DEPLOYING ORACLE SBC IN MICROSOFT AZURE PUBLIC CLOUD

Technical Application Note

ORACLE
COMMUNICATIONS

Disclaimer

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

Table of Contents

Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, and end users of the Oracle Enterprise Session Border Controller (E-SBC). It assumes that the reader is familiar with basic operations of the Oracle Communications Enterprise Session Border Controller and Azure Cloud Deployments.

Document Overview

You can deploy the Oracle Communications Session Border Controller (OCSBC) on Azure public cloud. Azure provides multiple ways of managing your environment(s), including via its web portal, using its PowerShell and its CLI interfaces. This document focuses on the portal. The portal provides navigation via a web-page pane with links to specified functions on the left side of portal pages. These procedures also assume you have reviewed Azure documentation and can access portal pages and navigation.

Related Documentation

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

Microsoft Azure

- Introduction to Azure
- Get started with Azure
- Azure security best practices and patterns

Requirements

1) A subscription for Azure portal

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

Create and Deploy on Azure

Prerequisites to Deploying an Azure Instance

You can create some of the objects required during the SBC deployment procedure prior to or during the deployment. When created prior to SBC deployment, these objects become selectable, typically from drop-down lists in the appropriate deployment dialogs. You may use these objects for a single deployment or for multiple deployments.

These Objects are as follows:

1) Resource Group
    i) Subscription
    ii) Region
2) Networking
    i) Virtual Networks
    ii) Subnets
    iii) Network Security Groups

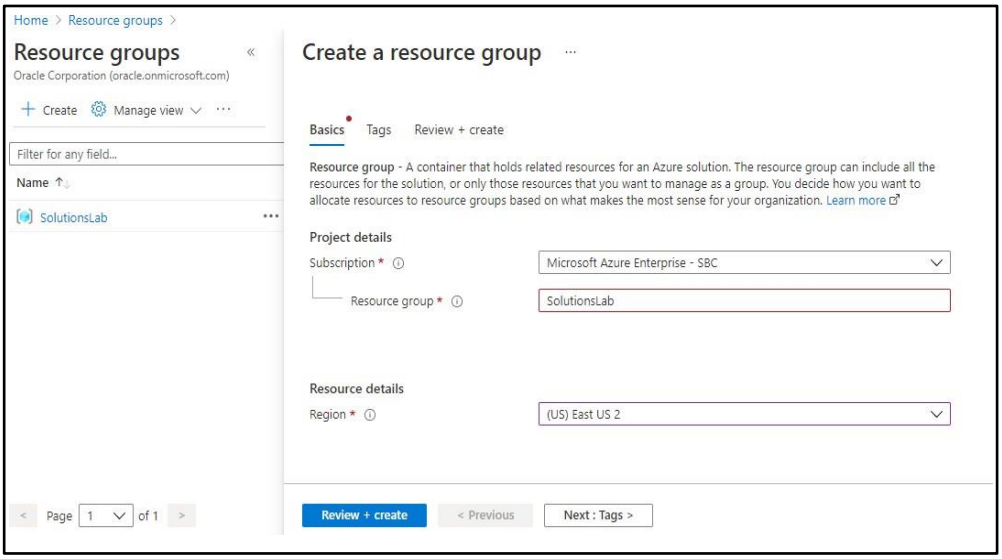
Resource Group

Resource group is a container that holds related resources like storage accounts, virtual networks, and VMs for an Azure solution. In Azure, you logically group related resources to deploy, manage, and maintain them as a single entity.

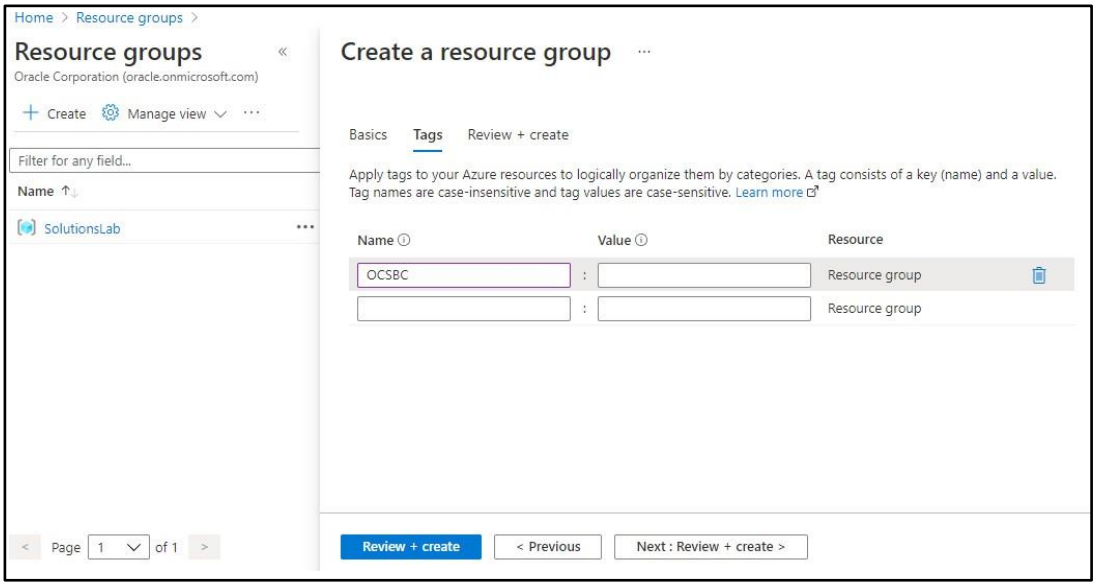
Creating a Resource Group

From the Azure Portal Home Page, on the left side, select “Resource Group”, and then click “Add”

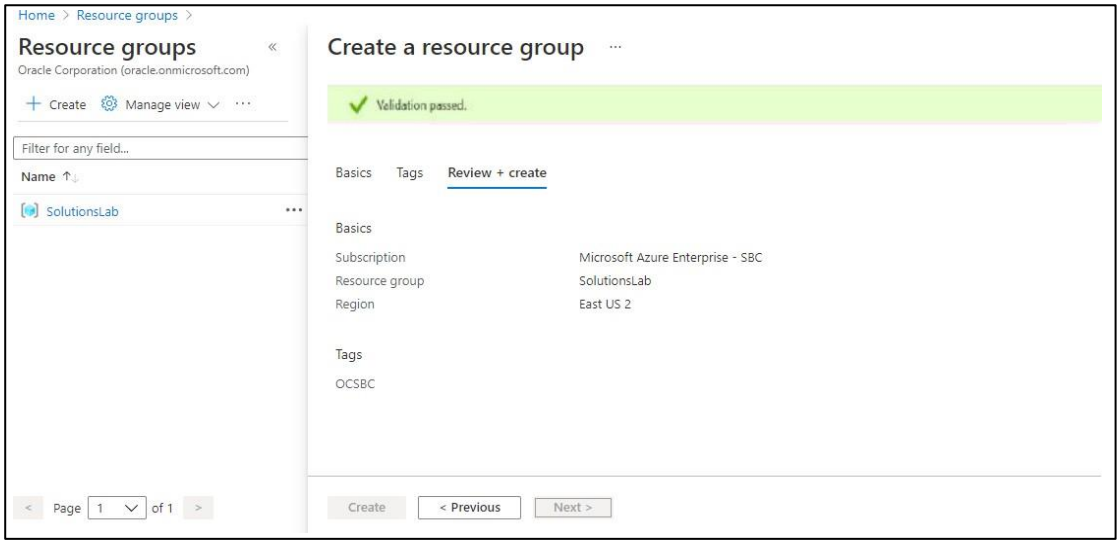
- Choose the correct Subscription from the drop down,
- Give the resource group a name
- Select the region that is right for you and your customers.
- At the bottom, click “Next : Tags”



- Enter a unique identifier under name
- Click Next: Review + Create



- Review the information and click Create



Network Security Groups

Network Security Groups are used to provide traffic control at the packet level.
You can filter network traffic to and from Azure resources in an Azure virtual network with a network security group. A network security group contains security rules that allow or deny inbound network traffic to, or outbound traffic from, several types of Azure resources.

For more detailed information, please see:

Enable Network Security Groups in Azure Security Center

Creating Network Security Groups

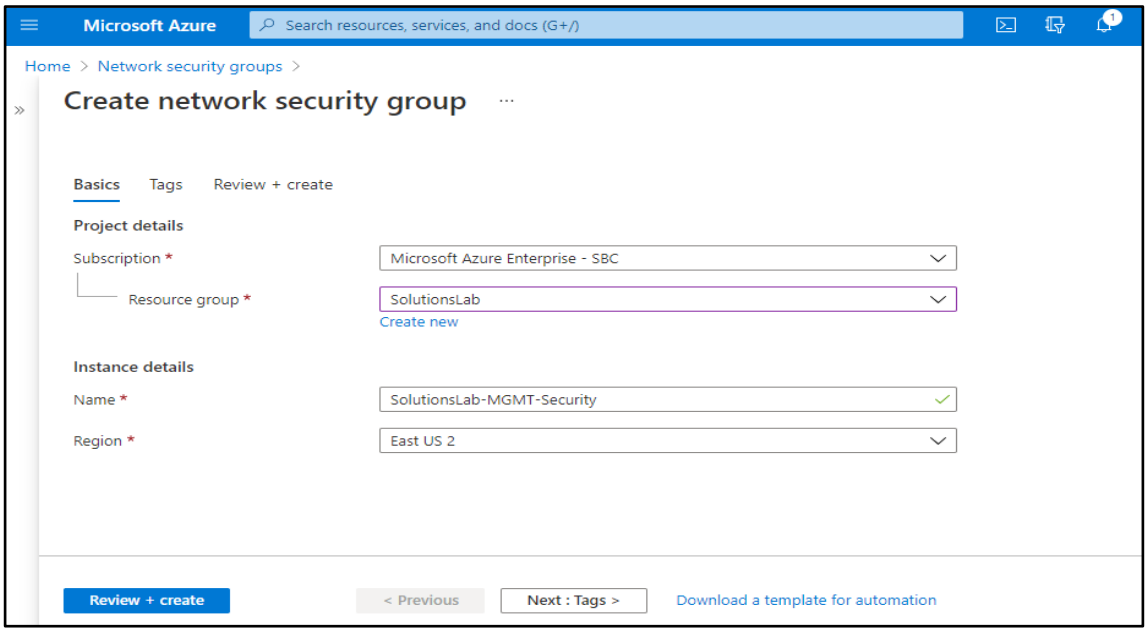
For Oracle SBC deployment in Azure, each Security Group specifies the type of traffic allowed on a particular type of subnet. **The SBC has 3 types of vNICs, including management (wancom0), and Media (s0p0, s1p0 etc).**
To maintain traffic separation, each of the vNICs should be connected to a separate subnet that can be configured and assigned to the Oracle SBC in Azure.

From Azure's navigation list on the left side of the portal, click Create a resource, Networking, Network Security Group.

Management Security Rules

Configure the following For Management Interface Network Security Group:

- Name
- Resource Group
- Location
- At the bottom, click “Next : Tags”



- Enter a unique identifier under name
- Click Next: Review + Create

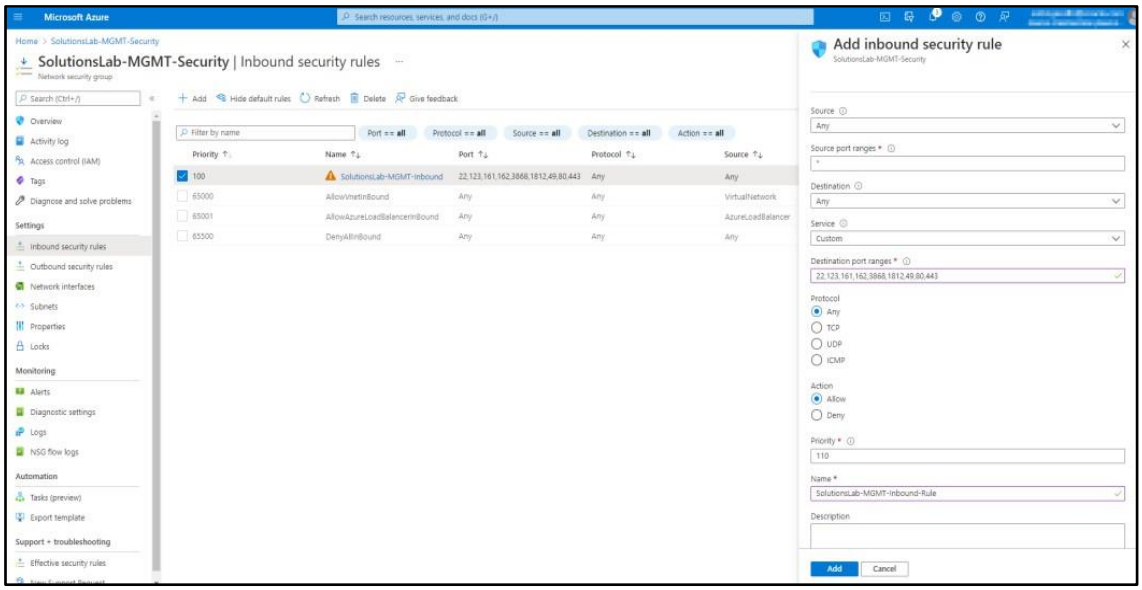
Once the security group is created, you should see it under Home/Recent Resources. Open it.

Under Settings, click on “inbound security rules”, then “add”

The following TCP/UDP protocols and/or ports should be opened for the Management Interface NSG.

Please note, the port matrix below is an example only. The ports opened during installation should depend on the environment needs and user preferences.

Protocol	Port	TCP	UDP
SSH	22	X	
SNMP	161/162	X	X
Radius	1812	X	X
NTP	123		X
HTTPS	443	X	
HTTP	80	X	
Tacacs	49	X	
Diameter	3868	X	



- Click “Add” at the bottom

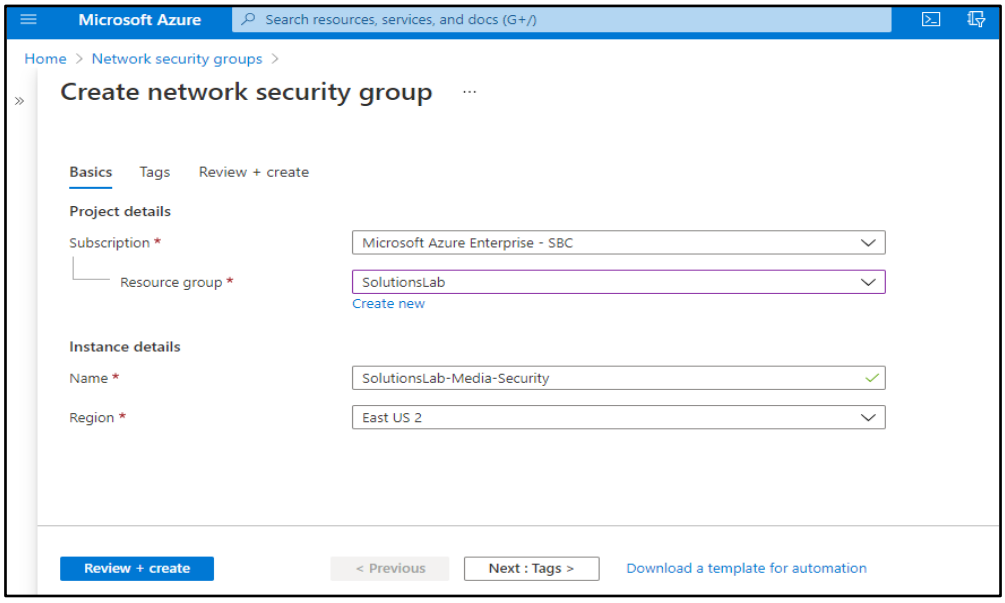
Next, follow the same procedure as above to create a second inbound security rule for ICMP traffic, using the following parameters:

- Source: Any
- Source Port Ranges: *
- Destination: Any
- Destination Port Ranges: *
- Priority: 130
- Name: MGMT_ICMP

Media Security Rules

Following the same procedure above under Creating Network Security Groups, configure the following for the Media Interface Network Security Group:

- Name
- Resource Group
- Location
- At the bottom, click “Next : Tags”

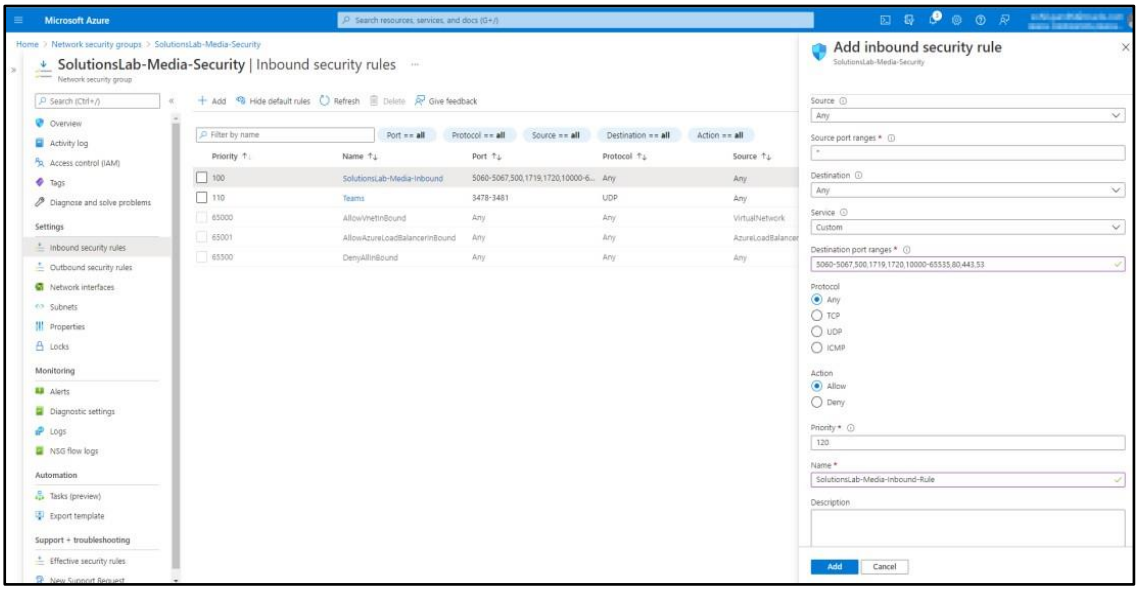


- Enter a unique identifier under name
- Click Next: Review + Create

The following TCP/UDP protocols and/or ports should be opened for the Media Interface NSG. This is not a complete list but should work for most applications.

Please note, the port matrix below is an example only. The ports opened during installation should depend on the environment needs and user preferences.

Protocol	Port	TCP	UDP
IKE	500		X
SIP	5060	X	X
SIPS	5061	X	
H.323	1719	X	X
H.323	1720	X	
RTP	10000-65535	X	X



- Click “Add”

Virtual Networks

Azure Virtual Network enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. A virtual network is scoped to a single region; however, multiple virtual networks from different regions can be connected together using Virtual Network Peering.

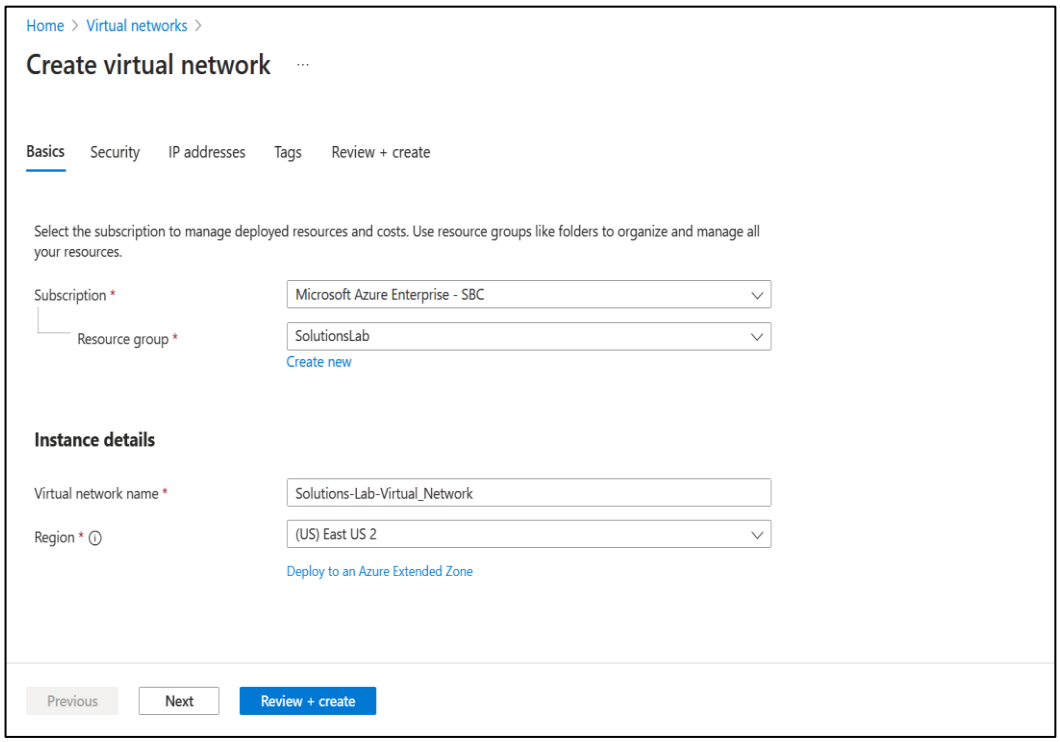
To deploy the SBC in a particular Resource Group, at least one virtual network (VN) must be created.

Creating a Virtual Network

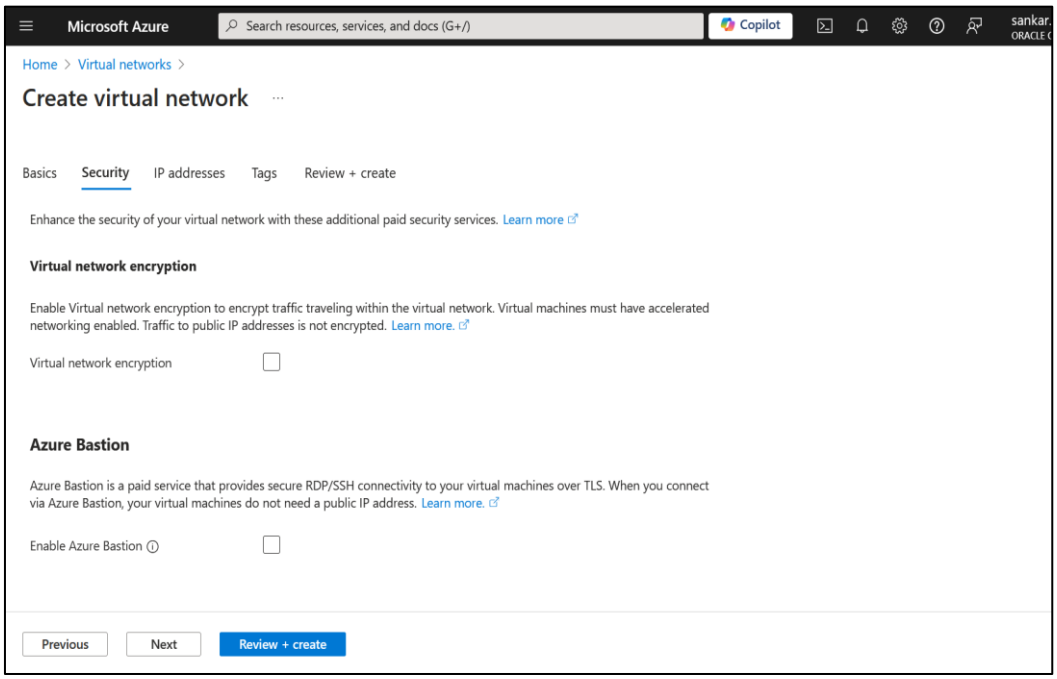
From the Azure portal Home Screen, Select “Virtual networks” from the left side menu, then click “Add”:

Provide the following information in the designated fields:

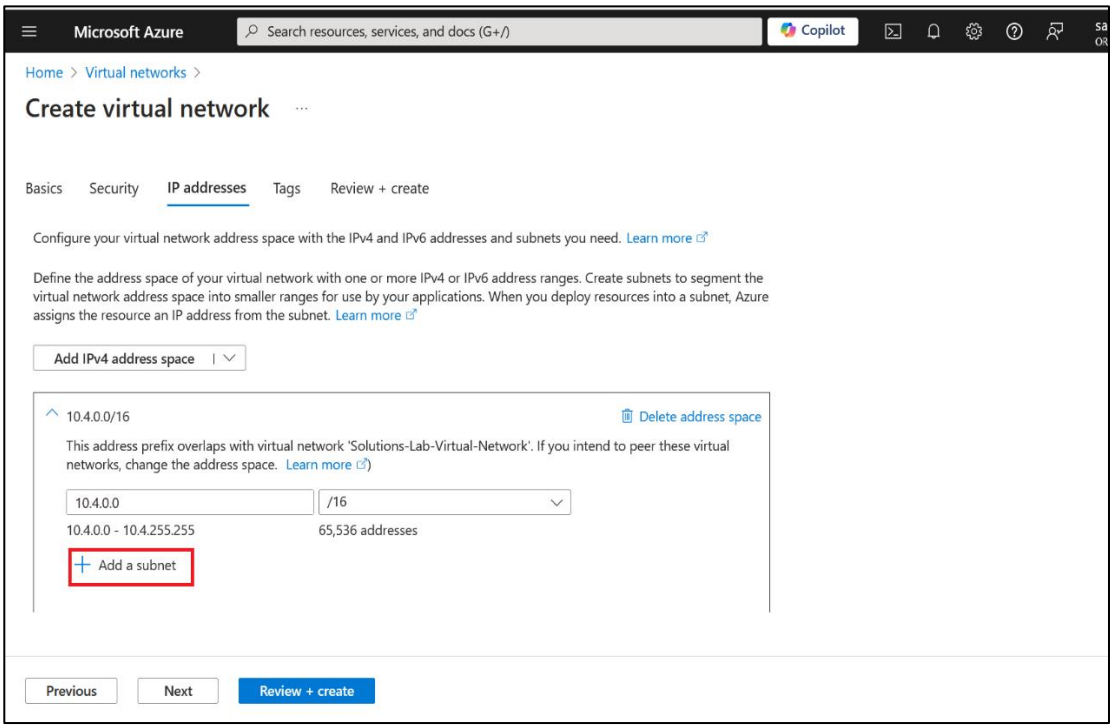
- Subscription
- Resource Group (created above)
- Virtual Network Name
- Region (same as Resource Group location)
- At the bottom, click “Next : IP Addresses”



You can select the appropriate values in Security tab.

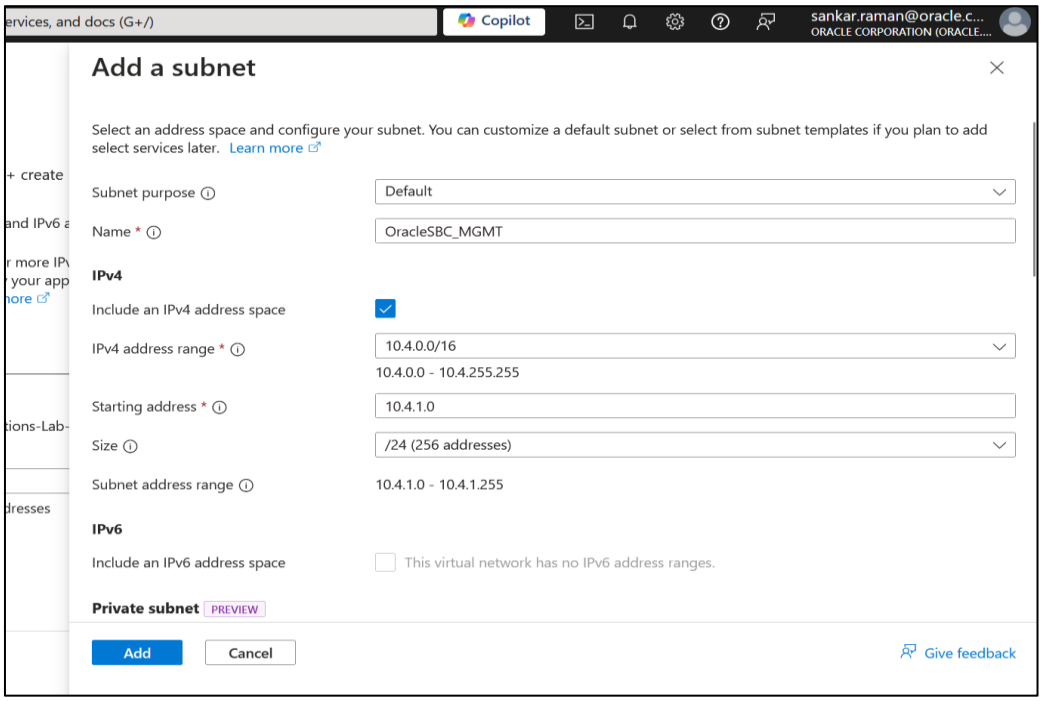


- IPv4 Address Space: (Ex..10.4.0.0/16)

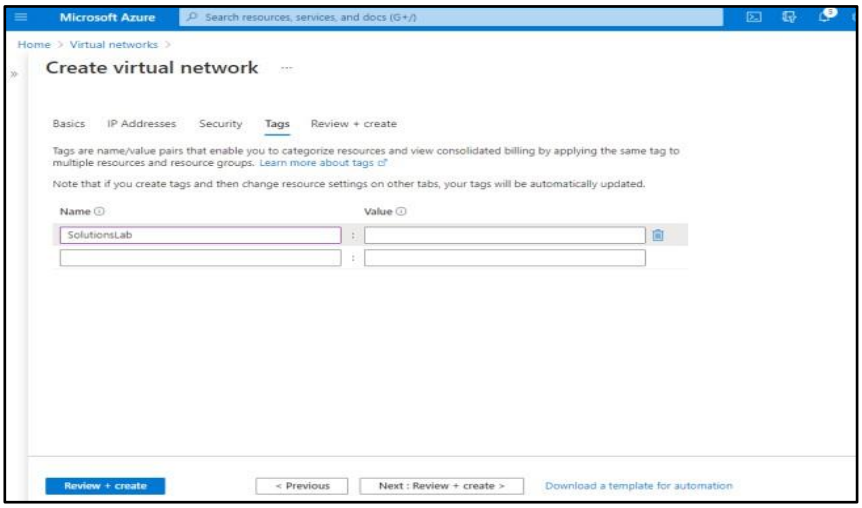


We'll also be creating the first subnet which will be used for the management interface (wancom0) of the SBC instance

- Click Add Subnet
- Subnet Name
- Subnet Address Range: (Ex..10.4.1.0/24)
- Click Add



- At the bottom, click “Next : Tags”
- Enter a unique identifier under name



- Click “Next : Review + Create” and the Virtual network is created successfully.

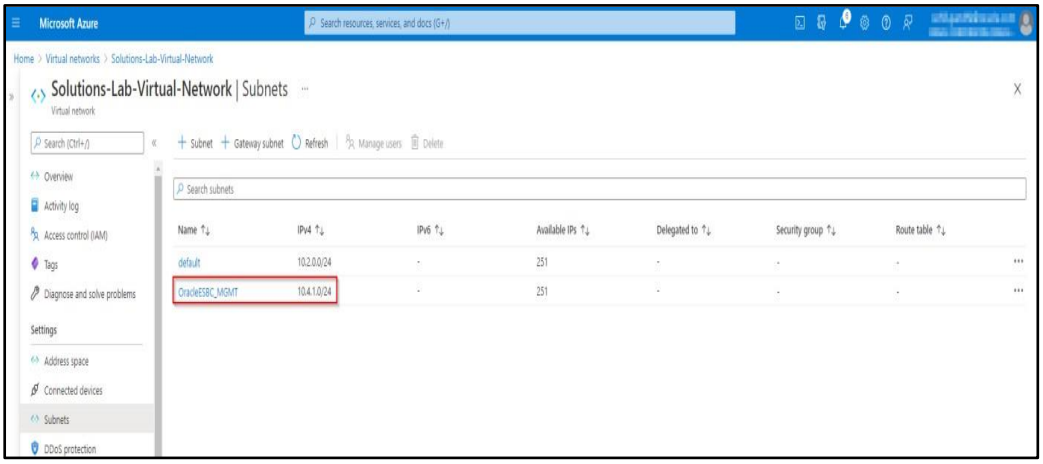
Once the Virtual network is successfully created, open it by clicking on the virtual network name, from here we will create the additional subnets needed for deployment.

Creating Additional Subnets

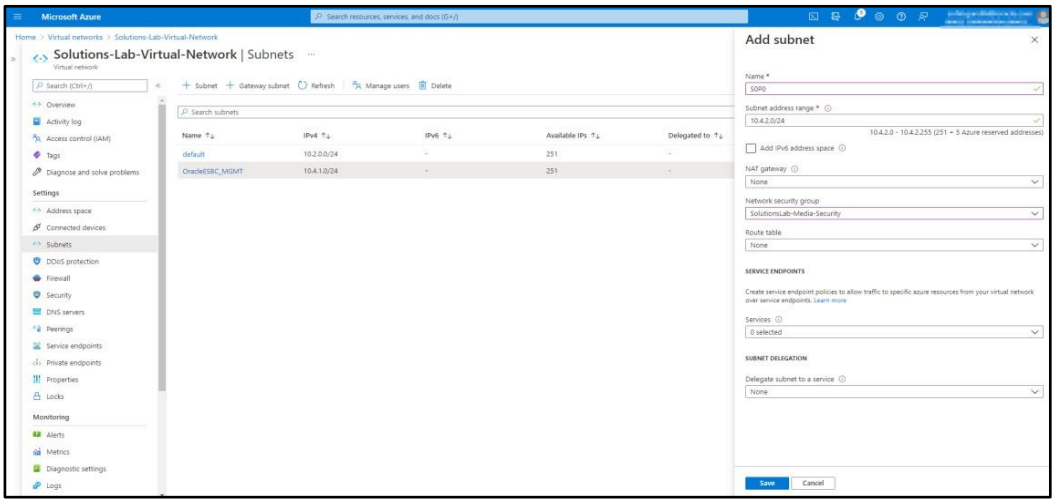
In this document, the Oracle SBC has 2 types of vNICs

- Management (wancom0)
- Media (s0p0, s1p0 etc.)

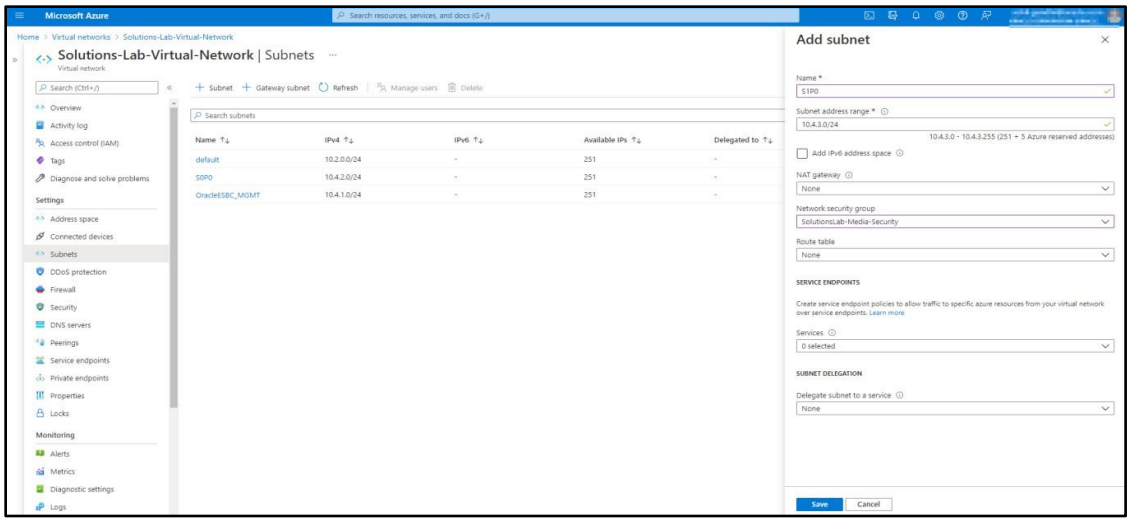
To maintain traffic separation, each of the vNICs should be connected to a separate subnet. Once you are in the Virtual Networks Dialog, click Subnets (in the settings section)

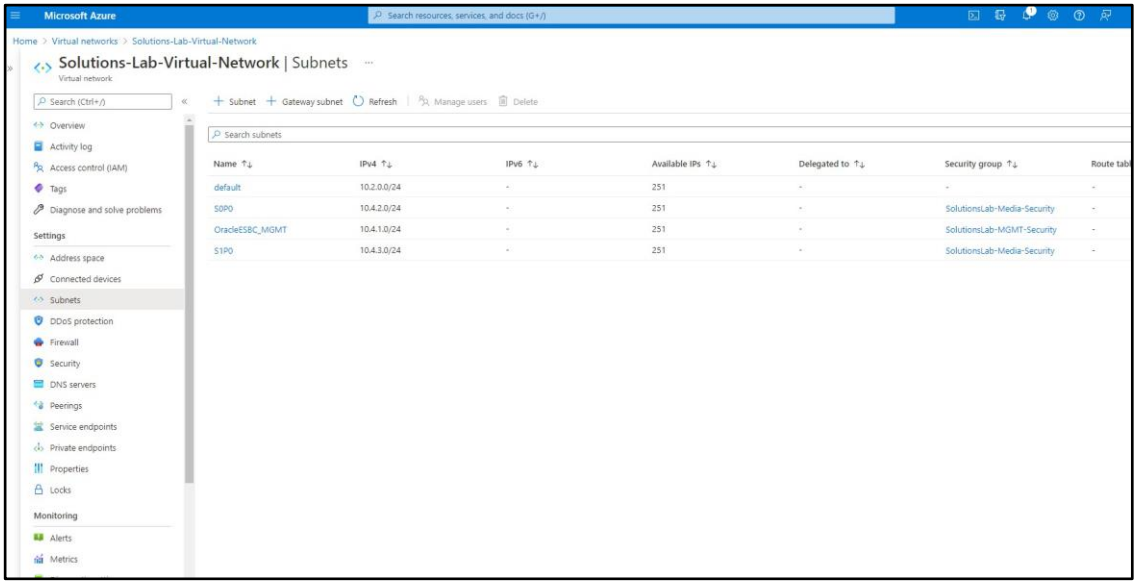


- At the top, click “+Subnet”
- Name (S0P0)
- Address Range (CIDR block) (10.4.2.0/24)
- Network Security Group: (SolutionsLab-Media-Security)
- Click “Save”



Repeat these steps to create additional subnets for your deployment needs. For the purpose of this example, we'll create one additional subnet with name of S1P0, and Address range of 10.4.3.0/24 to be used for a second media interface.

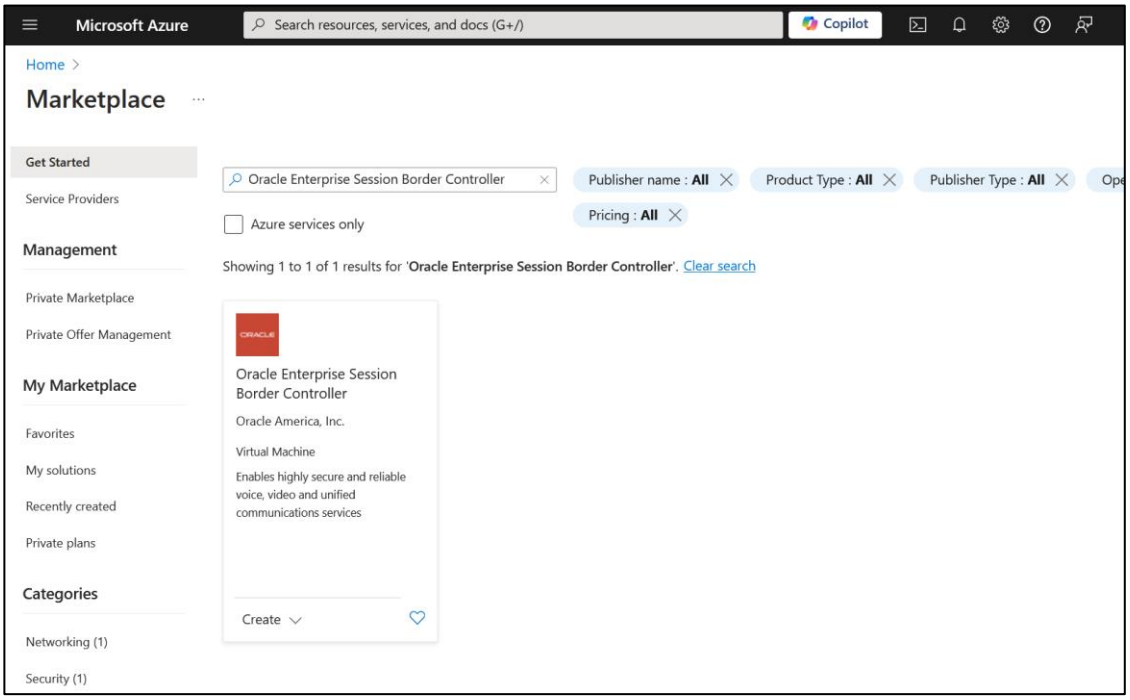




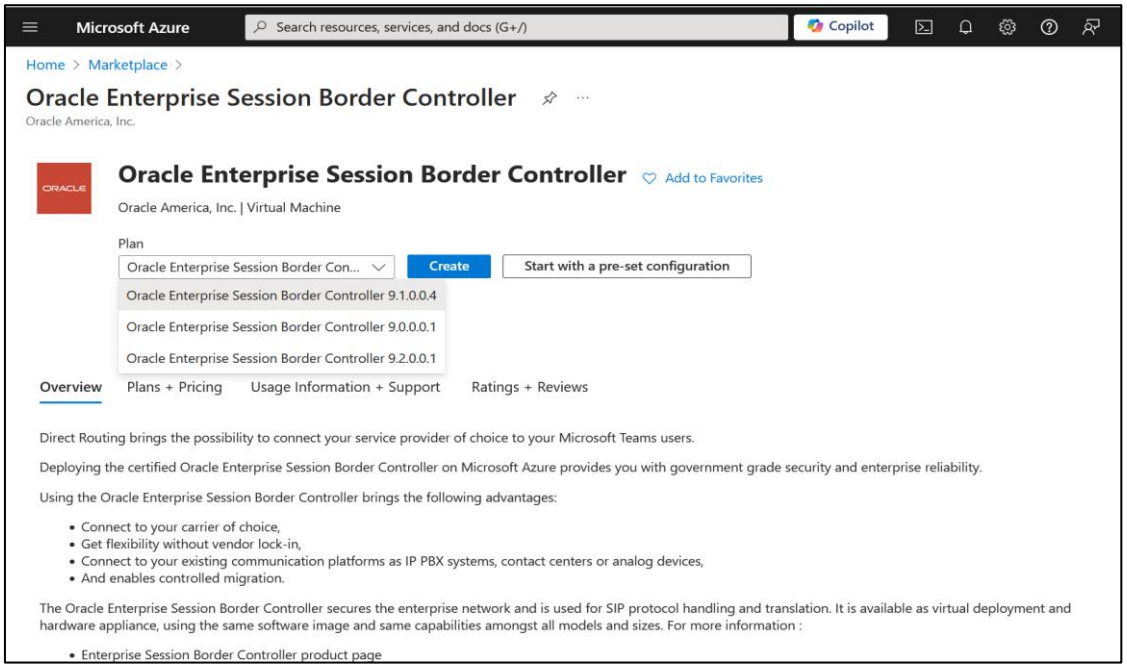
Create a Virtual Machine

This is the main instance configuration procedure. It includes a multi-dialog wizard that presents configuration options in the preferred sequence. The result of this wizard is an installed, operational OCSBC. You add media interfaces after deployment.

- From the Marketplace, at the marketplace search bar, search for “Oracle Enterprise Session Border Controller”



- Select “Oracle Enterprise Session Border Controller” and this should bring you the screen from where you can create the SBC instance and you can also select the image for SBC **(we have 9.0, 9.1 and 9.2 as of now)**



- Click “Create” and follow the below sequence of steps to create a VM

  The instance deployment wizard sequence includes:

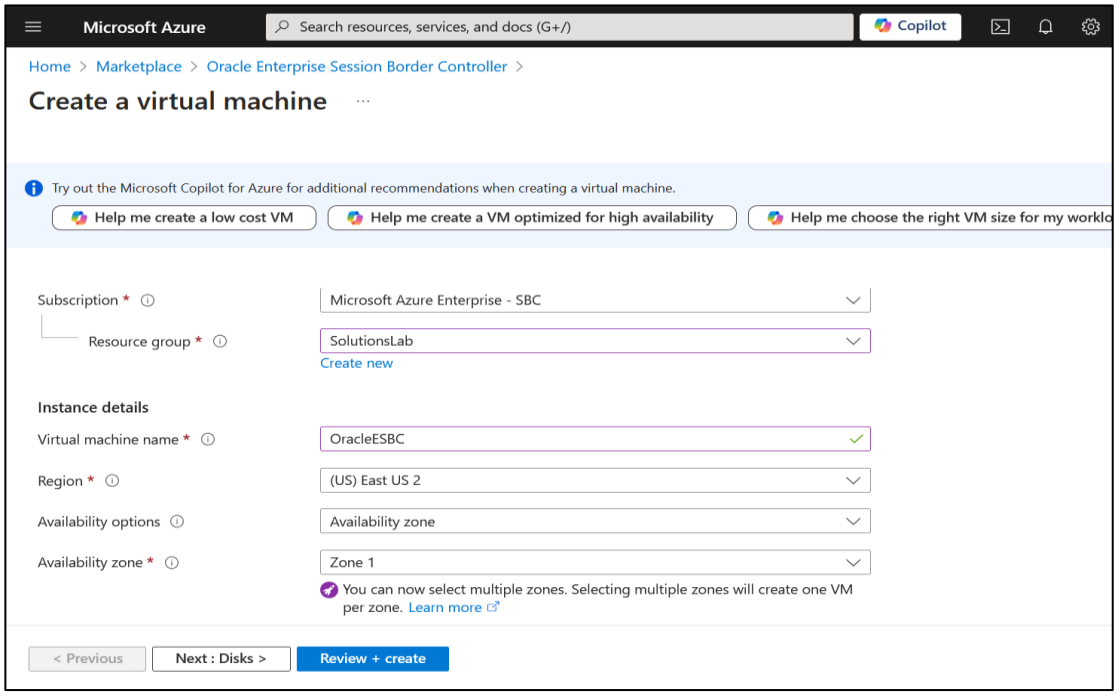
1. Basics
2. Disks
3. Networking
4. Management
5. Monitoring
6. Advanced
7. Tags
8. Review and Create

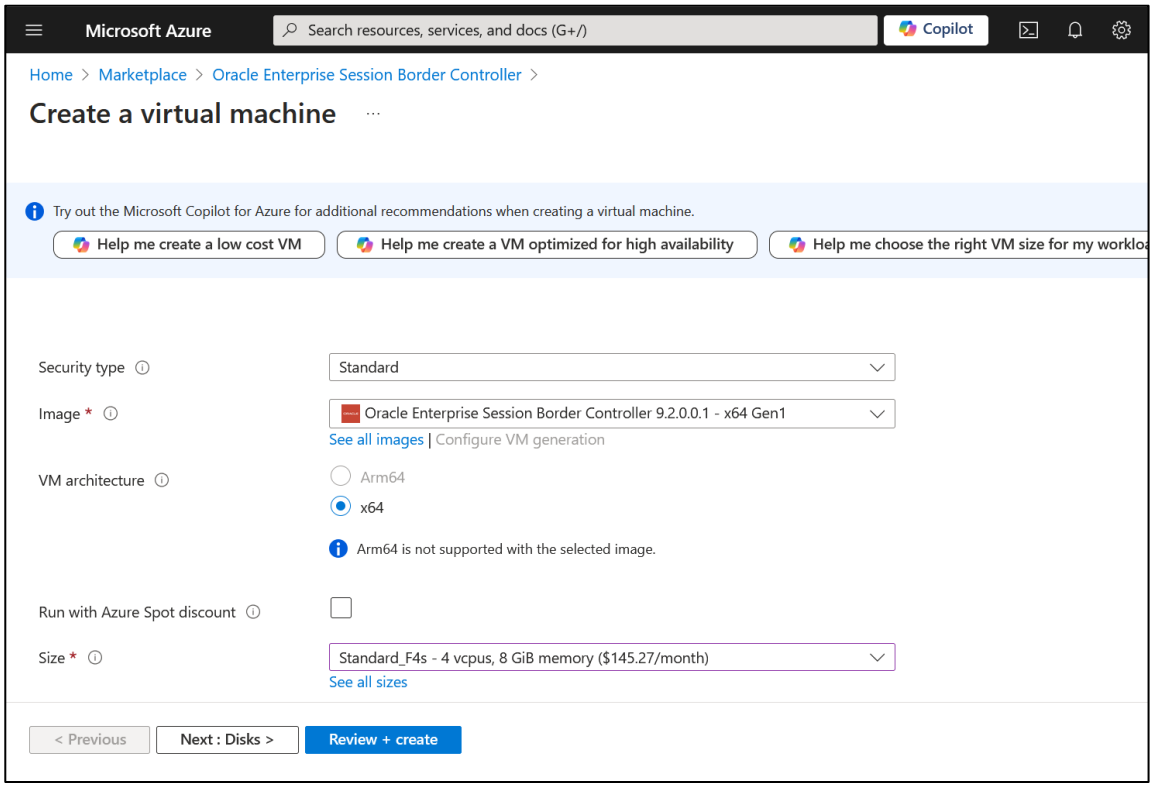
Your Azure workspace may present dialogs and fields that differ from this procedure. For full information on deploying Azure instances, see the Azure documentation.

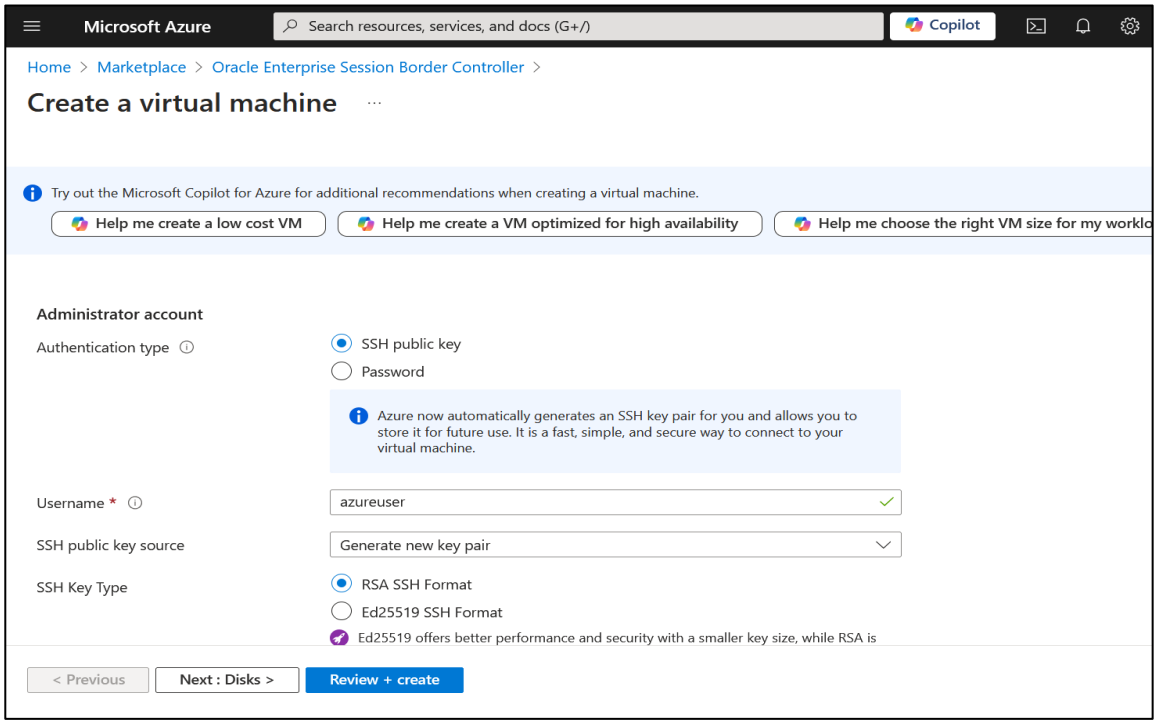
Basics

You will need to provide:

- Resource Group
- Virtual machine Name
- **Image should be populated with Marketplace image name (E.g., Oracle Enterprise Session Border Controller 9.2.0.0.1 - x64 Gen1)**
- Size: You must research size types and select the type you prefer prior to deployment, as it cannot be changed after deployment. For a list of Azure instances you can use for OCSBC, please see the Platform and Preparation Guide.
- Administrator Account (Create SSH public key pair and store it for future use in order to connect to your virtual machine)
- Inbound Port Rules (Check off all available in the drop-down menu under this field)



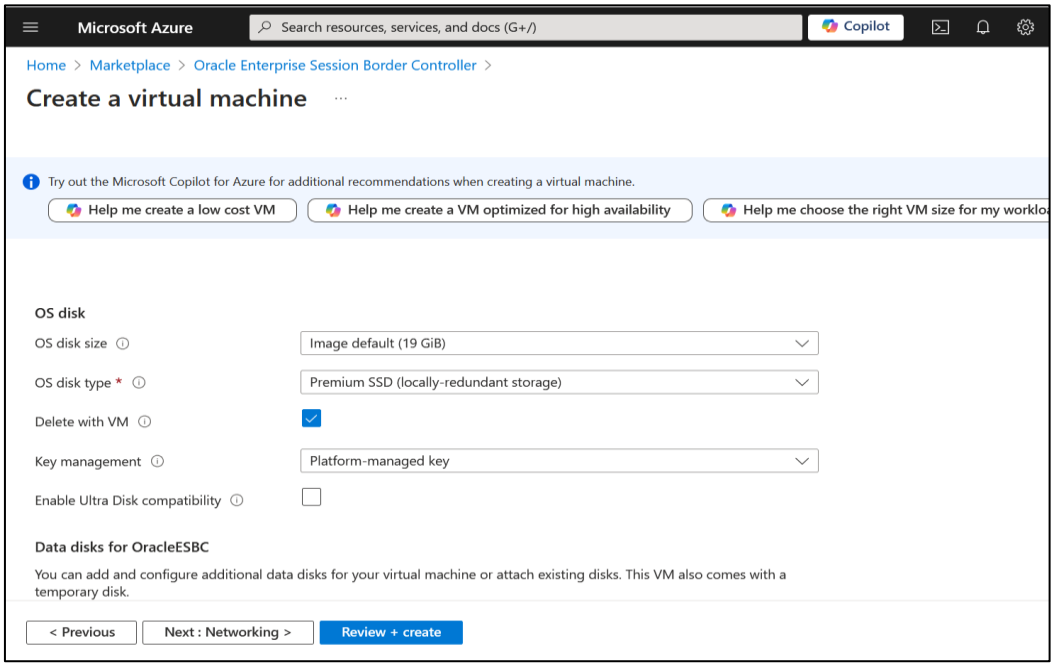




- Click “Next : Disks”

Disks

- Disk configuration includes setting the OS disk type to Premium SSD



- Click “Next: Networking”

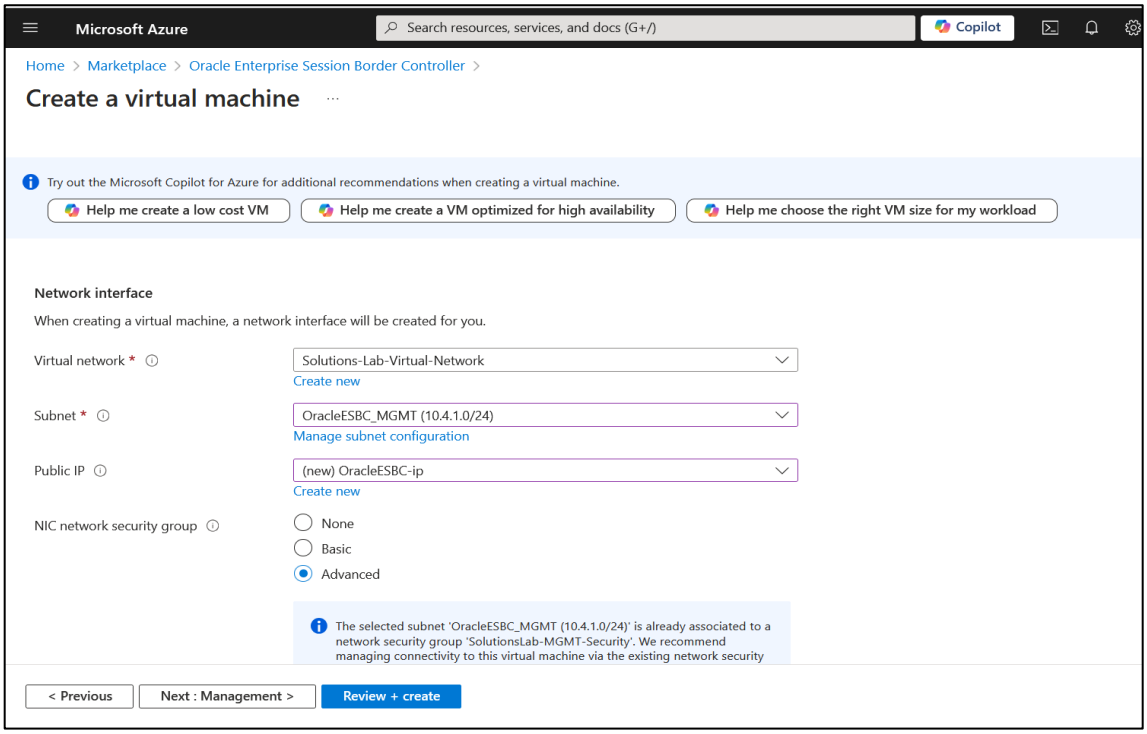
Networking

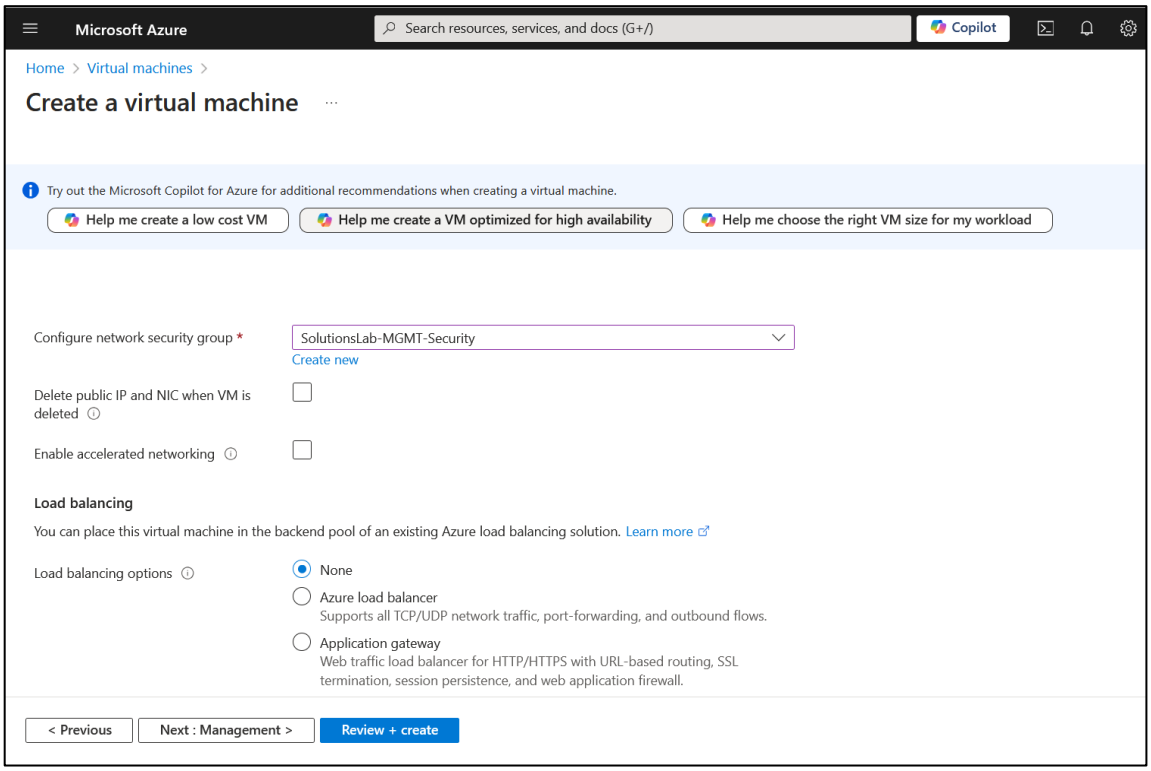
Configuration Fields:

- Virtual Network
- Subnet (Select <your_management_subnet> from drop down)
- Public IP (give it a name or use default name provided)
- Network Security Group (move radio button to advanced, and select the MGMT NSG configured previously in this document)
- Accelerated Networking set to “Off”
- Load Balancing set to “No”

Note: It is recommended to disable Accelerated Networking on management interface.
Enable it for media network interfaces for low network latency and increased network performance but doing so might incur additional charges from Azure.

Refer https://docs.microsoft.com/en-us/azure/virtual-network/create-vm-accelerated-networking-cli for additional information related to Accelerated networking.

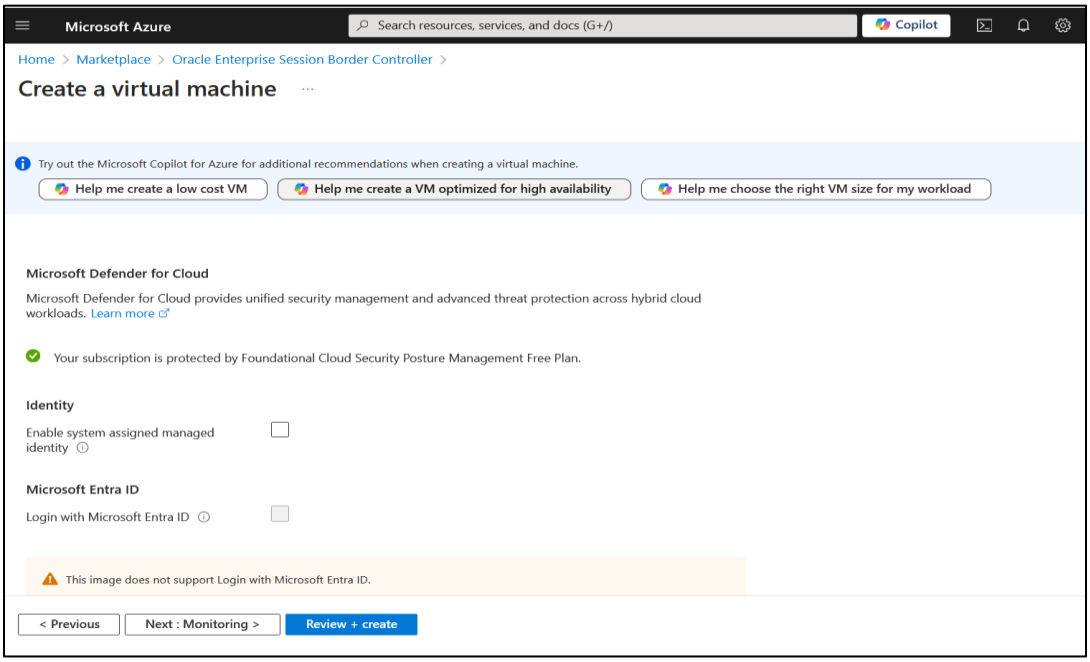




- Click “Next : Management”

Management

Select the default options in this tab.

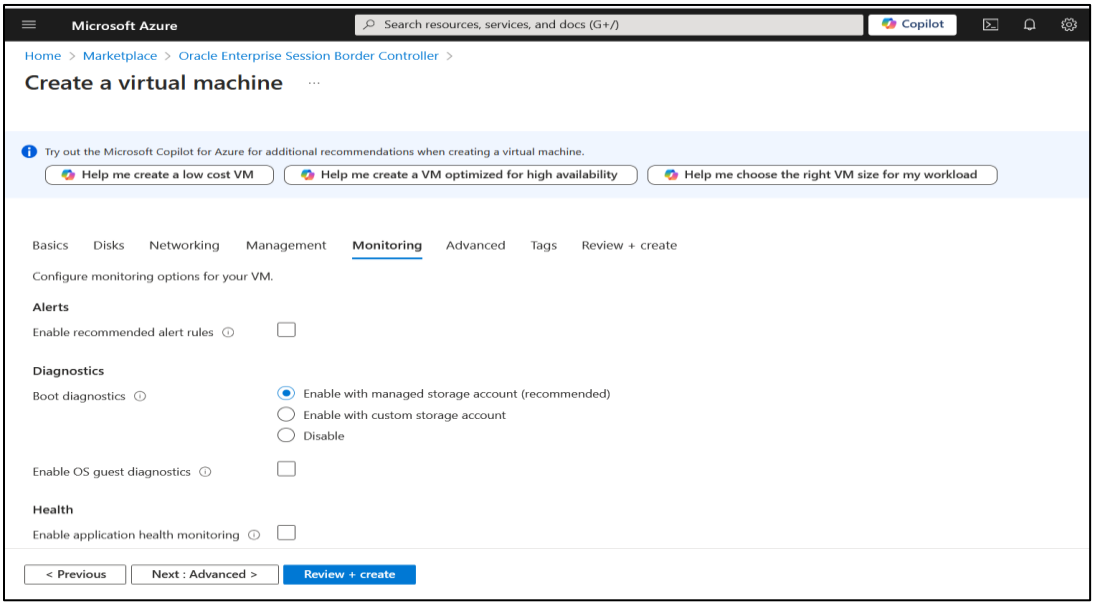


- Click “Next : Monitoring”

Monitoring

Monitoring Configuration Includes:

- Boot Diagnostics: Enable with managed storage account (recommended)
- Leave all other fields set to OFF.



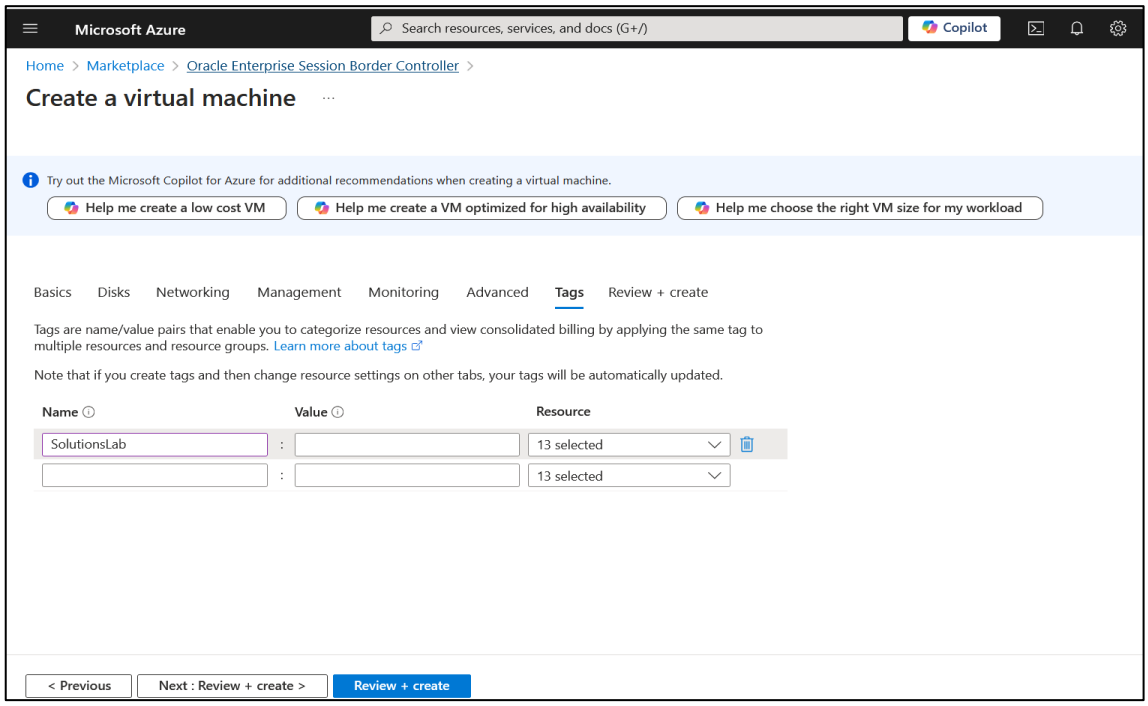
- Click “Next : Advanced”

Advanced

- No Changes Necessary in the Advanced configuration Page
- Click “Next : Tags”

Tags

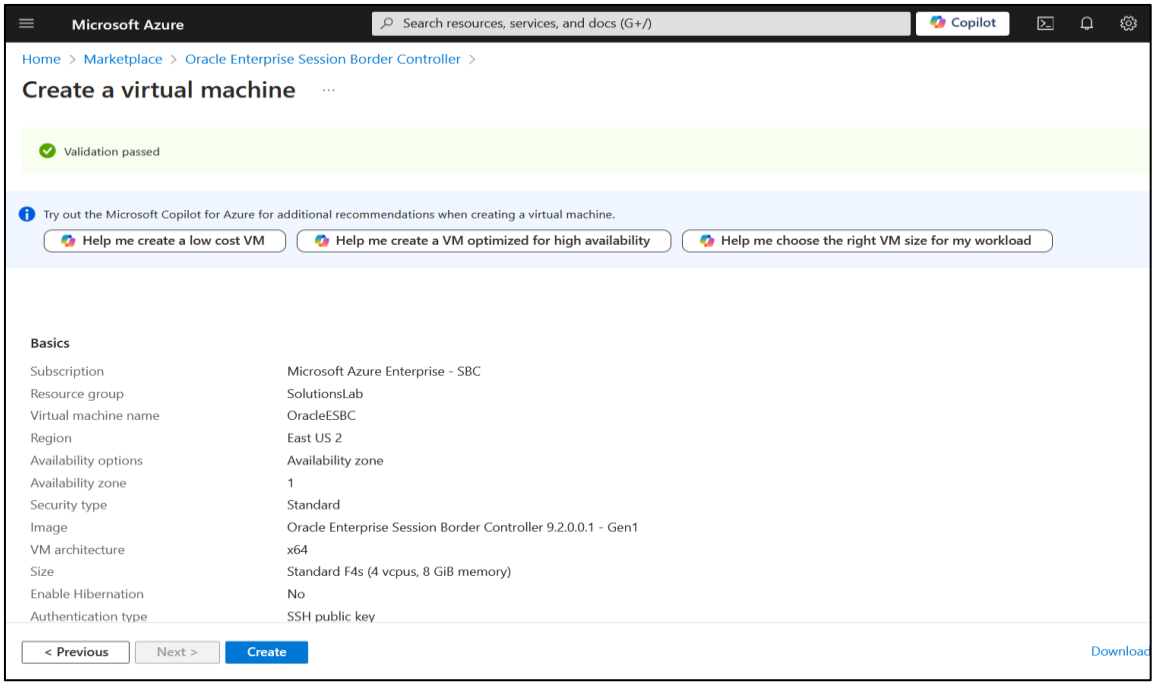
- Define the Tag we have been using throughout this guide.
- Select it from the drop down menu, Under Name

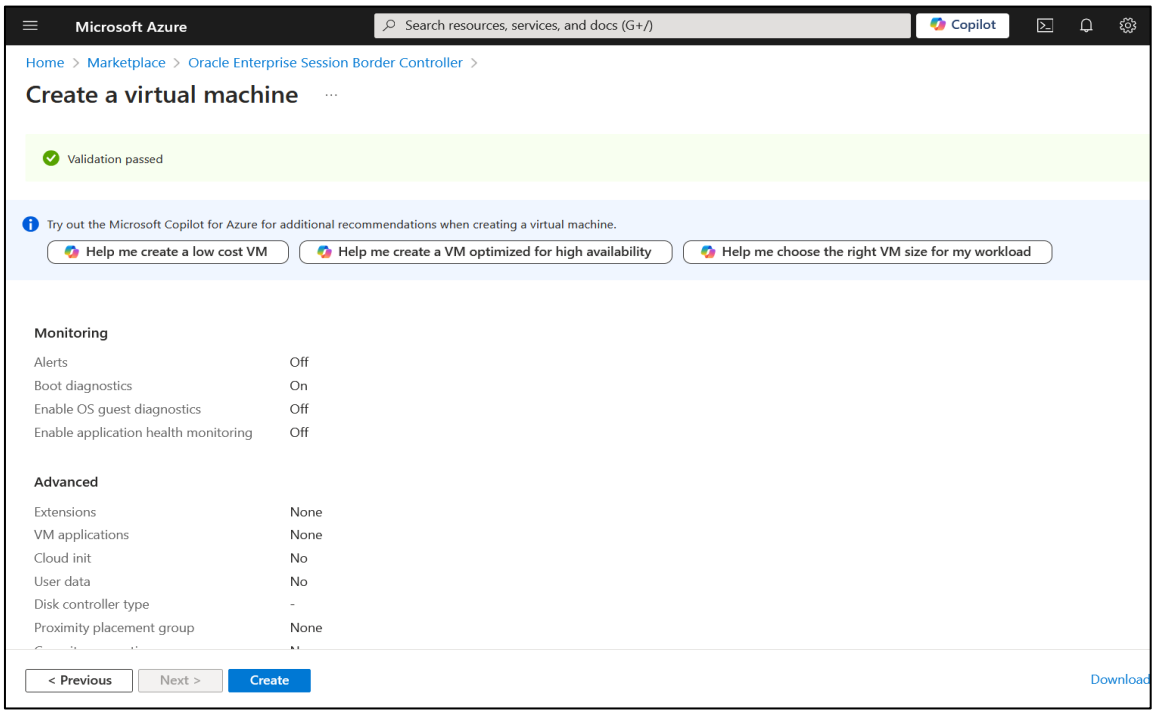


- Click “Next: Review + Create”

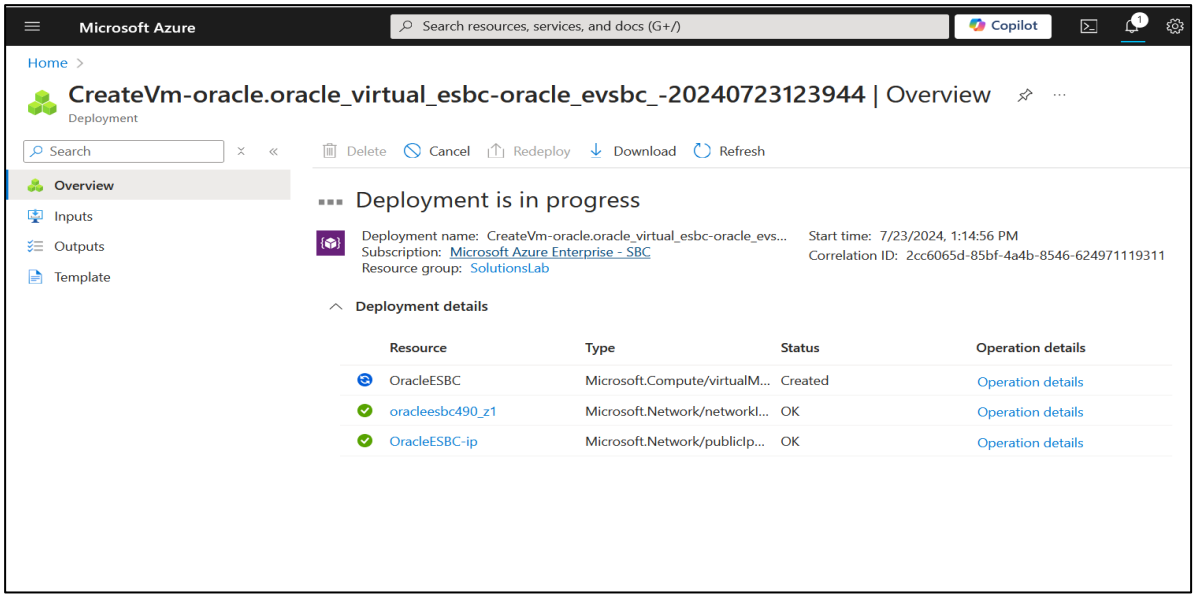
Review and Create

- Review the information for accuracy for your deployment.
- Verify Validation Passed is displayed at the top of the screen.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Marketplace > Oracle Enterprise Session Border Controller >
Create a virtual machine
Validation passed
Try out the Microsoft Copilot for Azure for additional recommendations when creating a virtual machine.
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Subscription Microsoft Azure Enterprise - SBC
Resource group SolutionsLab
Virtual machine name OracleESBC
Region East US 2
Availability options Availability zone
Availability zone 1
Security type Standard
Image Oracle Enterprise Session Border Controller 9.2.0.0.1 - Gen1
VM architecture x64
Size Standard F4s (4 vcpus, 8 GiB memory)
Enable Hibernation No
Authentication type SSH public key
< Previous
Next >
Create
Download


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Marketplace > Oracle Enterprise Session Border Controller >
Create a virtual machine
Validation passed
Try out the Microsoft Copilot for Azure for additional recommendations when creating a virtual machine.
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Monitoring
Alerts Off
Boot diagnostics On
Enable OS guest diagnostics Off
Enable application health monitoring Off
Advanced
Extensions None
VM applications None
Cloud init No
User data No
Disk controller type -
Proximity placement group None
< Previous
Next >
Create
Download

- Click Create, and you should see: “Your Deployment is Underway” progress page

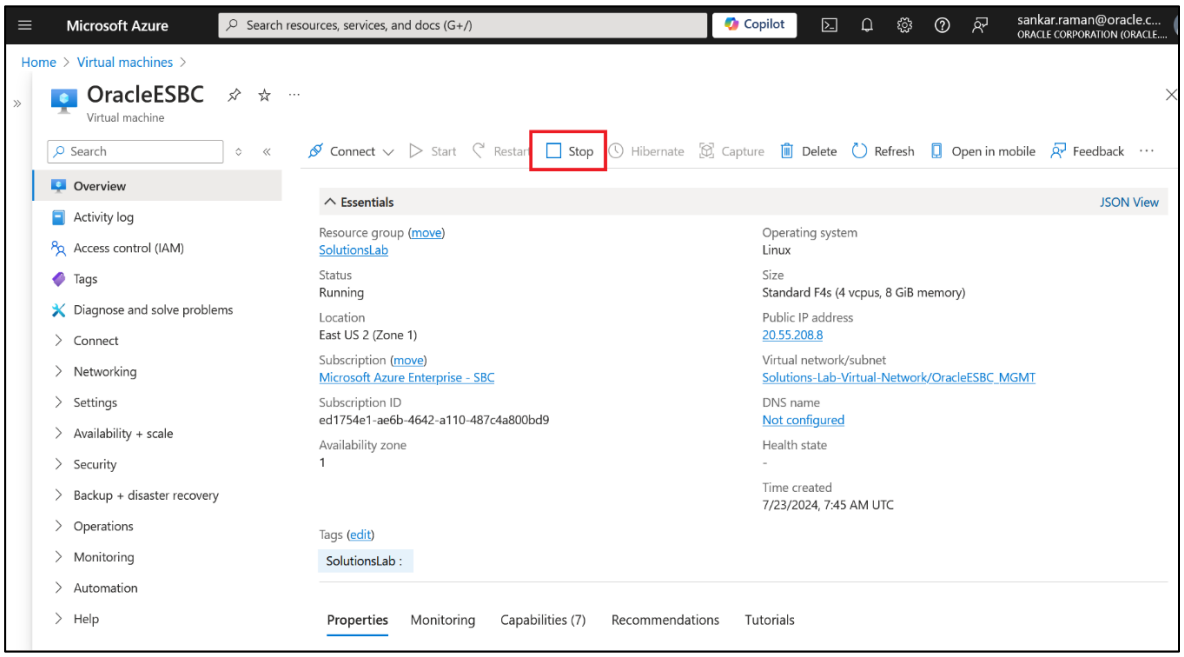


Create Networking for Media Interfaces

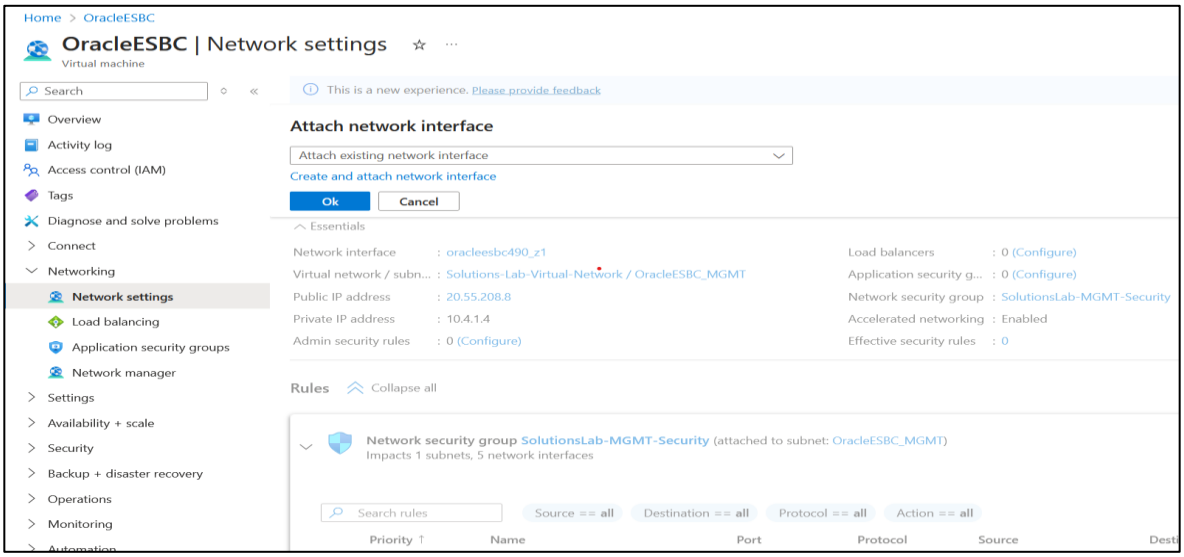
Creation of the SBC virtual machine includes establishing networking to the primary management interface,wancom0. Now we need to create networking for all other interfaces. Azure requires that we stop the SBC instance before we can create or attach additional networking interfaces for Media.

From Azure's navigation list, on the left side of the portal, select “Virtualmachines”

Select the instance we have just created. Once you select it, you will see displayed an instance-specific navigation pane on the left side of the dialog.



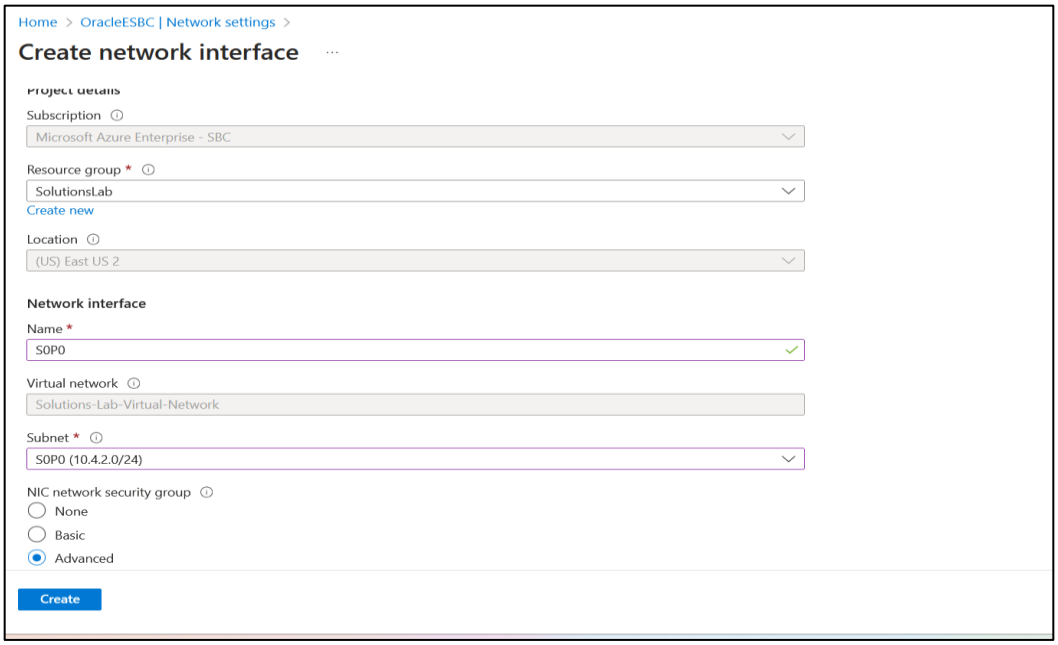
- At the top, click on “Stop”
- Once the VM is stopped and deallocated, click on Networking under Settings in the instance specific navigation menu.
- Next, “Attach Network Interface” then” Create and attach network Interface”

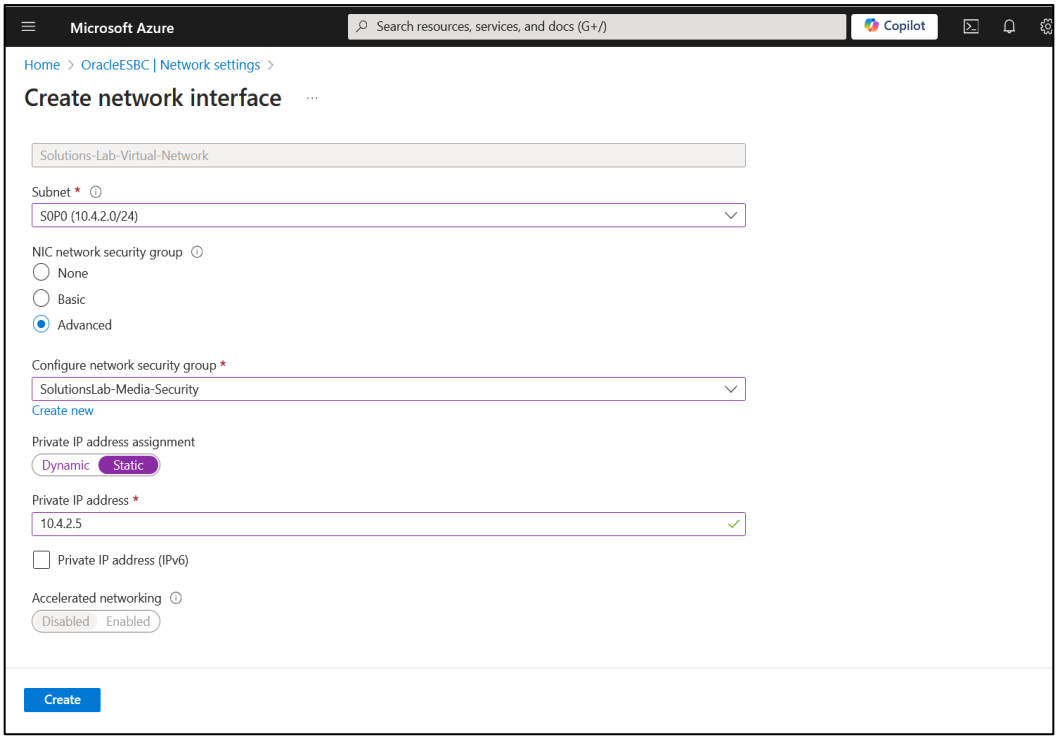


Create Network Interfaces

Configure the applicable Create Network interface fields, including:

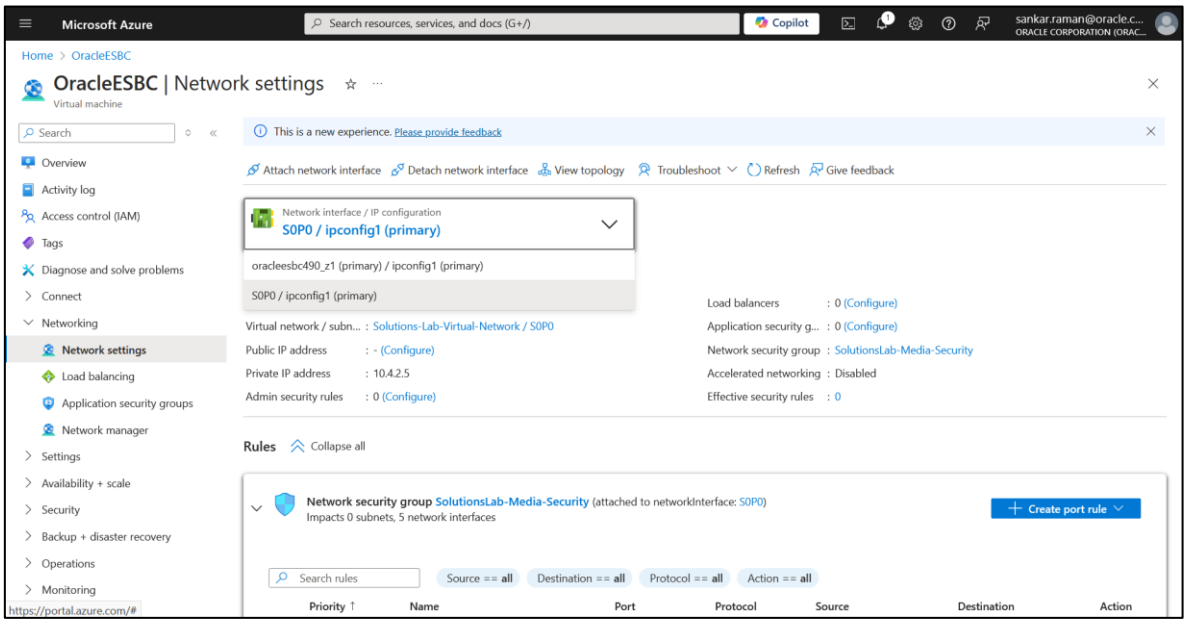
- Name: S0P0
- Subnet: From the drop down, select the subnet created for S0P0 interface
- Network Security Group (move radio button to advanced, and select the Media NSG configured previously in this document)
- Private IP: Set to static
- Private IP Address: Set to an address within the subnet, in this case, we’re using 10.4.2.5
- Accelerated Networking set to “Disabled” by default by Azure. The steps to enable the parameter is given in the next section for user information.





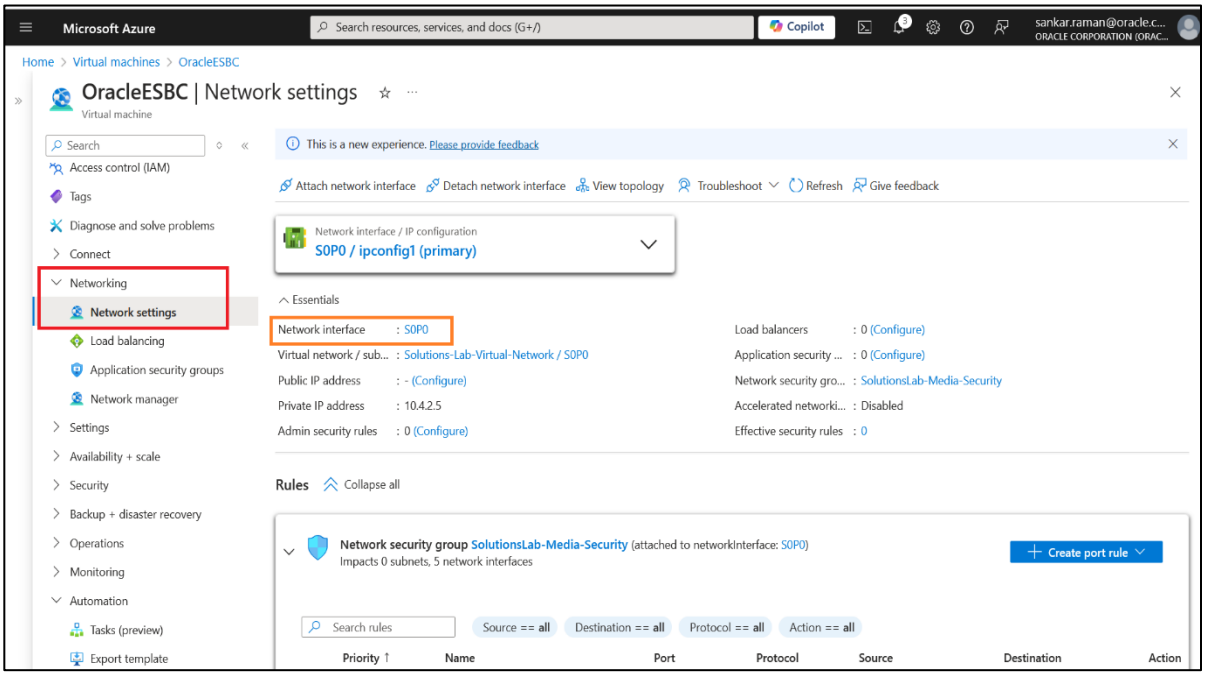
- At the bottom, Click “Create”

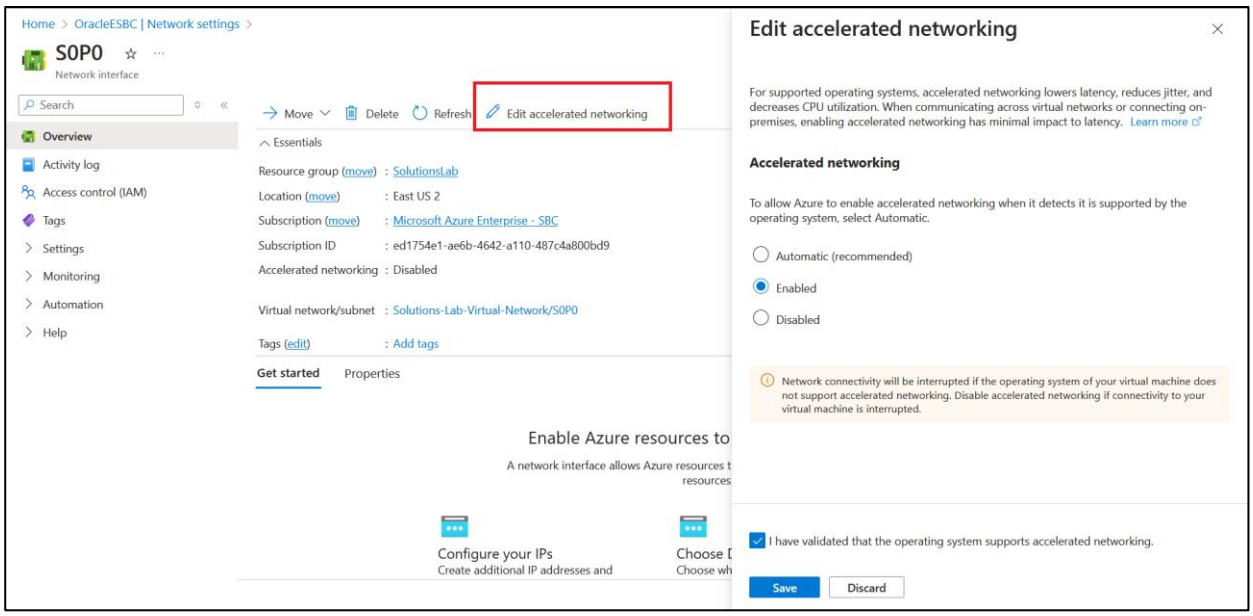
Once you press Create it will create the New Network Interface and also attach network interface, later it will bring you back to the main networking dialog.



In case you want to edit the settings of the accelerated networking for the media interfaces (S0P0, S1P0 etc.), please follow the steps given below.

1) From the Azure portal page for the VM, select Networking from the left menu.
2) On the Networking page, select the Network Interface and click on the network interface name.
3) At the top of the NIC Overview page, select Edit accelerated networking.
4) Select the options that you may require (Automatic, Enabled, or Disabled) and then select Save. In our example, we have enabled the option.





Follow this same procedure to create a second network interface with the following configuration:

- Name: S1P0
- Subnet: From the drop down, select the subnet created for S0P0 interface
- Network Security Group (move radio button to advanced, and select the Media NSG configured previously in this document)
- Private IP: Set to static
- Private IP Address: Set to an address within the subnet, in this case, we're using 10.4.3.5

Start your instance after creating and attaching all interfaces. Use the instance's Serial Console to connect to the virtual COM1 serial port. After boot-up, proceed with setting your OCSBC passwords from the OCSBC command line interface.

Initial access to SBC

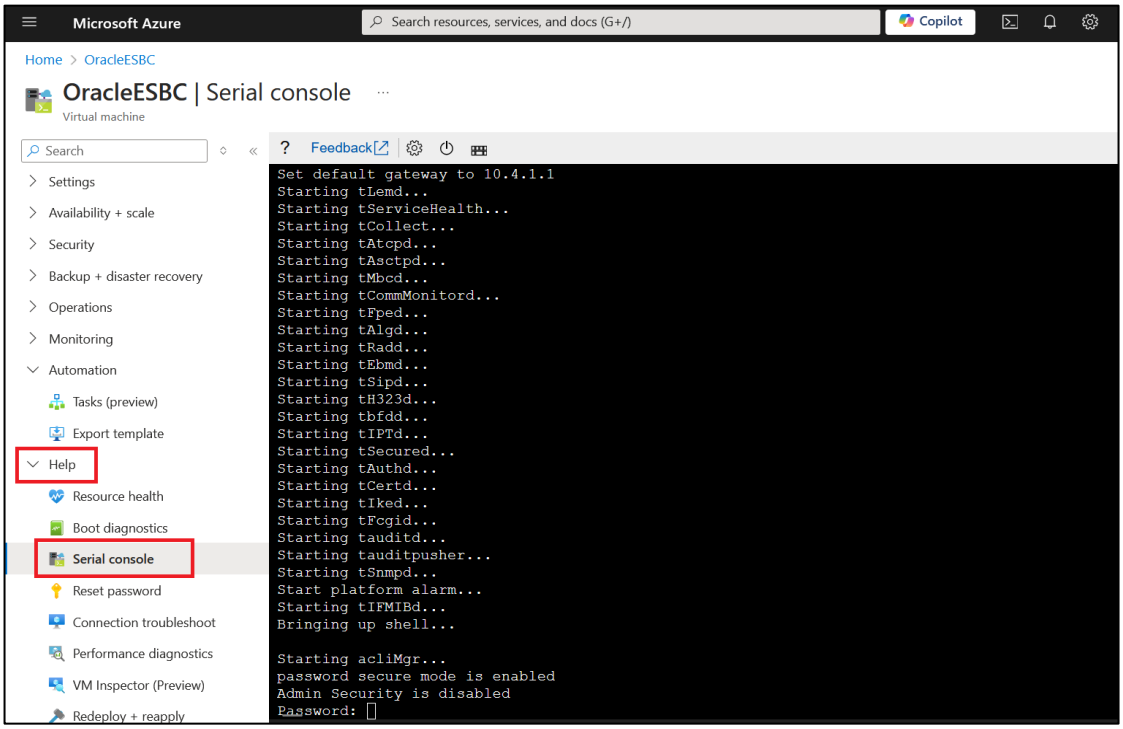
The procedure now turns to accessing the OCSBC, and steps required for initial setup

At this point, you could access the SBC in two ways:

1. SSH to the public IP address (or option DNS label name if configured), assigned to the management interface which can be easily located under the VME's "Overview" page
2. Access the SBC via the serial console in the Azure Portal (Only if custom storage account is enable in Boot Diagnostics setting)

For the purposes of this example, we will be utilizing the serial console for the initial access and setup procedure.

- To access the SBC serial console, click on serial console, under “Help”



Set User and Admin Passwords

You will need to set both the user and admin passwords when logging in for the first time

- At the password prompt, enter *“acme”* (*if accessing the SBC via SSH, username:”user”, password: “acme”*)
- When prompted, enter the new SBC user password twice, paying close attention to the rules displayed in the output

```
Starting acliMgr...
password secure mode is enabled
Admin Security is disabled
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:
```

- At the prompt, type “enable”
- Password: “packet”
- Enter the new admin password twice, paying close attention to the password rules displayed.

```
Password is acceptable.


Password changed successfully

Notifications:
- No Valid License Present! (aid: 327702, tid: 2907)
- Product not initialized; Please use 'setup product' (aid: 327725, tid: 2907)
> en
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:
```

Interface Mapping

The final step in deploying the Oracle SBC in Azure Public cloud is to verify the network interfaces have MAC addresses assigned to them.

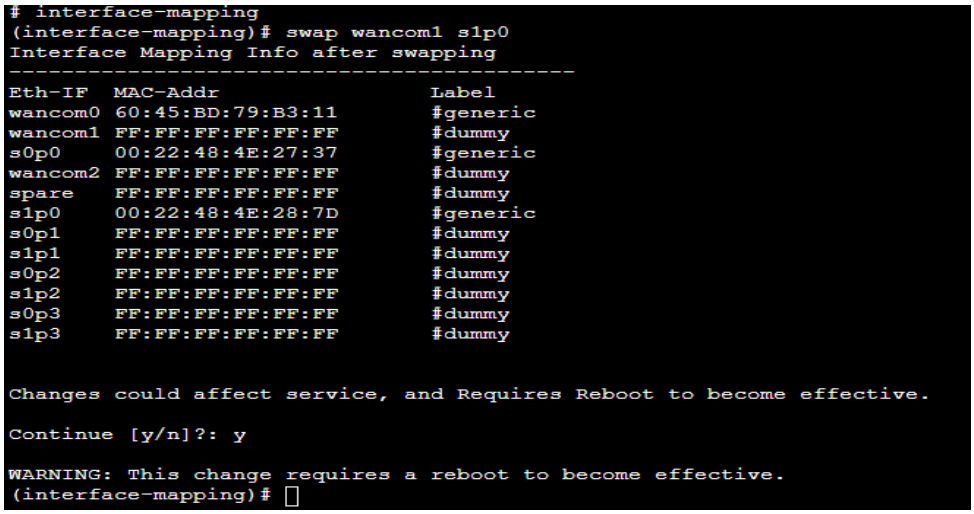
- Access the serial console through the azure portal under support + troubleshooting
- Log into enable mode
- Run the command

  >show interface mapping
  Interface Mapping Info:

```
# show interface mapping
Interface Mapping Info
------------------------------------------
Eth-IF  MAC-Addr                Label
wancom0 60:45:BD:79:B3:11       #generic
wancom1 00:22:48:4E:28:7D       #generic
s0p0    00:22:48:4E:27:37       #generic
wancom2 FF:FF:FF:FF:FF:FF       #dummy
spare   FF:FF:FF:FF:FF:FF       #dummy
s1p0    FF:FF:FF:FF:FF:FF       #dummy
s0p1    FF:FF:FF:FF:FF:FF       #dummy
s1p1    FF:FF:FF:FF:FF:FF       #dummy
s0p2    FF:FF:FF:FF:FF:FF       #dummy
s1p2    FF:FF:FF:FF:FF:FF       #dummy
s0p3    FF:FF:FF:FF:FF:FF       #dummy
s1p3    FF:FF:FF:FF:FF:FF       #dummy
```

- As you can see above, since we have not configured all eight network interfaces possible on the SBC, we’ll need to correct the interface to MAC address mappings.
- 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:



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

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

Oracle Corporation, World Headquarters
2300 Oracle Way
Austin, TX 78741, USA

Worldwide Inquiries
Phone: +1.650.506.7000 or
Phone: +1.800.392.2999

ORACLE

CONNECT WITH US


blogs.oracle.com


facebook.com/oracle


twitter.com/oracle


oracle.com/

Integrated Cloud Applications & Platform Services