources, services, documentation, and Marketplace US East (Ashburn)

Create compute instance

Boot volume
A [boot volume](#) is a detachable device that contains the image used to boot the compute instance.

Specify a custom boot volume size
[Volume performance](#) varies with volume size. Default boot volume size: 46.6 GB. When you specify a custom boot volume size, service limits apply.

Boot volume size (GB)
80
Integer between 50 GB and 32,768 GB (32 TB). Must be larger than the default boot volume size for the selected image.

Boot volume performance
VPU (i) **Balanced**
10 10 120

Target volume performance (i)
IOPS: 4800 IOPS
Throughput: 38.4 MB/s

Balanced choice for most workloads including those that perform random I/O such as boot disks. [Learn more](#)
Actual performance depends on the attached instance's shape. Select the

Create Save as stack Cancel

In this deployment, **we have deployed the 2 SBCs in same availability domain and different fault domain. As mentioned earlier, you can also deploy the SBC's in different availability domains altogether**

Once the instances are deployed, they are shown in Compute->Instances

Instances in CGBU_vSBC_CMP1 compartment

An [instance](#) is a compute host. Choose between virtual machines (VMs) and bare metal instances. The image that you use to launch an instance determines its operating system and other software.

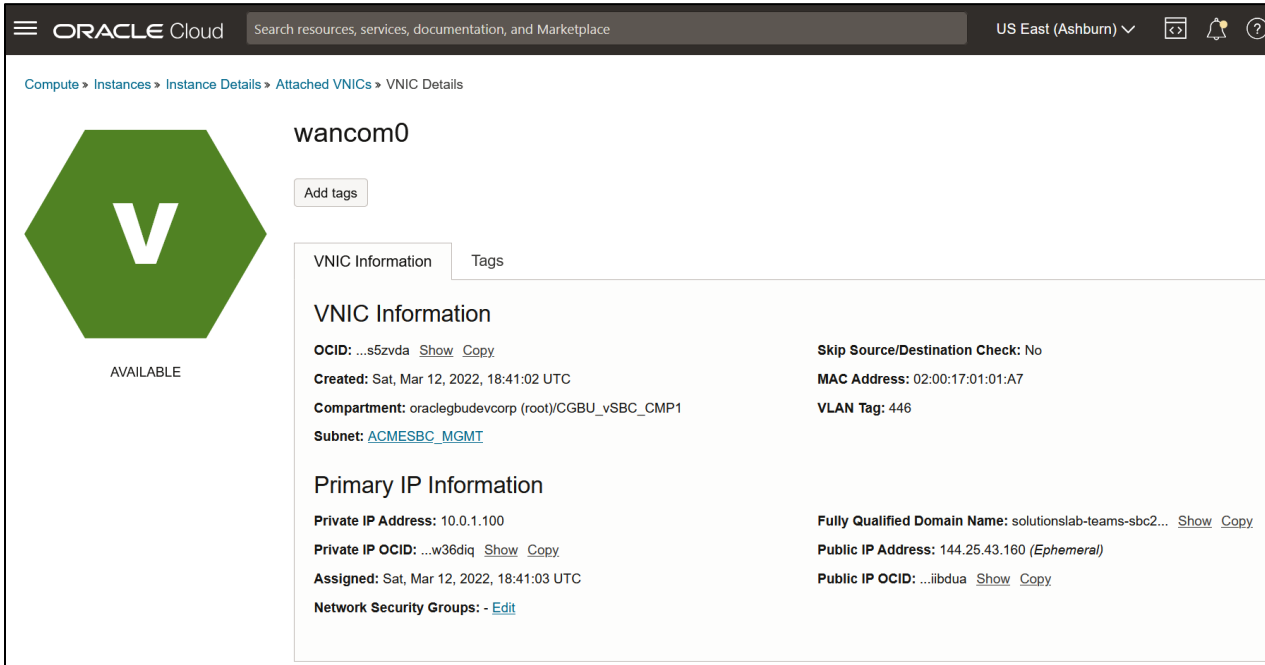
Create instance Actions

<input type="checkbox"/>	Name	State	Public IP	Private IP	Shape	OCPU count	Memory (GB)	Avai
<input type="checkbox"/>	Solutions OCI SBC2	● Running	144.25.90.73	10.0.1.146	VM.Standard2.4	4	60	AD-1
<input type="checkbox"/>	Solutions OCI SBC1	● Running	144.25.91.202	10.0.1.202	VM.Standard2.4	4	60	AD-1

6.1 Assigning VNIC's to the instances

Once the instances are deployed click on the Instance. Go to Resources->Attached VNIC's

At first there is only one VNIC attached to the instance. (Created when creating The instance). After assigning the VNIC's, reboot the instances, so that the changes are applied.



Now create VNIC's for the other subnets required, according to your deployment. Here we have deployed these subnets.

- Open Create VNIC dialog box, you specify which VCN and subnet to put the VNIC in.
- Enter the following:
 - Name
 - Subnet
 - Skip Source/Destination Check: By default, this check box is NOT selected, which means the VNIC performs the source/destination check. Only select this check box if you want the VNIC to be able to forward traffic.
 - See Source/Destination Check.
 - Private IP Address: An available private IP address of your choice from the subnet's CIDR (
 - Assign public IP address: Whether to assign an ephemeral public IP address to the VNIC's primary private IP.
 - Available only if the subnet is public. Not required in case of Oracle media and HA subnets, as we are creating reserved public IP for Media.
 - Hostname
 - Tags
- Click Create VNIC.

Create VNIC

VNIC name *Optional*

s0p0

Virtual cloud network in **CGBU_vSBC_CMP1** ([Change compartment](#))

ACMESBC_VCN

Network

Normal setup: subnet

The typical choice when adding a VNIC to an instance. ✓

Advanced setup: VLAN

Only for experienced users who have purchased the Oracle Cloud VMware Solution.

Subnet in **CGBU_vSBC_CMP1** ([Change compartment](#))

ACMESBC_s0p0 (regional)

Use network security groups to control traffic (optional) ⓘ

Skip source/destination check ⓘ

VNIC IP addresses

Save changes

[Cancel](#)

Create VNIC

The typical choice when adding a VNIC to an instance. ✓

Only for experienced users who have purchased the Oracle Cloud VMware Solution.

Subnet in **CGBU_vSBC_CMP1** ([Change compartment](#))

ACMESBC_s0p0 (regional)

Use network security groups to control traffic (optional) ⓘ

Skip source/destination check ⓘ

VNIC IP addresses

Private IPv4 address

Automatically assign private IPv4 address Manually assign private IPv4 address

IPv4 address

10.0.4.50

Must be within 10.0.4.0 to 10.0.4.255. Must not already be in use.

Public IPv4 address

Automatically assign public IPv4 address
If you're not sure whether you need a public IP address, you can always assign one later.



6.2 Assign Reserved Public IP's to Media Interfaces

For the media interfaces, (public IP's are required, if traffic flows through them), we have to assign reserved public IP's To assign a reserve public IP to the Media subnet

- Click on the attached VNIC (example s0p0) and go to IP address
- Click on the edit option and assign reserved public IP

Edit Private IP Address Help

10.0.4.50
Must be from 10.0.4.2 to 10.0.4.254. Cannot be in current use.

Hostname *Optional*

No spaces. Only letters, numbers, and hyphens. 63 characters max.

FQDN (i): <hostname>.acmesbcs0p0.acmesbcvcn.oraclevcn.com

Public IP Type
 No public IP
 Ephemeral public IP
The public IP's lifetime is bound to the lifetime of the private IP. You can unassign it from this private IP but not reassign it elsewhere. [Learn more.](#)
 Reserved public IP
You control the public IP's lifetime. You can unassign it or reassign it to another private IP in the same region. [Learn more.](#)

Select Existing Reserved IP Address Create new Reserved IP Address

Public IP Name

Create in Compartment

Assign reserved public IP only for primary SBC media interfaces (i.e only for one SBC)

Once the network interfaces are created, it will be shown like below in the primary SBC. We should create similar network interfaces in the Secondary SBC too.

Attached VNICs

A [virtual network interface card \(VNIC\)](#) attaches an instance to a subnet within a VCN and is required for connectivity with other endpoints.

Name	Subnet or VLAN <small>(i)</small>	State	FQDN <small>(i)</small>	VLAN tag	MAC address	
Sankar OCI SBC1 (Primary VNIC)	Subnet - ACMESBC_MGMT	● Attached	sankar-oci... Show Copy	1487	02:00:17:04:19:8E	⋮
s0p0	Subnet - ACMESBC_s0p0	● Attached	-	2188	02:00:17:10:48:19	⋮
s0p1	Subnet - ACMESBC_s0p1	● Attached	-	4091	02:00:17:21:1F:2F	⋮
wancom1	Subnet - ACMESBC_wancom1	● Attached	-	3286	02:00:17:34:70:28	⋮

6.3 Assigning utility addresses from OCI

For HA deployment we require pri-utility address and sec-utility address for the media interfaces. So, we must add an additional IP address to the media interfaces. Primary-utility address will be the address of media interface assigned to SBC1 and Sec-utility-address will be the address of media interface assigned to SBC2.

In the below screen, 10.0.4.55 is the primary utility IP address assigned to s0p0 media interface of Primary SBC. Please note that these IP address has to be assigned in the SBC network interface for media-interfaces.

Compute > Instances > Instance Details > Attached VNICs > VNIC Details

s0p0 AVAILABLE

[Delete](#) [Add tags](#)

VNIC Information

OCID: ...5lpquq [Show](#) [Copy](#) **Skip Source/Destination Check:** Yes
 Created: Wed, Aug 7, 2024, 11:28:50 UTC **MAC Address:** 02:00:17:10:48:19
 Compartment: oraclegbudevcorp (root)/CGBU_vSBC_CMP1 **VLAN Tag:** 2188
 Subnet: [ACMESBC_s0p0](#)

Primary IP Information

Private IP Address: 10.0.4.50 **Fully Qualified Domain Name:** -
 Private IP OCID: ...l6b2dq [Show](#) [Copy](#) **Public IP Address:** (Not Assigned)
 Assigned: Wed, Aug 7, 2024, 11:28:48 UTC
 Network Security Groups: - [Edit](#)

Pv4 Addresses

[Assign Secondary Private IP Address](#)

Private IP Address	Public IP Address	Fully Qualified Domain Name	Assigned
10.0.4.50 (Primary IP)	(Not Assigned)	-	Wed, Aug 7, 2024, 11:28:50 UTC
10.0.4.55	(Not Assigned)	-	Thu, Aug 8, 2024, 10:35:18 UTC

Showing 2 items

Similarly in the below screen, 10.0.4.51 is the secondary utility IP address assigned to s0p0 media interface of Primary SBC.

Compute > Instances > Instance Details > Attached VNICs > VNIC Details

s0p0

AVAILABLE

Delete Add tags

VNIC Information Tags

VNIC Information

OCID: ...xdkkca [Show](#) [Copy](#) Skip Source/Destination Check: No
 Created: Wed, Aug 7, 2024, 11:37:06 UTC MAC Address: 02:00:17:0B:E4:4C
 Compartment: oraclegbudevcorp (root)/CGBU_vSBC_CMP1 VLAN Tag: 2022
 Subnet: [ACMESBC_s0p0](#)

Primary IP Information

Private IP Address: 10.0.4.51 Fully Qualified Domain Name: -
 Private IP OCID: ...rbk5uq [Show](#) [Copy](#) Public IP Address: (Not Assigned)
 Assigned: Wed, Aug 7, 2024, 11:37:04 UTC
 Network Security Groups: - [Edit](#)

Pv4 Addresses

Assign Secondary Private IP Address

Private IP Address	Public IP Address	Fully Qualified Domain Name	Assigned
10.0.4.51 (Primary IP)	(Not Assigned)	-	Wed, Aug 7, 2024, 11:37:06 UTC

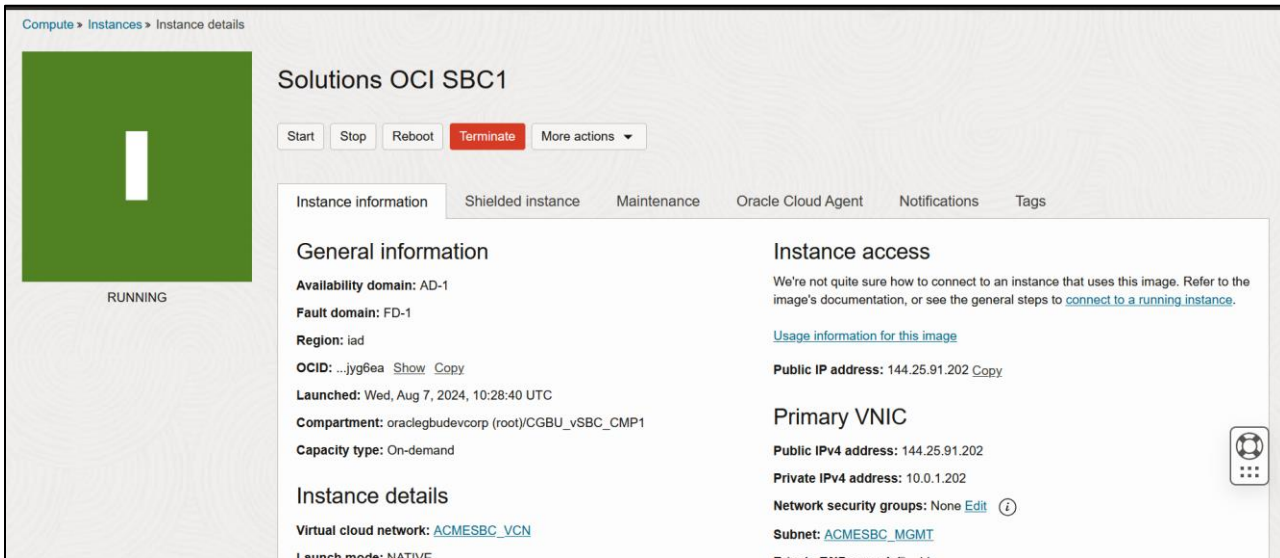
Showing 1 item

For more information on OCI layer 2 configurations for SBC, please refer the below link

<https://blogs.oracle.com/cloud-infrastructure/post/oracle-sbc-l2-ha-idnat>

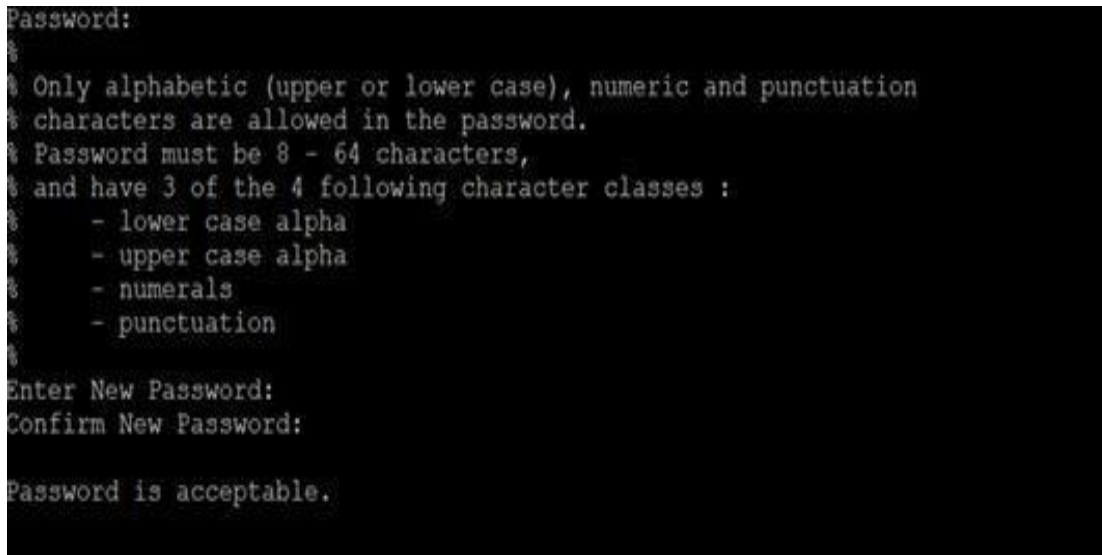
7. Configuring SBC for HA in OCI

After the configuration is completed, connect the SBC using Putty through the management IP assigned as shown. **Repeat the steps for both the SBC's**



Once we connect the instance using Putty, following window appears to change the password. The default username is “admin” and default password is “packet”+OCID (we can copy this from OCID from the above screen)

The password has to be changed according to the rules shown below.



Setup product type to “Enterprise Session Border Controller” as shown below.

To configure product type, type in setup product in the terminal

```
PE-6300-1# setup product
```

```
-----  
WARNING:
```

```
Alteration of product alone or in conjunction with entitlement  
changes will not be complete until system reboot
```

```
Last Modified 2019-09-11 13:57:32  
-----
```

```
1 : Product      : Enterprise Session Border Controller
```

```
Entitlements for Enterprise Session Border Controller  
Last Modified: Never
```

```
-----  
1 : Session Capacity      : 0  
2 :   Advanced            :  
3 : Admin Security        :  
4 : Data Integrity (FIPS 140-2) :  
5 : Transcode Codec AMR Capacity : 0  
6 : Transcode Codec AMRWB Capacity : 0  
7 : Transcode Codec EVRC Capacity : 0  
8 : Transcode Codec EVRCB Capacity : 0  
9 : Transcode Codec EVS Capacity : 0  
10: Transcode Codec OPUS Capacity : 0  
11: Transcode Codec SILK Capacity : 0
```

```
Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1
```

```
Session Capacity (0-128000)      : 500
```

```
Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 3
```

```
*****  
CAUTION: Enabling this feature activates enhanced security  
functions. Once saved, security cannot be reverted without  
resetting the system back to factory default state.  
*****
```

```
Admin Security (enabled/disabled) :
```

```
Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 5
```

```
Transcode Codec AMR Capacity (0-102375) : 50
```

```
Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 2
```

```
Advanced (enabled/disabled) : enabled
```

```
Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 10
```

```
Transcode Codec OPUS Capacity (0-102375) : 50
```

```
Enter 1 - 11 to modify, d' to display, 's' to save, 'q' to exit. [s]: 11
```

```
Transcode Codec SILK Capacity (0-102375) : 50
```

Enable the features for the ESBC using the setup entitlements command as shown.

Save the changes and reboot the SBC.

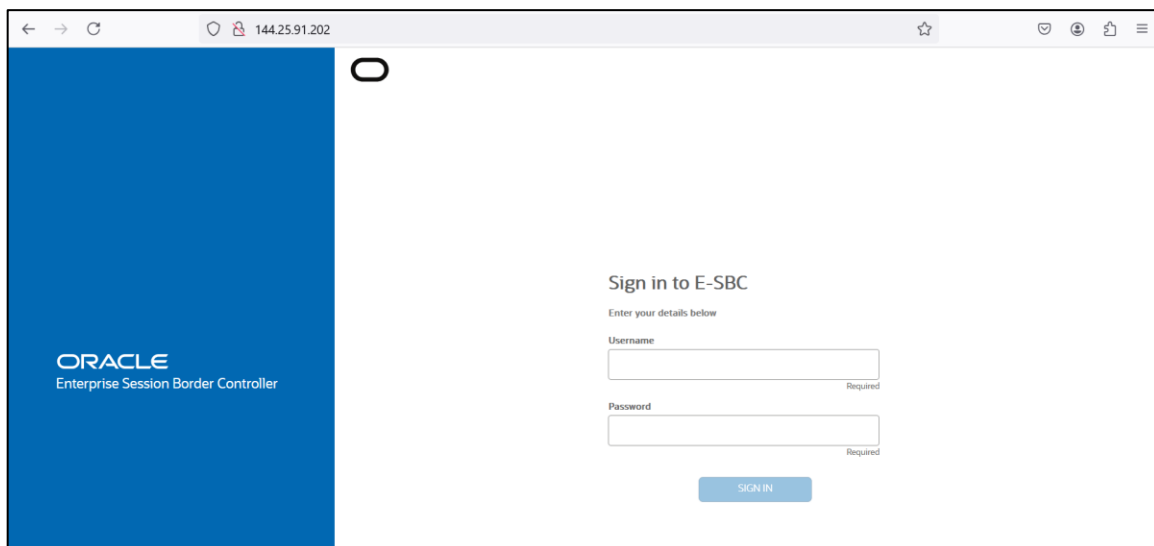
Go to configure terminal->system->http-server-config. Enable the http-server-config to access the SBC using Web GUI. Save and activate the config and the config looks as shown below.

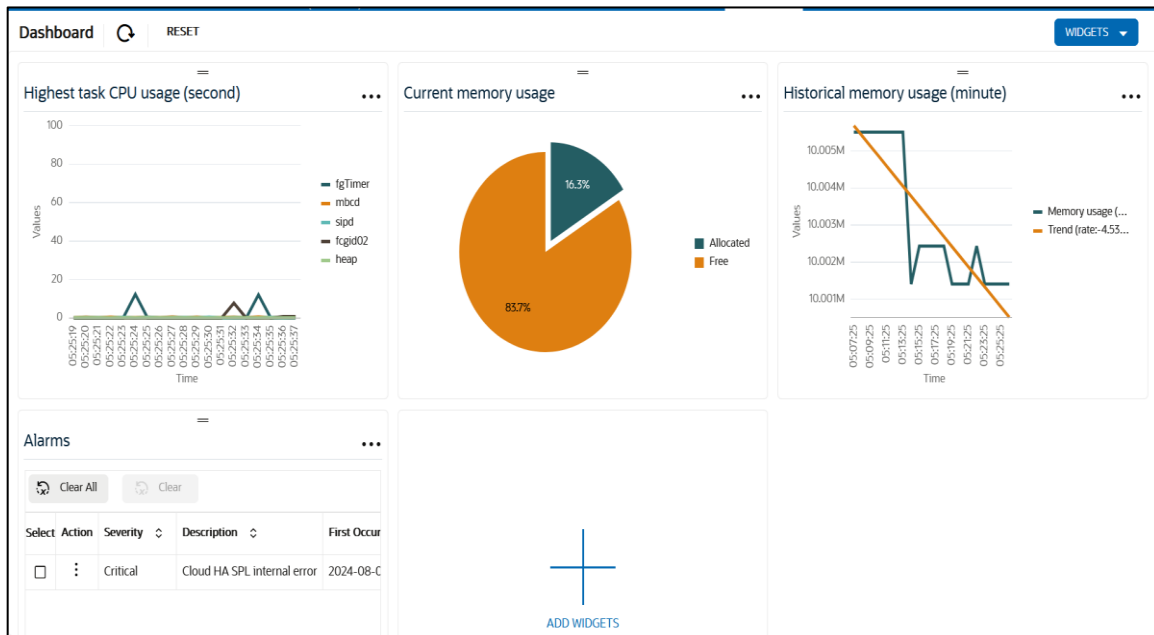
```
http-server
  name                Webserver
  state               enabled
  realm
  ip-address
  http-state          enabled
  http-port           80
  HTTP-strict-transport-security-policy disabled
  https-state         disabled
  https-port          443
  http-interface-list GUI
  http-file-upload-size 0
  tls-profile
  auth-profile
  last-modified-by    admin@209.17.43.241
  last-modified-date  2024-08-08 10:03:51
```

Once you have done the above step, the SBC can be accessed via GUI.

7.1. Configure SBC using Web GUI

The WebGUI can be accessed through the url `https://<SBC_MGMT_IP>`. The username and password is the same as that of CLI. We need to perform some more steps for HA configuration in SBC and we can perform those steps from SBC GUI or CLI. In our example we perform those steps from SBC GUI.





Go to Configuration as shown below, to configure the SBC

The Configuration GUI shows a sidebar with categories: media-manager, security, session-router (selected), and system. The main area displays "Configuration Objects" with the following table:

Name	Description
access-control	Configure a static or dynamic access control list
account-config	Configure Quality of Service accounting
authentication-profile	Configure authentication profile
certificate-record	Create, generate, and import a certificate
class-policy	Configure classification profile policies
codec-policy	Create and apply a codec policy to a realm and an agent
filter-config	Create a custom filter for SIP monitor and trace
fraud-protection	Configure fraud protection
host-route	Insert entries into the routing table
http-client	Configure an HTTP client
http-server	Configure an HTTP server
ldap-config	Configure an LDAP server, filter, and policy
local-policy	Configure a session request routing policy
local-routing-config	Configure local routing servers

Kindly refer to the GUI User Guide

<https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/9.2.0/webgui/web-gui-guide.pdf> for more information.

The expert mode is used for configuration.

Tip: To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.

7.2. Interface Mapping

The next step in deploying the Oracle SBC in HA mode is to verify the network interfaces have MAC addresses assigned to them.

Run the command `show interfaces mapping` and check the output as shown below

```
SolutionsOCISBC1# show interfaces mapping
Interface Mapping Info
-----
Eth-IF  MAC-Addr                Label
wancom0 02:00:17:04:19:8E        #present
wancom1 02:00:17:21:1F:2F        #generic
s0p0    02:00:17:10:48:19        #generic
s0p1    02:00:17:34:70:28        #generic
wancom2 FF:FF:FF:FF:FF:FF        #dummy
spare   FF:FF:FF:FF:FF:FF        #dummy
slp0    FF:FF:FF:FF:FF:FF        #dummy
slp1    FF:FF:FF:FF:FF:FF        #dummy
s0p2    FF:FF:FF:FF:FF:FF        #dummy
slp2    FF:FF:FF:FF:FF:FF        #dummy
s0p3    FF:FF:FF:FF:FF:FF        #dummy
slp3    FF:FF:FF:FF:FF:FF        #dummy

SolutionsOCISBC1#
```

Please check the interface mapping with the VNIC information of OCI and see whether the MAC address is correct for each interface.

Attached VNICs

A [virtual network interface card \(VNIC\)](#) attaches an instance to a subnet within a VCN and is required for connectivity with other endpoints.

[Create VNIC](#)

Name	Subnet or VLAN ⓘ	State	FQDN ⓘ	VLAN tag	MAC address
Sankar OCI SBC1 (Primary VNIC)	Subnet - ACMESBC_MGMT	● Attached	sankar-oci... Show Copy	1487	02:00:17:04:19:8E
s0p0	Subnet - ACMESBC_s0p0	● Attached	-	2188	02:00:17:10:48:19
s0p1	Subnet - ACMESBC_s0p1	● Attached	-	4091	02:00:17:21:1F:2F
wancom1	Subnet - ACMESBC_wancom1	● Attached	-	3286	02:00:17:34:70:28

- As you can see above, we'll need to correct the interface to MAC address mappings for wancom1 and s0p1.
- The interface mapping branch on the SBC includes a swap command, which allows us to make those adjustments. A reboot is required for the changes to take effect.
- While in enable mode in the SBC CLI, type:

```
> # interface-mapping (enter)
> (interface-mapping)# swap wancom1 slp0
```

Changes could affect service, and Requires Reboot to become effective. Continue [y/n]?: y (enter)

Below is the output after executing the swap command which now matches VNIC details.

```
SolutionsOCISBC1# show interfaces mapping
Interface Mapping Info
-----
Eth-IF  MAC-Addr                Label
wancom0 02:00:17:04:19:8E        #present
wancom1 02:00:17:34:70:28        #generic
s0p0    02:00:17:10:48:19        #generic
s0p1    02:00:17:21:1F:2F        #generic
wancom2 FF:FF:FF:FF:FF:FF        #dummy
spare   FF:FF:FF:FF:FF:FF        #dummy
slp0    FF:FF:FF:FF:FF:FF        #dummy
slp1    FF:FF:FF:FF:FF:FF        #dummy
s0p2    FF:FF:FF:FF:FF:FF        #dummy
slp2    FF:FF:FF:FF:FF:FF        #dummy
s0p3    FF:FF:FF:FF:FF:FF        #dummy
slp3    FF:FF:FF:FF:FF:FF        #dummy

SolutionsOCISBC1# █
```

When the SBC comes back up from reboot, it is now ready for full configuration.

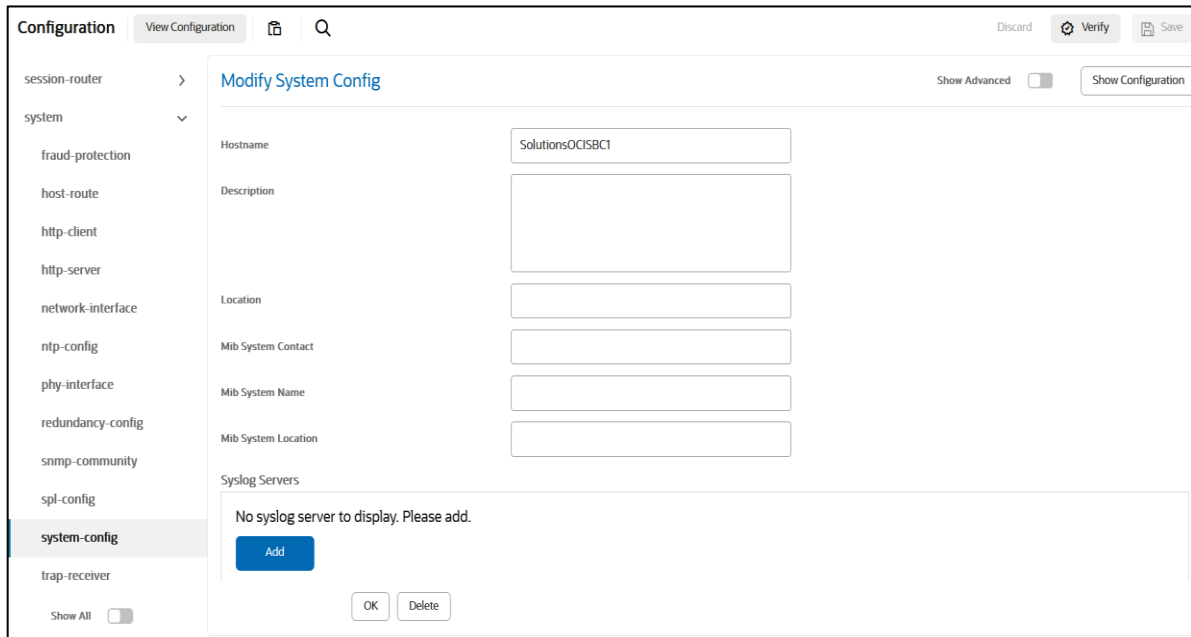
Also note that the usage of “swap” command is based on customer environment. Depending on the setup, the mapping may vary.

The interfaces should be checked and mapped in both the SBC’s (primary and secondary)

7.3. Configure system-config

For HA configuration, make sure the hostname is assigned in both primary and secondary.

In the WebGUI, Go to system->system-config



The CLI users can access the configuration by accessing configure terminal->system->system-config

```
SolutionsOCISBC1(system-config)# hostname SolutionsOCISBC1
SolutionsOCISBC1(system-config)# location Cloud
SolutionsOCISBC1(system-config)# done
```

The following configuration has to be applied only in the SBC which is going to be the Primary SBC. The configuration will be replicated later in the secondary SBC using acquire-config.

7.4. Configure Physical Interface Values

To configure physical interface values from the WebGUI, Go to system->phy-interface. Create the following physical interfaces in SBC1 from GUI as shown below:

Parameter Name	s0p0	s0p1	wancom1
Slot	0	0	0
Port	0	1	1
Operation Mode	Media	Media	Control

Configuration View Configuration [Icons] [Search] Discard Verify Save

system **Modify Phy Interface** Show Advanced [Toggle] Show Configuration

fraud-protection

host-route

http-client

http-server

network-interface

ntp-config

phy-interface

redundancy-config

snmp-community

spl-config

system-config

trap-receiver

Show All [Toggle]

Name: s0p0

Operation Type: Media

Port: 0 (Range: 0..5)

Slot: 0 (Range: 0..2)

Virtual Mac:

Duplex Mode: FULL

Speed: 100

Wancom Health Score: 50 (Range: 0..100)

OK Back

Configuration View Configuration [Icons] [Search] Discard Verify Save

media-manager >

security >

session-router >

system **Phy Interface** Show Configuration

[Icons] Delete all Phy Interface items Search [Search]

Select	Action	Name	Operation Type	Port	Slot	Virtual Mac	Admin State	Auto Negotiation
<input type="checkbox"/>	⋮	s0p0	Media	0	0		enabled	enabled
<input type="checkbox"/>	⋮	s0p1	Media	1	0		enabled	enabled
<input type="checkbox"/>	⋮	wancom1	Control	1	0		enabled	enabled

phy-interface

To configure from CLI, Go to configure terminal->system ->phy-interface

SolutionsOCISBC1# show running-config phy-interface

```

phy-interface
  name s0p0
  operation-type Media
  port 0
  slot 0
  virtual-mac
  admin-state enabled
  auto-negotiation enabled
  duplex-mode FULL
  speed 100
  wancom-health-score 50
  overload-protection disabled
  last-modified-by webHTTP-admin@209.17.43.241:55066
  last-modified-date 2024-08-08 10:27:55

```

```

phy-interface
  name s0p1
  operation-type Media
  port 1
  slot 0
  virtual-mac
  admin-state enabled
  auto-negotiation enabled
  duplex-mode FULL
  speed 100
  wancom-health-score 50
  overload-protection disabled
  last-modified-by webHTTP-admin@209.17.43.241:61998
  last-modified-date 2024-08-08 16:26:41
phy-interface
  name wancom1
  operation-type Control
  port 1
  slot 0
  virtual-mac
  admin-state enabled
  auto-negotiation enabled
  duplex-mode
  speed
  wancom-health-score 25
  overload-protection disabled
  last-modified-by webHTTP-admin@209.17.43.241:59959
  last-modified-date 2024-08-08 11:34:09
SolutionsOCISBC1#

```

7.5. Configure Network Interface Values

To configure network-interface from GUI, go to system->Network-Interface. Configure three interfaces, s0p0, s0p1 and wancom1. In the below example the s0p0 is shown. Configure the other interfaces in the same manner. Please note that these IP address should match the IP address that is assigned to the OCI VNIC configuration explained in Sec 6 of this application note document.

The table below lists the parameters, to be configured for all the interfaces and they should be modified according to the customer environment.

Name	s0p0	s0p1	Wancom1
IP address	10.0.4.50 (Private IP Address of s0p0 assigned in OCI for SBC1 instance)	10.0.6.50 (Private IP Address of s1p0 assigned in OCI for SBC1 instance)	
Pri-utility-addr	10.0.4.55 (Private IP Address of s0p0 assigned in OCI for SBC1 instance)	10.0.6.55 (Private IP Address of s1p0 assigned in OCI for SBC1 instance)	10.0.2.50 (Private IP Address of wancom1 assigned in OCI for SBC1 instance)
Netmask	255.255.255.0	255.255.255.0	

Gateway	10.0.4.1	10.0.5.1	
Sec-utility-addr	10.0.4.51 (Private IP Address of s0p0 assigned in OCI for SBC2 instance)	10.0.6.51 (Private IP Address of s1p0 assigned in OCI for SBC2 instance)	10.0.2.51 (Private IP Address of wancom1 assigned in OCI for SBC2 instance)

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The main heading is 'Modify Network Interface' for the interface 's0p0'. The configuration fields are as follows:

- Name: s0p0
- Sub Port Id: 0 (Range: 0..4095)
- Description: (Empty text area)
- Hostname: (Empty text field)
- IP Address: 10.0.4.50
- Pri Utility Addr: 10.0.4.55
- Sec Utility Addr: 10.0.4.51
- Netmask: 255.255.255.0
- Gateway: 10.0.4.1

Below the main configuration, there is a section for 'Gw Heartbeat' with the following settings:

- state: disabled
- heartbeat: 0
- retry-count: 0
- retry-timeout: 1
- health-score: 0

At the bottom, there is a 'bfd-config' section with the following settings:

- state: disabled
- health-score: 0
- options: (Empty text area)

Additional settings include 'dns-ip-primary' and 'dns-ip-backup1'.

To configure network interface through CLI, go to configure terminal->system->network-interface
SolutionsOCISBC1# show running-config network-interface

```

network-interface
  name                               s0p0
  sub-port-id                         0
  description
  hostname
  ip-address                          10.0.4.50
  pri-utility-addr                    10.0.4.55
  sec-utility-addr                    10.0.4.51
  netmask                             255.255.255.0
  gateway                             10.0.4.1
  sec-gateway
  gw-heartbeat
    state                             disabled
    heartbeat                          0
    retry-count                        0
    retry-timeout                      1
    health-score                       0
  bfd-config
    state                             disabled
    health-score                       0
    options
  dns-ip-primary
  dns-ip-backup1

```

```

dns-ip-backup2
dns-domain
dns-timeout 11
dns-max-ttl 86400
signaling-mtu 0
hip-ip-list 10.0.4.50
icmp-address
snmp-address
ssh-address
last-modified-by webHTTP-admin@209.17.43.241:55066
last-modified-date 2024-08-08 10:37:57
network-interface
name s0p1
sub-port-id 0
description
hostname
ip-address 10.0.6.50
pri-utility-addr 10.0.6.55
sec-utility-addr 10.0.6.51
netmask 255.255.255.0
gateway 10.0.6.1
sec-gateway
gw-heartbeat
state disabled
heartbeat 0
retry-count 0
retry-timeout 1
health-score 0
bfd-config
state disabled
health-score 0
options
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11
dns-max-ttl 86400
signaling-mtu 0
hip-ip-list 10.0.6.50
icmp-address
snmp-address
ssh-address
last-modified-by webHTTP-admin@209.17.43.241:55066
last-modified-date 2024-08-08 10:39:55
network-interface
name wancom1
sub-port-id 0
description
hostname
ip-address
pri-utility-addr 10.0.2.50
sec-utility-addr 10.0.2.51
netmask 255.255.255.0
gateway 10.0.2.1
sec-gateway
gw-heartbeat
state enabled
heartbeat 0
retry-count 0
retry-timeout 1
health-score 0
bfd-config
state disabled
health-score 0
options
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11

```

```

dns-max-ttl 86400
signaling-mtu 0
hip-ip-list
icmp-address
snmp-address
ssh-address
last-modified-by webHTTP-admin@209.17.43.241:64044
last-modified-date 2024-08-08 12:09:30
SolutionsOCISBC1#

```

7.6. Configure Redundancy

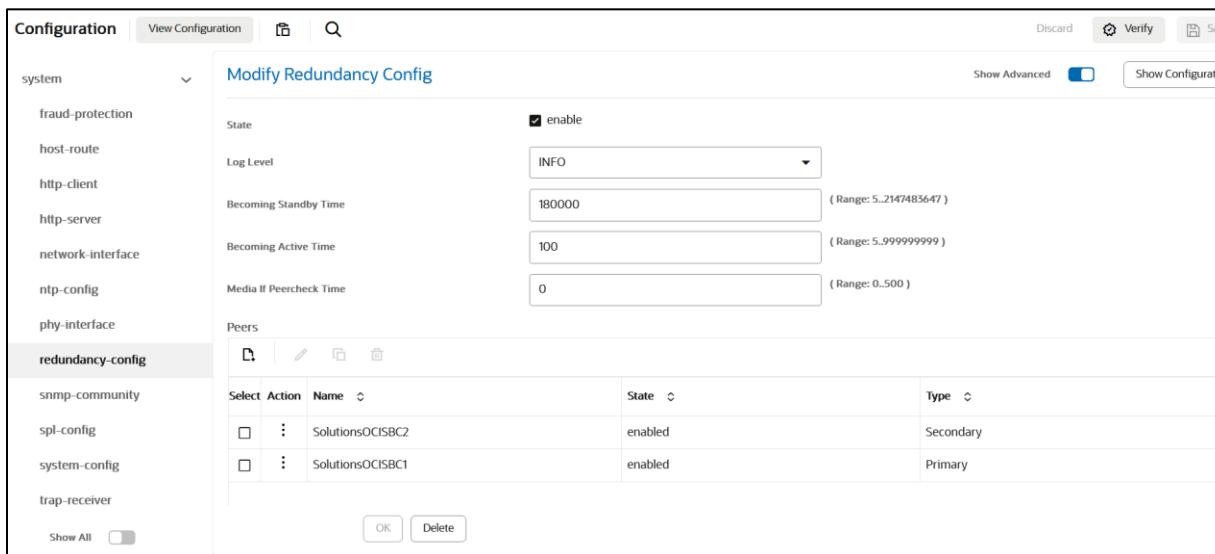
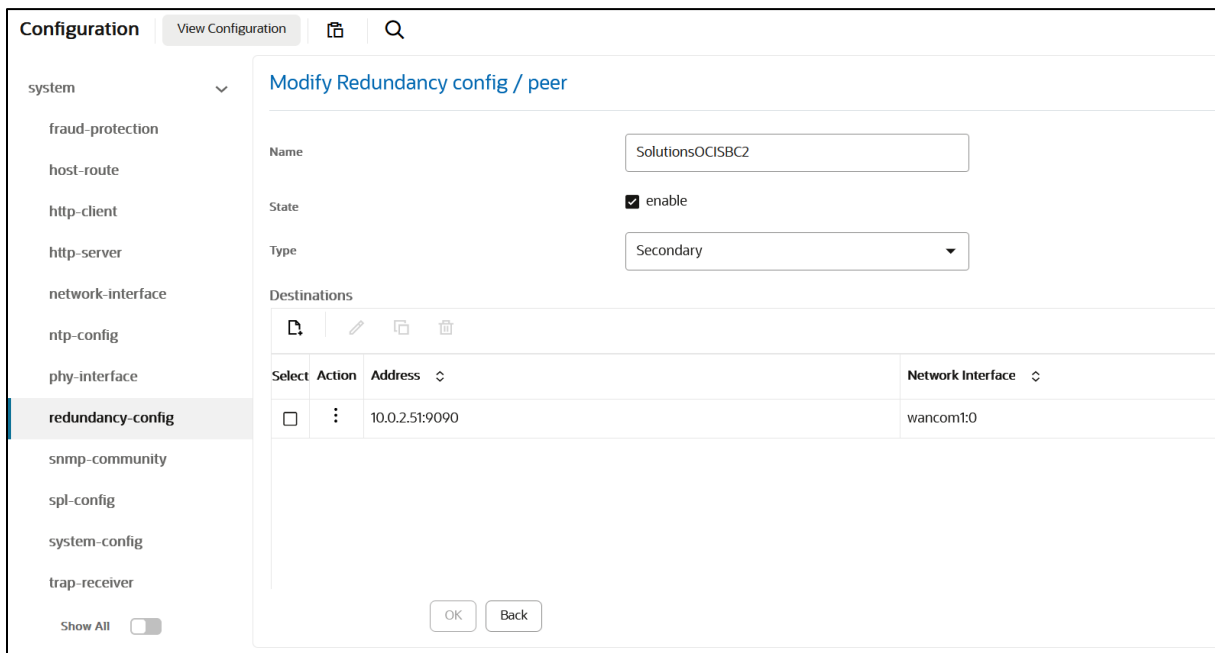
Here we assign the primary and secondary SBC's. The IP address used here are the addresses of wancom1 assigned to both SBC.

For configuring from WebGUI , go to system->redundancy-config and configure the peers.

The screenshot shows the 'Modify Redundancy config / peer' configuration page in a web interface. The left sidebar contains a navigation menu with the following items: system, fraud-protection, host-route, http-client, http-server, network-interface, ntp-config, phy-interface, **redundancy-config**, snmp-community, spl-config, system-config, and trap-receiver. The 'redundancy-config' item is highlighted. The main content area shows the configuration form for a peer named 'SolutionsOCISBC1'. The 'State' is checked and labeled 'enable', and the 'Type' is set to 'Primary'. Below the form is a table titled 'Destinations' with the following data:

Select	Action	Address	Network Interface
<input type="checkbox"/>	:	10.0.2.50:9090	wancom1:0

At the bottom of the form, there are 'OK' and 'Back' buttons.



To configure from CLI, go to conf t->system->redundancy config

SolutionsOCISBC1# show running-config redundancy-config

```

redundancy-config
state                enabled
log-level            INFO
health-threshold     75
emergency-threshold  50
port                 9090
advertisement-time   500
percent-drift        210
initial-time         1250
becoming-standby-time 180000

```

```

becoming-active-time          100
cfg-port                      1987
cfg-max-trans                 10000
cfg-sync-start-time          5000
cfg-sync-comp-time           1000
gateway-heartbeat-interval    0
gateway-heartbeat-retry       0
gateway-heartbeat-timeout     1
gateway-heartbeat-health      0
media-if-peercheck-time       0
peer
  name                        SolutionsOCISBC2
  state                       enabled
  type                         Secondary
  destination
    address                   10.0.2.51:9090
    network-interface         wancom1:0
peer
  name                        SolutionsOCISBC1
  state                       enabled
  type                         Primary
  destination
    address                   10.0.2.50:9090
    network-interface         wancom1:0

```

At this stage, we have completed the configuration in the primary SBC.

7.7. Acquiring configuration from the Primary SBC.

To configure the secondary SBC, please follow the below steps from SBC CLI mode.

- Delete configuration if any in the secondary SBC.
- Check whether the primary and secondary SBC are in ntp sync
- To acquire configuration from the primary SBC, execute the following command in the secondary SBC

SolutionsOCISBC2# acquire-config 10.0.1.202

(where 10.0.1.202 is the management interface of the primary SBC) Alternatively, we can use the Ephemeral IP assigned from the OCI VCN for that VNIC.

7.8. Switching over SBC

After configuring the SBC, check the health of the primary and secondary SBC's

SolutionsOCISBC1# show health

```

Media Synchronized           true
SIP Synchronized             true
REC Synchronized             disabled
XSERV Synchronized          disabled
Config Synchronized          true
Collect Synchronized         disabled
RADIUS CDR Synchronized     disabled
Rotated CDRs Synchronized   disabled
IPSEC Synchronized          disabled

```



```

Iked Synchronized           disabled
Lbpd Synchronized           disabled
tCCD Synchronized           disabled
Service Health Synchronized true
Active Peer Address

Redundancy Protocol Process (v3):
  State                       Active
  Health                       100
  Lowest Local Address         10.0.2.50:9090
  1 peer(s) on 1 socket(s):
  SolutionsOCISBC2: v3, Standby, health=100, max silence=1050
    last received from 10.0.2.51 on wancom1:0

Switchover log:

SolutionsOCISBC2# show health

Media Synchronized           true
SIP Synchronized             true
REC Synchronized             disabled
XSERV Synchronized           disabled
Config Synchronized          true
Collect Synchronized          disabled
RADIUS CDR Synchronized      disabled
Rotated CDRs Synchronized    disabled
IPSEC Synchronized           disabled
Iked Synchronized           disabled
Lbpd Synchronized           disabled
tCCD Synchronized           disabled
Service Health Synchronized true
Active Peer Address         10.0.2.50

Redundancy Protocol Process (v3):
  State                       Standby
  Health                       100
  Lowest Local Address         10.0.2.51:9090
  1 peer(s) on 1 socket(s):
  SolutionsOCISBC1: v3, Active, health=100, max silence=1050
    last received from 10.0.2.50 on wancom1:0

Switchover log:

```

We can switchover the SBC's by using the following command.

SolutionsOCISBC1# notify berpd force

Now the active SBC becomes standby and vice-versa.

8. Deploying SBC behind the OCI-NAT

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

Here, the SBC is placed behind the OCI NAT. The SBC behind SPL NAT plugin is essential for proper signaling and voice path between the SBC deployed on OCI cloud and PSTN

The plug-in changes information in SIP messages to hide the end point located inside the private network of OCI SBC. Configure the Support for SBC Behind NAT SPL plug-in for each SIP interface on the SBC. One public-private address pair is 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 reserved public IP address configured in OCI Cloud for particular network interface.

Here is an example configuration with SBC Behind NAT SPL config. The SPL is applied to the s0p0 interface. To configure SBC Behind NAT SPL Plug in using the GUI,

Go to session-router->sip-interface->spl-options.

Input the following value, save and activate.

The below value given in the screen is just an example and the users can give this value according to their network configuration.

The format of SPL option is given as below.

HeaderNatPublicSipIfIp=<Reserved Public IP of the s0p0 interface>

HeaderNatPrivateSipIfIP =<Private IP of the s0p0interface >

The screenshot shows the 'Add SIP Interface' configuration page. The 'SPL Options' field is highlighted with a red box and contains the text 'HeaderNatPublicSipIflp=20.110.135.150,HeaderNatPri'. Other fields include 'Secured Network' (checkbox), 'Uri Fqdn Domain', 'Options', 'Trust Mode' (dropdown), 'Max Nat Interval' (3600), 'Stop Recurse' (401,407), 'Port Map Start' (0), 'Port Map End' (0), and 'In Manipulationid' (dropdown). Buttons for 'OK' and 'Back' are at the bottom.

To configure header NAT SPL from ACLI

ACLI Path: config t→**session-router**→**sip-interface**

Choose the sip interface on which the header NAT SPL needs to be applied under spl-options.
Add the entry as per example shared below.

spl-options

HeaderNatPublicSipIflp=20.110.135.150,HeaderNatPrivateSipIflp=10.0.4.60



CONNECT WITH US

-  blogs.oracle.com
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com/

Oracle Corporation, World Headquarters

2300 Oracle Way
Austin, TX 78741, USA

Worldwide Inquiries

Phone: +1.650.506.7000 or
Phone: +1.800.392.2999

Integrated Cloud Applications & Platform Services

Copyright © 2024, 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