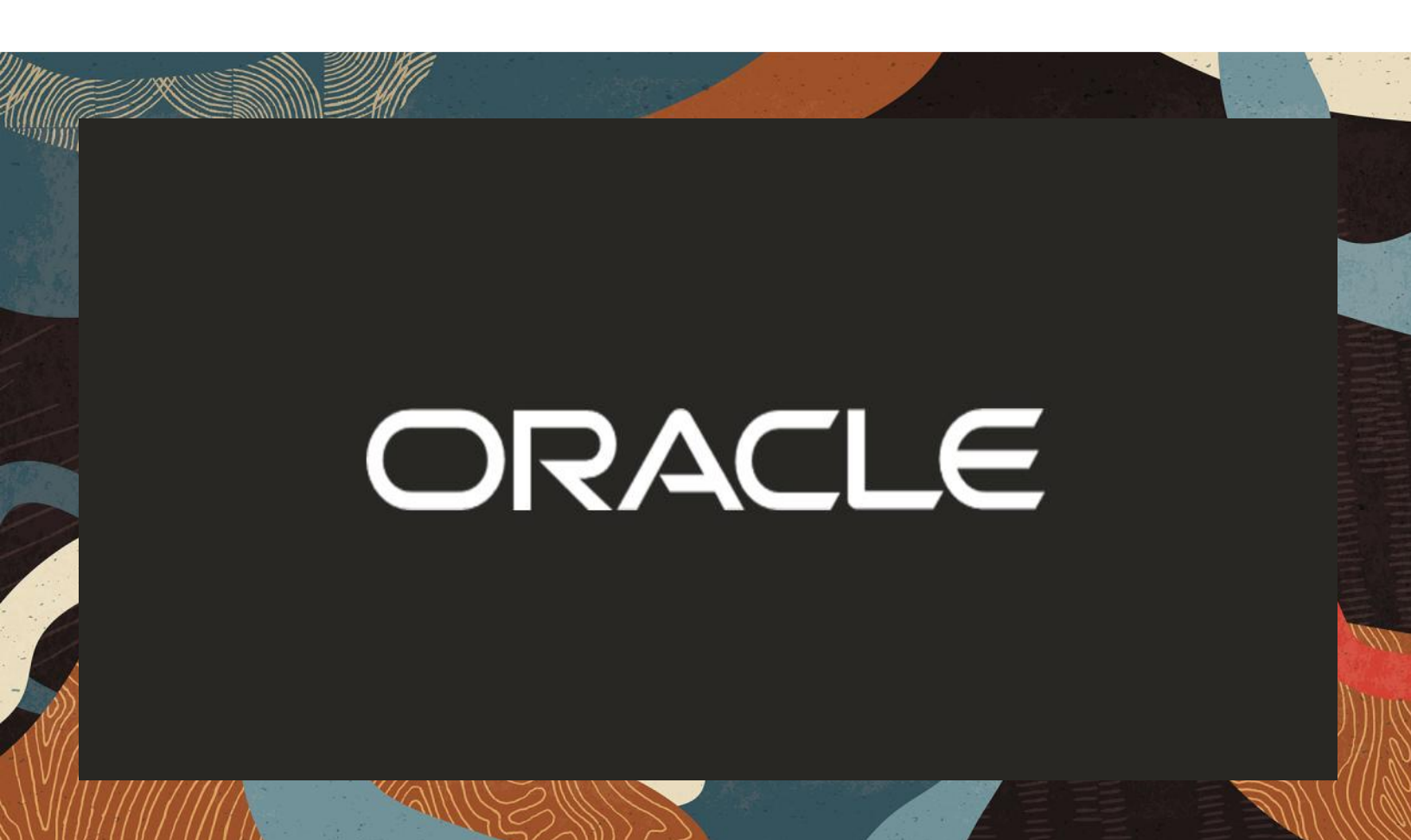




ORACLE

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
4.0	Added Section 8 for Layer 2 High Availability	24-08-2026

Table of Contents

DEPLOYING ORACLE SBC WITH HIGH AVAILABILITY IN ORACLE CLOUD INFRASTRUCTURE	1
1. INTRODUCTION	5
2. DOCUMENT OVERVIEW	5
3. RELATED DOCUMENTATION	5
3.1 ORACLE SBC.....	5
3.2 ORACLE CLOUD INFRASTRUCTURE	5
4. REQUIREMENTS	5
5. CREATE AND DEPLOY ON OCI	6
5.1 PREREQUISITES	6
5.2 SELECTING A REGION	6
5.3 SETTING UP/PICKING A COMPARTMENT	6
5.4 CREATING DYNAMIC GROUPS AND POLICY	7
5.5 SETTING UP NETWORKING	8
5.6 SUBNETS.....	16
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.....	25
6.3 ASSIGNING UTILITY ADDRESSES FROM OCI.....	26
7. CONFIGURING SBC FOR HA IN OCI	28
7.1. CONFIGURE SBC USING WEB GUI	31
7.2. INTERFACE MAPPING	33
7.3. CONFIGURE SYSTEM-CONFIG	34
7.4. CONFIGURE PHYSICAL INTERFACE VALUES	35
7.5. CONFIGURE NETWORK INTERFACE VALUES	36
7.6. CONFIGURE REDUNDANCY	40
7.7. ACQUIRING CONFIGURATION FROM THE PRIMARY SBC.	43
7.8. SWITCHING OVER SBC.....	44
8. LAYER 2 HIGH AVAILABILITY	45
8.1. PREREQUISITES AND CAVEATS	45
8.2. CREATE THE OCI VLAN	46
8.3. ATTACH VLAN-BACKED VNICs TO THE SBC	47
8.4. EXTERNAL ACCESS FOR VLAN MEDIA INTERFACES	48
8.5. SBC CONFIGURATION NOTES FOR LAYER 2HA.....	51
9. DEPLOYING SBC BEHIND THE OCI-NAT	51



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.

The screenshot shows the Oracle Cloud Identity console. The top navigation bar includes the Oracle Cloud logo, a search bar, and the region 'US East (Ashburn)'. The left sidebar contains a menu with 'Overview' selected, along with 'Domains', 'Network Sources', 'Policies', 'Compartments', and 'Federation'. The main content area is titled 'Overview' and features a 'Choose a compartment' section. This section includes a visual representation of a compartment filter and text instructions: 'Create compartments to organize your resources.' and 'View and manage your resources: choose a compartment and resource type using'. Below this, a 'List scope' section shows a search for 'vsbc' with a dropdown menu listing 'oraclegbudevcorp (root)', 'CGBU_vSBC_CMP1', and 'CGBU_vSBC_CMP2'. A note at the bottom states 'no tag filters applied'.

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.

The screenshot shows the 'Dynamic Group Details' page in the Oracle Cloud Identity console. The page title is 'Identity » Dynamic Groups » Dynamic Group Details'. The main content area features a large green circle with 'DG' inside, representing the dynamic group. To the right of the circle, the group name 'CGBU_vSBC_sbc-access' is displayed, along with a 'Delete' button. Below the name, the 'OCID' is shown as '...jbg03a' with a 'Show Copy' link, and the 'Created' timestamp is 'Wed, 28 Nov 2018 17:07:47 GMT'. A 'Description' field states 'SBC instance access to OCI services'. The left sidebar shows 'Resources' with 'Matching Rules (1)' selected. The main content area also has a 'Matching Rules' section, displaying one rule: 'instance.compartment.id = 'ocid1.compartment.oc1..aaaaaaa6pylpa3blzy5csm5xw2e5tzine24vtvqpguepm7g45r4rr7cla''. A button 'Edit All Matching Rules' is visible, and a note states 'Instances that meet the criteria defined by any of these rules will be included in the group'.

Create Policy

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

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

NAME
CGBU_vSBC_sbc_access_policy

DESCRIPTION
Policy to allow SBC instances to work with vNICs

Policy Versioning
☒ KEEP POLICY CURRENT
☐ USE VERSION DATE

Policy Statements

STATEMENT 1
Allow dynamic-group CGBU_vSBC_sbc-access to use private-ips in compartment CGBU_vSBC_CMP1

STATEMENT 2
Allow dynamic-group CGBU_vSBC_sbc-access to use vnics in compartment CGBU_vSBC_CMP1

STATEMENT 3
Allow dynamic-group CGBU_vSBC_sbc-access to use vnic-attachments in compartment CGBU_vSBC_CMP1

[+ Add Statement](#)

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 (apply a free-form tag)		

[+ Additional Tag](#)

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

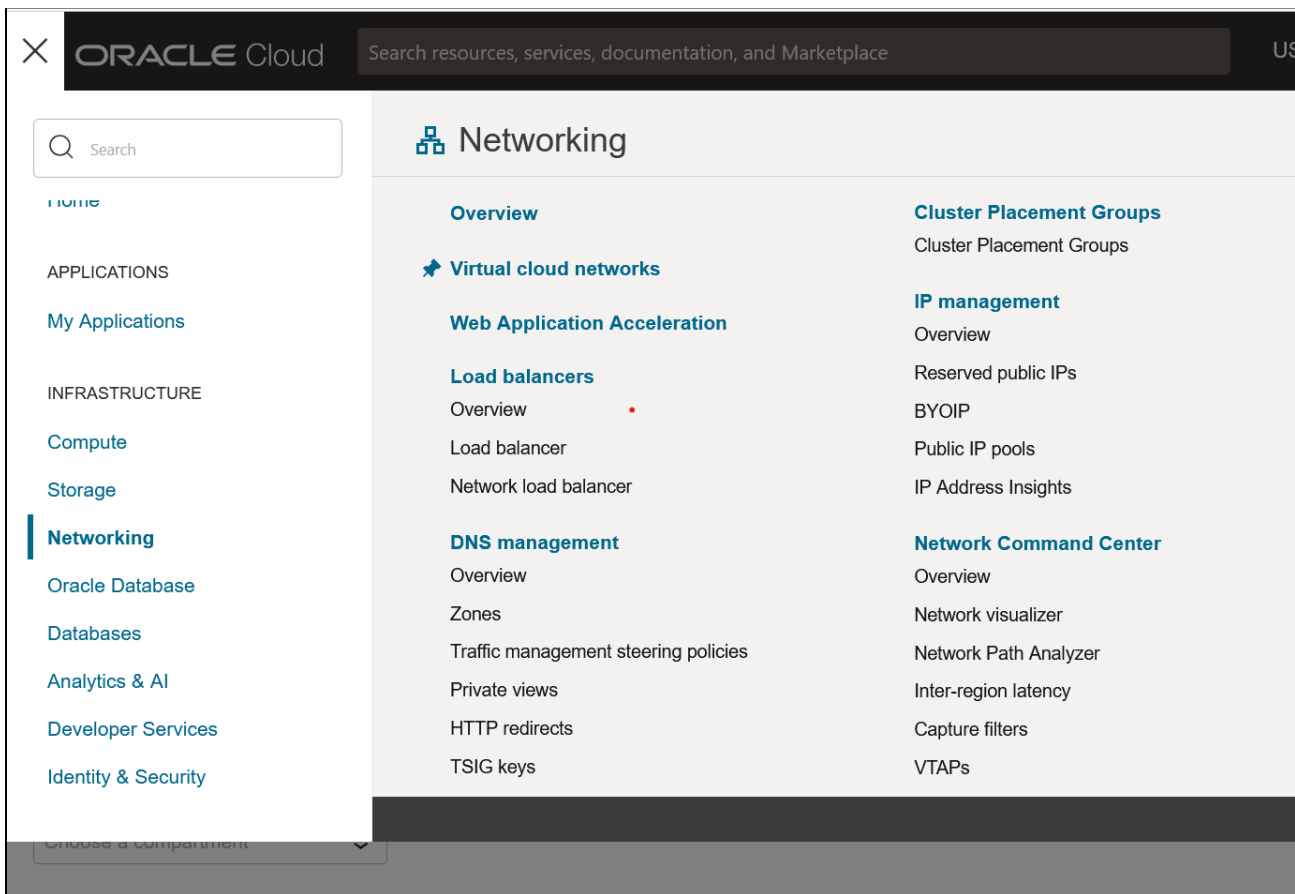
To setup networking on Oracle cloud, you have to create a Virtual Cloud Network (VCN) ,with all its resources.

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.

Network Security Groups (0)

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(wancomo)
- A route table with internet gateway added for media

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

ORACLE Cloud

Search resources, services, documentation, and Marketplace

US East (Ashburn)

RT

AVAILABLE

Default Route Table for vcn20190624063035

Move resource

Add tags

Terminate

Route Table Information

Tags

OCID: ...f3337a Show Copy

Compartment: CGBU_vSBC_CMP1

Created: Mon, Jun 24, 2019, 06:30:35 UTC

Resources

Route Rules (1)

Route Rules

Traffic within the VCN is handled by the VCN's local routing by default. Intra-VCN routing allows you more control over routing between subnets. [Learn more](#). If you're having problems, use [Network Path Analyzer](#) to check your connections.

Add Route Rules

Edit

Remove

☐	Destination	Target Type	Target	Route Type	Description
☐	0.0.0.0/0	Internet Gateway	Internet Gateway vcn20190624063035	Static	

0 selected

Showing 1 item < 1 of 1 >

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

ORACLE Cloud

Applications >

US East (Ashburn)

Resources

DHCP Options (1)

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.

5.5.6 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
SNMPTrap	162
Diameter	3868
Radius	1812

Protocol	Port
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

MGMT_SL

CREATE IN COMPARTMENT

CGBU_vSBC_CMP1

oraclegbudevcorp (root)/CGBU_vSBC_CMP1

Allow Rules for Ingress

Ingress Rule 2

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

☐ STATELESS ⓘ

SOURCE TYPE SOURCE CIDR IP PROTOCOL ⓘ

CIDR 0.0.0.0/0 TCP

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

SOURCE PORT RANGE OPTIONAL ⓘ DESTINATION PORT RANGE OPTIONAL ⓘ

All 22,3868,1812,443,80,49

Examples: 80, 20-22 Examples: 80, 20-22

Ingress Rule 3

Ingress Rule 1

Allows ICMP traffic for: all types and codes

☐ STATELESS ⓘ

SOURCE TYPE

CIDR

SOURCE CIDR

0.0.0.0/0

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

IP PROTOCOL ⓘ

ICMP

TYPE OPTIONAL ⓘ

All

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

CODE OPTIONAL ⓘ

All

Ingress Rule 2

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

14 | Page

Add Egress Rules
cancel

Egress Rule 1

All traffic for all ports

☐ STATELESS ⓘ

DESTINATION TYPE

CIDR

DESTINATION CIDR

0.0.0.0/0

IP PROTOCOL ⓘ

All Protocols

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

+ 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

None (add a free-form tag)

TAG KEY

VALUE

+ Additional Tag

Create Security List
Cancel

5.5.6.1 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(accordingtosteeringpoolconfig)

5.5.6.2 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 gogo 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 (wancomo), HA (wancom1/wancom2) and Media (sopo, s1po 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

- wancomo
- wancom1
- Network interfaces (sopo, s1po) (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
wancomo	Regional	yes	yes	n/a
sopo,sop1	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.

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

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)

SECURITY LIST

ACMESBC-MGMT-SL

⌵

✕

+ Additional Security List

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

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.

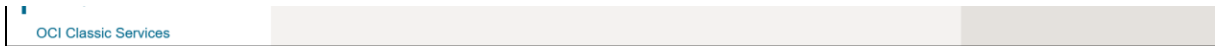
The supported VM shapes are listed as below:

Figure 1. Table 1 Supported VM shapes

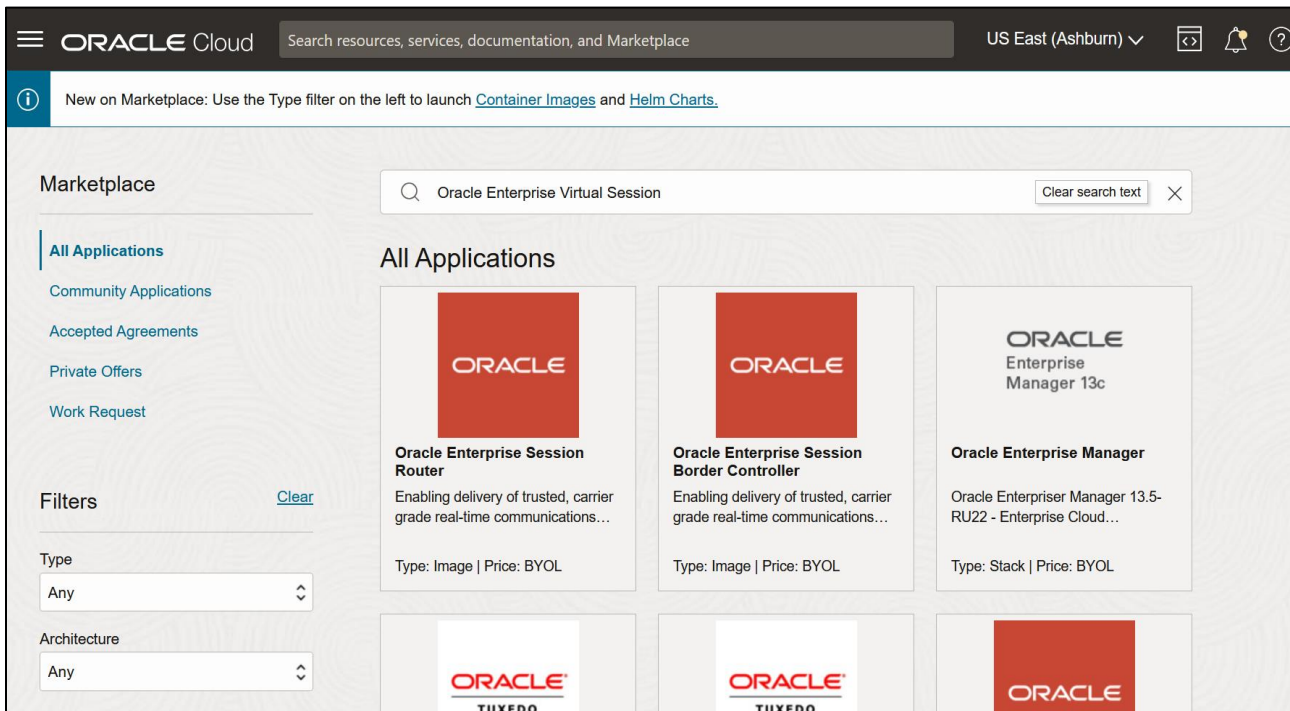
Shape	Supported	OCPUs/VCPUs	vNICs	Tx/Rx Queues	MAX Forwarding Cores	DOS Protection
VM.Standard1.1	N	1/2	2	2	0	N
VM.Standard1.2	Y	2/4	2	2	1	N
VM.Standard1.4	Y	4/8	4	2	2	Y
VM.Standard1.8	Y	8/16	8	2	2	Y
VM.Standard1.16	Y	16/32	16	2	2	Y
VM.Standard2.1	N	1/2	2	1	0	N
VM.Standard2.2	Y	2/4	2	1	1	N
VM.Standard2.4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

Search resources, services, documentation, and Marketplace

US East (Ashburn)

Marketplace > Oracle Enterprise Session Border Controller

Oracle Enterprise Session Border Controller

Enabling delivery of trusted, carrier grade real-time communications across IP networks

The Oracle Enterprise SBC protects IP Communications networks from cyber-threats, fraud and cures interoperability problems so that the users can enjoy highly secure and reliable voice, video and unified communications services.

Categories: Networking, Security

Type

Image

Version

9.2.0.0.7 (7/6/2024) - ...

Compartment

CGBU_vSBC_CMP1

oraclegbudevcorp (root)/CGBU_vSBC_CMP1

☒ I have reviewed and accept the [Oracle standard Terms and Restrictions](#).

Launch Instance

Reminder: Patch the instance once installed.

Software price per OCPU

BYOL

(Bring your own license)

There are additional fees for the infrastructure usage.

Overview

Provider

More apps

Usage instructions

- Populate Name for your instance
- Select "Availability Domain" and the "Instance Type" and fault Domain.

Search resources, services, documentation, and Marketplace

US East (Ashburn)

Create compute instance

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

Name

Solutions OCI SBC1

Create in compartment

CGBU_vSBC_CMP1

oraclegbudevcorp (root)/CGBU_vSBC_CMP1

Placement

[Collapse](#)

The availability domain helps determine which shapes are available.

Availability domain

AD 1

bwAI:US-ASHBURN-AD-1

AD 2

bwAI:US-ASHBURN-AD-2

AD 3

bwAI:US-ASHBURN-AD-3

[Show advanced options](#)

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

Create compute instance

Availability domain

AD 1
bwAI:US-ASHBURN-AD-1 ✓

AD 2
bwAI:US-ASHBURN-AD-2

AD 3
bwAI:US-ASHBURN-AD-3

[Hide advanced options](#)

Capacity type

☒ On-demand capacity
Place the instance on a shared host using on-demand capacity.

☐ Preemptible capacity
Place the instance on a shared host using [preemptible capacity](#). This instance can be reclaimed at any time.

☐ Capacity reservation
Place the instance on a shared host, and have it count against a [capacity reservation](#).

☐ Dedicated host
Place the instance on a [dedicated virtual machine host](#).

☐ Compute cluster
Place the instance on a remote direct memory access (RDMA) network, called a [compute cluster](#).

☐ Cluster placement group

Fault domain

FAULT-DOMAIN-1

[When should I specify a fault domain?](#)

Create Save as stack Cancel

- Choose the appropriate shape.

ORACLE Cloud Search resources, services, documentation, and Marketplace US East (Ashburn) < > 🔔 ?

Create compute instance

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

Image

Oracle Enterprise Session Border Controller
 Enabling delivery of trusted, carrier grade real-time communications across IP networks

Return to Marketplace

Shape

VM.Standard.E4.Flex
 Virtual machine, 1 core OCPU, 16 GB memory, 1 Gbps network bandwidth

Change shape

Create Save as stack Cancel

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

Create compute instance

Primary network

☒ Select existing virtual cloud network
 ☐ Create new virtual cloud network
 ☐ Enter subnet OCID

VCN in **CGBU_vSBC_CMP1** [\(Change compartment\)](#)

ACMESBC_VCN

Subnet

An IP address from a public subnet and an [internet gateway](#) on the VCN are required to make this instance accessible from the internet.

☒ Select existing subnet
 ☐ Create new public subnet

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

ACMESBC_MGMT (regional)

Primary VNIC IP addresses

Private IPv4 address

[Cancel](#)

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

US East (Ashburn) ▾

Create compute instance

ACMESBC_MGMT (regional)

Primary VNIC IP addresses

Private IPv4 address

☒ Automatically assign private IPv4 address
 ☐ Manually assign private IPv4 address

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.

IPv6 addresses

☐ Assign IPv6 addresses from subnet prefixes
You can only assign one IPv6 address per subnet prefix at first instance creation. Subnets can have more than one IPv6 prefix.

The selected VCN and subnet combination does not support IPv6 addresses. You must enable IPv6 addressing on the VCN and subnet before you can assign IPv6 addresses to this instance.

[Cancel](#)

Paste the public key in ssh keys



Create compute instance

Add SSH keys

Generate an [SSH key pair](#) to connect to the instance using a Secure Shell (SSH) connection, or upload a public key that you already have.

☐ Generate a key pair for me
 ☐ Upload public key files (.pub)
 ☒ Paste public keys
 ☐ No SSH keys

SSH keys

×

+ Another key

Example: ssh-rsa AAAAB3Nza...NWap6Prb ssh-key-2021-01-27 [See all supported key types](#)

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



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)

⌵

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 **Balanced**

⌵
10
120
⌵

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

Target volume performance

IOPS: 4800 IOPS

Throughput: 38.4 MB/s

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 ▾						
☐	Name	State	Public IP	Private IP	Shape	OCPU count	Memory (GB)	Avail
☐	Solutions OCI SBC2	● Running	144.25.90.73	10.0.1.146	VM.Standard2.4	4	60	AD-1
☐	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.

ORACLE Cloud

Search resources, services, documentation, and Marketplace

US East (Ashburn) ▾

🔍 🔔 ?

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



AVAILABLE

wancom0

Add tags

VNIC Information

Tags

VNIC Information

OCID: ...s5zvda [Show](#) [Copy](#)

Created: Sat, Mar 12, 2022, 18:41:02 UTC

Compartment: oraclebudevcorp (root)/CGBU_vSBC_CMP1

Subnet: [ACMESBC_MGMT](#)

Primary IP Information

Private IP Address: 10.0.1.100

Private IP OCID: ...w36diq [Show](#) [Copy](#)

Assigned: Sat, Mar 12, 2022, 18:41:03 UTC

Network Security Groups: - [Edit](#)

Skip Source/Destination Check: No

MAC Address: 02:00:17:01:01:A7

VLAN Tag: 446

Fully Qualified Domain Name: solutionslab-teams-sbc2... [Show](#) [Copy](#)

Public IP Address: 144.25.43.160 (Ephemeral)

Public IP OCID: ...iibdua [Show](#) [Copy](#)

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.

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 sopo) and go to IP address
- Click on the edit option and assign reserved public IP

Edit Private IP Address

[Help](#)

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 ⓘ: <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



Update

[Cancel](#)

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.

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	⋮

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 sopo media interface of Primary SBC.

Please note that these IP address has to be assigned in the SBC network interface for media-interfaces.

ORACLE Cloud

Search resources, services, documentation, and Marketplace

US East (Ashburn)

Compute

Instances

Instance Details

Attached VNICs

VNIC Details

V

AVAILABLE

Delete

Add tags

VNIC Information

Tags

VNIC Information

OCID: ...5lpquq Show Copy

Created: Wed, Aug 7, 2024, 11:28:50 UTC

Compartment: oraclegbudevcorp (root)/CGBU_vSBC_CMP1

Subnet: ACMESBC_s0p0

Skip Source/Destination Check: Yes

MAC Address: 02:00:17:10:48:19

VLAN Tag: 2188

Primary IP Information

Private IP Address: 10.0.4.50

Private IP OCID: ...l6b2dq Show Copy

Assigned: Wed, Aug 7, 2024, 11:28:48 UTC

Network Security Groups: - Edit

Fully Qualified Domain Name: -

Public IP Address: (Not Assigned)

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.

ORACLE Cloud

Search resources, services, documentation, and Marketplace

US East (Ashburn)

Compute

Instances

Instance Details

Attached VNICs

VNIC Details

V

AVAILABLE

Delete

Add tags

VNIC Information

Tags

VNIC Information

OCID: ...xdkkca Show Copy

Created: Wed, Aug 7, 2024, 11:37:06 UTC

Compartment: oraclegbudevcorp (root)/CGBU_vSBC_CMP1

Subnet: ACMESBC_s0p0

Skip Source/Destination Check: No

MAC Address: 02:00:17:0B:E4:4C

VLAN Tag: 2022

Primary IP Information

Private IP Address: 10.0.4.51

Private IP OCID: ...rbk5uq Show Copy

Assigned: Wed, Aug 7, 2024, 11:37:04 UTC

Network Security Groups: - Edit

Fully Qualified Domain Name: -

Public IP Address: (Not Assigned)

Pv4 Addresses

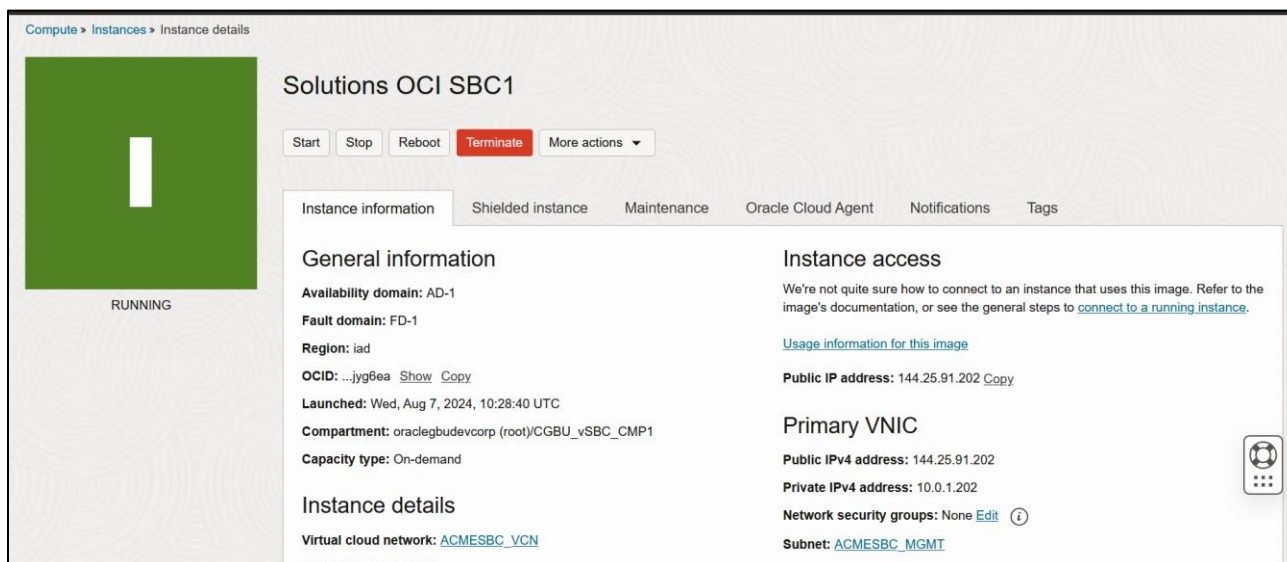
Assign Secondary Private IP Address				
Private IP Address	Public IP Address	Fully Qualified Domain Name	Assigned	
10.0.4.51 (Primary IP)	(Not Assigned)	-	Wed, Aug 7, 2024, 11:37:06 UTC	
Showing 1 item				

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



The screenshot shows the OCI Instance details page for 'Solutions OCI SBC1'. The instance is in a 'RUNNING' state, indicated by a green square icon. The page is divided into several sections: 'General information' (Availability domain: AD-1, Fault domain: FD-1, Region: iad, OCID: ...jyg6ea, Launched: Wed, Aug 7, 2024, 10:28:40 UTC, Compartment: oraclegbudevcorp (root)/CGBU_vSBC_CMP1, Capacity type: On-demand), 'Instance details' (Virtual cloud network: ACMESBC_VCN, Launch mode: NATIVE), 'Instance access' (Public IP address: 144.25.91.202, Private IP address: 10.0.1.202, Network security groups: None), and 'Primary VNIC' (Public IPv4 address: 144.25.91.202, Private IPv4 address: 10.0.1.202, Subnet: ACMESBC_MGMT). The 'Instance access' section also includes a link to 'Usage information for this image' and a note about connecting to the instance.

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.



```
Password:
%
% 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:

Password is acceptable.
```

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.

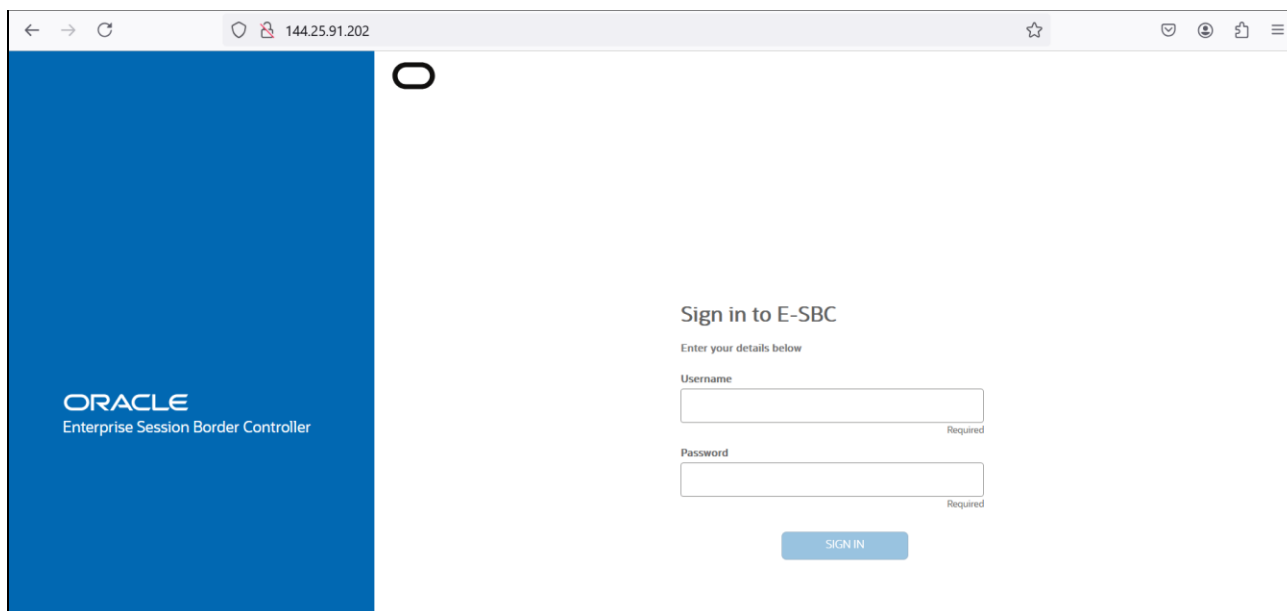
Go to configure terminal->system->http-server-config. Enable the http-server-config to access the SBC using Web GUI. Save and activate the config and the config looks as shown below.

```
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.



← → ↻ 🔒 144.25.91.202 ☆ 📧 🏠 ☰

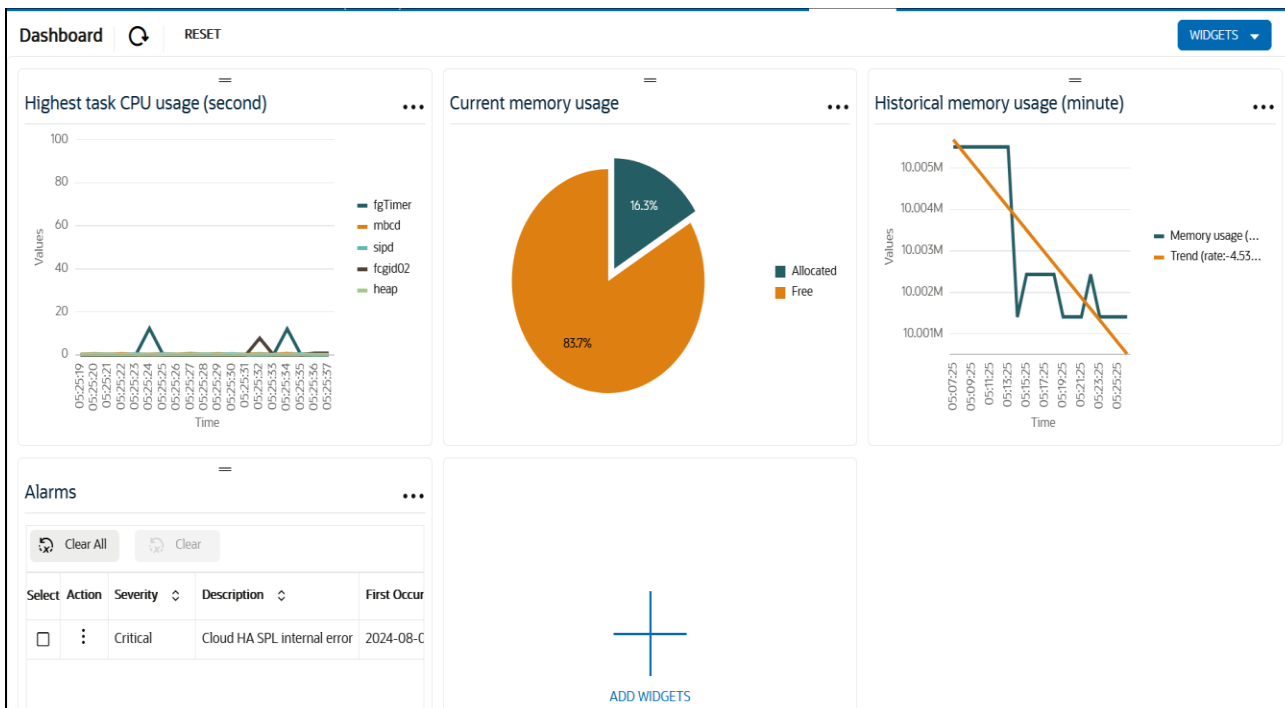
ORACLE
Enterprise Session Border Controller

Sign in to E-SBC
Enter your details below

Username Required

Password Required

SIGN IN



Go to Configuration as shown below, to configure the SBC

Configuration View Configuration Discard Verify Save

media-manager >

security >

session-router >

system >

Configuration Objects

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

Showing 1 - 14 of 40

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 interface 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 sop1.
- 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 s1p0

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 screenshot shows the 'Modify System Config' page in the WebGUI. The left sidebar has a tree view with 'system-config' selected. The main area contains the following fields and sections:

- Hostname:** SolutionsOCISBC1
- Description:** (empty text area)
- Location:** (empty text field)
- Mib System Contact:** (empty text field)
- Mib System Name:** (empty text field)
- Mib System Location:** (empty text field)
- Syslog Servers:**
 - Message: No syslog server to display. Please add.
 - Button: Add
- Buttons:** OK, Delete

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	sopo	sop1	wancom1
Slot	0	0	0
Port	0	1	1
Operation Mode	Media	Media	Control

Show All

OKBack

phy-interface

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

SolutionsOCISBC1# show running-config phy-interface

phy-interface

name sopo

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 sop1

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, sopo, sop1 and wancom1. In the below example the sopo 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	sopo	sop1	Wancom1
IP address	10.0.4.50 (PrivateIP	10.0.6.50 (PrivateIP Address	

Name	sopo	sop1	Wancom1
	Address of sopo assigned in OCI for SBC1 instance)	of s1po assigned in OCI for SBC1 instance)	
Pri-utility-addr	10.0.4.55 (PrivateIP Address of sopo assigned in OCI for SBC1 instance)	10.0.6.55 (PrivateIP Address of s1po assigned in OCI for SBC1 instance)	10.0.2.50(PrivateIP 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 (PrivateIP Address of sopo assigned in OCI for SBC2 instance)	10.0.6.51 (PrivateIP Address of s1po assigned in OCI for SBC2 instance)	10.0.2.51(PrivateIP Address of wancom1 assigned in OCI for SBC2 instance)

ORACLE Enterprise Session Border Controller

SolutionsOCIS... 10.01.202 SCZ92.0 Patch 7 (Build 240)

Dashboard Configuration Monitor and Trace Widgets System

Configuration View Configuration

media-manager >
security >
session-router >
system >
fraud-protection >
host-route >
http-client >
http-server >
network-interface
ntp-config >
phy-interface >
redundancy-config >
snmp-community >
spl-config >
system-config >
trap-receiver >

Modify Network Interface

Name: sop0

Sub Port Id: 0 (Range: 0..4095)

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

▼ Gw Heartbeat

Show Advanced Show Configuration

OK Back

To configure network interface through CLI, go to configure terminal->system->network-interface

SolutionsOCISBC1# show running-config network-interface

network-interface

name sop0

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 o
retry-count o
retry-timeout 1
health-score o
bfd-config
state disabled
health-score o
options
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11
dns-max-ttl 86400
signaling-mtu o
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 sop1
sub-port-id o
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 o
retry-count o
retry-timeout 1
health-score o
bfd-config
state disabled
health-score o
options
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout 11
dns-max-ttl 86400
signaling-mtu o
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 o
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.

Configuration

View Configuration



system



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



Modify Redundancy config / peer

Name

SolutionsOCISBC1

State

☒ enable

Type

Primary

Destinations



Select

Action

Address



Network Interface



10.0.2.50:9090

wancom1:0

OK

Back

Configuration

View Configuration

system

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

Modify Redundancy config / peer

Name

SolutionsOCISBC2

State

☒ enable

Type

Secondary

Destinations

Select	Action	Address	Network Interface
☐	:	10.0.2.51:9090	wancom1:0

OKBack

Configuration

View Configuration

Discard

Verify

Save

system

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

Modify Redundancy Config

Show Advanced

Show Configuration

State

☒ enable

Log Level

INFO

Becoming Standby Time

180000

(Range: 5..2147483647)

Becoming Active Time

100

(Range: 5..999999999)

Media If Peercheck Time

0

(Range: 0..500)

Peers

Select	Action	Name	State	Type
☐	:	SolutionsOCISBC2	enabled	Secondary
☐	:	SolutionsOCISBC1	enabled	Primary

OKDelete

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. Layer 2 High Availability

Layer 2 Network Virtualization is the recommended OCI design for SBC HA media interfaces where the feature is enabled in the tenancy. In this model, OCI VLANs provide Layer 2 network virtualization for the SBC media-side VNICs and the SBC owns the IP addressing used on those interfaces.

Configure wancomo and wancom1/wancom2 interfaces with regular OCI subnets as described in the earlier deployment sections. Configure media interfaces such as s0p0 and s0p1 with OCI VLAN-backed VNICs. No special SBC HA configuration is required for Layer 2 Network Virtualization beyond the existing HA configuration, but the OCI VLAN and SPL caveats below must be followed.

VLAN-backed VNIC list for SBC media interfaces.

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.							
Search and Filter Search Create VNIC Grid							
Name	Subnet or VLAN	Subnet/VLAN link	State	Route table	FQDN	VLAN tag	MAC address
s1p0-Internal	VLAN	Media-Internal	Attached	—	—	2360	02:00:17:0D:19:4C
s0p0-External	VLAN	Media-External	Attached	—	—	2189	02:00:17:0D:F2:E3
wancom1	Subnet	HA	Attached	Default Route Table for session-delivery	—	1034	02:00:17:05:88:DD
SBC-9.0p1 Primary VNIC	Subnet	Management	Attached	Default Route Table for session-delivery	...clevcn.com	3505	02:00:17:0D:FF:F0
Previous Next Page 1 of 1 (1 - 4 of 4 total items) Items per page 25							

8.1. Prerequisites and caveats

- The OCI Layer 2 Network Virtualization feature must be enabled by OCI Product Management for the customer tenancy because the feature is under Controlled Availability. OCI has special dispensation to use it for SBC deployments.
- OCI does not support a virtual MAC address for this deployment model. Leave the virtual-mac field blank on all phy-

interface elements.

- The Layer 3 API HA SPL can periodically raise alarms when Layer 2 Network Virtualization is used. These alarms do not affect HA operation, but the SPL should be disabled when the deployment uses Layer 2 HA.

Disable the OCI HA SPL with the following configuration:

spl-config

spl-options

plugins

state disabled

name OCIHAClient.1.o.spl

8.2. Create the OCI VLAN

Create one OCI VLAN for each required media Layer 2 segment. Choose an unused CIDR block and select whether the VLAN should be regional or availability-domain specific. For SBC HA deployments, use a regional VLAN unless the customer design requires AD-specific placement.

Under the VCN, select VLANs and click Create VLAN. If the Create VLAN button is greyed out, the tenancy does not yet have Layer 2 Network Virtualization enabled.

Create VLAN from the VCN VLANs page.

Virtual Cloud Networks

session-delivery Available

Virtual Cloud Network

Details IP administration Subnets Gateways Routing Private service access Security **VLANs** Work requests Tags

VLANs

VLAN Description: A virtual local area network (VLAN) is a broadcast domain within a VCN created by partitioning and isolating a network at the data link layer (layer 2). VLANs work by using IEEE 802.1Q VLAN tags. A VLAN is analogous to a subnet, which partitions the VCN at the network layer (layer 3).

Search and Filter

Applied filters: Compartment **Session-Delivery**

Create VLAN

Name	State	IEEE 802.1Q VLAN Tag	VLAN Gateway CIDR	Created
Media-External	Available	3892	172.16.33.0/24	Sep 15, 2021, 09:00:51 UTC
Media-Internal	Available	3718	172.16.32.0/24	Sep 15, 2021, 08:57:35 UTC

Page 1 of 1 (1 - 2 of 2 total items)

Items per page: 25

Provide the VLAN name, specify the CIDR block, select the required Network Security Group, and click Create.

Create VLAN details: name, CIDR block, and network security group.

The 'Create VLAN' form includes the following fields and options:

- VLAN name:** Media-PSTN (Annotation 1 points to this field).
- Create In Compartment:** Session-Delivery (dropdown).
- VLAN Type:** Two options:
 - Regional:** Instances in the VLAN can be created in any availability domain in the region. Useful for high availability.
 - Availability Domain-specific:** Instances in the VLAN can only be created in one availability domain in the region.
- VLAN Tag:** IEEE802.1Q VLAN Tag (text field).
- CIDR Block:** VLAN Gateway CIDR: 172.16.34.0/24 (Annotation 2 points to this field).
- Route Table compartment:** Session-Delivery (dropdown).
- Route Table:** Default Route Table for session-delivery (dropdown).
- Network security group compartment:** Session-Delivery (dropdown).
- Network security group:** Voice-LAN (Annotation 3 points to this dropdown).
- Buttons:** Cancel and Create VLAN (Annotation 4 points to the 'Create VLAN' button).

8.3. Attach VLAN-backed VNICs to the SBC

Navigate to the SBC instance under Compute, open the Networking tab, and create a new VNIC. If the deployment already has a suitable VNIC, modify the existing VNIC instead.

Create or update the SBC VNIC from the Compute instance Networking tab.

The 'Attached VNICs' page shows a table of existing VNICs and a 'Create VNIC' button (Annotation 2 points to this button).

Name	Subnet or VLAN	Subnet/VLAN link	State	Route table	FQDN	VLAN tag	MAC address	
s1p0-Internal	VLAN	Media-Internal	Attached	—	—	2360	02:00:17:0D:19:4C	...
s0p0-External	VLAN	Media-External	Attached	—	—	2189	02:00:17:0D:F2:E3	...
wancom1	Subnet	HA	Attached	Default Route Table for session-delivery	—	1034	02:00:17:05:88:DD	...
SBC-9.0p1 Primary VNIC	Subnet	Management	Attached	Default Route Table for session-delivery	...clevcn.com	3505	02:00:17:0D:FF:F0	...

Page 1 of 1 (1 - 4 of 4 total items) Items per page: 25

Give the VNIC a name, select the VCN, choose Advanced Setup: VLAN, select the VLAN created for the media interface, and submit the change.

Select Advanced Setup: VLAN and attach the VNIC to the VLAN.

Create VNIC

VNIC name: sOp0-PSTN **1.**

Virtual cloud network compartment: Session-Delivery

Virtual cloud network: session-delivery **2.**

Network

Normal setup: subnet
The typical choice when adding a VNIC to an instance.

Advanced setup: VLAN **3.**
Only for experienced users who have purchased the Oracle Cloud VMware Solution.

Advanced setup: VLAN compartment: Session-Delivery

Advanced setup: VLAN: Media-PSTN **4.**

VNIC IP addresses

Private IPv4 address

☒ Automatically assign private IPv4 address

☐ Manually assign private 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.

Cancel **Submit** **5.**

Do not specify an OCI private IP address on this VNIC. IP management is delegated through the VLAN to the SBC. Configure the SBC network-interface IP addresses, utility addresses, netmask, and gateway values according to the customer addressing plan used for the VLAN.

8.4. External Access for VLAN media interfaces

External Access is optional. Configure it only when another OCI network or an Internet-facing public IP must reach the SBC on the VLAN media interface.

To configure External Access, navigate to the VCN, select the VLAN from the VLANs tab, and open the External Access tab.

Open the VLAN details page for External Access configuration.

Networking

Overview **1.**

Virtual cloud networks

Web Application Acceleration

Load balancers >

DNS management >

Customer connectivity >

Cluster Placement Groups

IP management >

Network Command Center >

Virtual Cloud Networks

session-delivery Available

Virtual Cloud Network

Details IP administration Subnets Gateways Routing Private service access Security **VLANs** **2.** Work requests Tags

VLANs

VLAN Description: A virtual local area network (VLAN) is a broadcast domain within a VCN created by partitioning and isolating a network at the data link layer (layer 2). VLANs work by using IEEE 802.1Q VLAN tags. A VLAN is analogous to a subnet, which partitions the VCN at the network layer (layer 3).

Search and Filter

Applied filters: Compartment Session-Delivery

Create VLAN

Name	State	IEEE 802.1Q VLAN Tag	VLAN Gateway CIDR	Created
Media-PSTN 3.	Available	2365	172.16.34.0/24	Jun 10, 2020, 15:54:37 UTC
Media-External	Available	3892	172.16.33.0/24	Sep 15, 2021, 09:00:51 UTC
Media-Internal	Available	3718	172.16.32.0/24	Sep 15, 2021, 08:57:35 UTC

Page 1 of 1 (1 - 3 of 3 total items)

Items per page: 25

Select the External Access tab for the VLAN.

Networking

session-delivery

Media-PSTN Available

Vlan

Details External access 4. Tags

External Access

External access allows VLAN workloads to communicate with resources outside the VLAN such as subnets, on-premises hosts, or the internet. A private IP is assigned to the VLAN to provide a "next hop" for network routing to the VLAN. If internet access is required, a reserved public IP can also be assigned. [Learn more](#)

Search and Filter Search

Add External Access 5. Remove

Name	Private IP Address	Public IP Address	Date Assigned
No items to display			

Create new items or search again using different filters or search terms.

Use Route Target Only when connectivity is required only from another VCN or OCI network path. Specify the IP address that will be configured on the SBC. Multiple route targets can be added when required.

Route Target Only external access for private reachability from OCI networks.

Add External Access

External Access Type

Route Target Only 1.
Assign a private IP address that can be used as a route target to the VLAN.

Public Access
Assign a private IP address and a reserved public IP address to provide internet access to the VLAN.

Private IP address

Name

Private IP Address 2.
172.16.34.10

Tags

Add tags to organize your resources. [What can I do with tagging?](#)

No items to display

Add tag

Cancel Add External Access 3.

Use Public Access when Internet connectivity is required through a public IP address. Add the private IP that will be configured on the SBC, then select one of the available public IP addresses in the VCN. OCI performs NAT between the specified public and private IP addresses.

Public Access option for Internet-facing reachability.

Add External Access

External Access Type

Route Target Only
Assign a private IP address that can be used as a route target to the VLAN.

Public Access
Assign a private IP address and a reserved public IP address to provide internet access to the VLAN. 1.

Private IP address

A private IP is required to provide an attachment object for the reserved public IP used for public access. You can choose an existing private IP from within the VLAN gateway CIDR, or have one created for you.

Name

Private IP Address 172.16.34.10 2.

Tags

Add tags to organize your resources. [What can I do with tagging?](#)

No items to display

Cancel Add External Access

Select the available public IP for the VLAN External Access mapping.

Add External Access

Private IP Address 172.16.34.10

Tags

Add tags to organize your resources. [What can I do with tagging?](#)

No items to display

Add tag

Reserved Public IP Address

A reserved public IP address provides resources such as VMs and VNICS within the VLAN with public access. You can choose an existing reserved public IP, or create one. The reserved public IP address is attached to the private IP address object.

☐ Select Existing 3.

☒ Create New

Name PSTN-Public 4.

Advanced Options

Tags

Cancel Add External Access 5.

After the mapping is added, it is displayed in the VLAN External Access list.

Completed External Access entry for the VLAN.

← session-delivery

Media-PSTN Available

Vlan

Actions

Details External access Tags

External Access

External access allows VLAN workloads to communicate with resources outside the VLAN such as subnets, on-premises hosts, or the internet. A private IP is assigned to the VLAN to provide a "next hop" for network routing to the VLAN. If internet access is required, a reserved public IP can also be assigned. [Learn more](#)

Search and Filter Search

Add External Access Remove

☐	Name	Private IP Address	Public IP Address	Date Assigned
☐	privateip20260610160902	172.16.34.10	129.153.12.229	...

Page 1 of 1 (1 - 1 of 1 total items) Items per page 25

8.5. SBC configuration notes for Layer 2HA

Continue with the SBC HA configuration described in the previous section, Configuring SBC for HA in OCI. The redundancy peers, network-interface values, utility addresses, and switchover checks remain the same in principle; only the OCI media VNIC attachment model changes from subnet-backed VNICs to VLAN-backed VNICs.

- Configure wancom interfaces on standard OCI subnets for management and HA communication.
- Configure the SBC media interfaces on VLAN-backed VNICs and leave virtual-mac blank in each phy-interface.
- Apply the same VLAN-backed media interface design on both SBC instances in the HA pair.
- Disable the OCIHAClient.1.o.spl plugin when the deployment uses Layer 2 Network Virtualization instead of the Layer 3 API HA method.

9. 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 sopo 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 sopo interface>

HeaderNatPrivateSipIfIP =<Private IP of the sopointerface >

Configuration

View Configuration

Q

Discard

Verify

filter-config

ldap-config

local-policy

local-routing-config

media-profile

session-agent

session-group

session-recording-group

session-recording-server

session-translation

sip-config

sip-feature

sip-interface

sip-manipulation

Show All

Add SIP Interface

Show Advanced

Show Configur

Secured Network

☐ enable

Uri Fqdn Domain

Options

SPL Options

HeaderNatPublicSipIfIp=20.110.135.150,HeaderNatPri

Trust Mode

all

Max Nat Interval

3600

(Range: 0..999999999)

Stop Recurse

401,407

Port Map Start

0

(Range: 0,1025..65535)

Port Map End

0

(Range: 0,1025..65535)

In Manipulationid

OK

Back

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

HeaderNatPublicSipIfIp=20.110.135.150,HeaderNatPrivateSipIfIp=10.0.4.60

ORACLE	Oracle Corporation, World Headquarters 2300 Oracle Way Austin, TX78741, USA	Worldwide Inquiries Phone: +1.650.506.7000 or Phone: +1.800.392.2999
CONNECT WITH US blogs.oracle.com facebook.com/oracle twitter.com/oracle oracle.com	Integrated Cloud Applications & Platform Services Copyright © 2024, Oracle and/or its affiliates. All rights reserved. This document is provided <i>for</i> 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	