QUICK START GUIDE

RUCKUS Virtual SmartZone Getting Started Guide

Part Number: 800-72269-001 Rev J
Publication Date: December 2022

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.commscope.com/ruckus and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://community.ruckuswireless.com
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.commscope.com/ruckus .

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{**x**| **y**| **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x|**y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About This Guide

About This Guide

This Virtual SmartZone (vSZ) Getting Started Guide provides information on how to set up the vSZ virtual appliance on the network. You can install the vSZ on any of the supported hypervisors.

Topics covered in this guide include preparing your chosen hypervisor, installing the vSZ image on to the hypervisor, and completing the vSZ Setup Wizard.

This guide is intended for use by those responsible for installing and setting up network equipment. Consequently, it assumes a basic working knowledge of local area networking, wireless networking, and wireless devices.

> **NOTE**
> If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Networks support website at https://support.ruckuswireless.com/documents.

New In This Document

TABLE 2 Key Features and Enhancements (September 2022)

Feature	Description	Reference
Doc defect: SCG-138492	**Updated**: A note is added pointing to the Upgrade Guide to know the hypervisor supported for a respective release.	Preparing a Hypervisor on page 21
Resource table	**Updated**: Support for vSZ-H and vSZ-E resources.	• Virtual SmartZone Minimum Requirements on page 14
Minor edits	**Updated**: Minor edits	• Creating the vSZ Instance on page 171 • Step 5: Configure the Cluster Settings on page 210 • Setting Up the vSZ with One Interface on page 185 • Installing AWS CLI on page 161

Installation Preparation

Obtaining the vSZ Distribution

You have to download the .OVA file and documentation for the controller from the vSZ download page on the Ruckus Networks support website. The vSZ distribution package, which is based on the Open Virtualization Format (OVF) framework, consists of a virtual appliance.

Open Virtualization Format contains the following files:

- Description file (.ovf)
- Manifest file (.mf)
- Virtual machine state file (.vmdk)

Preparing the vSZ Interface Settings to Use

vSZ comes with the option to operate with either one (1) network interface or three (3) network interfaces. Once the network interface configuration has been made and setup executed, the number of network interfaces can no longer be modified.

CAUTION
vSZ supports one (1) network interface on public cloud. Three (3) network interfaces option is only for on-premises vSZ.

CAUTION
If you choose to operate the vSZ with three network interfaces, you must configure the three vSZ interfaces to be on three different subnets when you run the Setup Wizard. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

- IP address
- Netmask
- Gateway
- Primary DNS server
- Secondary DNS server

TABLE 3 vSZ interfaces

Interface	Description
AP	Used for AP configuration and client traffic
Cluster	Used for cluster traffic
Management (Web)	Used for management traffic. The IP address that you assign to this interface will be the IP address at which you can access the vSZ web interface.

Virtual SmartZone Minimum Requirements

NOTE
One or more resources can be higher than the specified requirements. For example, if the instance requires 24Gb RAM, assigning 32Gb RAM is supported.

NOTE
Supported version of the hypervisor may change for every vSZ release. To know the hypervisor version supported for a specific release, refer to the respective release of the Upgrade Guide.

Hypervisor Hardware Performance Requirements

vSZ requires enough hardware resources to sustain the service. vSZ cannot support deployment in low performance hypervisor.

- Sharing hardware server to multiple vSZ instances is not recommended.
- vSZ needs to be deployed on dedicated hardware resource to avoid different VM instance grabbing CPU or IO resources, which can impact vSZ stability in a hypervisor, especially in a scenario where thousands of APs per node are deployed.
- vSZ needs to reach both CPU and IO requirement. Measure the hypervisor hardware performance before deploying vSZ.
- Disks IO is most important in vSZ cluster. Disk IO is the slowest subsystem in a server, which means that write-heavy clusters can easily saturate their disks, which in turn become the bottleneck of the cluster. Avoid network-attached storage (NAS). People routinely claim their NAS solution is faster and more reliable than local drives. NAS is often slower, displays larger latencies with a wider deviation in average latency, and is a single point of failure.

Hypervisor CPU/IO Requirements - Private Hypervisor

CPU Performance Requirement

- CPU single core events per second/per core need > 180 events/sec
- Required CPU level is higher than the Intel Xeon CPU E5-4620 v4 with 2.10 GHz

IO performance requirement detail

vSZ require high IO performance deploy environment. Measure the hypervisor IO performance before deployment. vSZ IO throughput requirements :

- IO requirement per resource level - Refer to the **Disk IO Requirement** column in the resource table.
- Avoid network-attached storage (NAS/SAN). The general claim is that the NAS/SAN solution is faster and more reliable than the local drives. NAS/SAN is often slower, displays larger latencies with a wider deviation in average latency, and is a single point of failure.
- Virtual Disk - Preallocated/Eager Zeroed/Fixed Size is required to provide good performance and low latency for IO. Avoid using "Thick Provision Lazy Zeroed/Dynamic Expanding" to impact IO performance. **[*]**.

How to benchmark vSZ CPU/IO Performance

- The vSZ setup process will detect the IO performance at first setup step.
- Use the SZ CLI in **debug-tools** > **system** > **system performance**. The command will run system benchmark on CPU and IO for vSZ.

Network Latency Requirement between vSZ nodes

A fast and reliable network is important for performance in a distributed system. Low latency helps ensure that nodes can communicate easily, while high bandwidth helps shared movement and recovery. Avoid clusters that span multiple data centers, even if the data centers are located in close proximity. It is highly recommended to avoid clusters that span large geographic distances.

vSZ requires low network latency between vSZ nodes on the control & cluster interface network. vSZ cannot support deployment in high network latency environment.

vSZ interface network latency between nodes: Cluster Interface network latency need < 60 ms.

Before upgrading vSZ to this release, verify that the virtual machine on which vSZ is installed has sufficient resources to handle the number of APs, wireless clients and ICX Switches that you plan to manage. See the tables below for the **required** virtual machine system resources.

The values for vCPU, RAM, and Disk Size are linked together and cannot be changed individually. When changing one of these parameters, all three values need to **match exactly** with an existing Resource Level. Taking vSZ-H Resource Level 5 as an example: when adjusting the number of vCPU from 4 to 6, the amount of RAM needs to be adjusted to 22GB and the Disk Size needs to be adjusted to 300GB, thereby matching all the values of Resource Level 6.

NOTE
The vSZ deployed in the Nutanix Hypervisor introduces more overhead on memory. The 10K AP per node is not sustained on 48GB memory setting. **[SCG-113477]**
Workaround: When deploying vSZ on Nutanix it is recommended to allocate more memory for vSZ usage. For a 10K AP resource level, setup needs 24 core CPU and 50 GB (+2GB) memory to control. Alternatively decrease to 25% AP deployment in vSZ resource level. For example, 7500 AP in 10K AP resource level.

WARNING
These vSZ required resources may change from release to release. Before upgrading vSZ, always check the required resource tables for the release to which you are upgrading.

NOTE
When initially building up the network it can use a higher Resource Level than needed for the number of APs first deployed, if all the three parameters (vCPU, RAM and Disk Size) **match exactly** with that higher Resource Level.

ATTENTION
It is recommended that there should be only one concurrent CLI connection per cluster when configuring vSZ.

In the following tables the high scale resources are broken into two tables for easy readability. These tables are based on the *AP Count Range*.

TABLE 4 vSZ High Scale required resources

AP Count Range		Max Clients	Nodes per Cluster	AP Count per Node (without Switch)	AP/Switch Capacity Ratio	Maximum Switch (w/o AP)
From	**To**			**Max**		**Max**
10,001	30,000	300,000	4	10,000	5 : 1	6,000
	20,000	200,000	3		5 : 1	4,000
10,001	30,000	300,000	4	10,000	5 : 1	6,000
	20,000	200,000	3		5 : 1	4,000
6,001	10,000	100,000	1-2	10,000	5 : 1	2,000
5,001	6,000	60,000	1-2	6,000	5 : 1	1,200
3,001	5,000	50,000	1-2	5,000	5 : 1	1,000
2,501	3,000	30,000	1-2	3,000	5 : 1	600
1,001	2,500	25,000	1-2	2,500	5 : 1	500
501	1,000	20,000	1-2	1,000	5 : 1	200
101	500	10,000	1-2	500	5 : 1	100

TABLE 4 vSZ High Scale required resources (continued)

AP Count Range		Max Clients	Nodes per Cluster	AP Count per Node (without Switch)	AP/Switch Capacity Ratio	Maximum Switch (w/o AP)
From	**To**			**Max**		**Max**
1	100	2,000	1-2	100	5 : 1	20

TABLE 5 vSZ High Scale required resources

AP Count Range		Minimum vCPU per node	Minimum RAM per node[1]	Minimum Disk Size per node[2]	Minimum Disk IO Requirement per node	Preserved Event/Alarm Days	Concurrent CLI Connection	Resource Level
From	**To**	**Logic Processor**	**GB**	**GB**	MiB/s	**Max**	**Max** (per node not per cluster)	
10,001	30,000	24	56	600	45	3/7 Days	4	9[5]
	20,000							
10,001	30,000	24	48	600	45	3/7 Days	4	8
	20,000							
6,001	10,000	24	48	600	45	3/7 Days	4	7
5,001	6,000	16	30	300	35	3/7 Days	2	6.6
3,001	5,000	12	28	300	30	3/7 Days	2	6.5
2,501	3,000	8	24	300	30	3/7 Days	2	6.1
1,001	2,500	6	22	300	25	3/7 Days	2	6
501	1,000	4-6[*4]	18	150	20	3/7 Days	2	5
101	500	4	16	150	15	3/7 Days	2	4
1	100	2-4[*3]	13	150	15	3/7 Days	2	3

In the following tables the essential scale resources are broken into two tables for easy readability. These tables are based on the *AP Count Range*.

TABLE 6 vSZ Essentials required resources

AP Count Range		Maximum Clients	Nodes per Cluster	AP Count per Node	AP/Switch Capacity Ratio	Maximum Switch (w/o AP)
From	**To**			**Max**		**Max**
1025	3,000	60,000	4	1,024	5 : 1	600
	2,000	40,000	3		5 : 1	400
501	1,024	25,000	1-2	1,024	5 : 1	204
101	500	10,000	1-2	500	5 : 1	100
1	100	2,000	1-2	100	5 : 1	20

NOTE

The recommended vCPU core for the vSZ-E with **AP Count Range** 1 through 100 is 2-4.

TABLE 7 vSZ Essentials required resources

AP Count Range		Minimum vCPU per node	Minimum RAM per node [1]	Minimum Disk Size per node[2]	Minimum Disk IO Requirement	Preserved Event/ Alarm Days	Concurrent CLI Connection	Resource Level
From	**To**	**Logic Processor**	**GB**	**GB**	MiB/s	**Max**	**Max** (per node not per cluster)	
1025	3,000	8	20	250	20	7 Days	2	3
	2,000							
501	1,024	8	20	250	20	7 Days	2	2
101	500	4	16	150	15	7 Days	2	1.5
1	100	2-4[*3]	13	150	15	7 Days	2	1

NOTE

[1] - vSZ-H and vSZ-E have different report interval. For example, AP sends the status to vSZ-E every 90 seconds but to vSZ-H it is sent every 180 seconds, which means that vSZ-E need more RAM in scaling environment based on the resource level.

[2] - NICs assigned to direct IO cannot be shared. Moreover, VMware features such as vMotion, DRS, and HA are unsupported.

Public Cloud Platform - Instance Resource Type

In the following tables the high scale resources are broken into two tables for easy readability. These tables are based on the *AP Count Range*.

TABLE 8 vSZ High Scale

AP Count Range		Max Clients	Nodes per Cluster	AP Count per Node (without Switch)	Maximum Switch (w/o AP)
From	**To**			**Max**	**Max**
10,001	30,000	300,000	4	10,000	6,000
	20,000	200,000	3		4,000
6,001	10,000	100,000	1-2	10,000	2,000
3,001	6,000	60,000	1-2 [*4]	6,000	1,200
1,001	3,000	30,000	1-2	3,000	600
501	1,000	20,000	1-2	1,000	200
101	500	10,000	1-2	500	100
1	100	2,000	1-2	100	20

TABLE 9 vSZ High Scale

AP Count Range		Minimum Disk Size	Recommended Machine Type for AWS	Recommended Machine type for AZure	Disk IO Requirement
From	**To**	**GB**			
10,001	30,000	600	c5.9xlarge (36 vCPU/72 GB RAM)	F32s_v2 (32 vCPU/64 GB RAM)	45
	20,000				
6,001	10,000	600	c5.9xlarge (36 vCPU/72 GB RAM)	F32s_v2 (32 vCPU/64 GB RAM)	45
3,001	6,000	300	c5.4xlarge (16 vCPU/32 GB RAM)	F16s_v2 (16 vCPU/32 GB RAM)	35

TABLE 9 vSZ High Scale (continued)

AP Count Range		Minimum Disk Size	Recommended Machine Type for AWS	Recommended Machine type for AZure	Disk IO Requirement
From	**To**	**GB**			
1,001	3,000	300	m5.2xlarge (8 vCPU/32 GB RAM)	D8s_v3 (8 vCPU/32 GB RAM)	25
501	1,000	150	r5.xlarge (4 vCPU/32GB RAM)	E4s_v3 (4 vCPU/32 GB RAM)	20
101	500	150	m5.xlarge (4 vCPU/16 GB RAM)	D4s_v3 (4 vCPU/16 GB RAM)	15
1	100	150	r5.large (2 vCPU/16 GB RAM)	DS11_v2 (2 vCPU/14 GB RAM) or D4s_v3 (4 vCPU/16 GB RAM)	15

In the following tables the essential scale resources are broken into two tables for easy readability. These tables are based on the *AP Count Range*.

TABLE 10 vSZ Essentials required resources

AP Count Range		Maximum Clients	Nodes per Cluster	AP Count per Node	Maximum Switch (w/o AP)
From	**To**			**Max**	**Max**
1025	3,000	60,000	4	1,024	600
	2,000	40,000	3		400
501	1,024	25,000	1-2	1,024	204
101	500	10,000	1-2	500	100
1	100	2,000	1-2	100	20

NOTE

The recommended vCPU core for the vSZ-E with **AP Count Range** 1 through 100 is 2-4.

TABLE 11 vSZ Essentials required resources

AP Count Range		Minimum Disk Size	Recommended Machine Type for AWS	Recommended Machine type for AZure	Disk IO Requirement
From	**To**	**GB**			
1025	3,000	250	m5.2xlarge (8 vCPU/32 GB RAM)	D8s_v3 (8 vCPU/32 GB RAM)	20
	2,000				
501	1,024	250	m5.2xlarge (8 vCPU/32 GB RAM)	D8s_v3 (8 vCPU/32 GB RAM)	20
101	500	150	m5.xlarge (4 vCPU/16 GB RAM)	D4s_v3 (4 vCPU/16 GB RAM)	15
1	100	150	r5.large (2 vCPU/16 GB RAM)	DS11_v2 (2 vCPU/14 GB RAM) or D4s_v3 (4 vCPU/16 GB RAM)	15

NOTE

- [1] - Increase the vSZ total memory 2~4 GB when running on special or extreme deploy environment when vSZ raise a memory exceed (90%) alarm. For example:
  - Deploy 4-node vSZ cluster on Nutanix with full 30K AP capacity.
  - One vSZ node down in 4-node vSZ cluster to long term sustain 30K AP in 3 alive vSZ nodes.

    The solution should be recovered the fail vSZ node as soon as possible. But if user need run 3 nodes with 30K AP in long term sustain, it need to increase the vSZ memory to run.
  - All APs with full statistic reports (AVC, HCCD, UE, ...) to SZ on full load stress condition.
- [2] - Required Disk Type
  - AWS: General Purpose SSD (gp2)
  - GCE: SSD
  - Azure: Standard-SSD
- [3] - If deployed hardware CPU computing performance is not good as recommended in 100 AP resource level, the 2 cores CPU setting cannot be supported. Upgrade to 4 cores instead of 2 cores in this case.
- [4] - If deployed hardware CPU computing performance is not good as recommended Hypervisor (like Hyper-V) in 4-CPU setting to support 1000K AP, upgrade to 6 cores instead of 4 cores in this case.
- [5] - Resource level 9 is added for cases that does not sustain the loading with resource level 8.
- The 6000 AP resource profile level could support to 4 nodes cluster. The total supported AP number will be up to 18,000 APs in a 4 node vSZ cluster.
- Workaround if virtualization platform always need Thin Provision/Lazy Zeroed/Dynamic Expanding case.

Change Log of vSZ Resource Plan

- New support for 3000, 6000 APs resource level for more flexibile deployment and better cost effectiveness for customer.
- Due to system limitation for the minimum disk requirement, the base disk size requirement is increased from 100 GB to 150 GB on low level resource profile. No impact for user to upgrade from previous version. Requires new setup vSZ to follow new disk size.
- As the resource level has hit the system limitation in some case, for the vSZ-E 1024 APs resource level memory is increased from 18 GB to 20 GB. No impact for user to upgrade from previous version. User need to change only the memory setting when encountering memory usage alarm exceeding 90%.
- Adding additional notes vSZ memory required in extreme vSZ deployment and cases.
- New session, vSZ-H instance Resource Allocate Instruction, is added.

Clustering Limitations

The following are the limitations for vSZ-H and vSZ-E.

Clustering Limitations for vSZ-H

- vSZ-H supports up to 10,000 APs per node or 30,000 APs per cluster, assuming proper system resources are made available. It supports clustering of up to 4 nodes when using Resource Level 8.
- At 4 nodes, the maximum number of APs and clients that can be supported are 30,000 and 300,000 respectively.

Clustering Limitations for vSZ-E

- vSZ-E supports up to 1,024 APs per node or 3000 APs per cluster, assuming proper system resources are available. It supports clustering of up to 4 nodes when using Resource Level 3.
- At 4 nodes, the maximum number of APs and clients that can be supported are 3,000 and 60,000 respectively.
- NAT operation for vSZ cluster: Currently, each node requires its own public IP address for its NAT'ed interface. As such, a 1:1 NAT is recommended for setting up a cluster behind a NAT environment.

Installing the vSZ on a Hypervisor

Preparing a Hypervisor

NOTE
Supported version of the hypervisor may change for every vSZ release. To know the hypervisor version supported for a specific release, refer to the respective release of the Upgrade Guide.

Hypervisor CPU/IO Requirements - Self Own Hypervisor

Benchmarking vSZ CPU/IO Performance

Refer to the SZ System Benchmark Tool (`SZ_System_Benchmark_Tool_0.ksp`) released by Ruckus to measure vSZ in Hypervisor performance. This tool provides the benchmark result and performance measure to run vSZ on CPU (Central Processing Unit) and IO (Input Output).

Performance Requirement

CPU	CPU single core events per second/per core need > 180.
IO	Requirements change per resource level. Refer to resource table for minimum values (column 'Disk IO requirement')

NOTE
This benchmark tool is relevant for SmartZone releases 3.4.2, 3.6.2 and 5.1.1. From release 5.2, the system benchmark tool will be inbuilt through CLI command.

NOTE
You can download the `SZ_System_Benchmark_Tool_0.ksp` from the support website: https://support.ruckuswireless.com/software/2138-smartzone-5-1-1-mr1-virtual-smartzone-system-benchmark-tool-ksp.

Installing the vSZ on VMWare vSphere Hypervisor

You have to install the vSZ on a VMWare vSphere hypervisor.

Before You Begin

You have to complete the prerequisites before installing the vSZ on VMWare vSphere.

Verify that you have the prerequisites before installing the vSZ on VMWare vSphere.

- Verify that vSphere client is installed.

- You can deploy the vSZ only on hosts that are running ESXi version 5.5 and later (6.7 or later recommended).
- The vSZ appliance requires at least 150GB of disk space and is limited to a maximum size of 600GB. The vSZ appliance can be deployed with thin provisioned virtual disks that can grow to the maximum size of 600GB.
- Preallocated/Eager Zeroed/Fixed Size is required to provide good performance and low latency for IO.
- Avoid using "Thick Provision Lazy Zeroed/Dynamic Expanding" to impact IO performance.

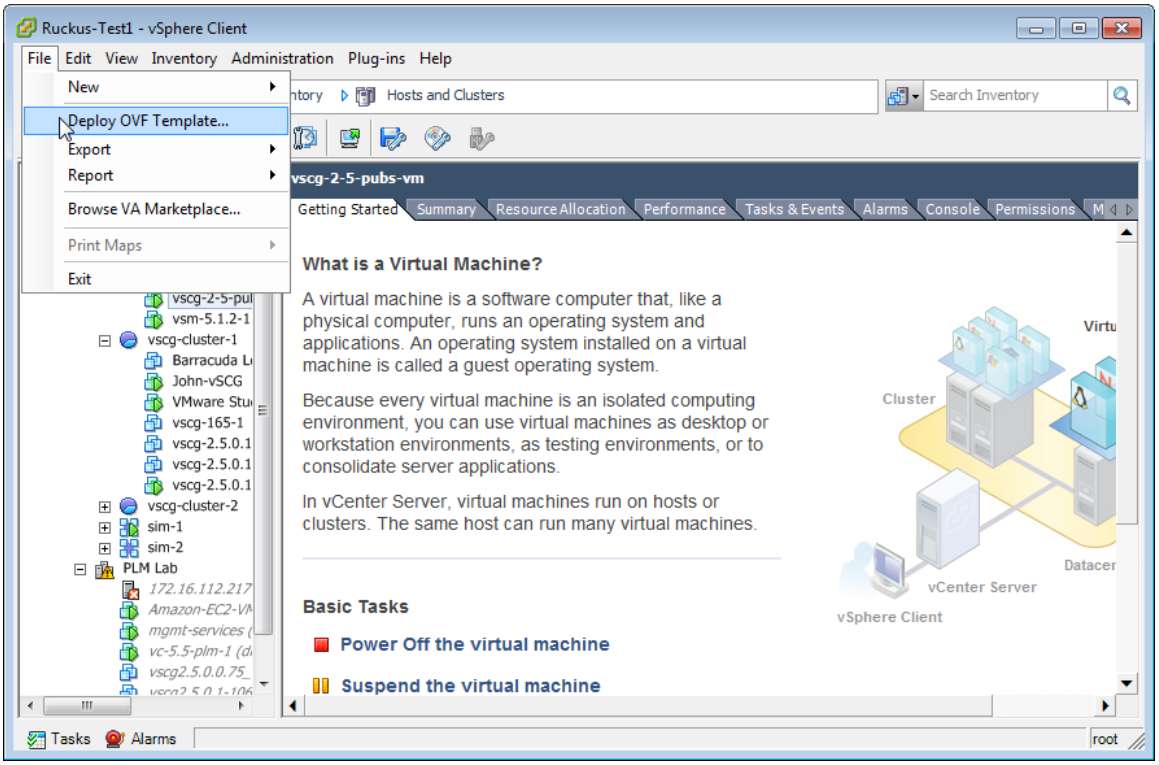
Creating a vSZ Instance from the OVA File

You can create a vSZ instance using the vSphere Web Client.

Before continuing, ensure you have already downloaded the vSZ distribution package. See Obtaining the vSZ Distribution for more information. Follow these steps to create a vSZ instance from the OVA file.

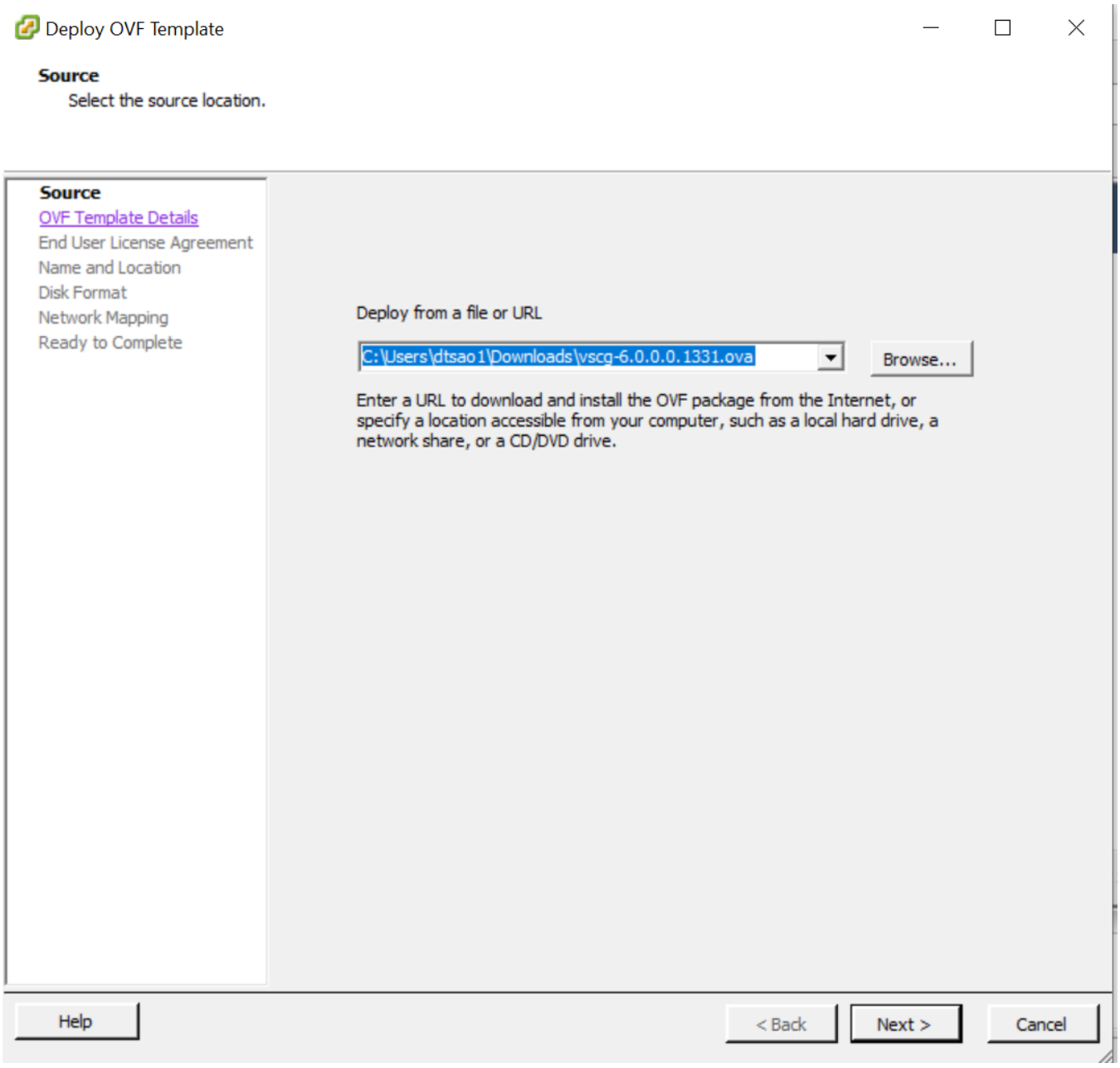
1. Use the VMWare vSphere client to log on to the ESXi management interface.
2. Click **File**> **Deploy OVF Template**. The Source screen of the **Deploy OVF Template** wizard appears.

FIGURE 1 Click Deploy OVF Template



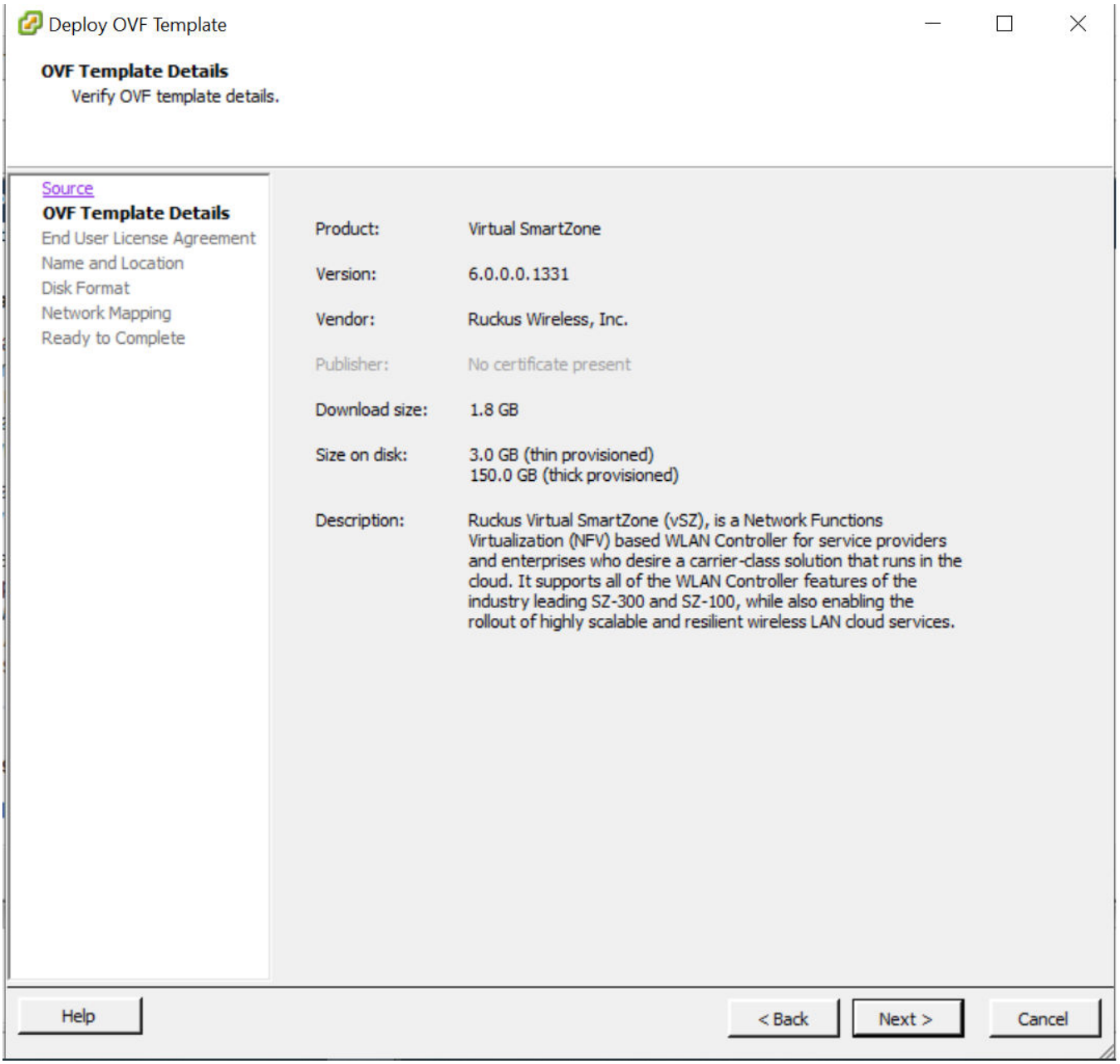
3. Click **Browse** to locate the .ova file that you downloaded earlier. Select the template.

FIGURE 2 Click Browse, and then locate and select .ova file



4. Click **Next**. The **OVF Template Details** screen appears.

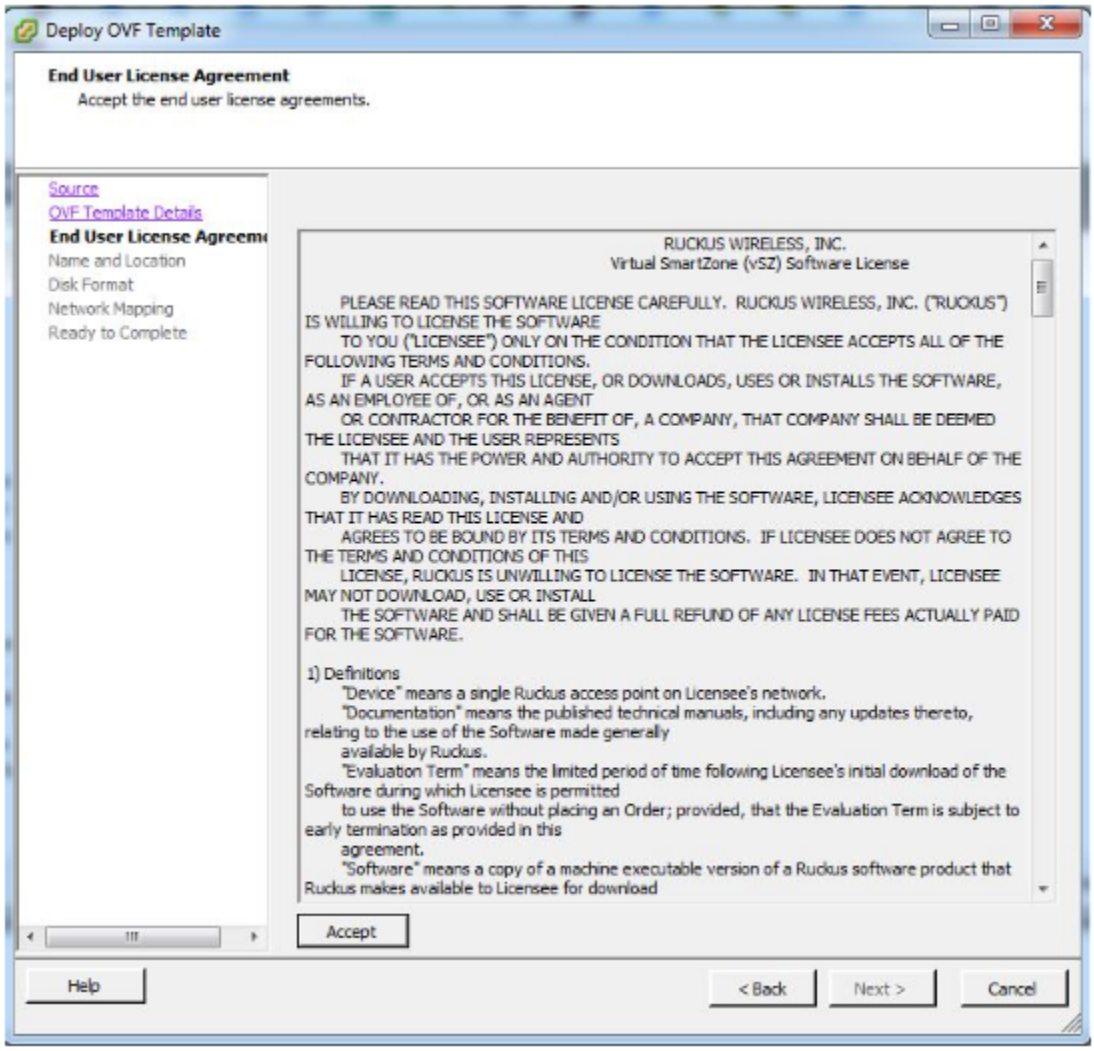
FIGURE 3 The OVF Template Details screen



5. Review the OVA virtual appliance details, and then click **Next**. The End User License Agreement (EULA) screen appears.

6. Click **Accept** to agree to the EULA terms, and then click **Next**.

FIGURE 4 Accept the EULA for the vSZ OVA



7. Select the disk format that is appropriate for your deployment scenario. Options include:
   - Thick Provision Lazy Zeroed
   - Thick Provision Eager Zeroed
   - Thin Provision

FIGURE 5 Select the disk format for your deployment scenario

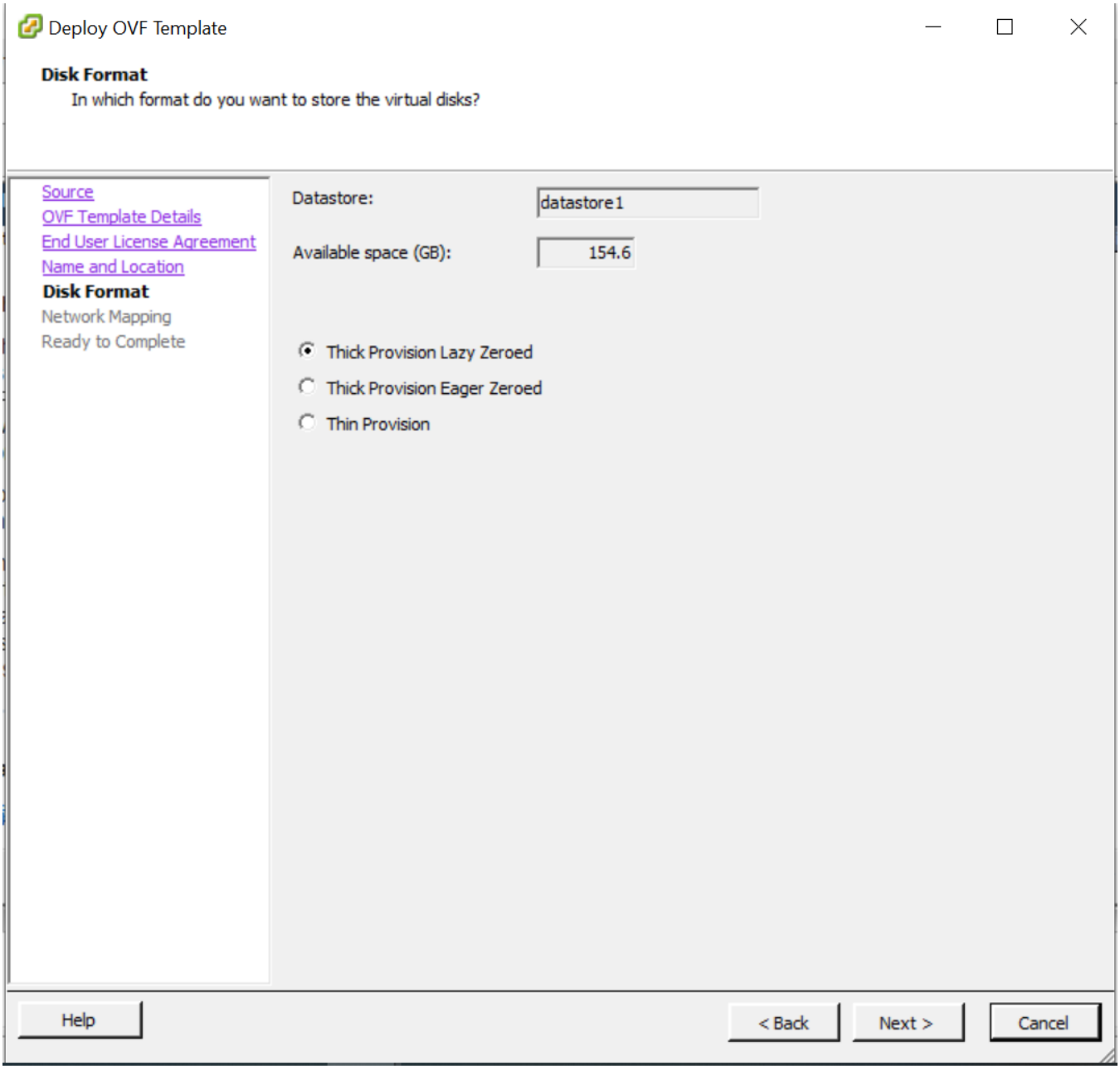
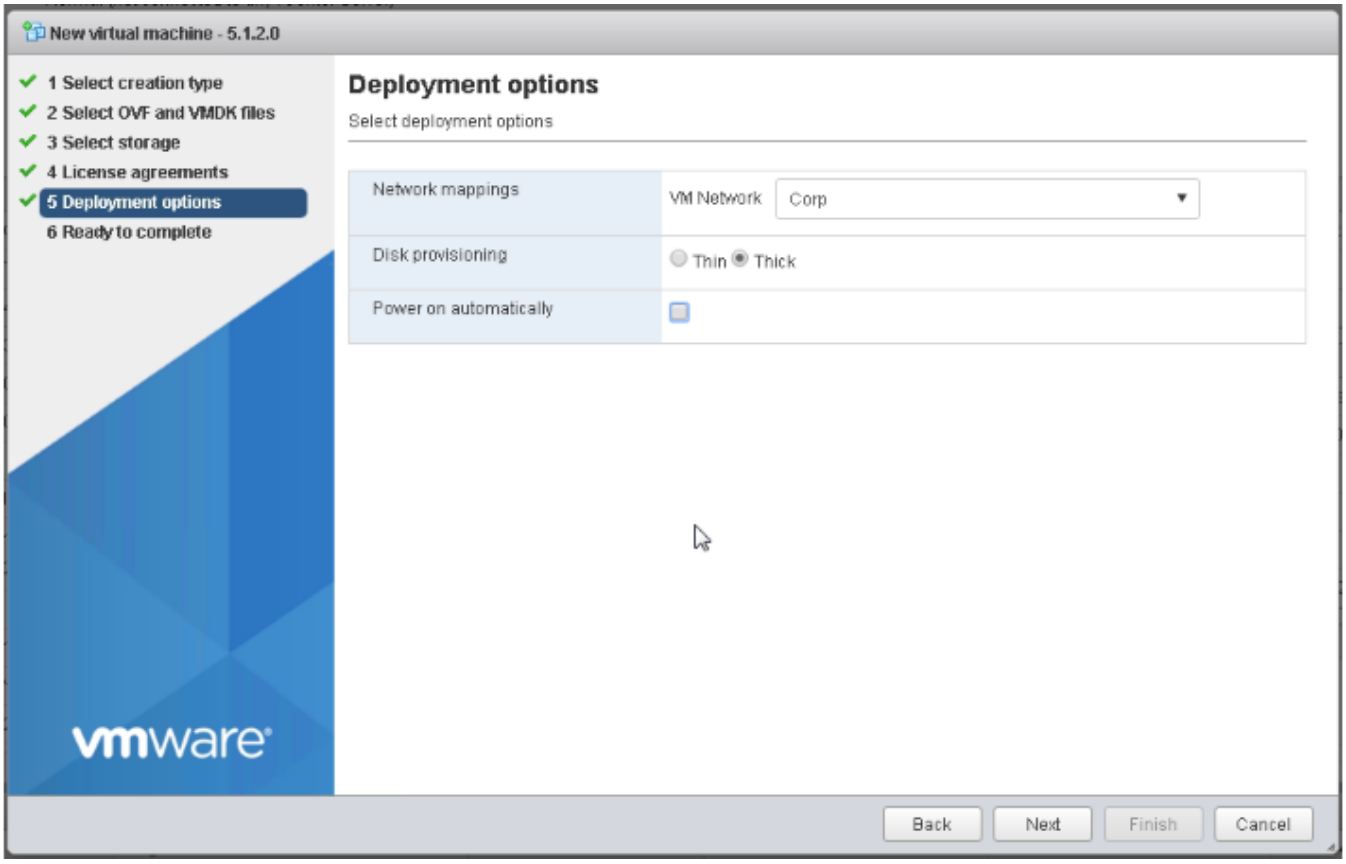


FIGURE 6 ESXi 6.7 with two options

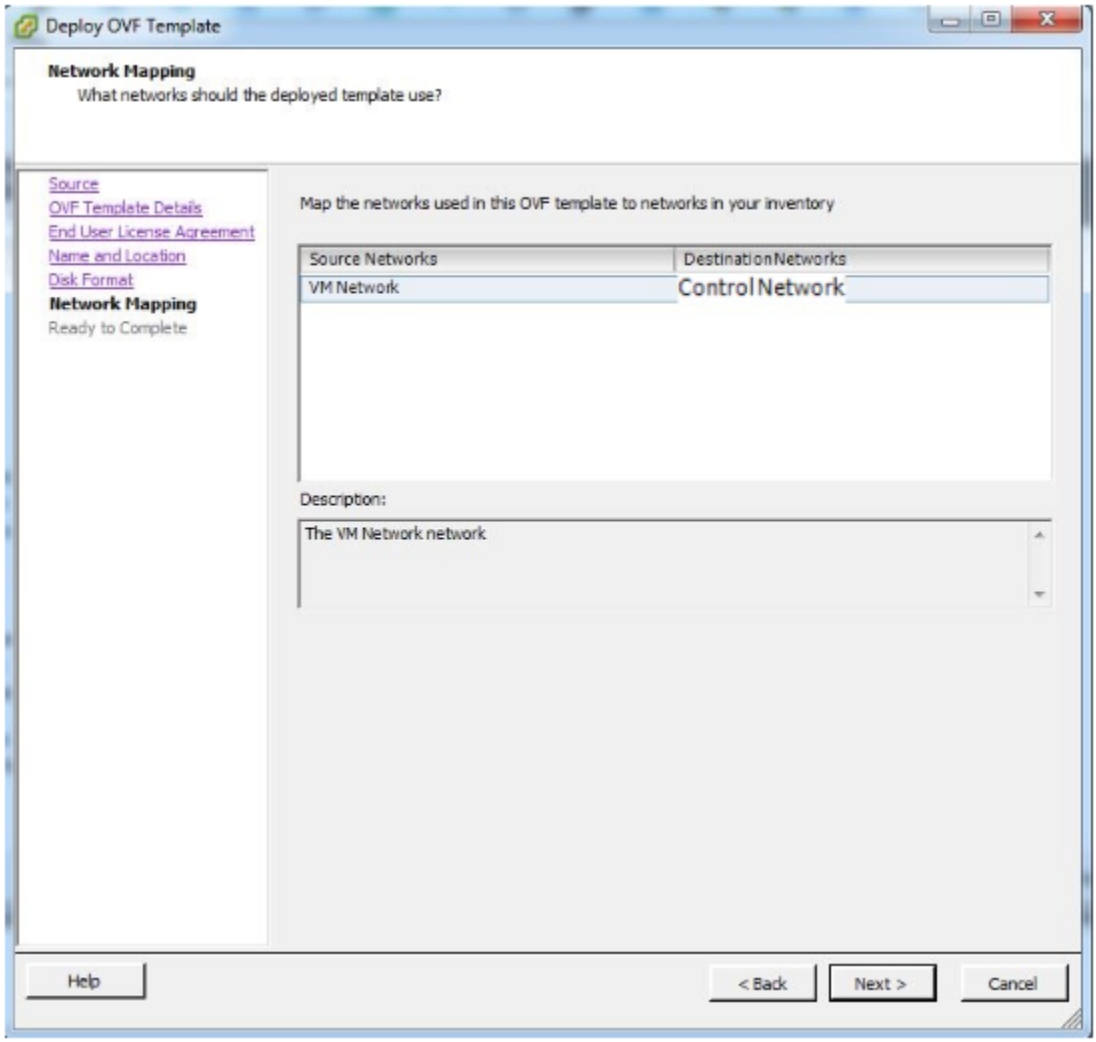


8. Click **Next**. The **Network Mapping** screen appears.

9. Select the ESXi virtual network interface that you want to use for the control interface, and then click **Next**. The **Ready to Complete** screen appears.

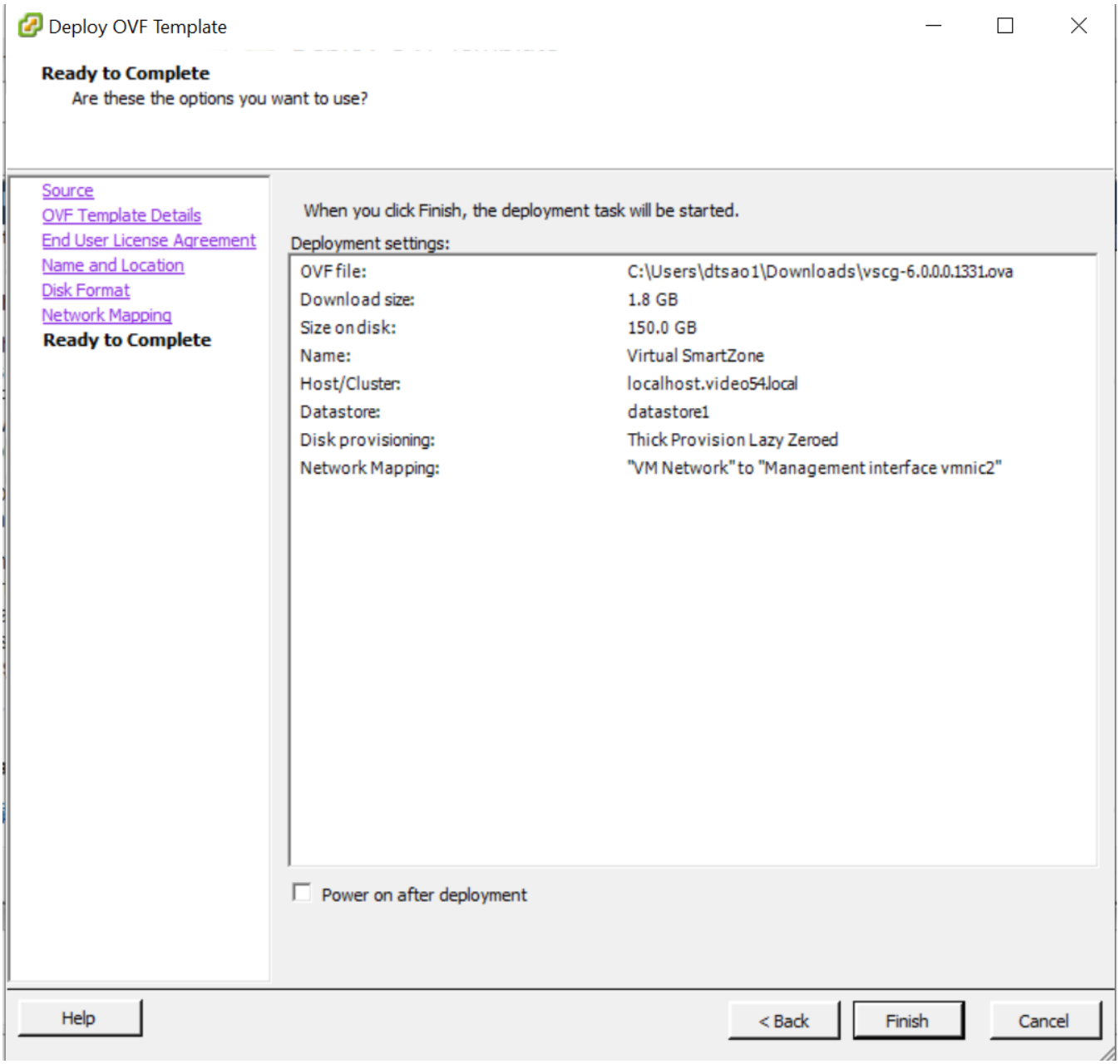
   The installation screen only allows you to select the virtual network interface for the control interface. After you complete the installation (and before you power on and set up the vSZ), you will need to adjust the cluster and management interfaces as appropriate.

   FIGURE 7 Select the virtual network interface that the template will use



10. Review the settings that you have configured on the previous screens. If you find a setting that you want to change, click **Back** until you reach the screen where you can edit the setting. Update the setting, and then click **Next** until you reach the **Ready to Complete** screen again.

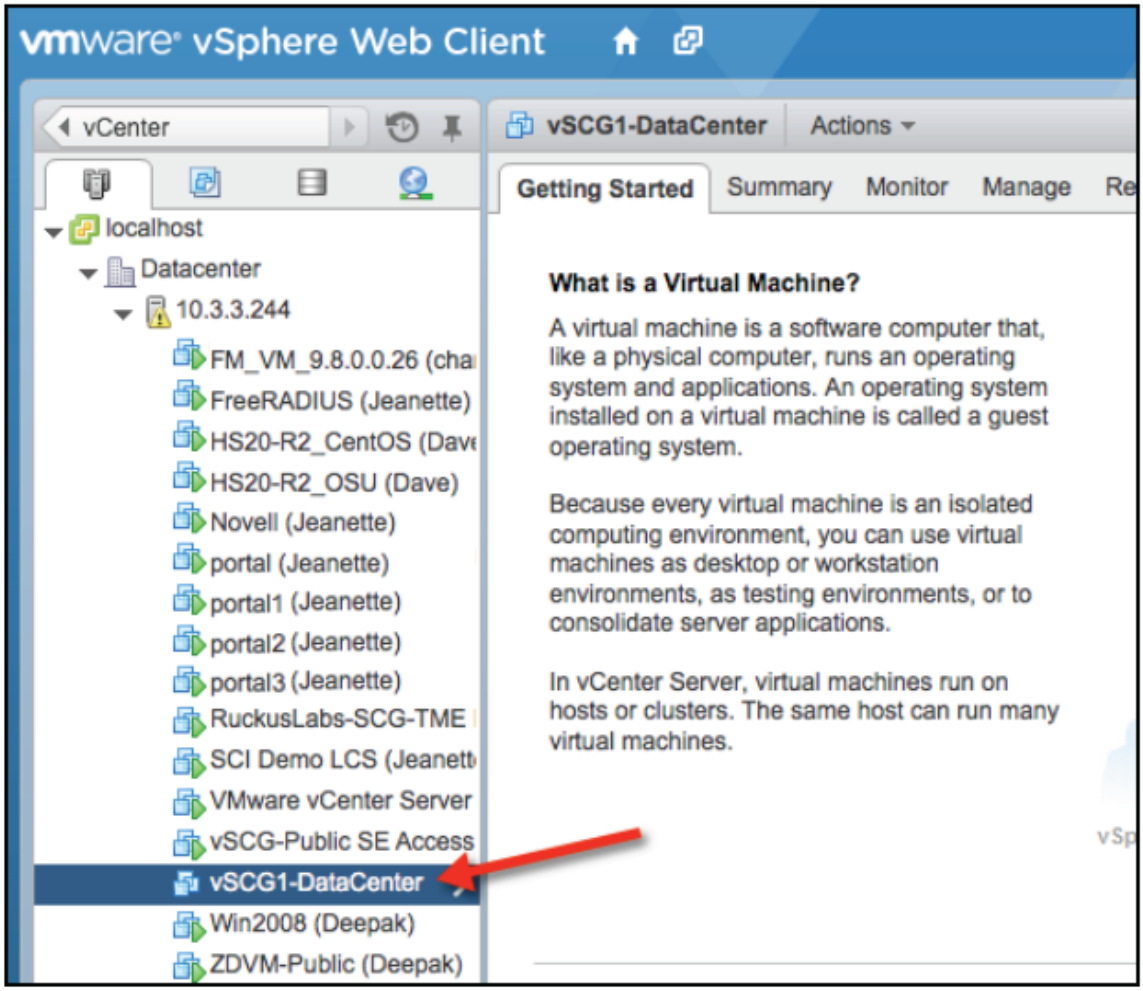
FIGURE 8 Review the settings that you have configured



11. Make sure that the **Power on after deployment** check box is clear so you can adjust the network settings before the vSZ setup.**Caution**: If you power on the vSZ after installation, you will no longer be able to adjust the network settings.
12. Click **Finish**.

ESXi deploys the new vSZ instance. When ESXi completes the deployment, the new vSZ instance appears on the list of installed virtual machines on the target host.

FIGURE 9 The vSZ instance appears on the list of installed VMs



You have completed creating a vSZ instance from the OVA file.

Allocating Resources and Assigning Network Interfaces

Before starting the vSZ instance for the first time, edit the virtual machine settings to allocate CPU and memory resources to the vSZ and to assign the ESXi network interfaces to the remaining vSZ interfaces (cluster and management).

Ensure that you read steps 1-7 before starting the application.

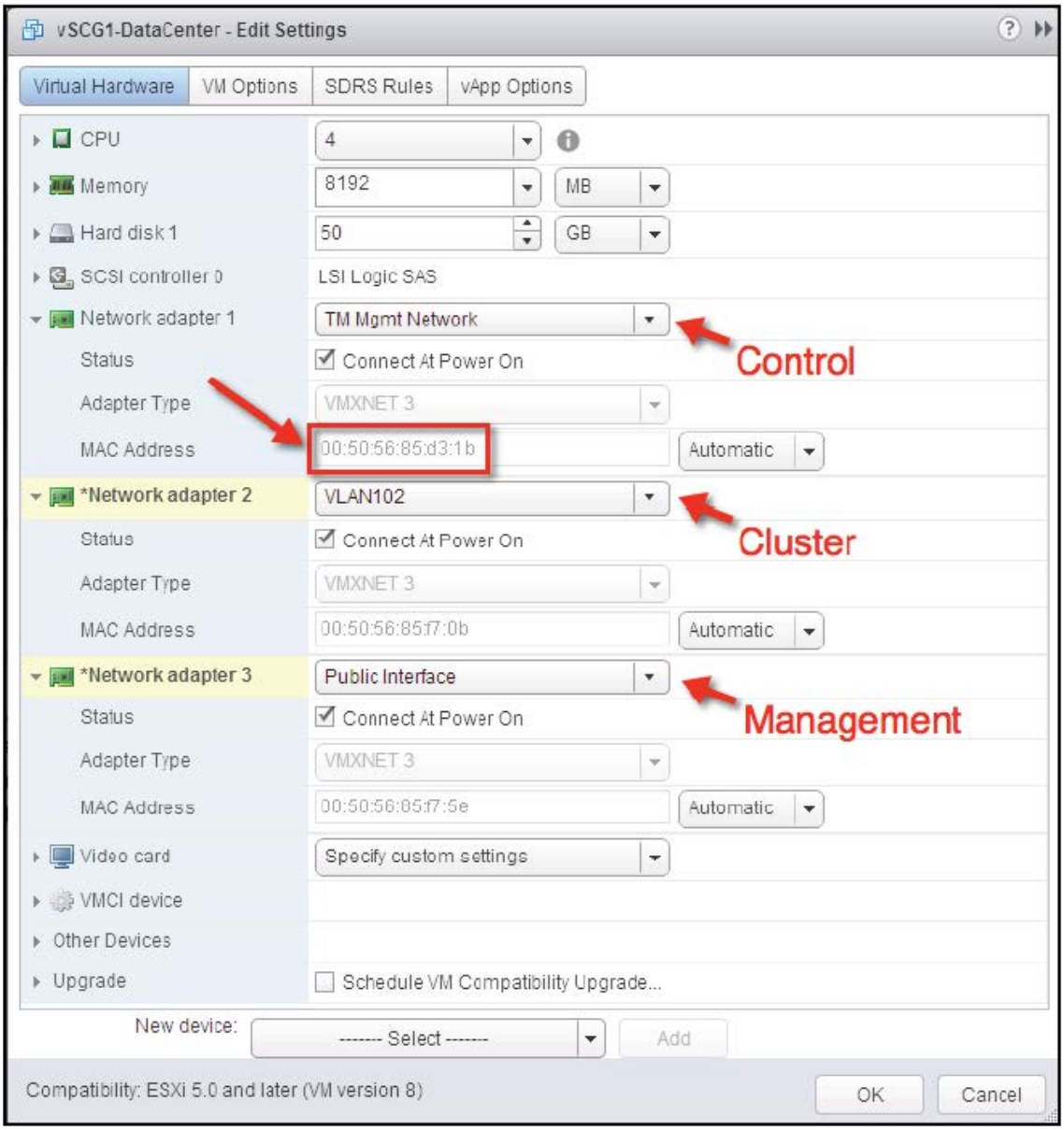
Follow these steps to allocate resources and assign network interfaces to the vSZ.

1. On the list of virtual machines, click the new vSZ instance.
2. Click **Actions** to display the additional options, and then click **Edit Settings**.
3. Set the number of CPUs and the amount of RAM to allocate to the vSZ instance. By default, the OVA template is set to 4 CPUs and 13GB of RAM.

4. Under **Network adapter 1**, verify that it is the same ESXi network interface that you selected for the control interface during the OVA import process. Ensure that the **Connect at Power On** check box is selected.
5. Under **Network adapter 2**, select the ESXi network interface for the cluster interface from the drop-down list. Ensure that the **Connect at Power On** option is selected.
6. Under **Network adapter 3**, select the ESXi network interface for the management interface from the drop-down list. Ensure that the **Connect at Power On** option is selected.

NOTE
All three interfaces, if used, must be of the same adaptor type. For example, E1000 or VMXNET3.

FIGURE 10 Select the interfaces to use



7. Click **OK**. You have completed allocating resources and assigning network interfaces to the vSZ.

Powering on the vSZ virtual machine

The next step is to power on the vSZ virtual appliance.

1. From the list of virtual machines on the host, click the vSZ instance.
2. Under **Basic Tasks**, click **Power on the virtual machine**.

   FIGURE 11 Click Power on the virtual machine

3. Open a console window to monitor the startup process. To do this, click the *Action* menu, and then click **Open Console**.

   After the vSZ completes its startup process, you are ready to perform the initial IP address setup of the vSZ. You will use the console connection to perform this task.

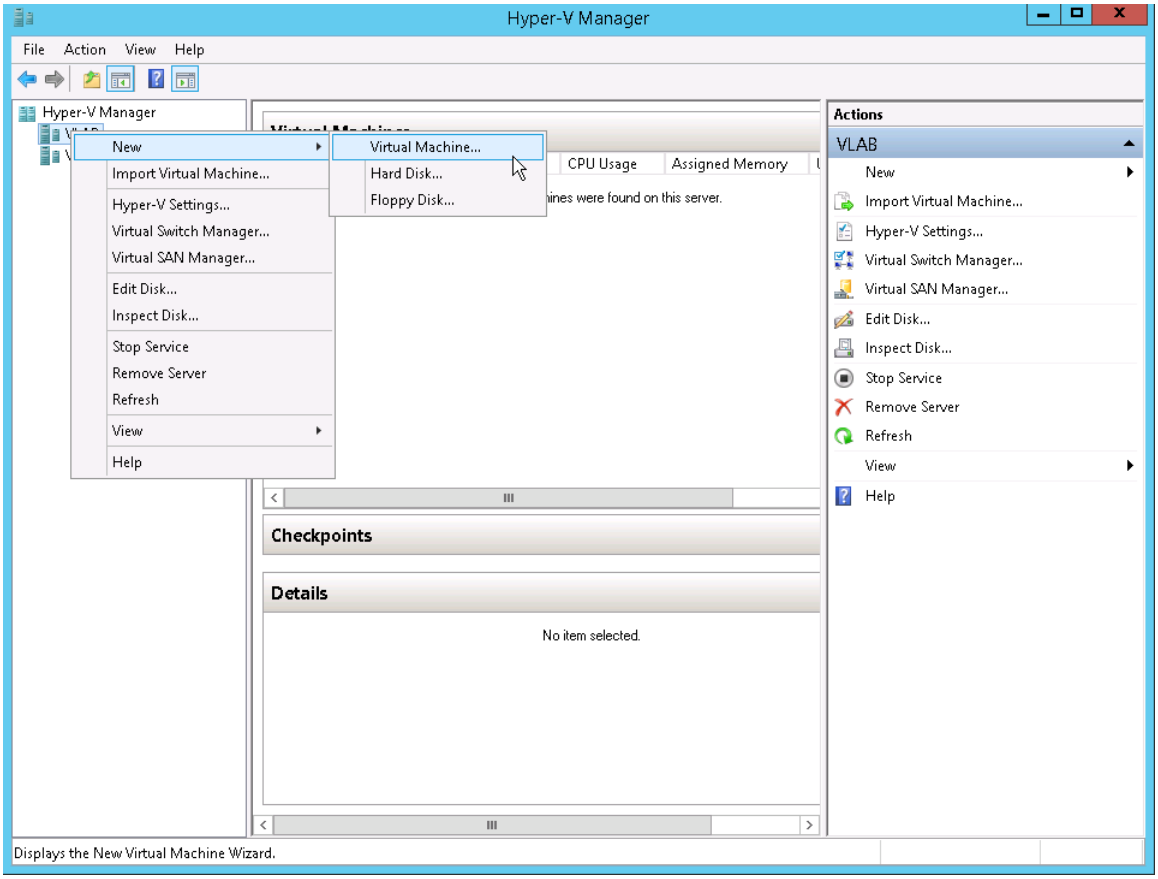
Installing the vSZ on Windows Server Hyper V

Before you begin, verify that Hyper-V is enabled on Windows Server. Follow these steps to install the vSZ on Windows Server Hyper-V.

1. Obtain a copy of the vSZ image in VHD format.
2. Extract the vSZ image to the .vhd disk file.
3. Copy the image to the Windows Server on which you are running Hyper-V.
4. On the Windows Server, click **Start** > **Administrative Tools**, and then double-click **Hyper-V Manager**.

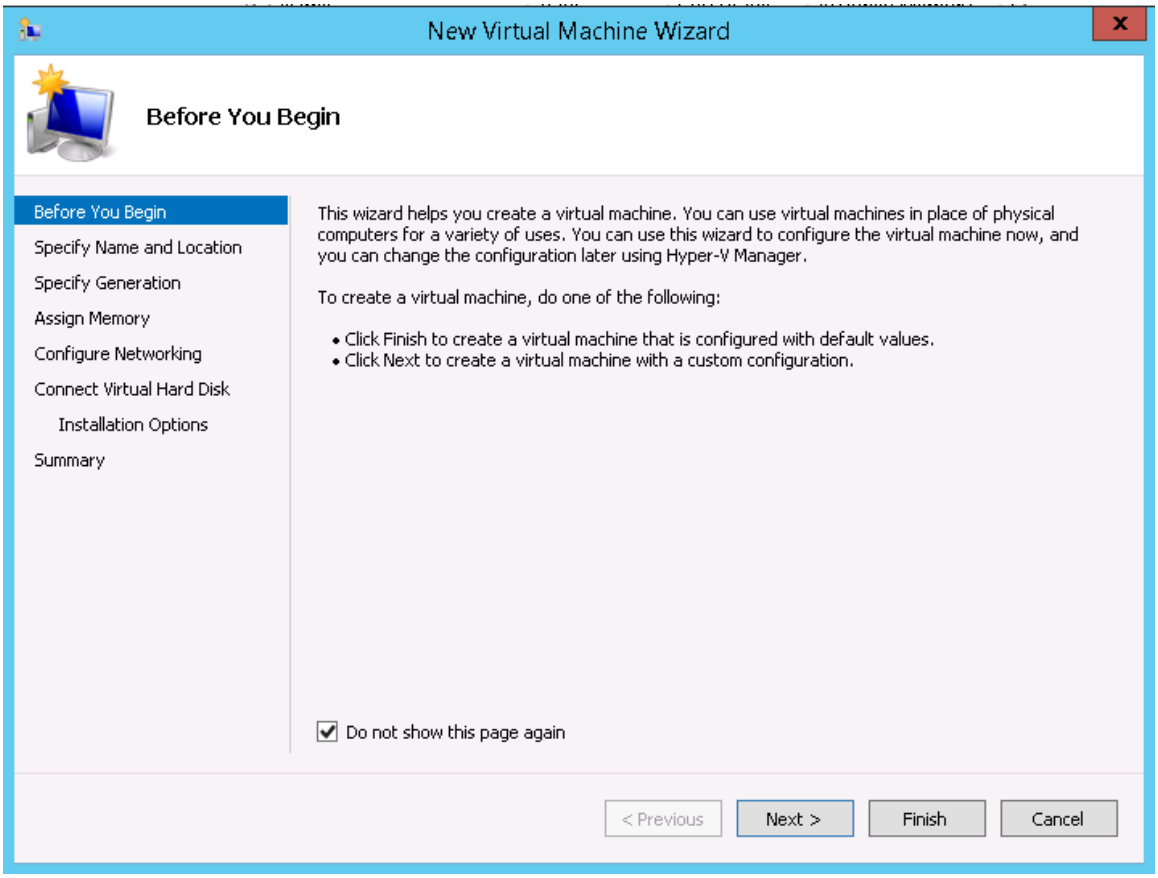
5. In the Hyper-V Manager, select the Hyper-V core for which you want to create a virtual machine and click **Virtual Machine** > **Action** > **New** > **New Virtual Machine Wizard**. The appears and displays the **Before You Begin** screen.

FIGURE 12 Click Action > New > Virtual Machine



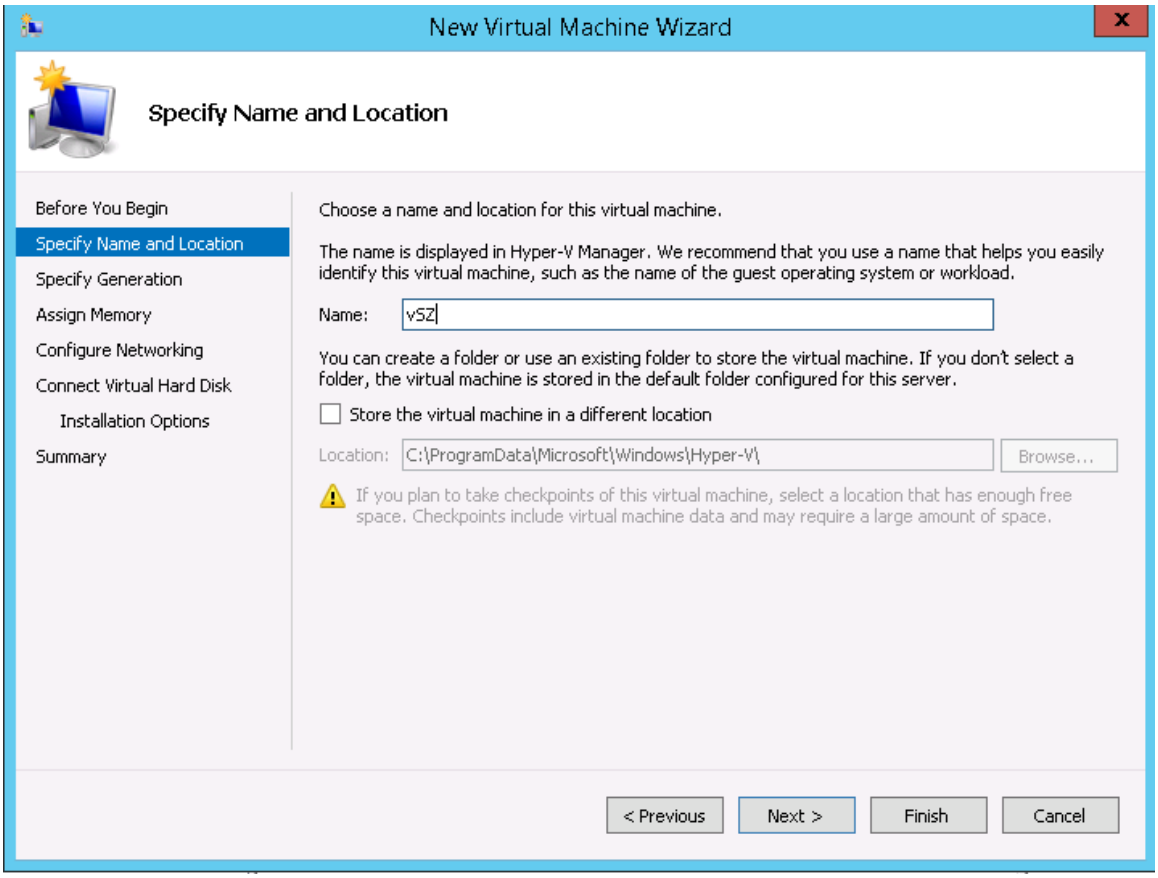
6. Click **Next**. The **Specify Name and Location** screen appears.

FIGURE 13 The New Virtual Machine Wizard screen



7. In **Name**, type a name for the virtual machine that you are installing (for example, Virtual SmartZone).

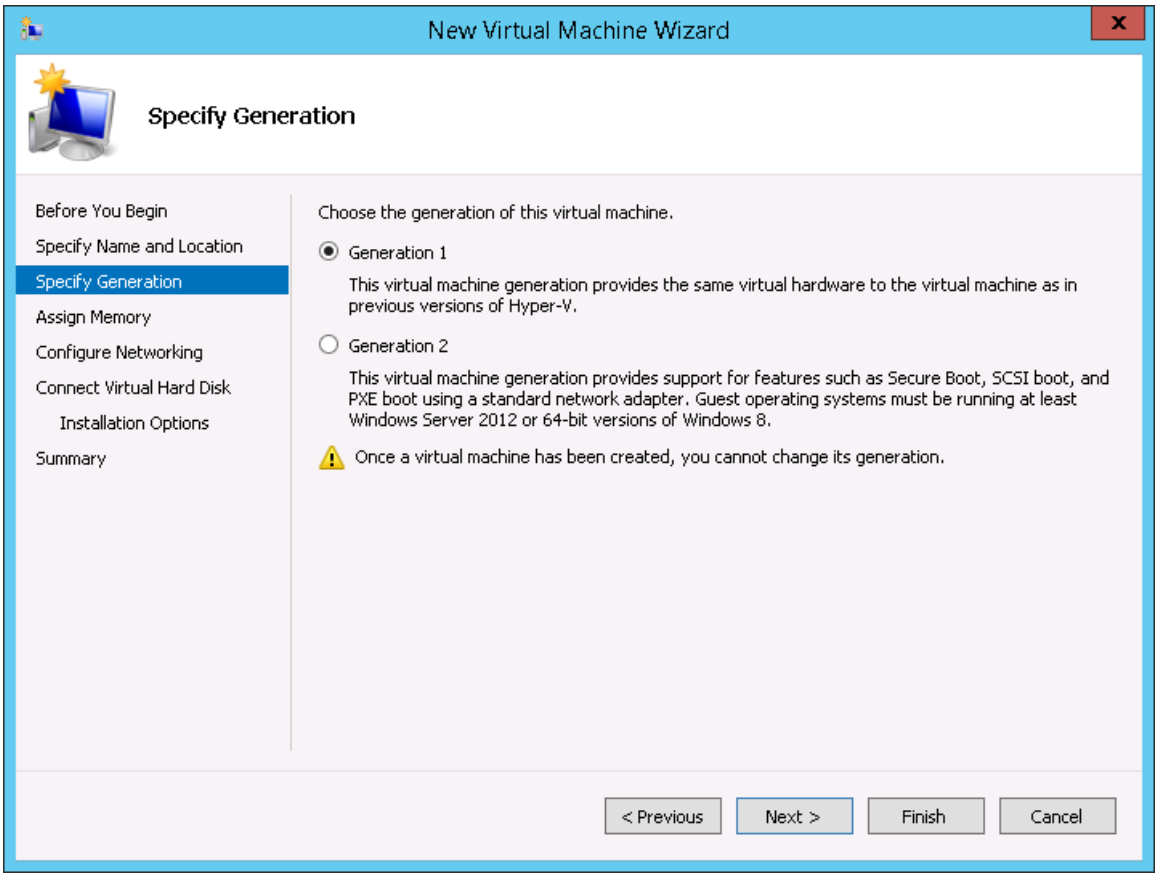
FIGURE 14 Specify Name and Location



8. Specify the folder on the server where you want to install the virtual machine.
   a) To install the virtual machine in the default location, make sure that the Store the virtual machine in a different location check box is clear.
   b) To install the virtual machine in a location other than the default, select and Store the virtual machine in a different location check box, and then browse to or type the new location.

9. Click **Next**. The **Specify Generation** screen appears.

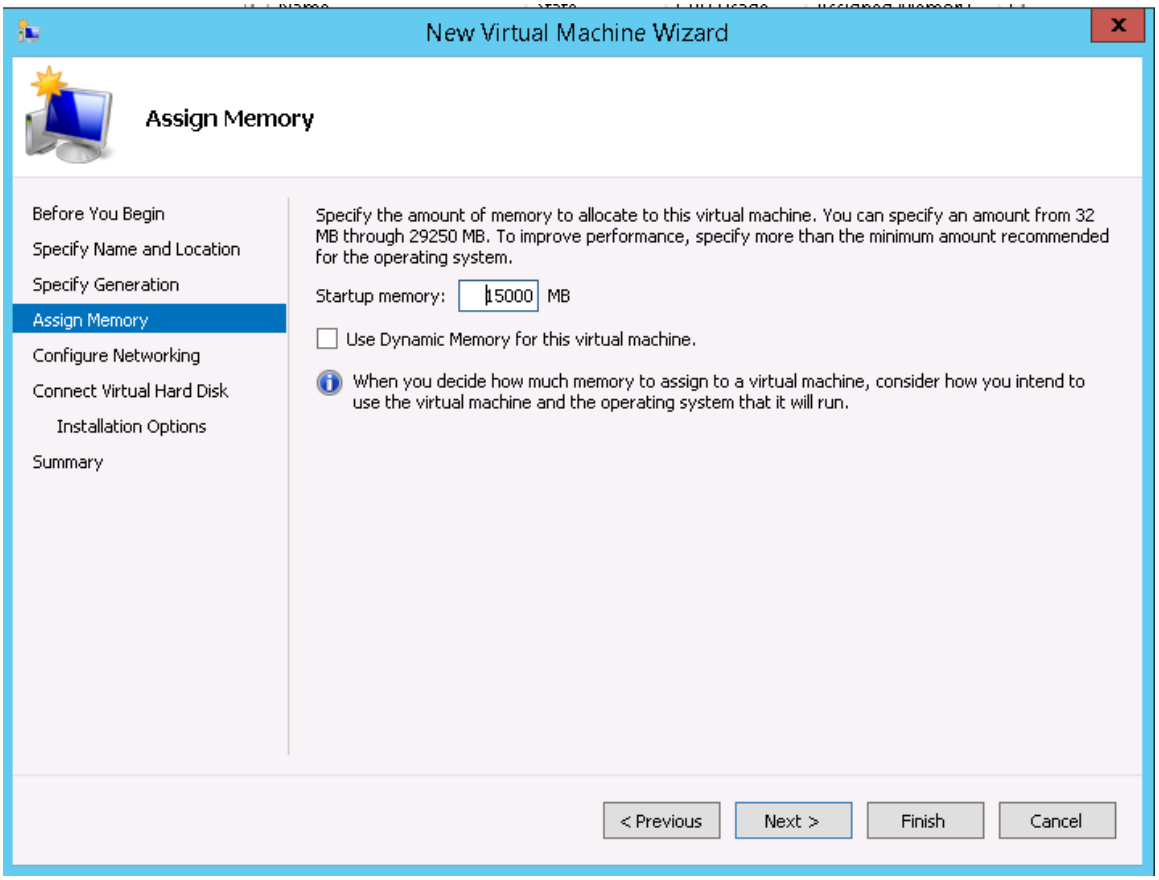
FIGURE 15 Specify Generation



10. Select **Generation 1** for the virtual machine that you are installing. Hyper-V offers Generation 1 and Generation 2. See the Hyper-V documentation for more information about these two generations.

11. Click **Next**. The **Assign Memory** screen appears.

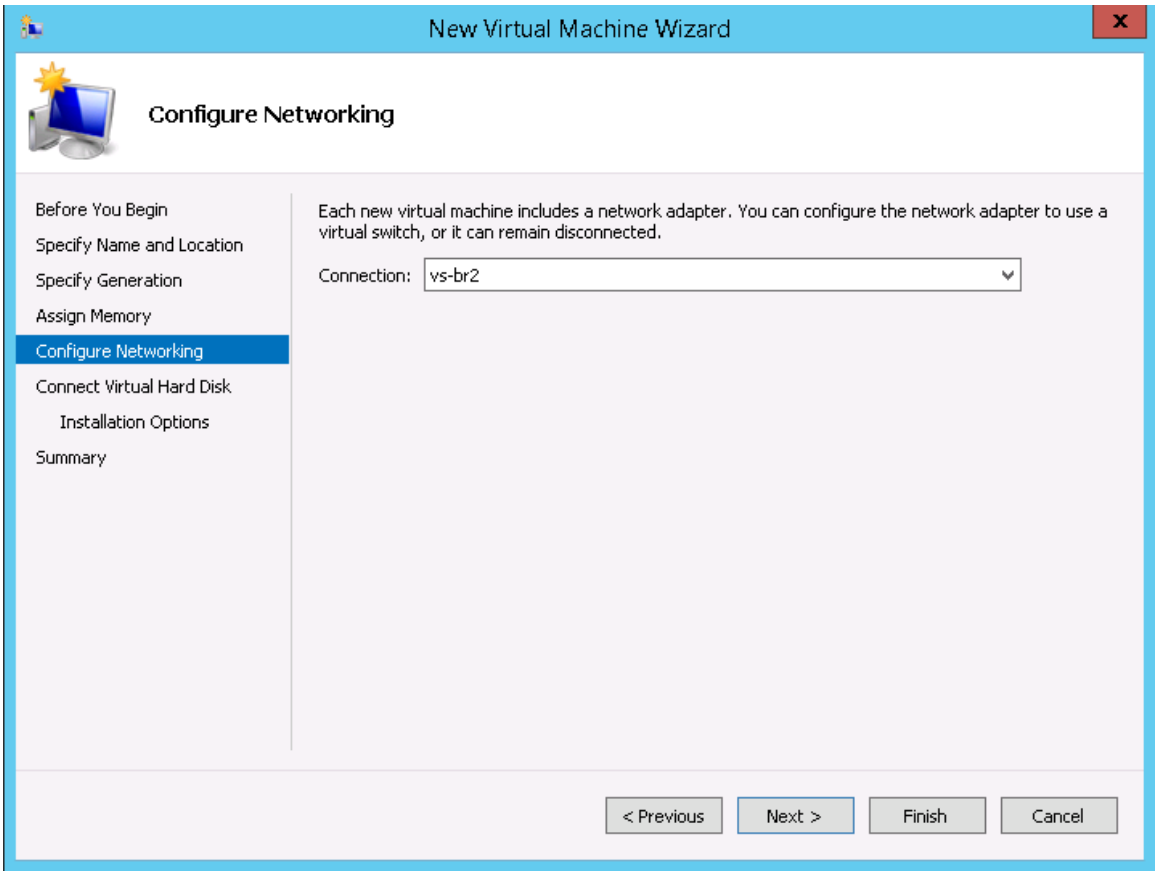
FIGURE 16 Assign Memory



12. In **Startup memory**, type 13GB for vSZ High Scale or 13GB for vSZ Essentials (as relevant), which are the minimum memory that Ruckus Networks recommends for deploying vSZ. You can type a higher value if more memory is available on the server. For more information, see Table 4 and Table 5.

13. Click **Next**. The **Configure Networking**

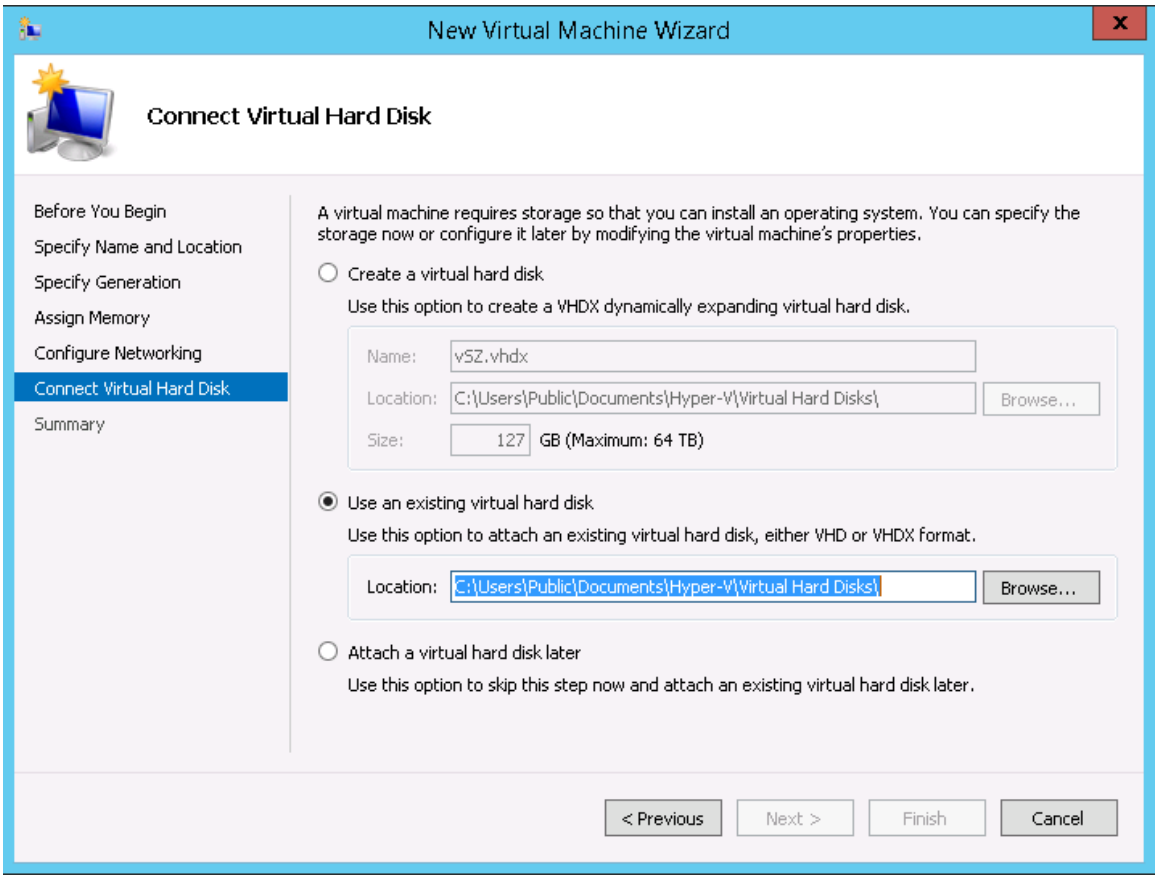
FIGURE 17 Configuring Network



14. In **Connection**, select the network adapter that you want the virtual machine to use.

15. Click **Next**. The **Connect Virtual Hard Disk** screen appears.

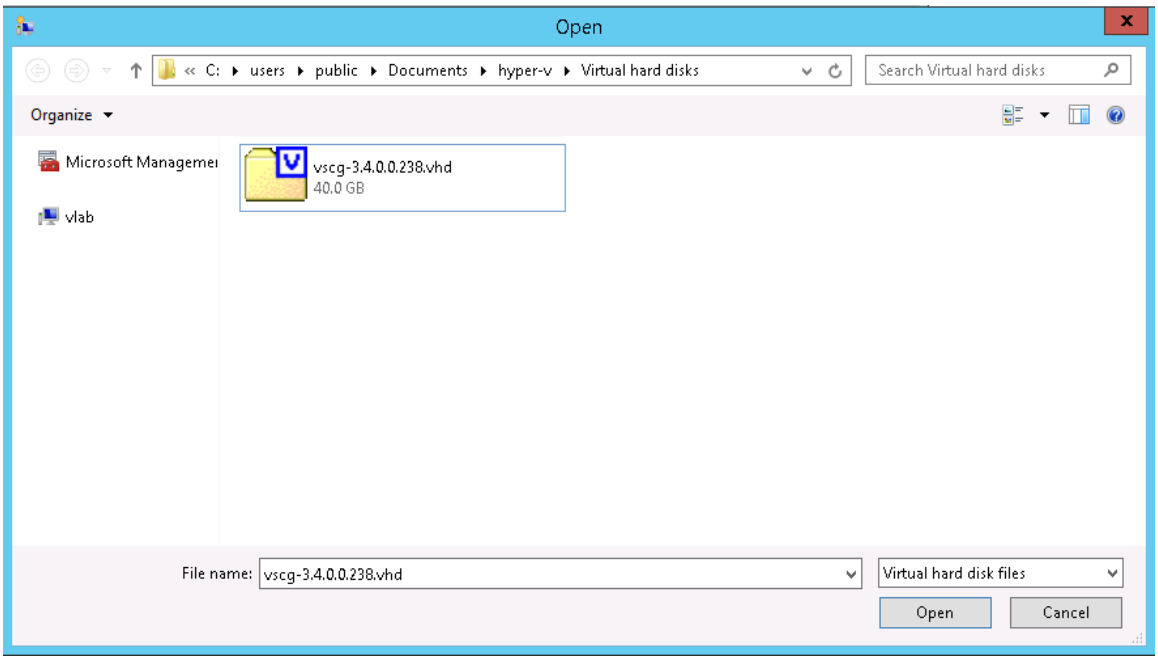
FIGURE 18 Connect Virtual Hard Disk



16. Select **Use an existing virtual hard disk**.

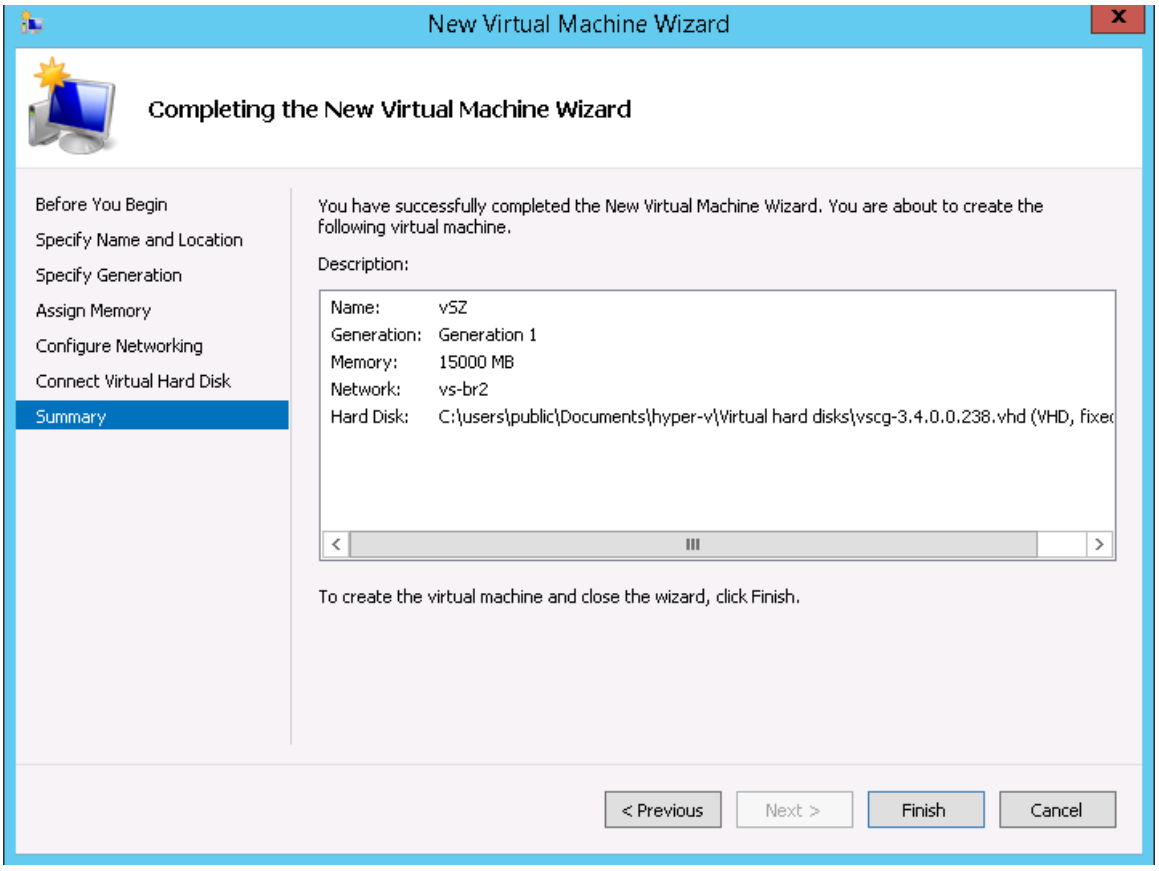
17. Click **Browse** to specify the location of the existing virtual hard disk for the virtual machine to use.

FIGURE 19 Selecting Virtual Hard Disk



18. Click **Next**. The **Completing New Virtual Machine Wizard** screen appears.

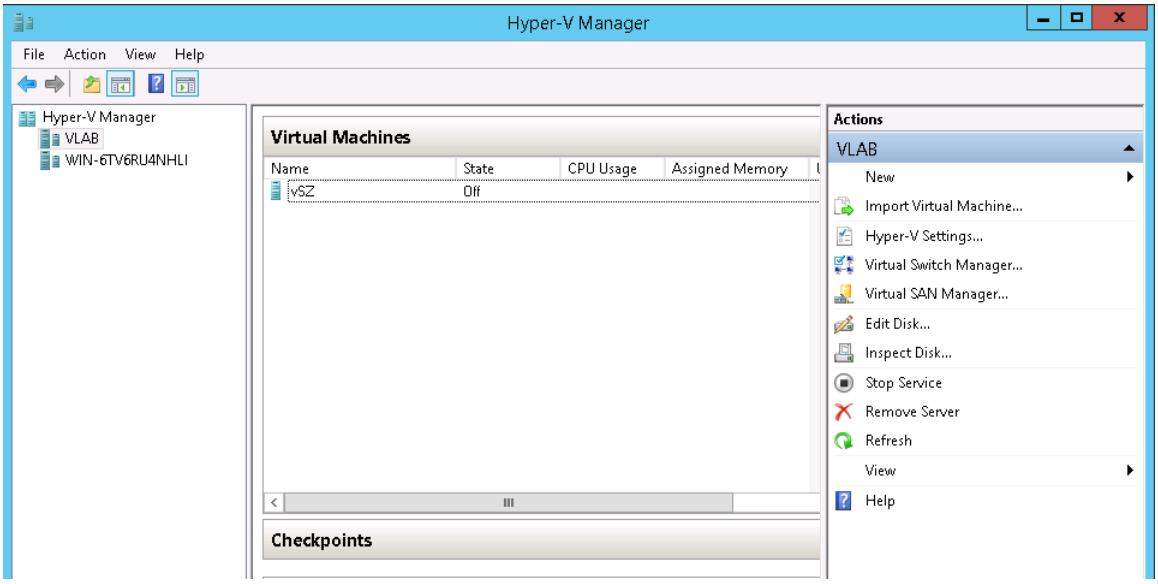
FIGURE 20 Completing New Virtual Machine Wizard



19. Review the settings that you can configure for the virtual machine. If you find any setting that need to be changed, click **Previous** until you reach the screen where you can update the setting. Update the setting, and then click **Next** until the **Completing New Virtual Machine Wizard** screen appears again.

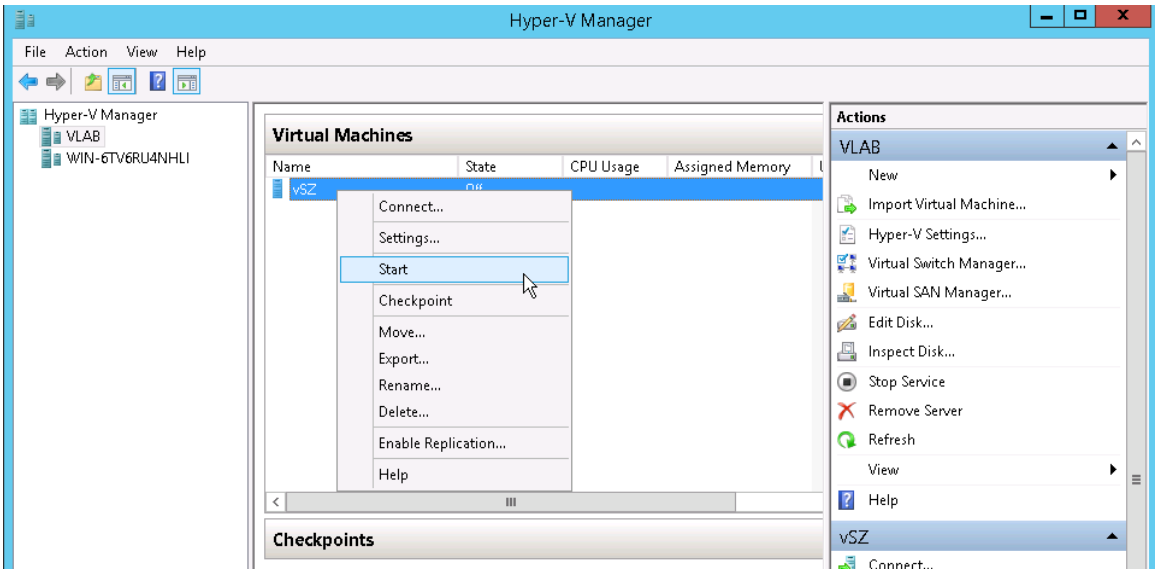
20. Click **Finish** to install the virtual machine. When Windows Server completes installing the virtual machine, the **New Virtual Machine Wizard** disappears and the virtual machine you installed appears on the list of virtual machines on Hyper-V Manager.

FIGURE 21 The virtual machine you installed appears on the list of virtual machines on Hyper- V Manager



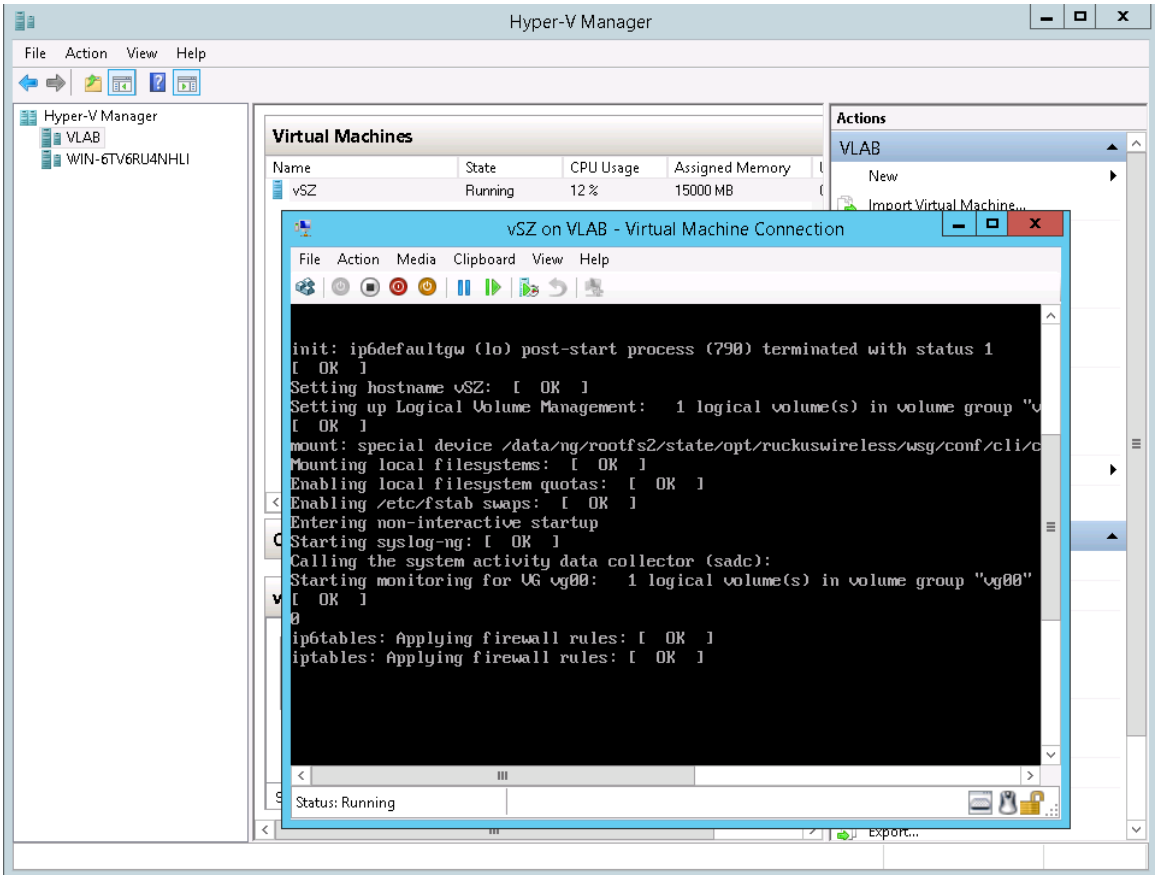
21. Right-click the virtual machine you installed, and then click **Start** to power on the virtual machine.

FIGURE 22 Right-click the virtual machine, and then click Start



The Virtual Machine Connection screen appears.

FIGURE 23 Virtual Machine Connection



22. Login to the virtual machine with your credentials.

You have now completed installing the vSZ on Windows Server Hyper-V.

Installing the vSZ on a Kernel based Virtual Machine Hypervisor

This section describes how to install the vSZ on a KVM hypervisor.

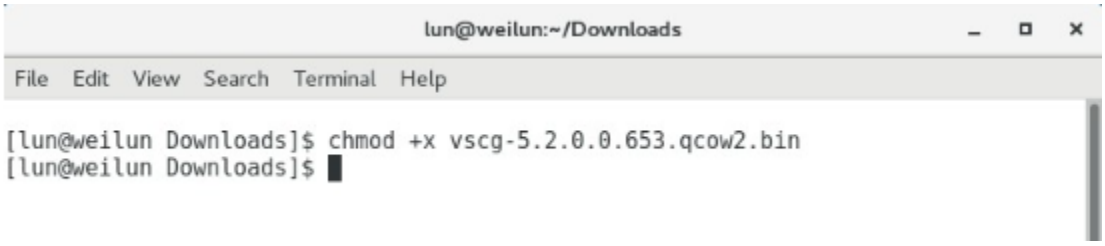
Extracting the vSZ Image

The vSZ image for a kernel-based virtual machine (KVM) is distributed in QCOW2 format.

1. Obtain the vSZ image in QCOW2 format.
2. Copy the image to the KVM.
3. Open the terminal window.

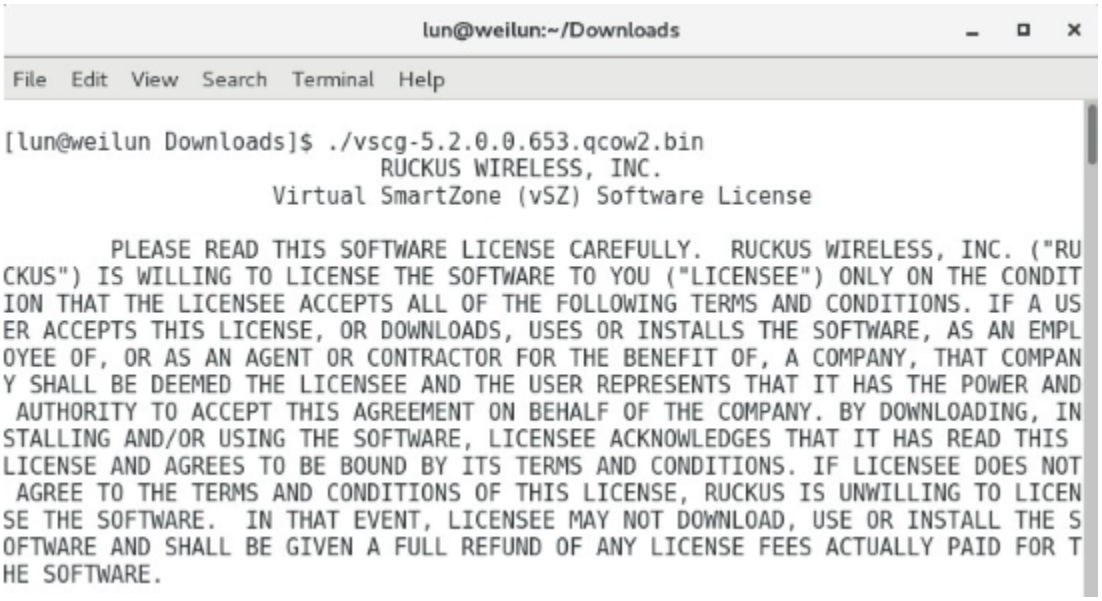
4. Make the image bin file executable by entering the following command: **chmod +x {file name of the controller QCOW bin}** See Figure for an example.

FIGURE 24 Make the bin file executable



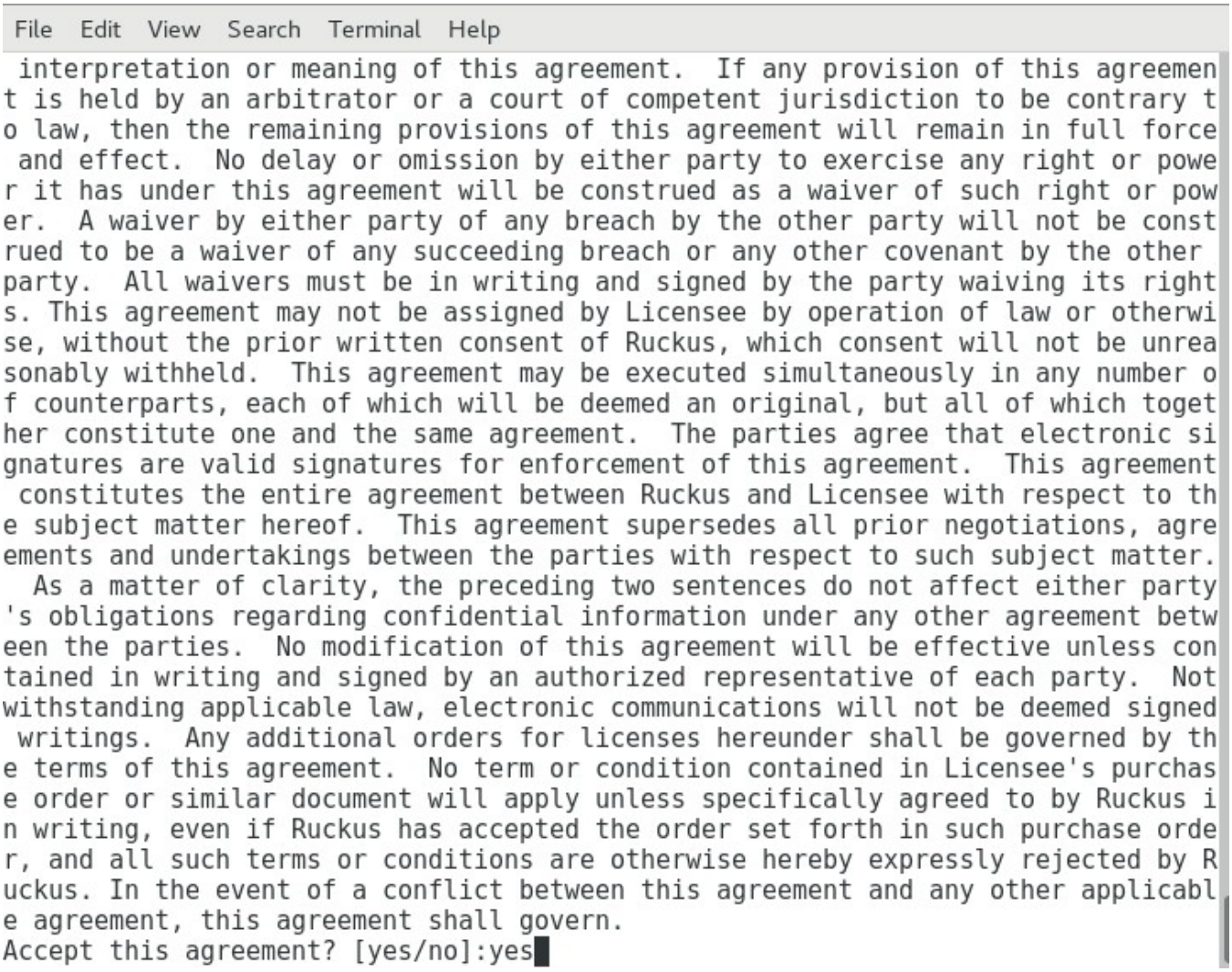
5. Extract the contents of the QCOW2 bin file.

FIGURE 25 Extract the contents of the QCOW2 image



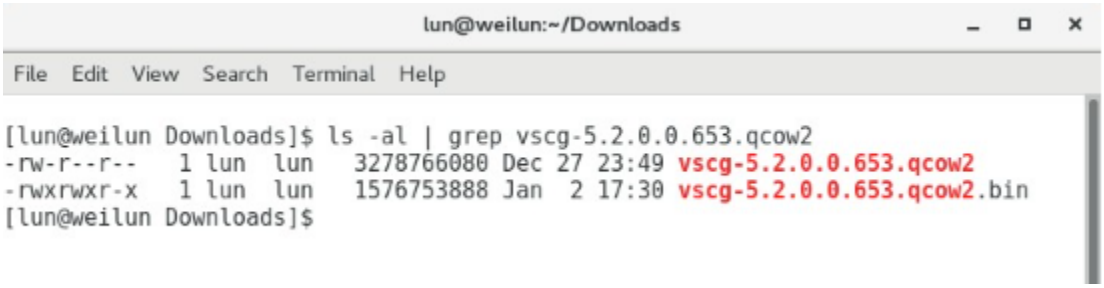
6. At the **Accept this agreement? [yes/no]** prompt, enter **yes**.

FIGURE 26 Accept the EULA terms



The KVM continues to extract the contents of the image. When the extraction process is complete, the QCOW2 file appears in the same directory as the .bin file.

FIGURE 27 The QCOW2 file appears in the same directory as the .bin file



NOTE
If the “uudecode: command not found” error appears during the extraction process, install the “sharutils” package on the KVM, and then try extracting the image again.

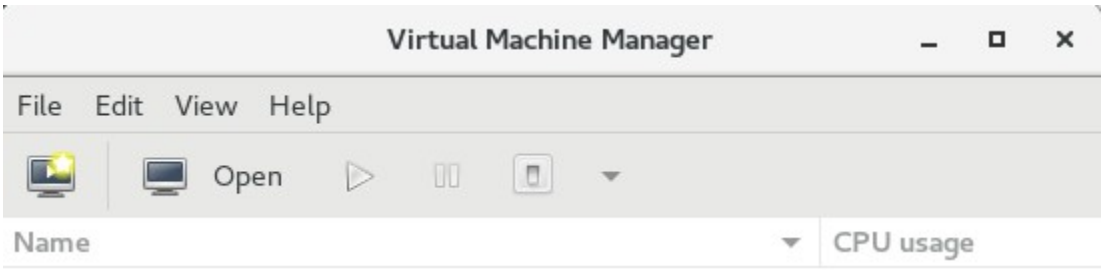
7. Resize the vSZ disk image, if necessary. By default, the vSZ disk size is 50GB. If you want to allocate more disk space to the vSZ, run the qemu-img command. The complete syntax is as follows: **qemu-img resize {file name of the controller QCOW bin} +size**

Setting Up the vSZ

You can set up the vSZ using the Red Hat Virtual Machine Manager (also known as “virt-manager”). If you are installing the vSZ on a different hypervisor or virtual machine monitor, the procedure may be slightly different. Refer to the hypervisor documentation for more information.

1. Start the Virtual Machine Manager by clicking Applications > System Tools > Virtual Machine Manager. Or double-click the Virtual Machine Manager icon if it appears on the desktop. The Virtual Machine Manager interface appears.

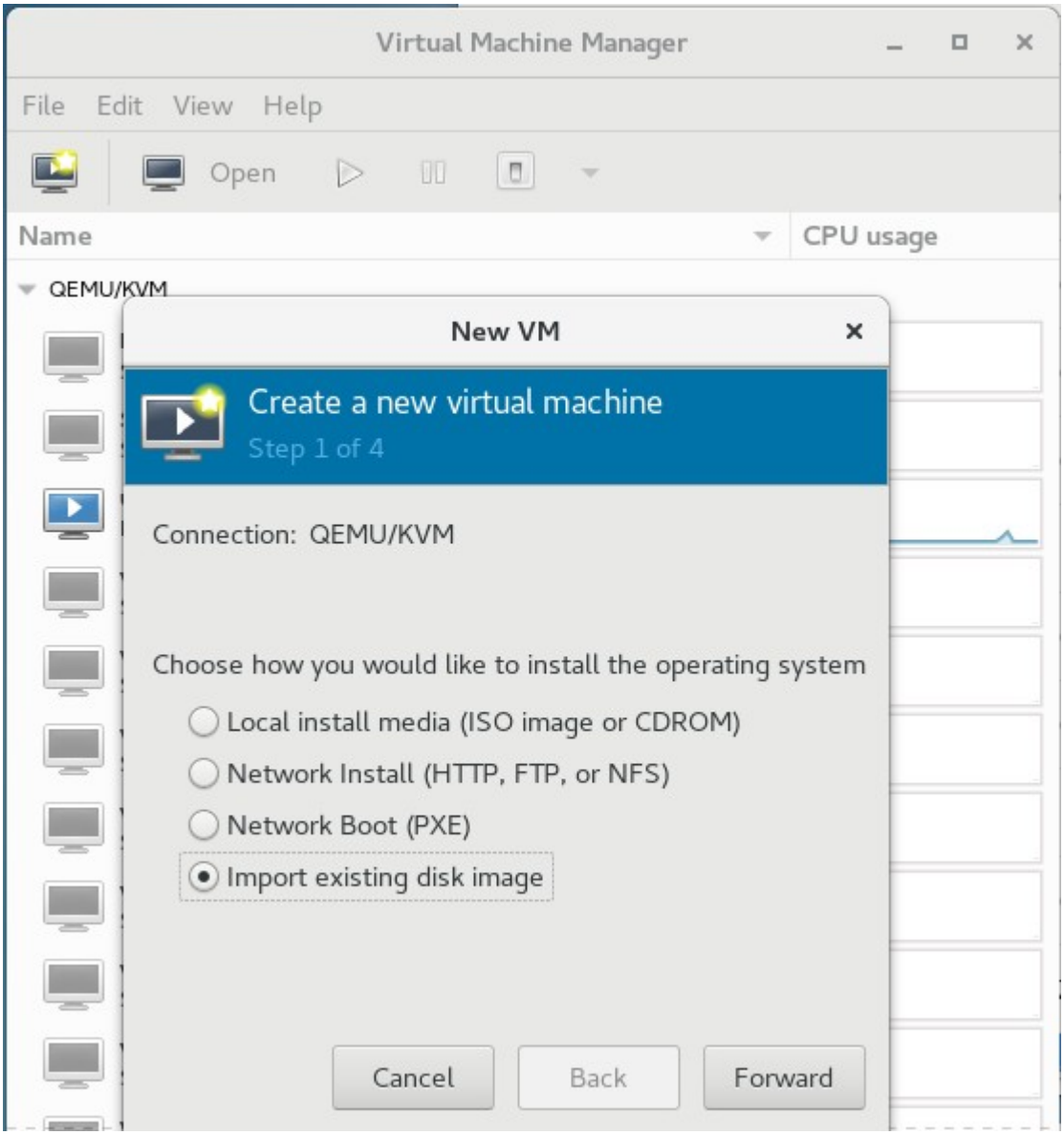
   FIGURE 28 The Virtual Machine Manager interface



2. In **File**, click **Create New VM**. Or click the **New VM** icon. **The New VM** screen appears

3. Configure the options on the **New VM (Step 1 of 4)** screen.
   a) In **Name**, type a name that you want to assign to the virtual machine.
   b) In **Choose how you would like to install the operating system**, click **Import existing disk image**.

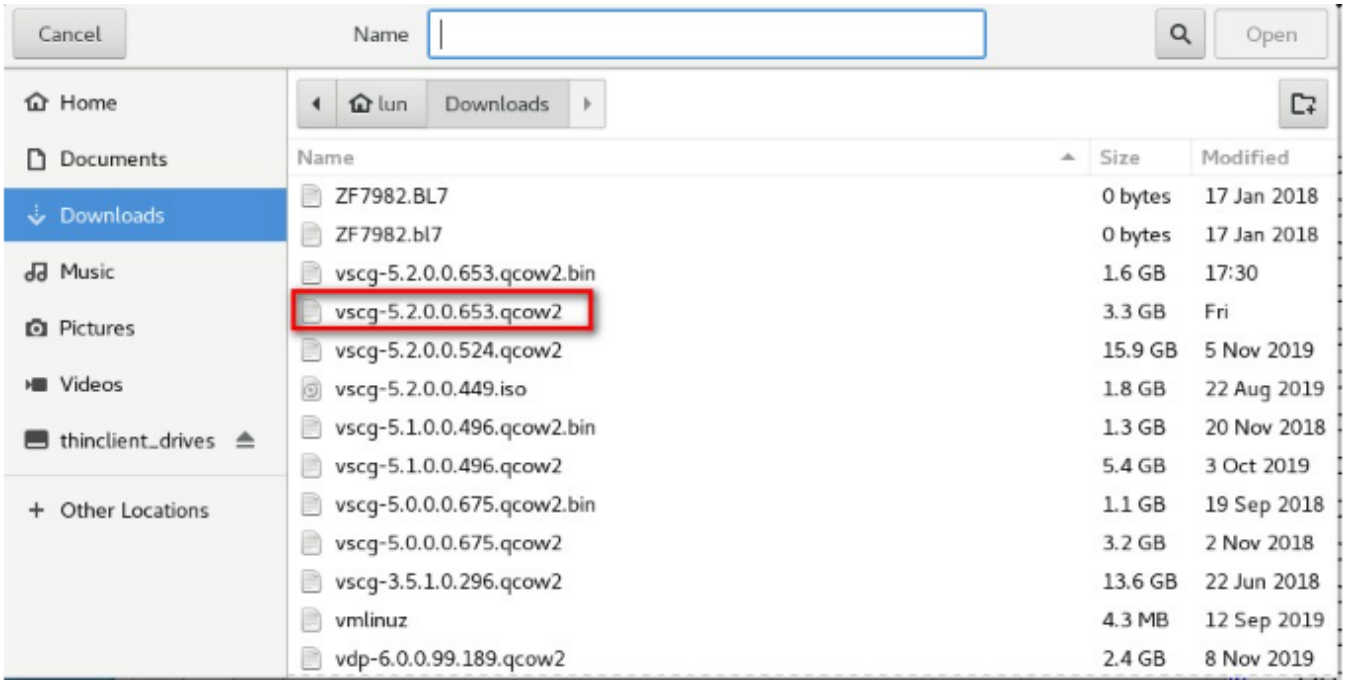
FIGURE 29 Type a name and select how you want to install the operating system



4. Click **Forward**. The **Locate Existing Storage** dialog box appears.

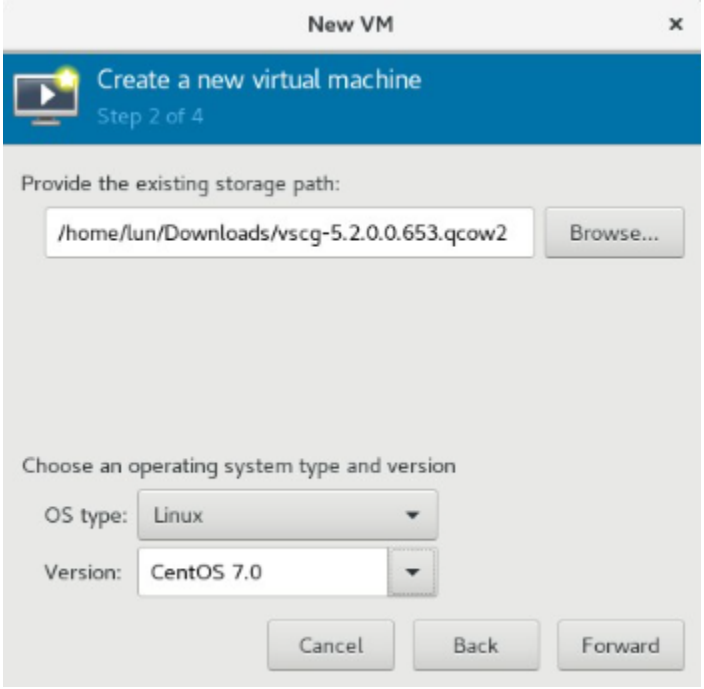
5. Browse to the location of the vSZ QCOW2 image, select the image file, and then click Open. The **New VM (Step 2 of 4)** screen reappears and displays the storage path to the QCOW2 image file that you selected.

FIGURE 30 Browse to the vSZ QCOW2 image



6. In the lower portion of the **New VM (Step 2 of 4)** screen, select the operating system type and version.
   a) In **OS type**, select **Linux**.
   b) In **Version**, select **Generic 2.6.x kernel**.

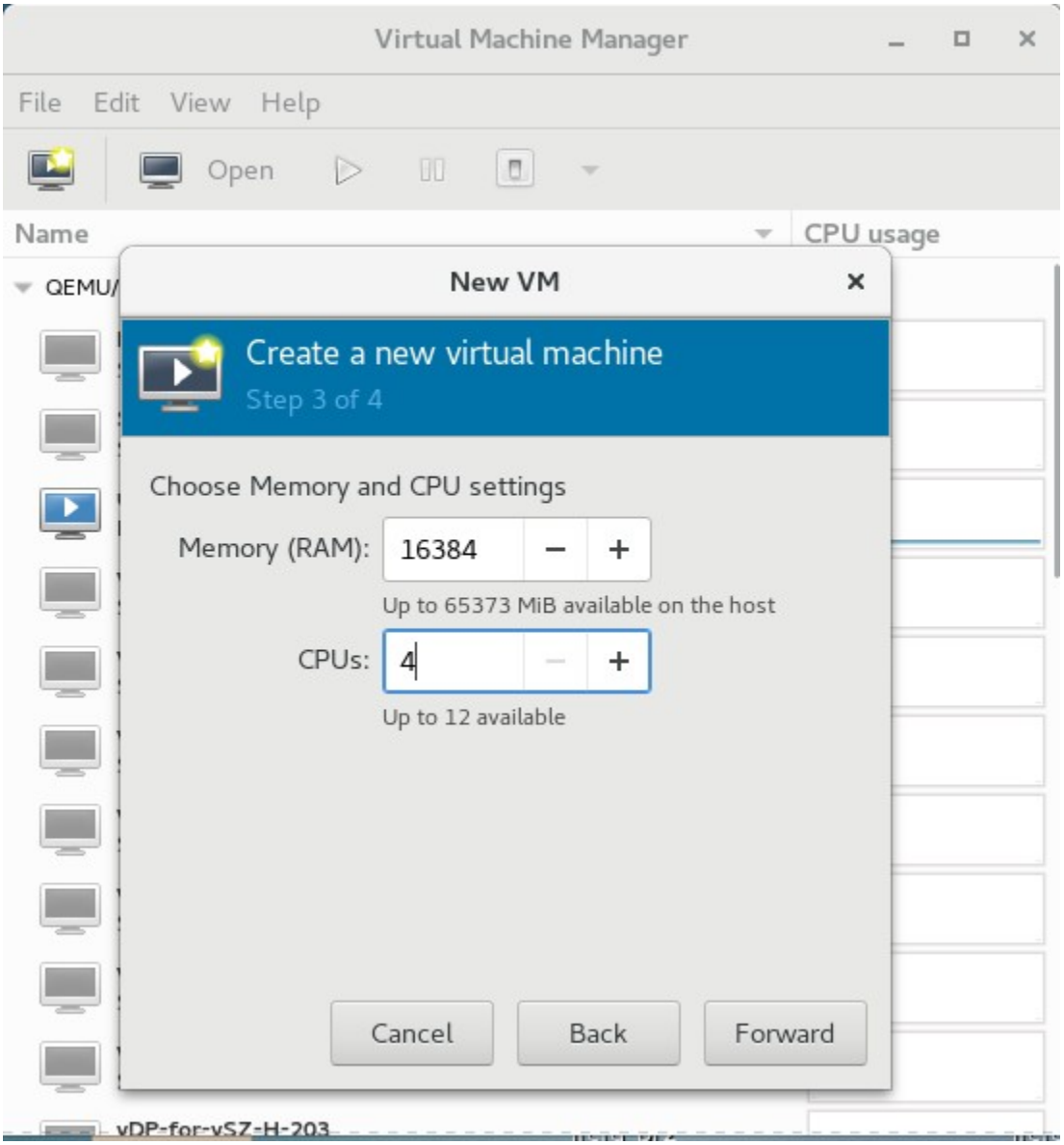
   FIGURE 31 Select the operating system and version



7. Click **Forward**. The **New VM (Step 3 of 4)** screen appears.

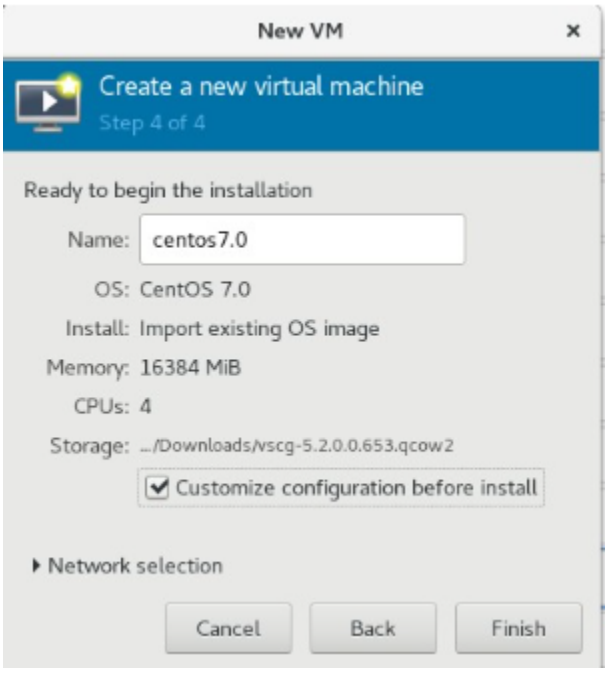
8. Configure the memory and CPU settings of the virtual machine.
   a) In **Memory (RAM)**, set to memory (in MB) that you want to allocate to the vSZ.
   b) In **CPU**, set the number of CPUs that you want to allocate to the vSZ.

FIGURE 32 Configure the memory and CPU settings



9. Click **Forward**. The **New VM (Step 4 of 4)** screen appears and displays a summary of the settings you configured.

   FIGURE 33 A summary of the settings you configured appears

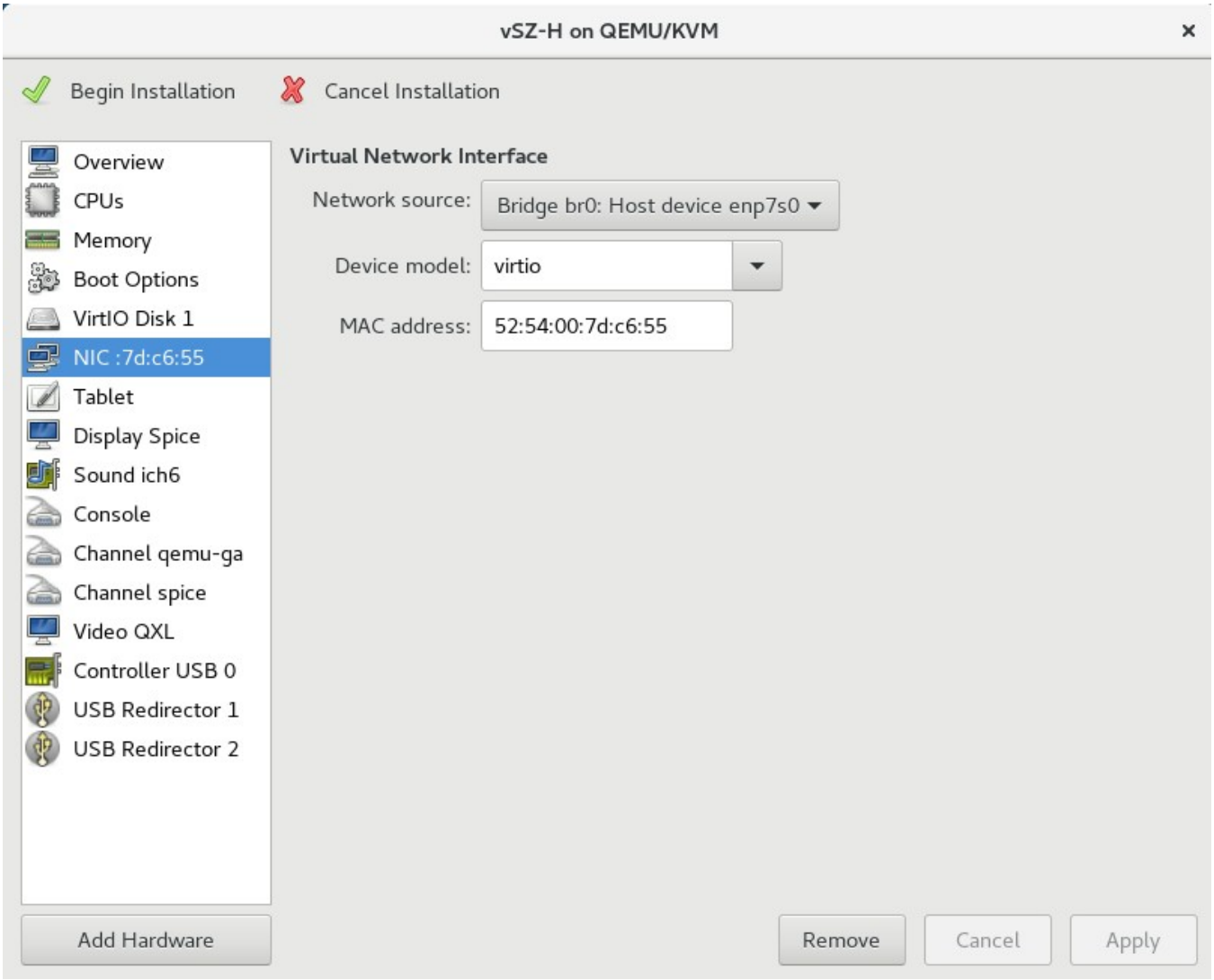


10. Verify that the settings you configured on the previous screens are correct. If you need to make changes to any of the settings, click **Back** until you reach the screen on which the setting appears, make the change, and then click Forward until you reach the **New VM (Step 4 of 4)** screen again.
11. Click **Finish** to install the vSZ on the virtual machine.

12. After you complete installing the vSZ on the virtual machine, decide how many interfaces you want the vSZ to use. The vSZ supports either a single interface or three interfaces. By default, a single interface exists after installation.
    - If you want the vSZ to use a single interface, you do not need to take action in this step. Continue to the next step.
    - If you want the vSZ to use three interfaces, you must create the two additional interfaces before the initial bootup of the vSZ. Once the vSZ has completed its initial bootup, you will no longer be able to change the number of interfaces.

    If you want to add interfaces, you must do so before the initial bootup of the vSZ. After the initial bootup, you will no longer be able to change the number of interfaces.

    FIGURE 34 By default, a single interface exists



13. Power on the virtual machine. The vSZ performs its initial bootup.
14. When the **vSZ login** prompt appears, enter **admin**.

You have completed setting up the vSZ on a KVM hypervisor. You are now ready to start the vSZ Setup Wizard. See Using the Setup Wizard to Install vSZ for more information.

Installing the vSZ on an OpenStack Hypervisor

You have to install the vSZ on an OpenStack hypervisor.

Configuring System Settings

1. Login the system as a `root`user.
2. Stop and disable the Firewall since OpenStack uses iptables.

```
systemctl stop firewalld
systemctl disable firewalld
```

3. Stop and disable NetworkManager.

```
systemctl stop NetworkManager
systemctl disable NetworkManager
```

4. Assign static IP address to all the interfaces. Else, DHCP will cause network issue while deploying an instance.

example: interface name is enp1s0

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=no
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp1s0
UUID=d320d308-f1e6-46cc-a5db-68848e9ab5d6
DEVICE=enp1s0
ONBOOT=yes
IPADDR=172.17.21.242
PREFIX=23
GATEWAY=172.17.20.1
IPV6_PRIVACY=no
```

example: interface name is enp3s0

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=no
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp3s0
UUID=b0dd6767-3ef5-4d63-9c12-aa3cc4771a31
DEVICE=enp3s0
ONBOOT=yes
IPADDR=192.168.66.2
PREFIX=24
GATEWAY=192.168.66.1
IPV6ADDR=2001:66::2/64
IPV6_DEFAULTGW=2001:66::1
IPV6_PRIVACY=no
```

example: interface name is enp6s0

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=enp6s0
UUID=5d9762b5-2b43-47ce-83af-35cf741901cd
DEVICE=enp6s0
ONBOOT=yes
IPADDR=10.10.30.2
PREFIX=16
GATEWAY=10.10.0.1
DNS1=8.8.8.8
IPV6ADDR=2001:b030:2516:164::2/64
```

```
IPV6_DEFAULTGW=2001:b030:2516:164::1
IPV6_PRIVACY=no
```

5. Update the system package.

```
yum -y update
```

6. Reboot the system using the CLI command.

```
Reboot
```

7. Verify if all the interfaces use the correct IP.

```
ip addr
ifconfig
```

8. Use the install net-tools package by command.

```
yum install net-tools
```

9. Change the hostname to the one that we use.

```
hostnamectl set-hostname "openstack.example.com"
```

10. Append hostname and IP mapping to **/etc/hosts** based on the network topology. The IP address could be any interface on the OpenStack Sever, and ensure you use the same hostname used in the previous step.

```
vi /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
10.10.30.2 openstack.example.com
```

11. Add repositories to the system for installing the OpenStack (refer to https://www.rdoproject.org/).

```
yum install -y centos-release-openstack-rocky
```

12. Login the system as a `root` user using SSH, modify /etc/ssh/sshd_config.

```
vi /etc/ssh/sshd_config
PermitRootLogin yes <—unmark this line.
systemctl restart sshd
```

13. Install the Packstack package.

```
yum install -y openstack-packstack
```

Installing OpenStack

1. Generate the OpenStack answer file.

```
packstack --gen-answer-file=/root/answer.txt
```

2. Edit the `/root/answer.txt` file, and modify the content based on your environment,

   NOTE
   Plan how you want to map the OVS interfaces (extnet), bridge interfaces(br-ex) and physical interfaces(enp1s0). You will need these information while deploying a vSZ instace. In this case, extnet=br-ex=enp1s0

```
# Skip the provision of Demo project
CONFIG_PROVISION_DEMO=n

# Change Admin Password - Used to Login to OpenStack Dashboard
CONFIG_KEYSTONE_ADMIN_PW=xxx

# Config OpenStack Dashboard over SSL
CONFIG_HORIZON_SSL=y

# Map physical network bridge to the logical name. <Logical Name:Bridge Name>
CONFIG_NEUTRON_OVS_BRIDGE_MAPPINGS=extnet:br-ex,extnet1:br-ex1,extnet2:br-ex2

# Create bridge for external connectivity. <Bridge Name: NW card name>
CONFIG_NEUTRON_OVS_BRIDGE_IFACES=br-ex:enp1s0,br-ex1:enp3s0,br-ex2:enp6s0

# external-physnet="extnet"
CONFIG_NEUTRON_OVS_EXTERNAL_PHYSNET=extnet,extnet1,extnet2
```

3. Run the Packstack installer with the `answer.txt`. It will take about 30-60 minutes to complete installation.

```
packstack --answer-file=/root/answer.txt
```

4. Verify if the newly created bridge interfaces use the correct IP address; physical interface will not have IP address setting.

5. Check the network script. If the scripts are not modified automatically, edit them properly, and then restart the network by using the command **systemctl restart network**.

[root@localhost ~]#ifconfig

```
br-ex: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet 172.17.21.242 netmask 255.255.254.0 broadcast 172.17.21.255
 inet6 fe80::7cf0:cfff:fe87:f54b prefixlen 64 scopeid 0x20<link>
 ether 68:05:ca:20:92:be txqueuelen 1000 (Ethernet)
 RX packets 8053 bytes 529150 (516.7 KiB)
 RX errors 0 dropped 3370 overruns 0 frame 0
 TX packets 14 bytes 900 (900.0 B)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

br-ex1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet 192.168.66.2 netmask 255.255.255.0 broadcast 192.168.66.255
 inet6 fe80::f8db:3cff:fe23:4f48 prefixlen 64 scopeid 0x20<link>
 ether 74:d4:35:51:e6:46 txqueuelen 1000 (Ethernet)
 RX packets 0 bytes 0 (0.0 B)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 14 bytes 900 (900.0 B)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

br-ex2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet 10.10.30.2 netmask 255.255.0.0 broadcast 10.10.255.255
 inet6 fe80::788c:5cff:fefd:e347 prefixlen 64 scopeid 0x20<link>
 inet6 2001:b030:2516:164:6a05:caff:fe20:9ec9 prefixlen 64 scopeid 0x0<global>
 ether 68:05:ca:20:9e:c9 txqueuelen 1000 (Ethernet)
 RX packets 26860 bytes 32501357 (30.9 MiB)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 17037 bytes 2002913 (1.9 MiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet6 fe80::6a05:caff:fe20:92be prefixlen 64 scopeid 0x20<link>
 ether 68:05:ca:20:92:be txqueuelen 1000 (Ethernet)
 RX packets 11772 bytes 965550 (942.9 KiB)
 RX errors 0 dropped 1732 overruns 0 frame 0
 TX packets 18 bytes 1498 (1.4 KiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
 device interrupt 16 memory 0xf7ec0000-f7ee0000

enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet6 fe80::76d4:35ff:fe51:e646 prefixlen 64 scopeid 0x20<link>
 ether 74:d4:35:51:e6:46 txqueuelen 1000 (Ethernet)
 RX packets 6734 bytes 430976 (420.8 KiB)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 246 bytes 21098 (20.6 KiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp6s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
 inet6 fe80::6a05:caff:fe20:9ec9 prefixlen 64 scopeid 0x20<link>
 ether 68:05:ca:20:9e:c9 txqueuelen 1000 (Ethernet)
 RX packets 236349 bytes 306637429 (292.4 MiB)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 143142 bytes 12982731 (12.3 MiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
 device interrupt 16 memory 0xf7cc0000-f7ce0000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
 inet 127.0.0.1 netmask 255.0.0.0
 inet6 ::1 prefixlen 128 scopeid 0x10<host>
 loop txqueuelen 1000 (Local Loopback)
 RX packets 3188295 bytes 411123149 (392.0 MiB)
 RX errors 0 dropped 0 overruns 0 frame 0
 TX packets 3188295 bytes 411123149 (392.0 MiB)
 TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

[root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-enp1s0

```
DEVICE=enp1s0
NAME=enp1s0
DEVICETYPE=ovs
TYPE=OVSPort
OVS_BRIDGE=br-ex
ONBOOT=yes
BOOTPROTO=none
```

[root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-enp3s0

```
DEVICE=enp3s0
NAME=enp3s0
DEVICETYPE=ovs
TYPE=OVSPort
OVS_BRIDGE=br-ex1
ONBOOT=yes
BOOTPROTO=none
```

[root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-enp6s0

```
DEVICE=enp6s0
NAME=enp6s0
DEVICETYPE=ovs
TYPE=OVSPort
OVS_BRIDGE=br-ex2
ONBOOT=yes
BOOTPROTO=none
```

[root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-br-ex

```
PROXY_METHOD=none
BROWSER_ONLY=no
DEFROUTE=no
UUID=d320d308-f1e6-46cc-a5db-68848e9ab5d6
ONBOOT=yes
IPADDR=172.17.21.242
PREFIX=23
GATEWAY=172.17.20.1
DEVICE=br-ex
NAME=br-ex
DEVICETYPE=ovs
OVSBOOTPROTO=static
TYPE=OVSBridge
OVS_EXTRA="set bridge br-ex fail_mode=standalone"
```

[root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-br-ex1

```
PROXY_METHOD=none
BROWSER_ONLY=no
DEFROUTE=no
UUID=b0dd6767-3ef5-4d63-9c12-aa3cc4771a31
ONBOOT=yes
IPADDR=192.168.66.2
PREFIX=24
GATEWAY=192.168.66.1
DEVICE=br-ex1
NAME=br-ex1
DEVICETYPE=ovs
OVSBOOTPROTO=static
TYPE=OVSBridge
OVS_EXTRA="set bridge br-ex1 fail_mode=standalone"
```

[root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-br-ex2

```
PROXY_METHOD=none
BROWSER_ONLY=no
DEFROUTE=yes
UUID=5d9762b5-2b43-47ce-83af-35cf741901cd
ONBOOT=yes
IPADDR=10.10.30.2
```

```
PREFIX=16
GATEWAY=10.10.0.1
DEVICE=br-ex2
NAME=br-ex2
DEVICETYPE=ovs
OVSBOOTPROTO=static
TYPE=OVSBridge
OVS_EXTRA="set bridge br-ex2 fail_mode=standalone"
```

6. Check the OpenStack package version.

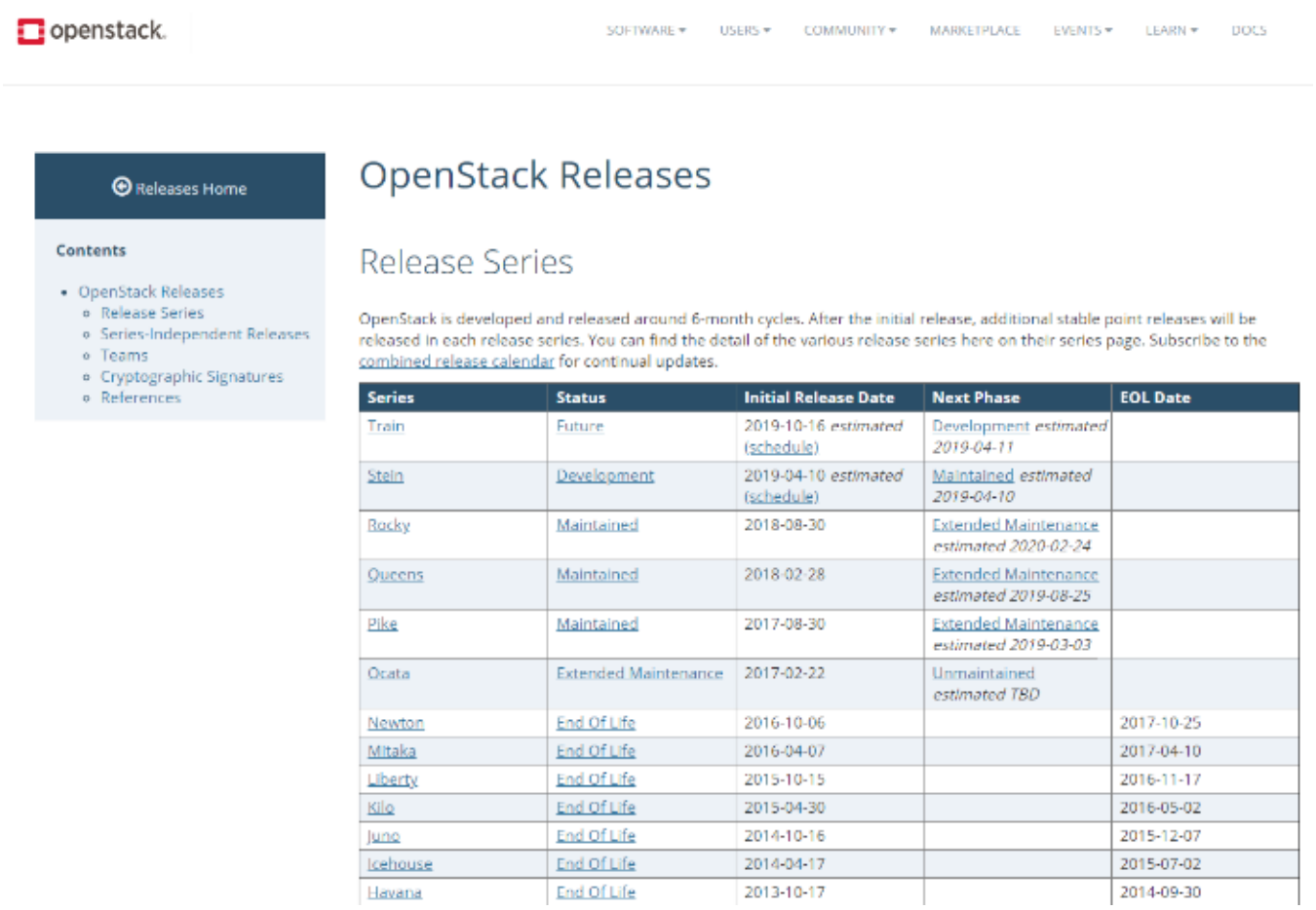
   [root@localhost ~]# source ./keystonerc_admin

   [root@openstack1 ~(keystone_admin)]# nova-manage --version

   ```
   17.0.5
   ```

7. Check https://releases.openstack.org/ and make sure you have installed the correct version with the supported service projects.

   FIGURE 35 OpenStack Version



Accessing the OpenStack Dashboard

1. Open https://IP_Address/dashboard or https://fqdn/dashboard if the fqdn can be resolved.

   NOTE
   Use the Firefox browser to access the link.

FIGURE 36 OpenStack Login

2. Login OpenStack using the Administrator **User Name** and the **Password**.

   NOTE
   If you forget the password, you can get it from the file `/root/keystore_admin`.

[root@openstack ~]# cat keystonerc_admin

```
unset OS_SERVICE_TOKEN
export OS_USERNAME=admin
export OS_PASSWORD='admin'
export OS_AUTH_URL=http://10.10.30.2:5000/v3
export PS1='[\u@\h \W(keystone_admin)]\$ '

export OS_PROJECT_NAME=admin
export OS_USER_DOMAIN_NAME=Default
export OS_PROJECT_DOMAIN_NAME=Default
export OS_IDENTITY_API_VERSION=3
```

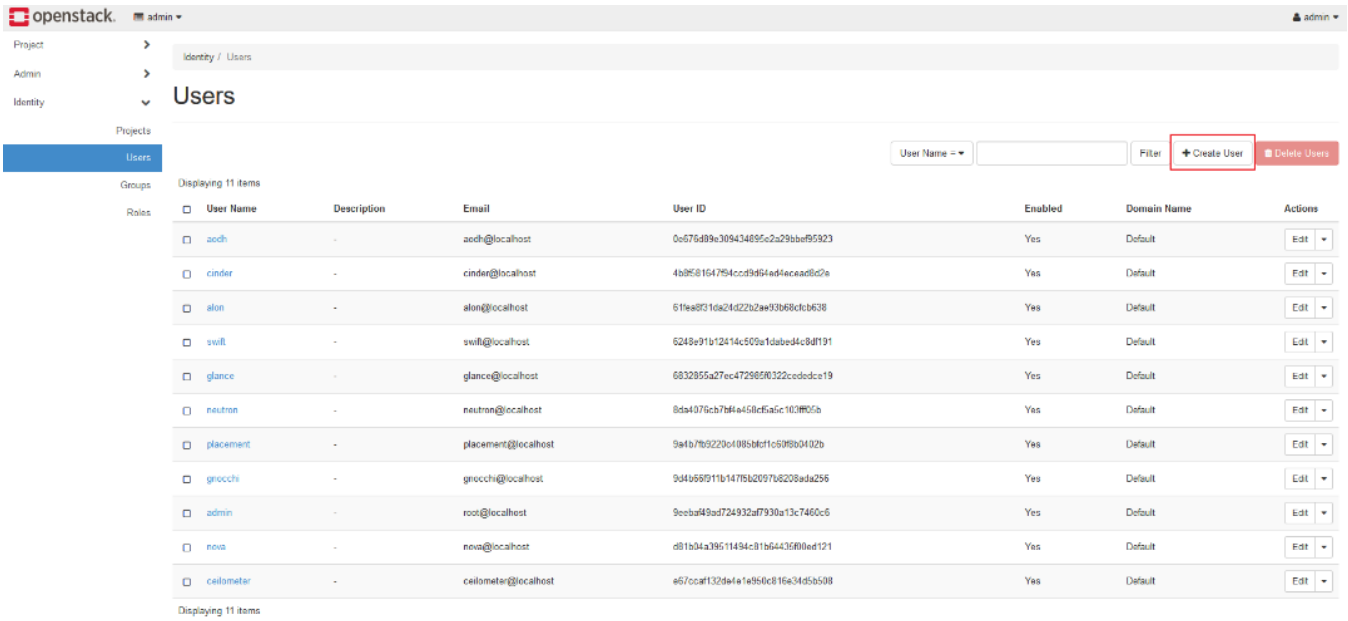
Creating Global Items

Creating a New User

1. From the OpenStack homepage, click **Identity** > **Users**.

   The Users page appears as shown in the following image.

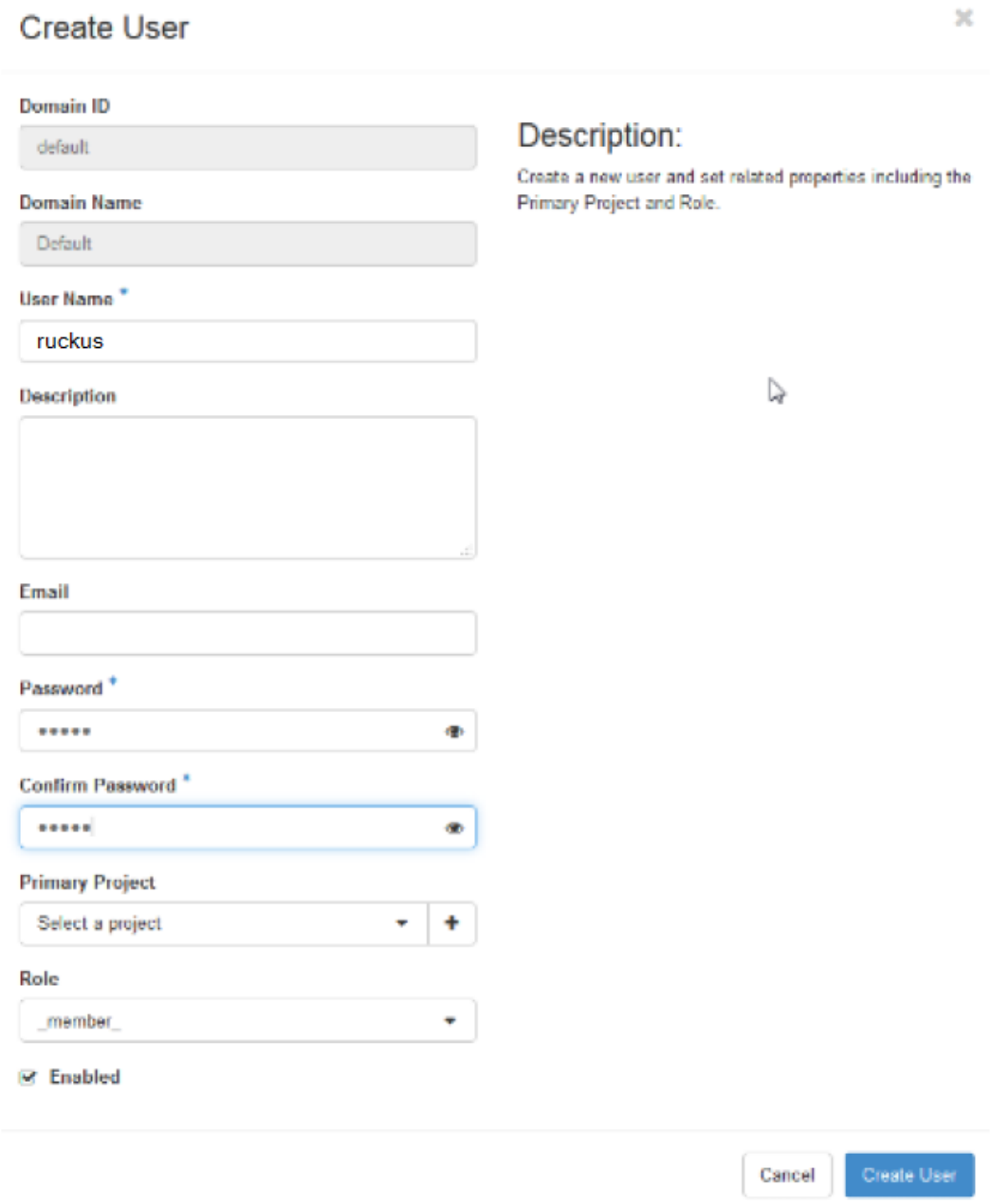
FIGURE 37 OpenStack Home Page



2. Click **Create User**.

   The Create User page appears as shown in the following image.

   FIGURE 38 Creating a User



3. Enter the **User Name**, **Password**, **Confirm Password** and click **Create User**.

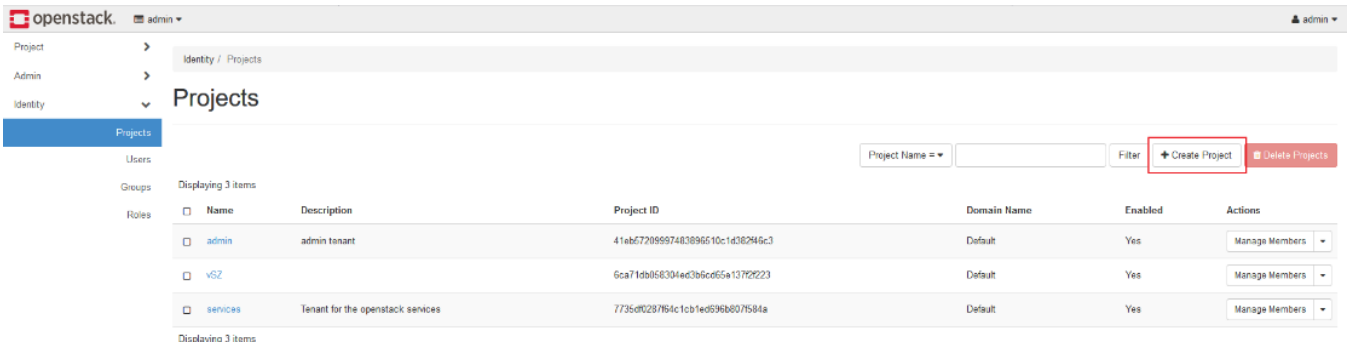
   You have created a new user.

Creating a New Project

1. From the OpenStack homepage, click **Identity** > **Projects**.

   The **Projects** page appear as shown in the following image.

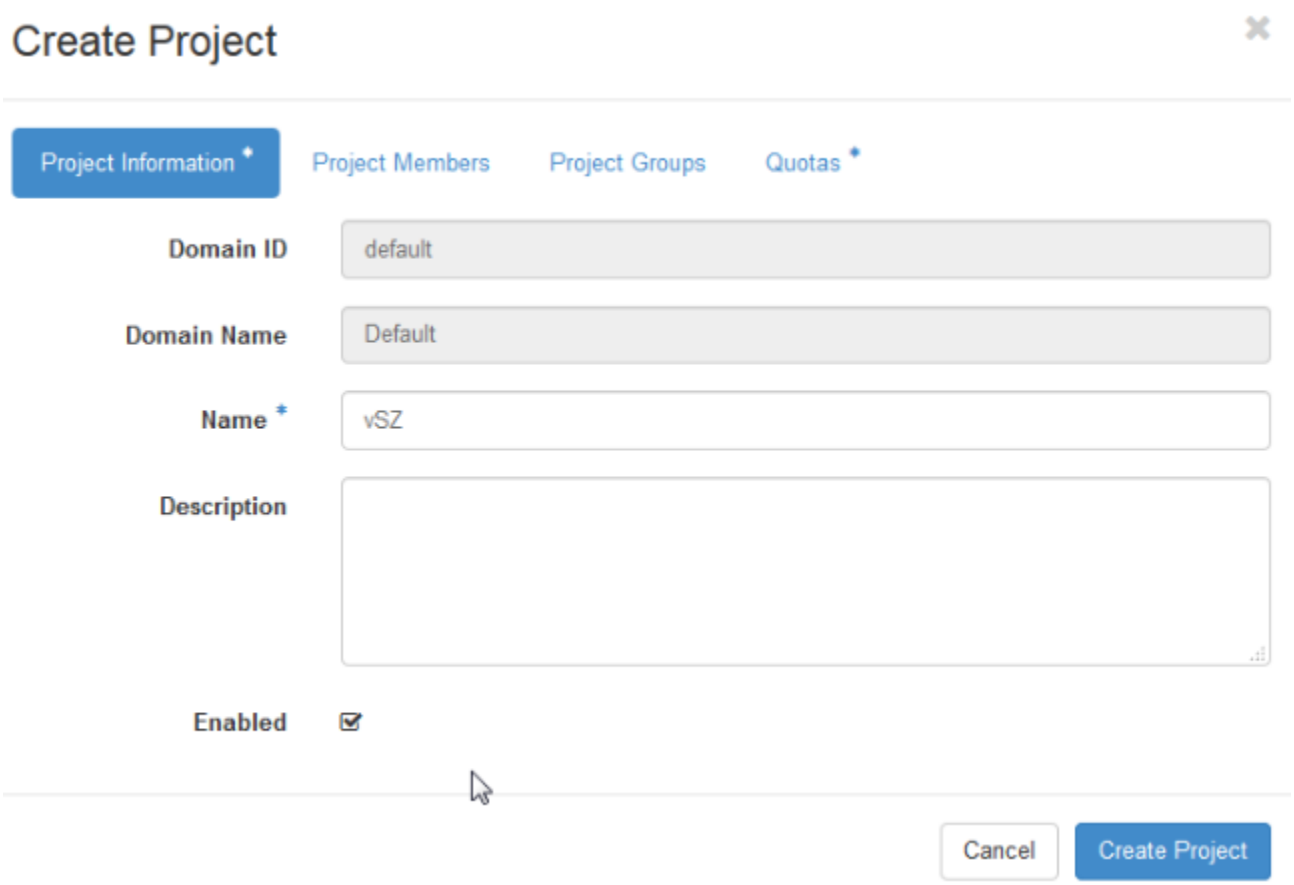
   FIGURE 39 OpenStack Project Page



2. Click **Create Project**.

   The **Create Project** page appear as shown in the following image.

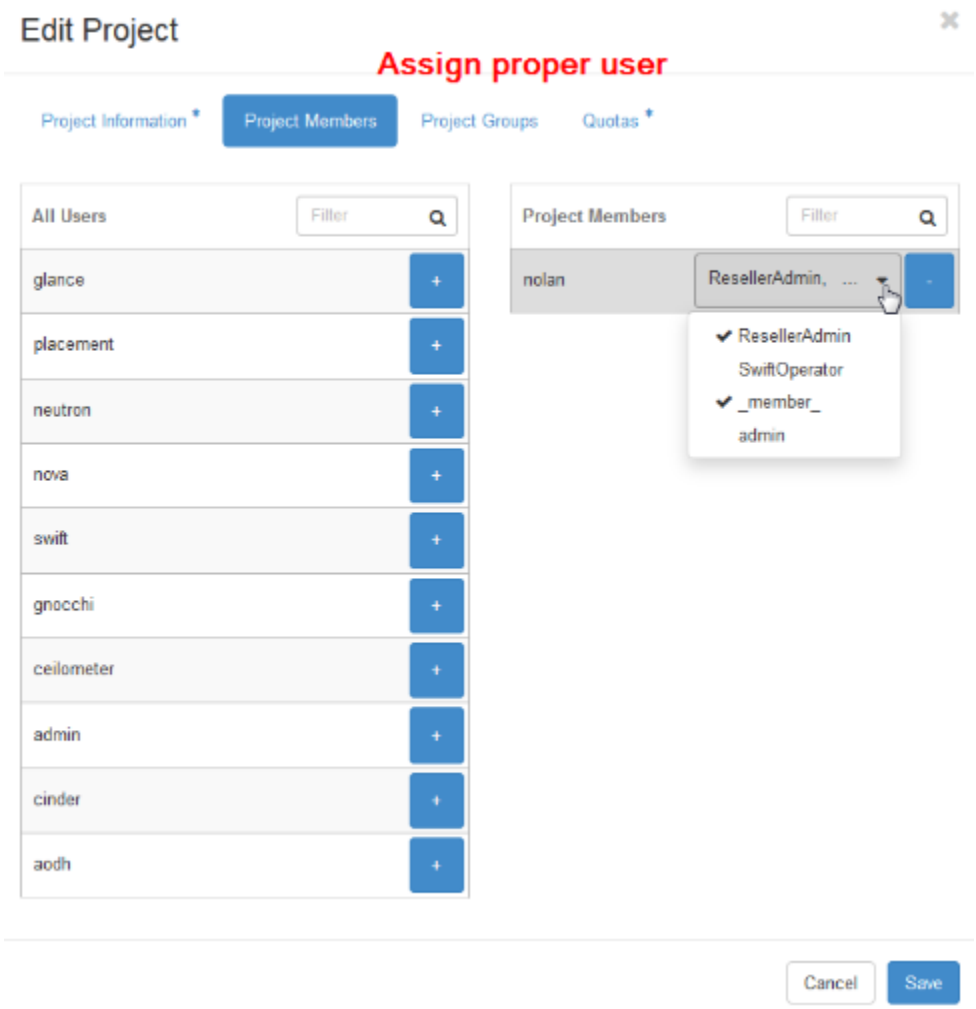
   FIGURE 40 Creating a Project



3. From the **Project** Information tab, enter the **Name** for the project.

4. Select the **Project Members** tab.

   The **Edit Project** page appear as shown in the following image.



5. From the list of **All Users**, click the add + button to select the required user.

   The selected users are moved to the **Project Members** list.

6. From the drop-down select the rights to be assigned to each user.
7. Select the **Quotas** tab and assign the required resource pool for the project.
8. Click **Create Project**.

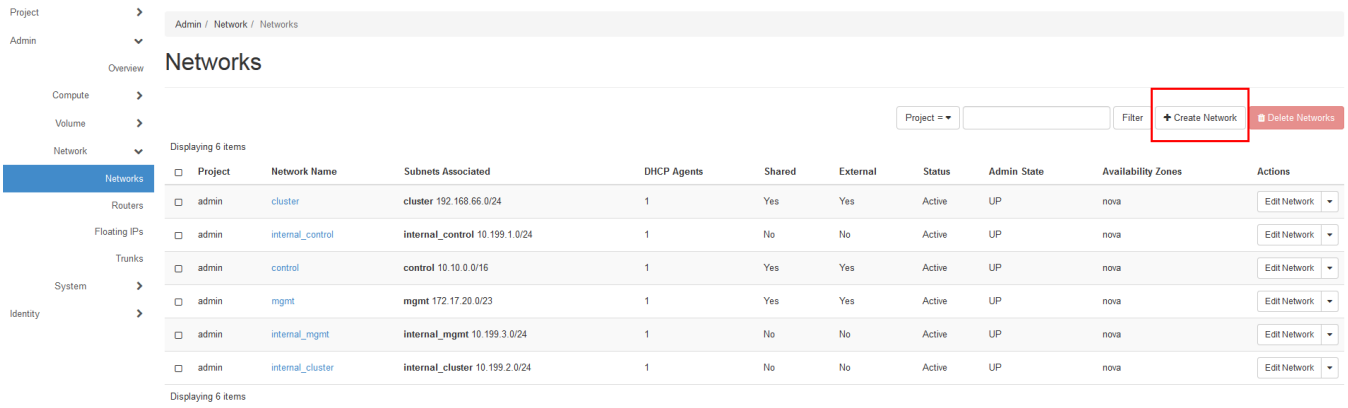
   You have created a new project.

Creating an External Network

1. From the OpenStack homepage, click **Admin** > **Network** > **Networks**.

   The **Networks** page appears as shown in the following image.

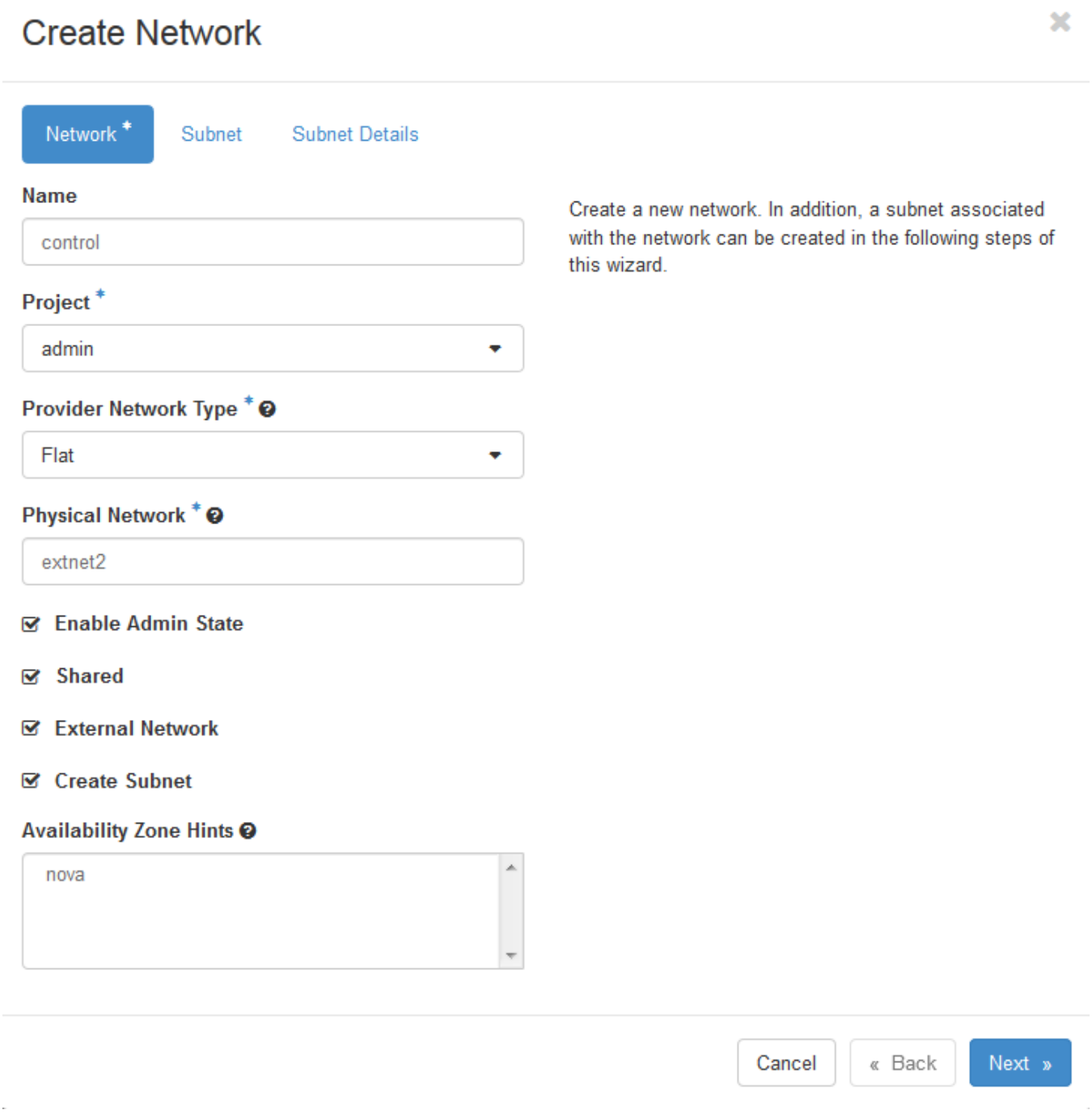
   FIGURE 41 Networks Page



2. Click **Create Networks**.

   The **Create Networks** page appears as shown in the following image.

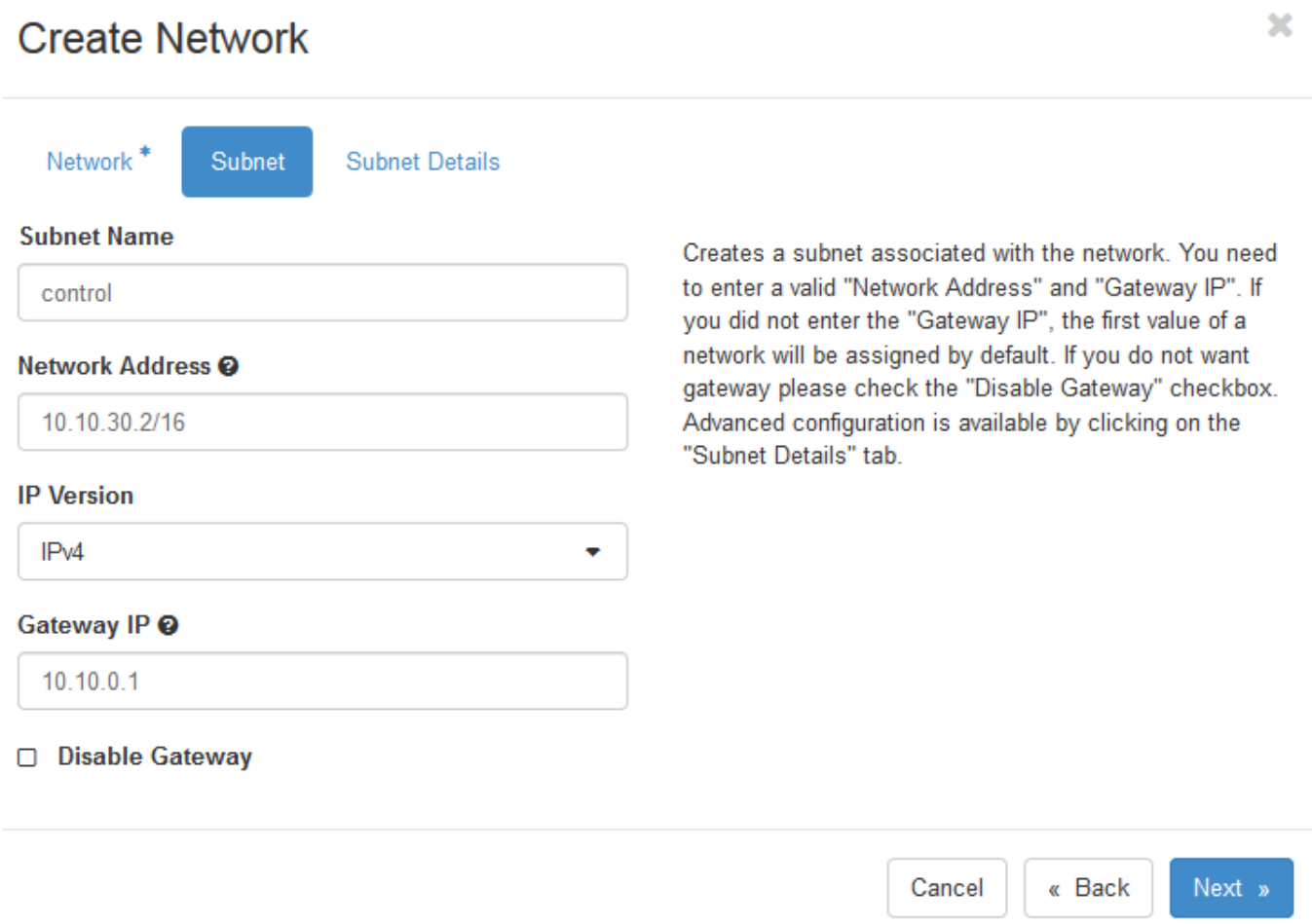
   FIGURE 42 Network tab page



3. Update the following information:
   - **Name**: Enter the interface name.
   - **Project**: From the drop-down menu, first select admin and then select other projects.
   - **Provider Network Type**: From the drop-down menu select **Flat**.
   - **Physical Network**: Enter the OVS physical interface name.
   - Select the following check boxes :
     a. **Enable Admin State**
     b. **Shared**
     c. **External Network**
     d. **Create Subnet**
4. Click **Next**.

   The **Subnet** page appear as shown in the following image.

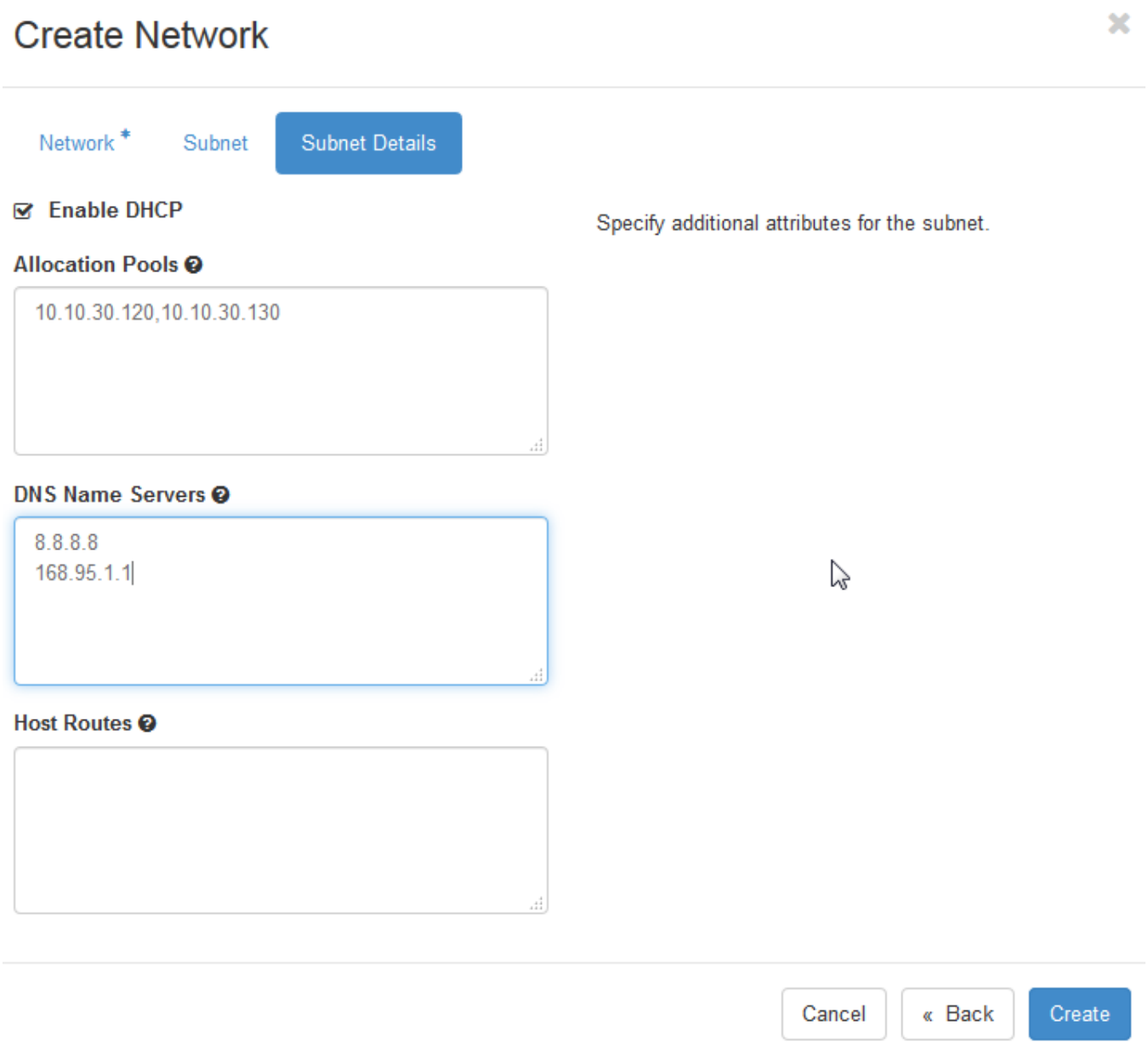
FIGURE 43 Subnet tab page



5. Update the following information:
   - **Subnet Name**: Enter the subnet name.
   - **Network Address**: Enter the static IP of your OVS bridge.
   - **IP Version**: Select the IP Version
   - **Gateway IP**: Enter the gateway IP of this OVS bridge.
6. Click **Next**.

   The **Subnet Details** tab page appear as shown in the following image.

FIGURE 44 Subnet Details tab page



7. Select the **Enable DHCP** check box.
8. For **Allocation Pools**, enter the DHCP pool range. Separate the range with a comma.
9. For **DNS Name Servers**, enter the DNS server address, one address per line.
10. Click **Create**.

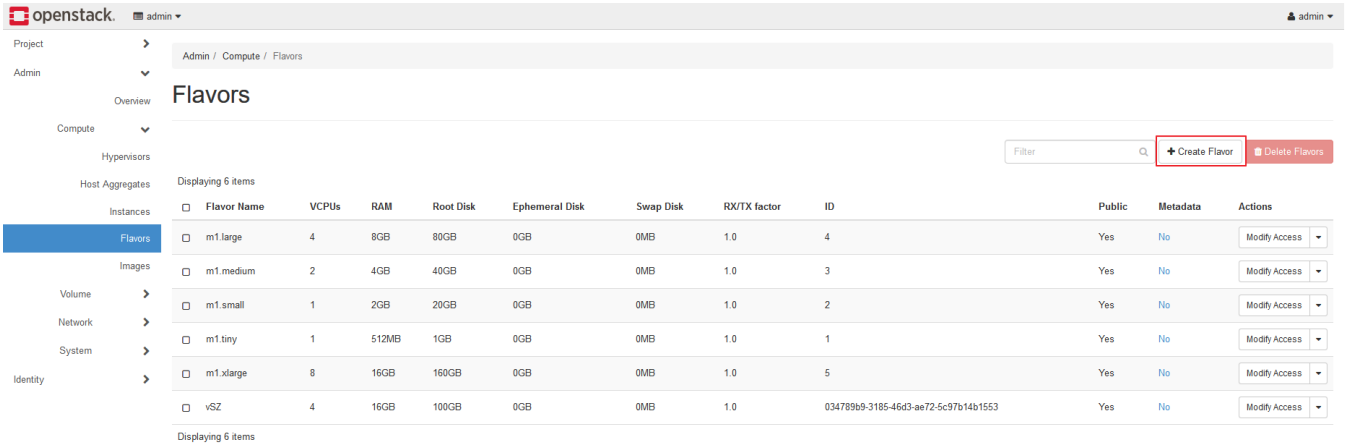
NOTE
Repeat the procedure until you create an external interface for Control, Cluster and Management interface.

Creating Flavors

1. From the OpenStack homepage, click **Admin** > **Compute** > **Flavors**.

   The **Flavors** page appears.

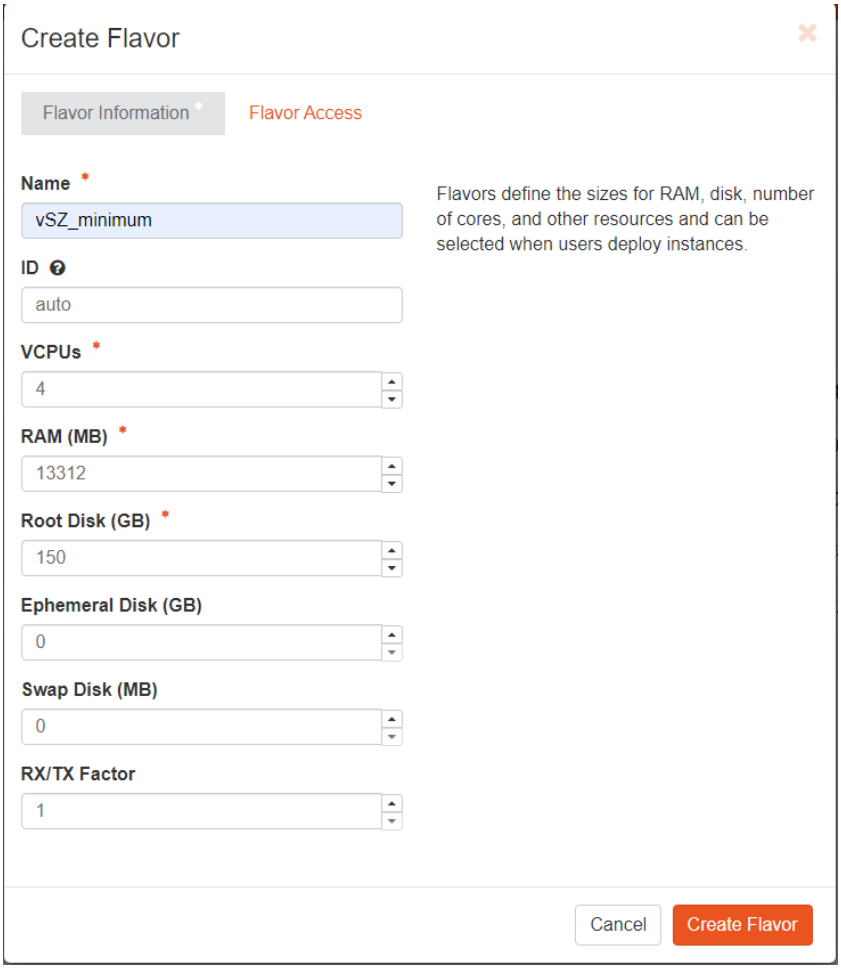
FIGURE 45 Flavors Page



2. Click **Create Flavor**.

   The **Create Flavor** page appears.

   FIGURE 46 Flavor Settings page



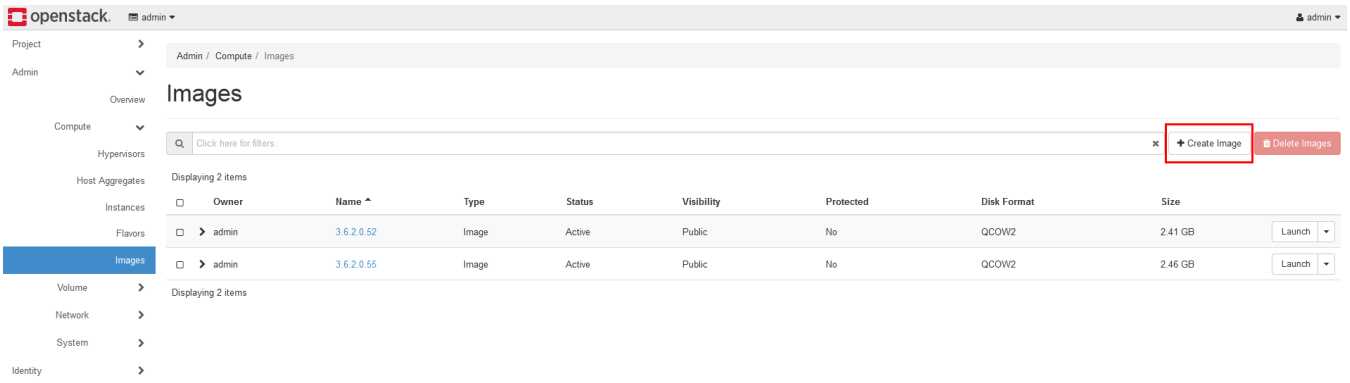
3. Enter a **Name** for the flavor you create.
4. Assign the hardware resource that you are going to deploy.
5. Click **Create Flavor**.

Creating an Image

1. From the OpenStack homepage, click **Admin** > **Compute** > **Images**.

   The **Images** page appears.

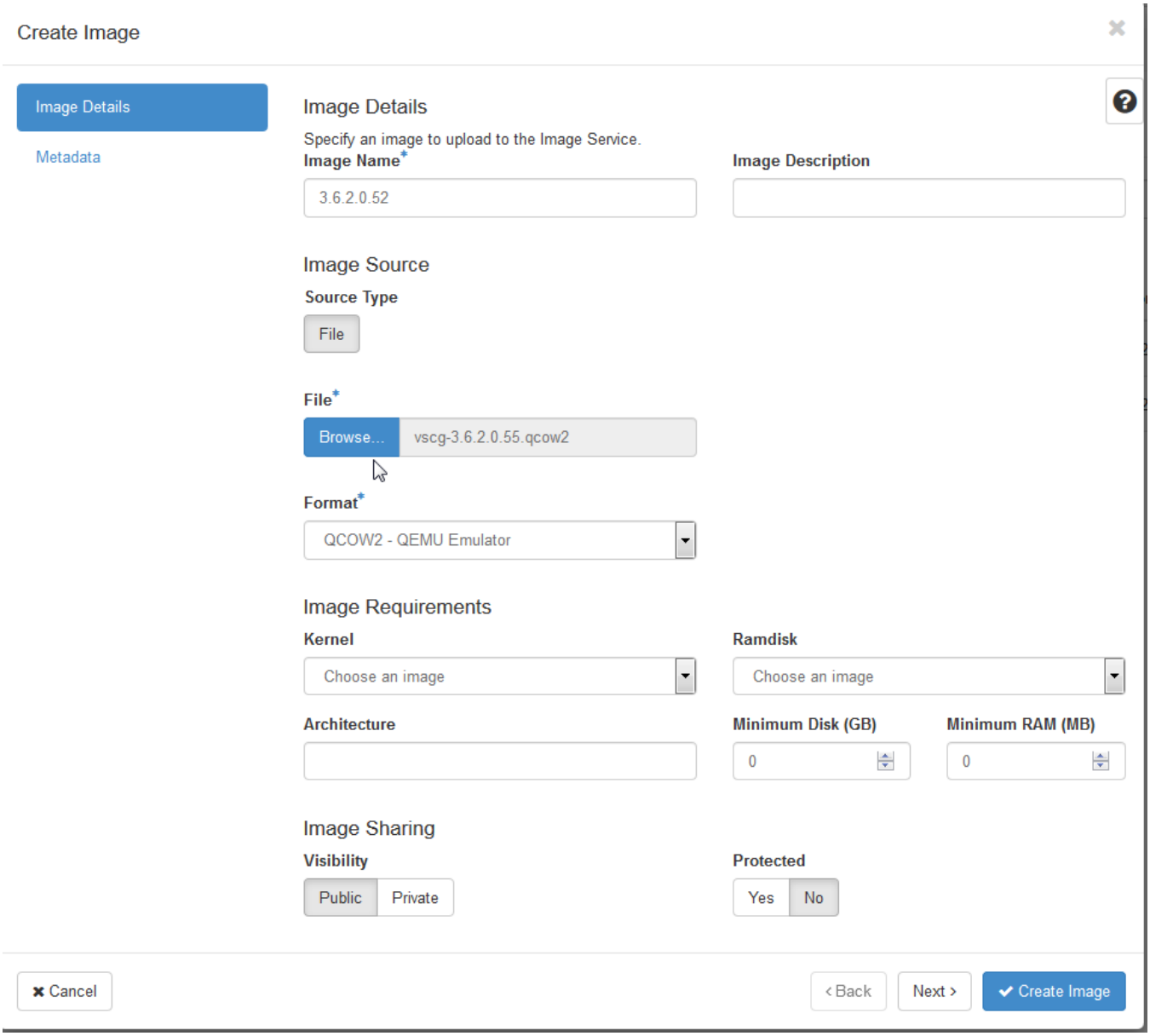
   FIGURE 47 Images Page



2. Click **Create Image**.

   The **Create Image** page appears.

   FIGURE 48 Image Settings page



3. **Image Name**: Enter a name.
4. Click **Browse** and select the vSZ `qcow2` file
5. **Format**: Select **QCOW2-QEMU Emulator**.

6. Click **Create Image**.

NOTE
Logout openstack.

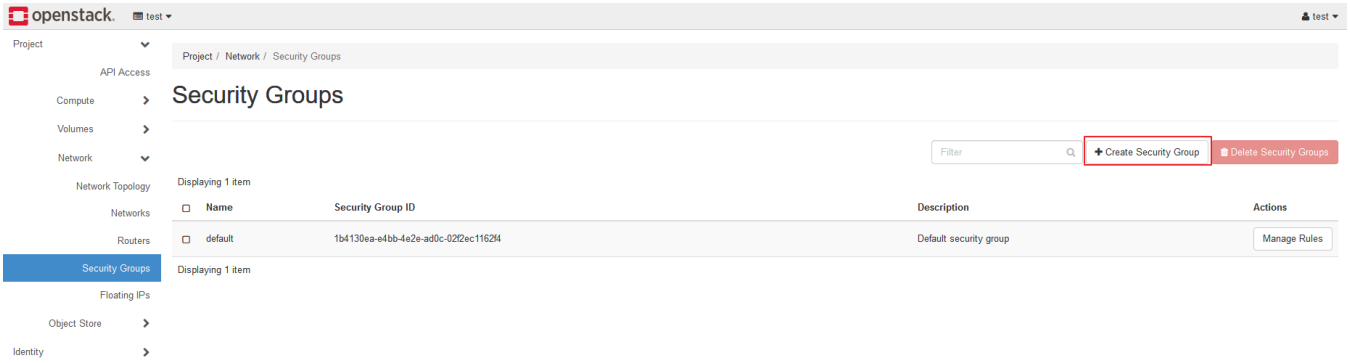
Creating Project Items

Creating Security Groups

1. Login OpenStack with the user credential created in Creating a New User on page 62.
2. From the homepage, click **Project** > **Network** > **Security Groups**.

   The **Security Groups** page is displayed.

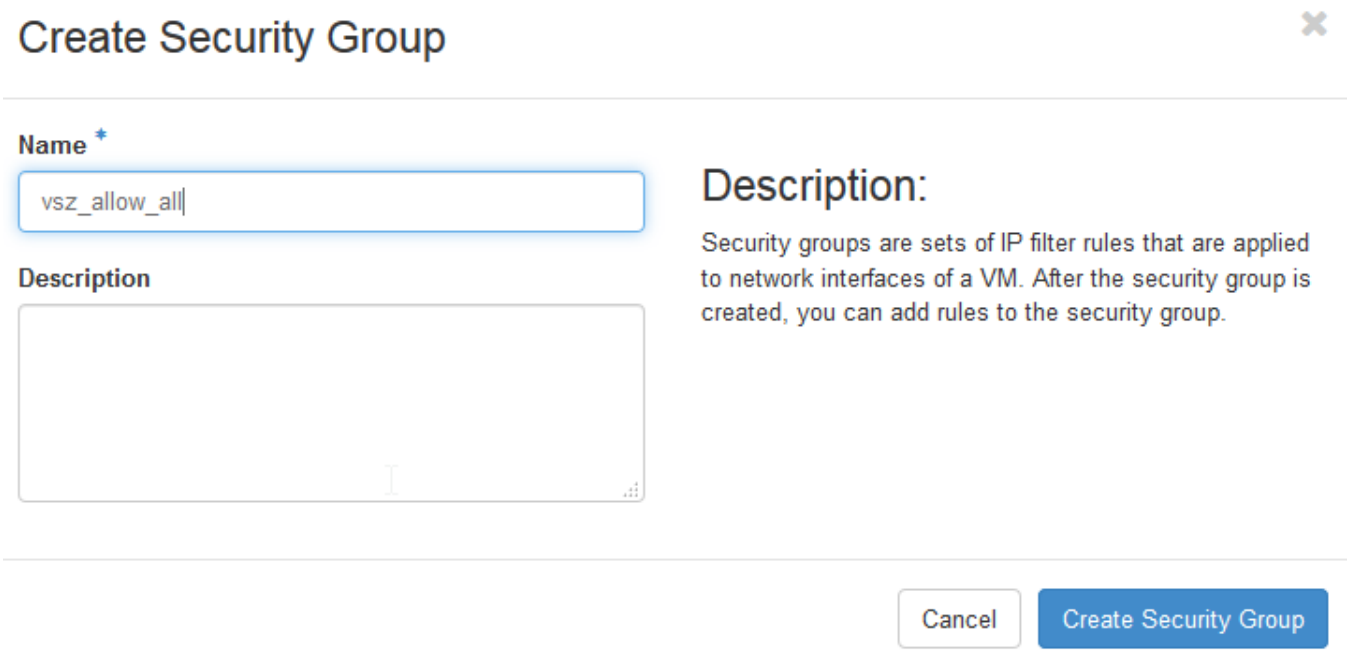
FIGURE 49 Security Group Page



3. Click **Create Security Group**.

   The **Create Security Group** page is displayed.

   FIGURE 50 Creating a Security Group



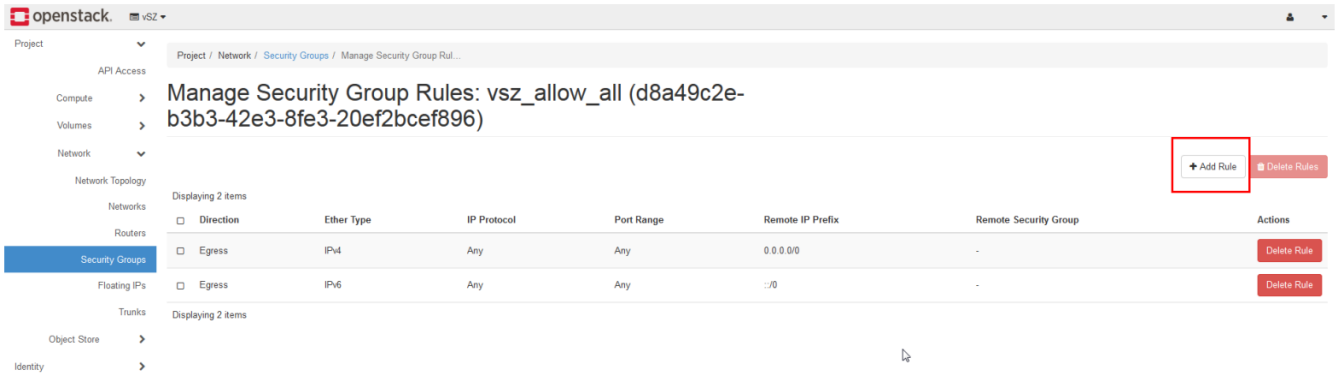
4. Enter a **Name** for the security group and click **Create Security Group**.

   The new group is listed in the **Security Groups** page.

5. Select the group from the list and click **Manage Rules**.

   The **Manage Security Group Rules** page is displayed.

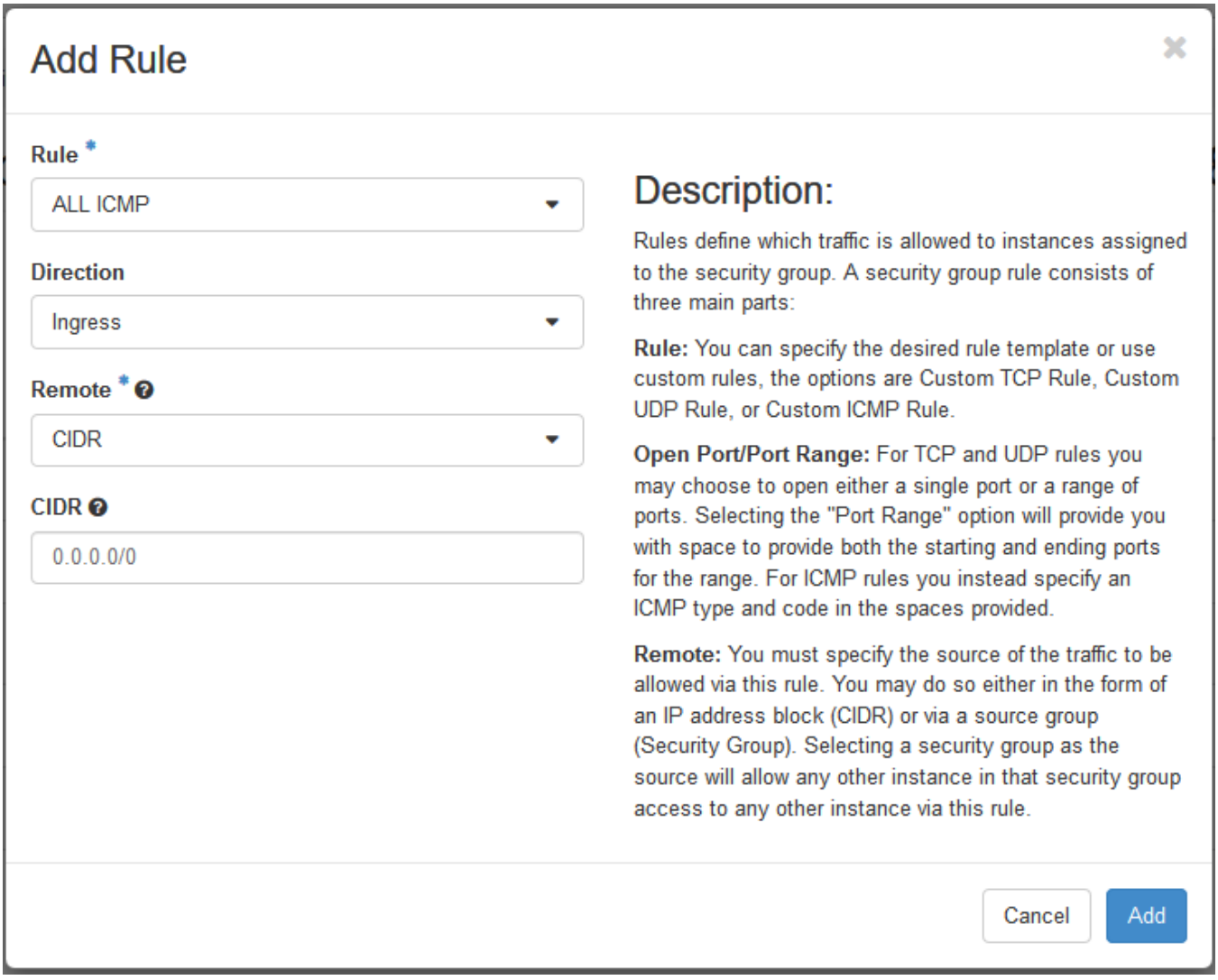
   FIGURE 51 Managing Rules



6. Click **Add Rule**.

   The **Add Rule** page is displayed.

FIGURE 52 Adding Rules



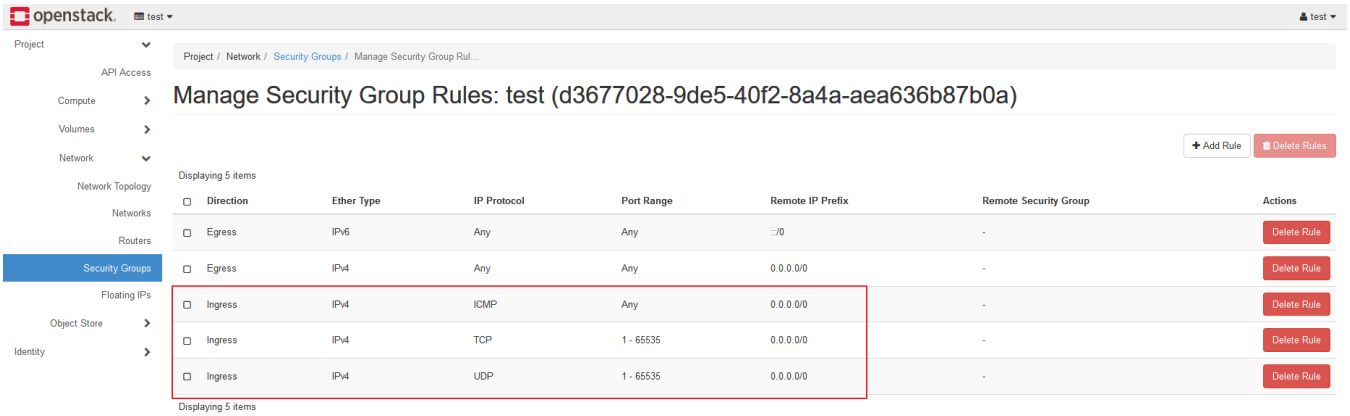
7. **Rule**: Select the rule for this security group.
8. **Direction**: Select the traffic direction.

   NOTE
   Refer the *Administrator Guide* for port configuration.

9. Click **Add**, the system takes a few seconds to complete the action..

   The new rules are listed in the **Manage Security Group Rules** page .

   FIGURE 53 New Rules

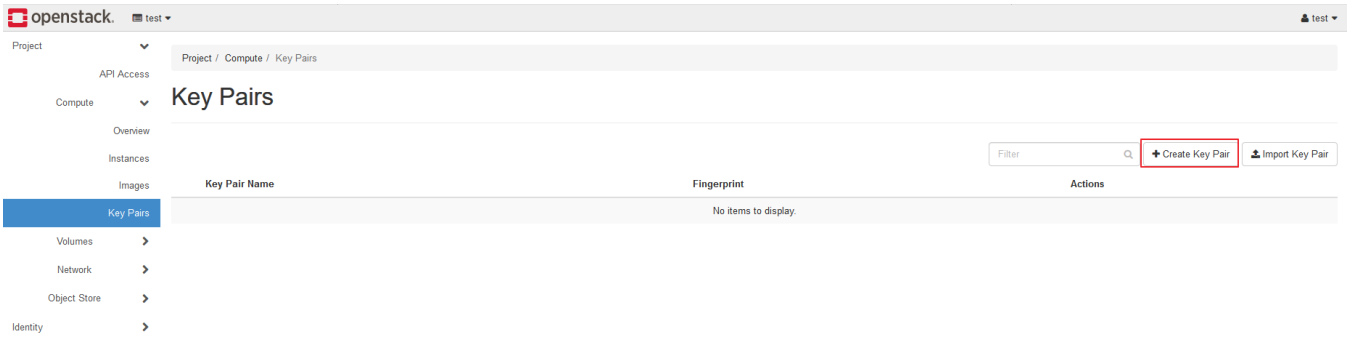


Creating Key Pairs

1. From the homepage, click **Project** > **Compute** > **Key Pairs**.

   The **Key Pairs** page is displayed.

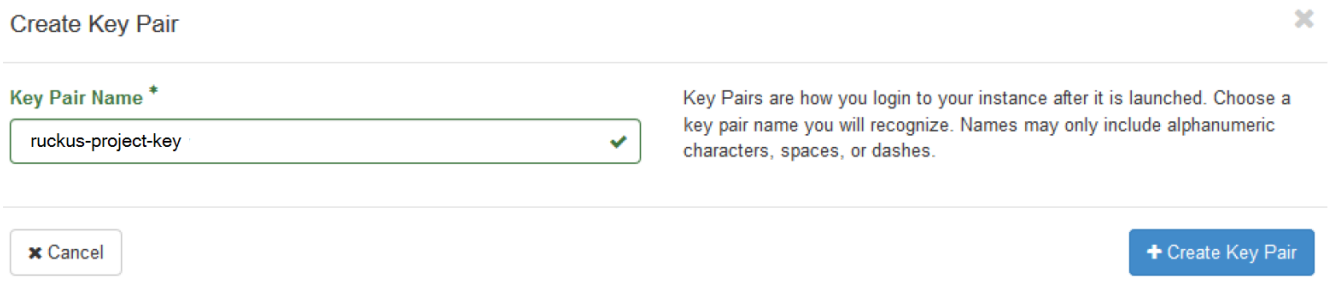
   FIGURE 54 Key Pairs Page



2. Click **Create Key Pairs**.

   The **Create Key Pair** page is displayed.

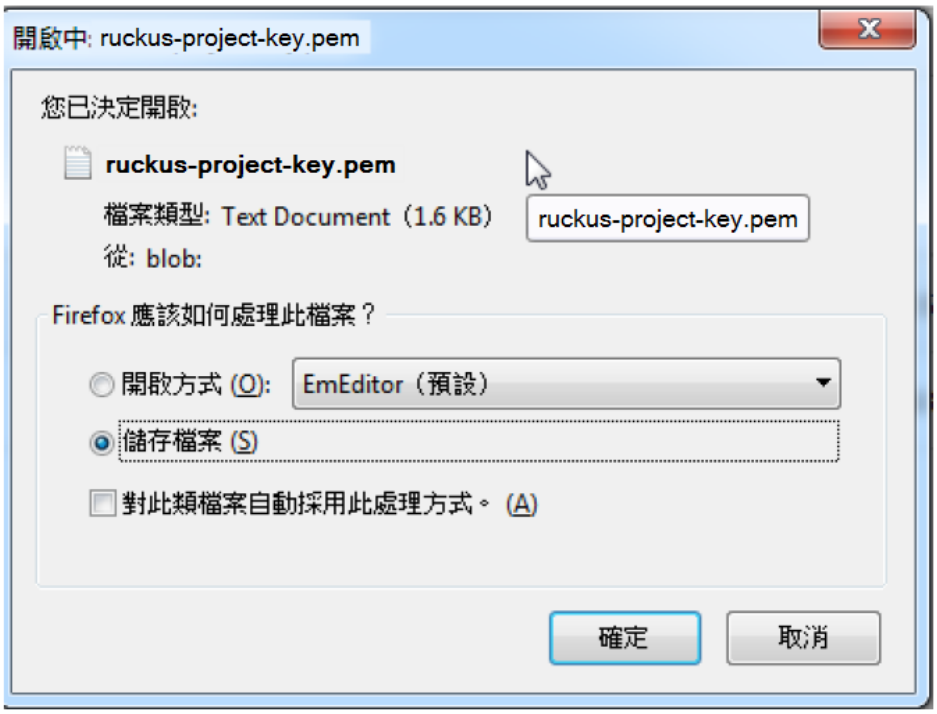
   FIGURE 55 Creating Key Pairs



3. Enter the **Key Pair Name** and click **Create Key Pair**.

   The `key.pem` file download window should appear automatically.

   FIGURE 56 Key.pem File Download



4. Save the file to the Linux PC and change permission using command **chmod 600 test.pem**.

   It is used to establish ssh vSZ connection with floating IP address. Other terminal tools also can use this key file to establish ssh connection with vSZ.

Deploying three-interface vSZ without built-in SNAT

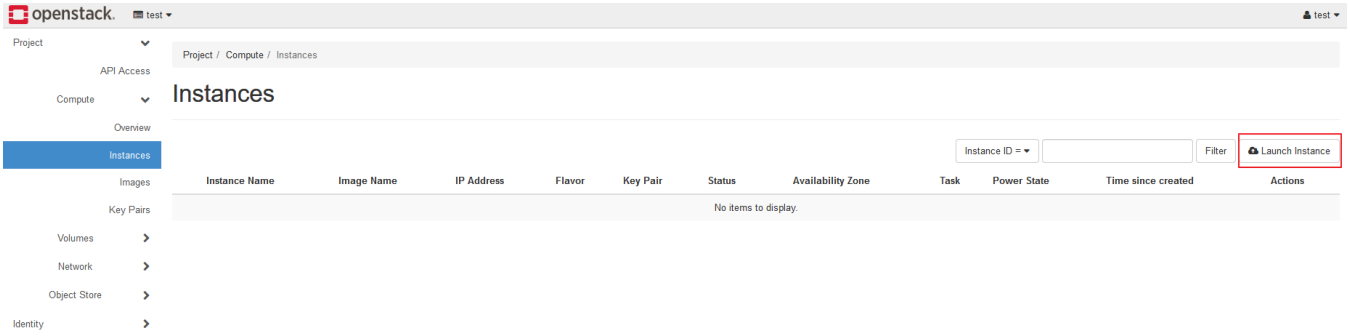
Launching an Instance for three-interface vSZ

NOTE
Login OpenStack with user account that we just created.

1. From the homepage, click **Project** > **Compute** > **Instances**.

   The **Instances** page is displayed.

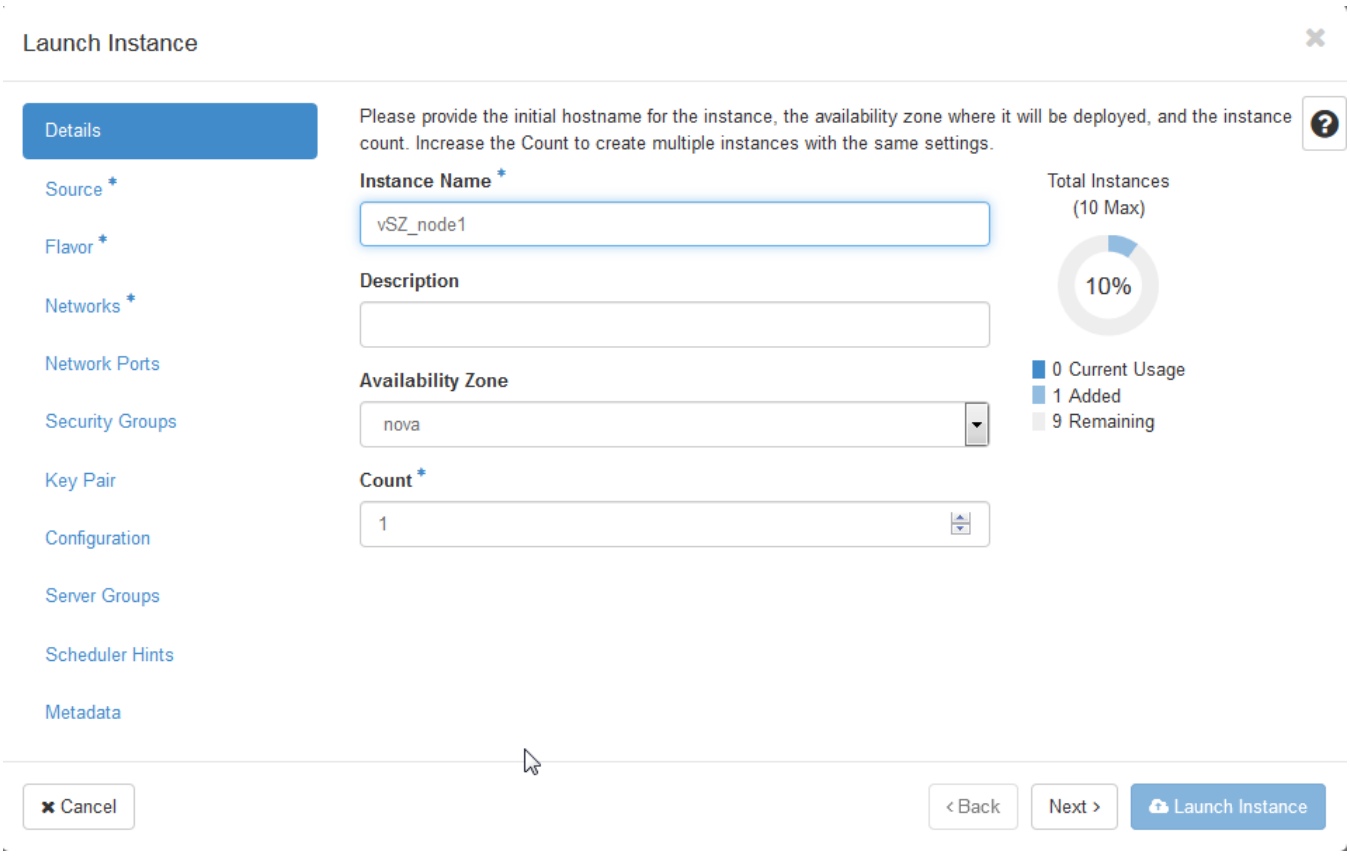
FIGURE 57 Instances Page



2. Click **Launch Instance**.

   The **Launch Instance** page is displayed.

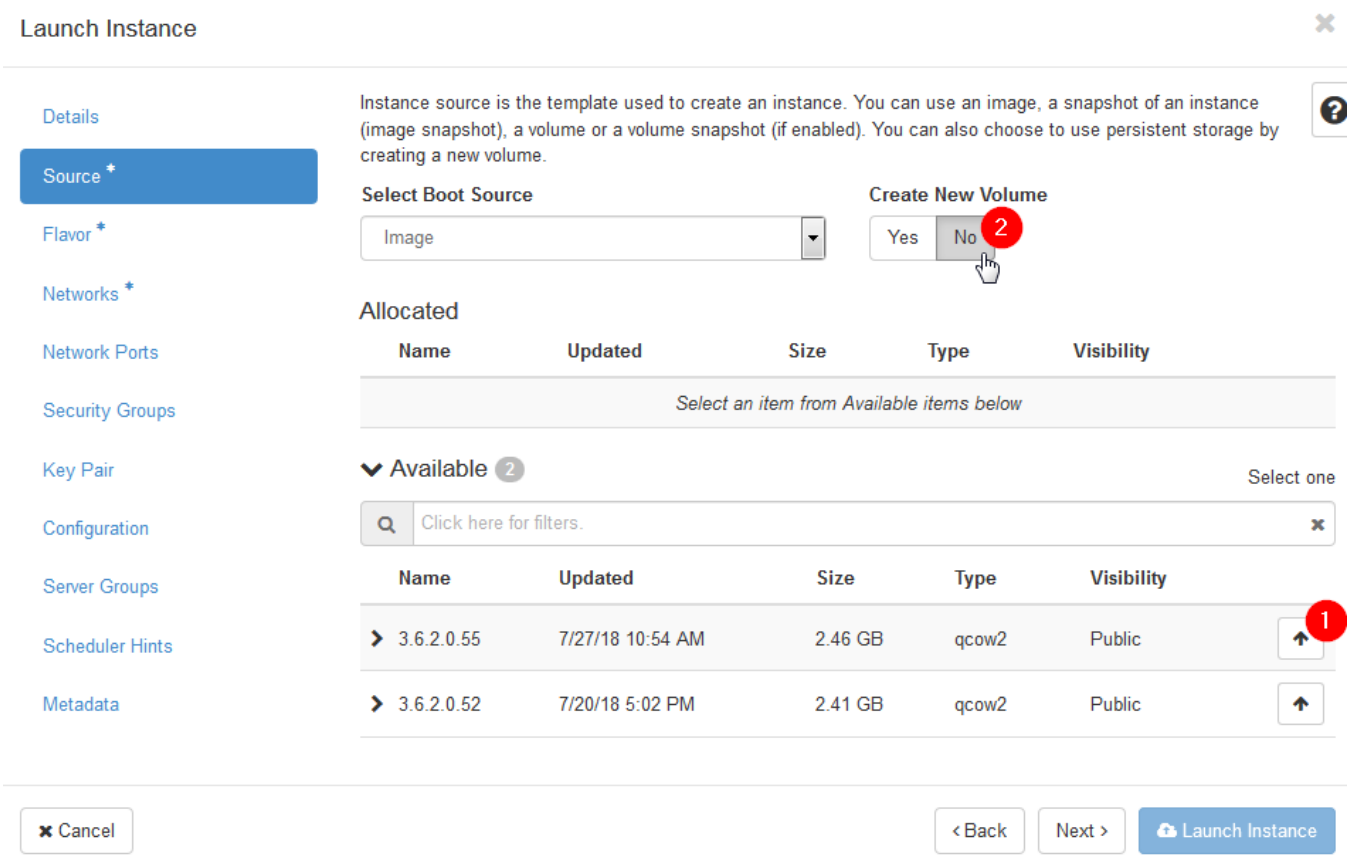
FIGURE 58 Launch Instance Page



3. From the **Details**, enter the **Instance Name** and click **Next**.

   The **Source** tab is displayed.

   FIGURE 59 Source Tab Page

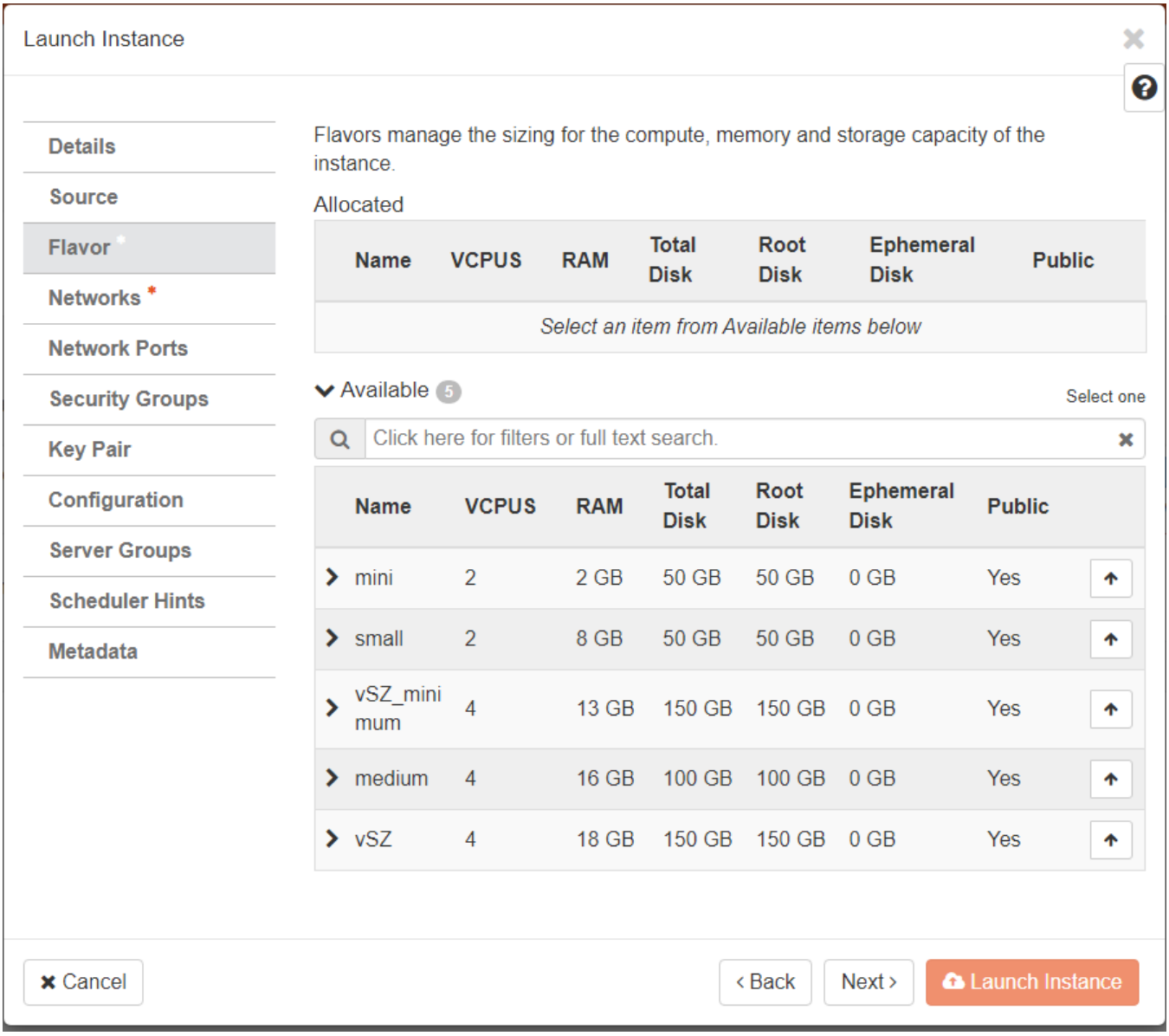


4. From the **Available** list, click **Move** to move the image to the **Allocated** list.
5. For **Create New Volume**, select **No**.

6. Click **Next**.

   The **Flavor** tab is displayed.

FIGURE 60 Flavor Tab Page

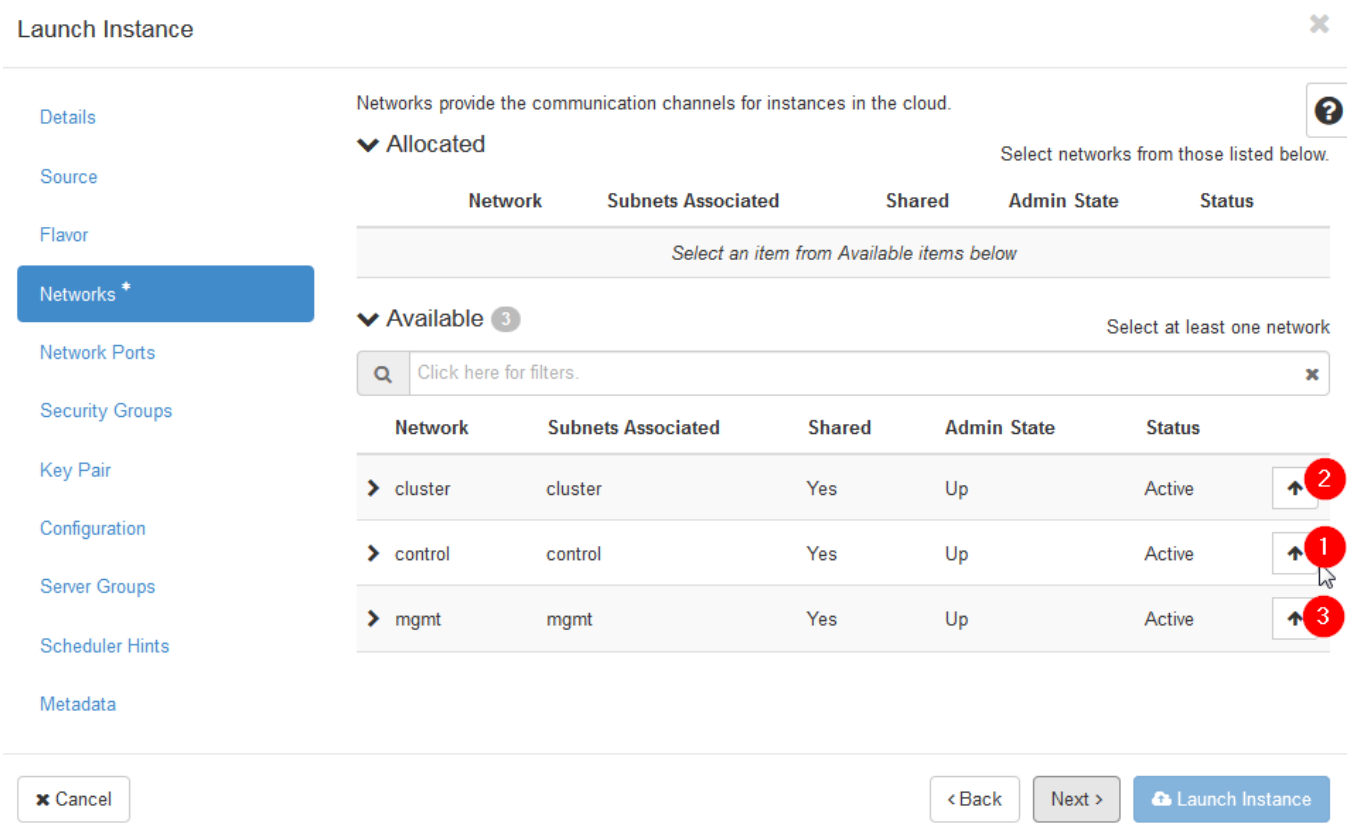


7. From the **Available** list, click **Move** to move the resource plan to the **Allocated** list.

8. Click **Next**.

   The **Networks** tab is displayed.

   FIGURE 61 Networks Tab Page



9. From the **Available** list, click **Move**  to move the network interfaces to the **Allocated** list.

   Interfaces must be selected in the following order:

   a. Control interface
   b. Cluster interface
   c. Management interface

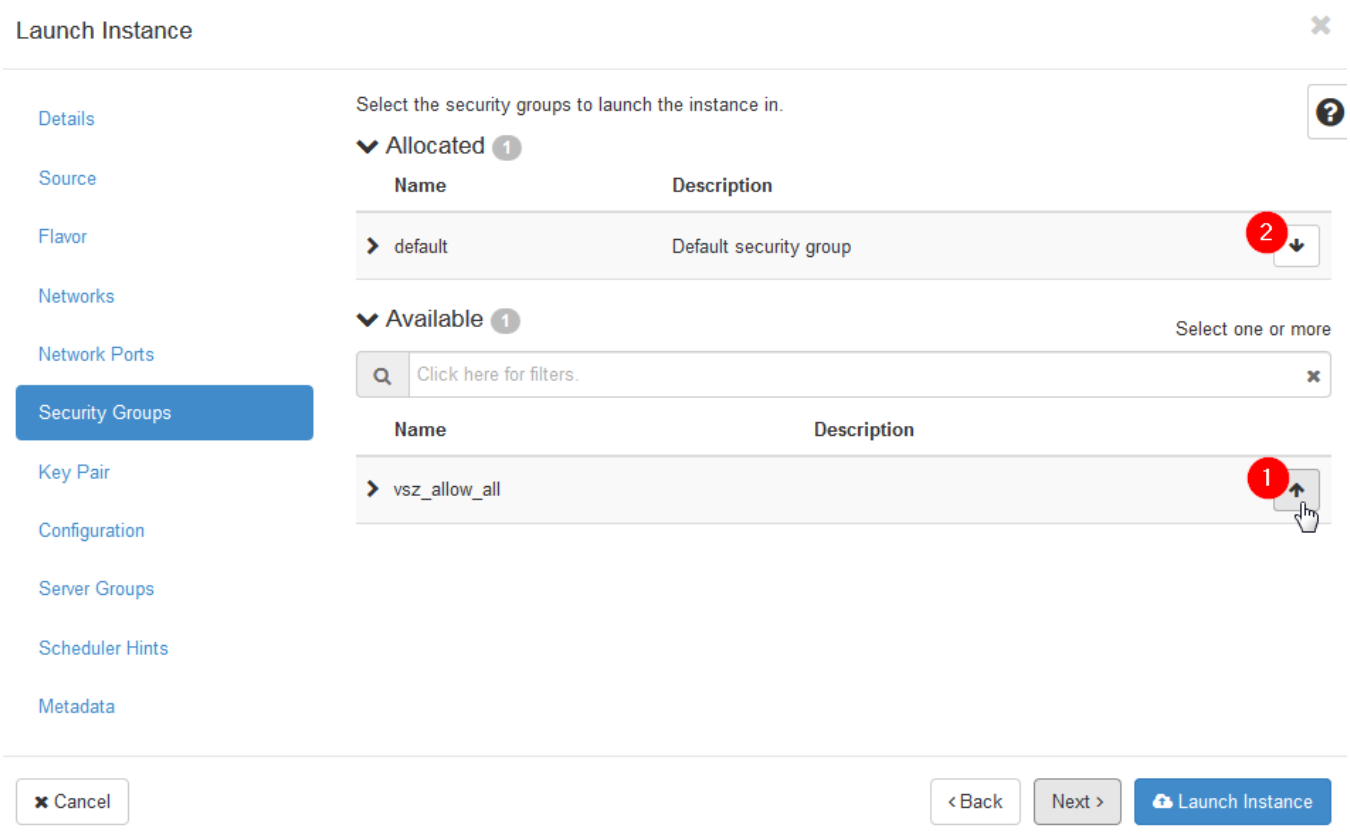
10. Click **Next**.

    The **Network Ports** tab is displayed.

11. Click **Next**.

    The **Security Groups** tab is displayed.

    FIGURE 62 Security Groups Tab Page



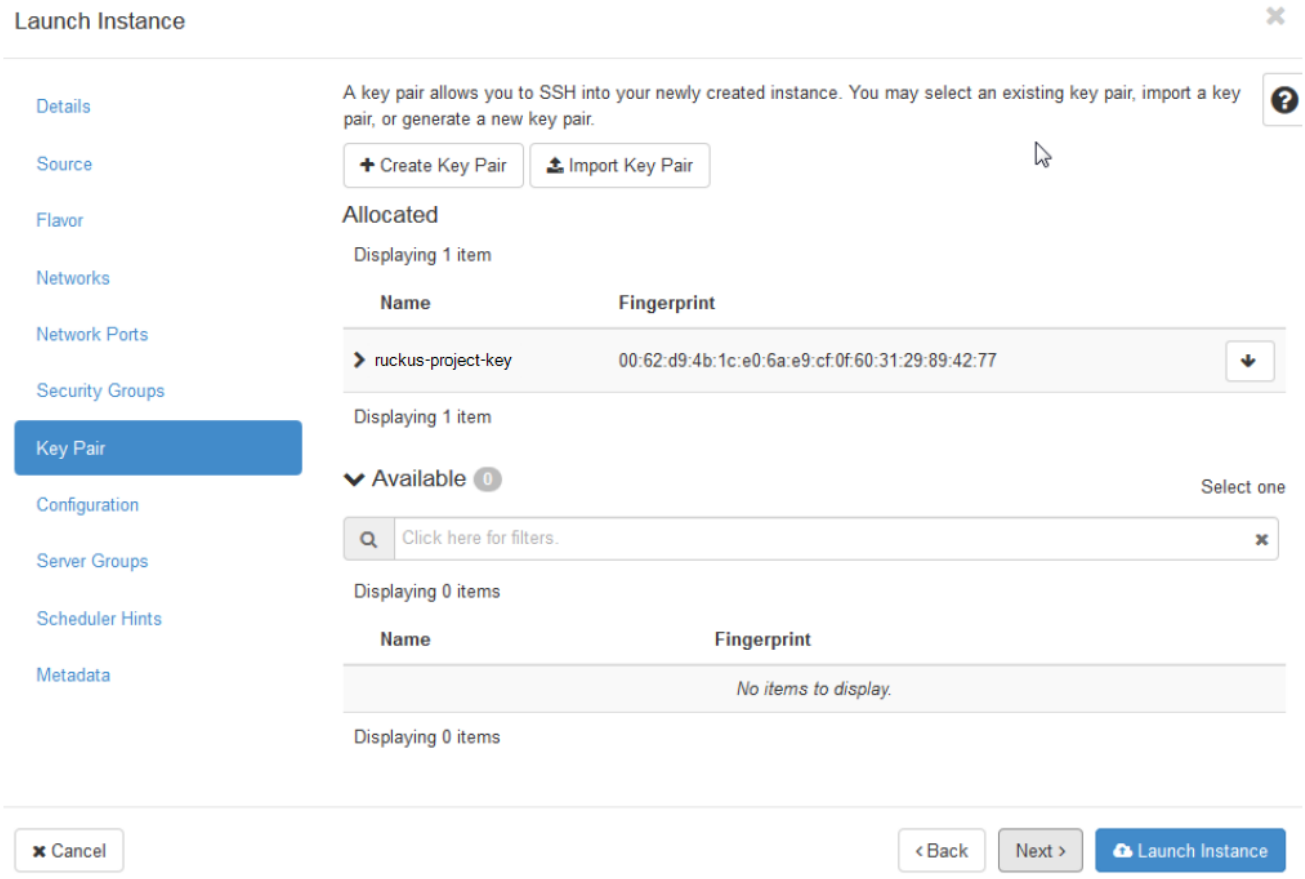
12. From the **Available** list, click **Move** to move the rule to the **Allocated** list.

13. From the **Allocated** list, click the **Remove** to delete the default rule.

14. Click **Next**.

    The **Key Pair** tab is displayed.

    FIGURE 63 Key Pair Tab Page

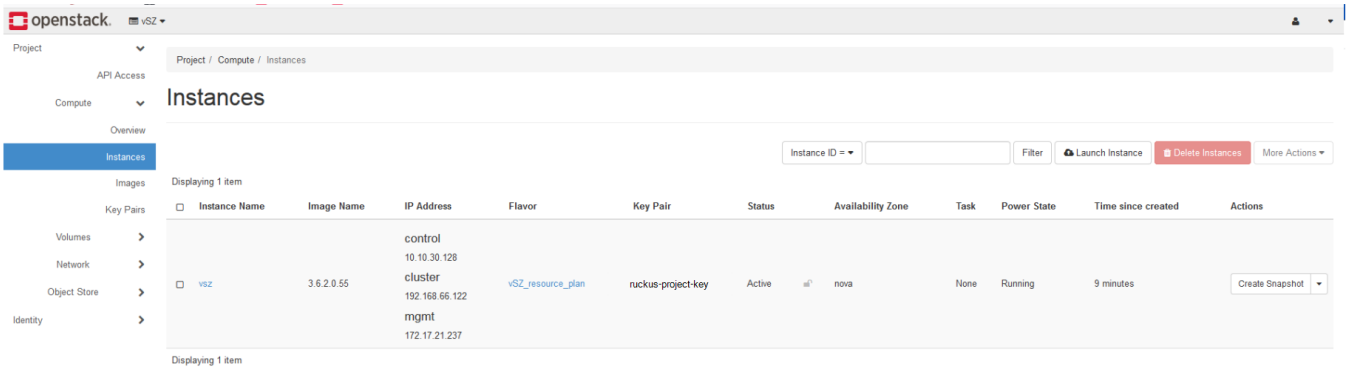


15. From the **Available** list, click **Move** to move the key pair to the **Allocated** list. If there is only one key pair, the system will automatically move it to the **Allocated** list.

16. Click **Launch Instance** to configure.

    The system will take a few minutes to complete the process. Once it is done, you can see the **Power State** change to **Running**.

    FIGURE 64 Instances Page



Deploying One-interface vSZ with built-in SNAT

Creating an Internal Network

NOTE
Login OpenStack with user account that we just created.

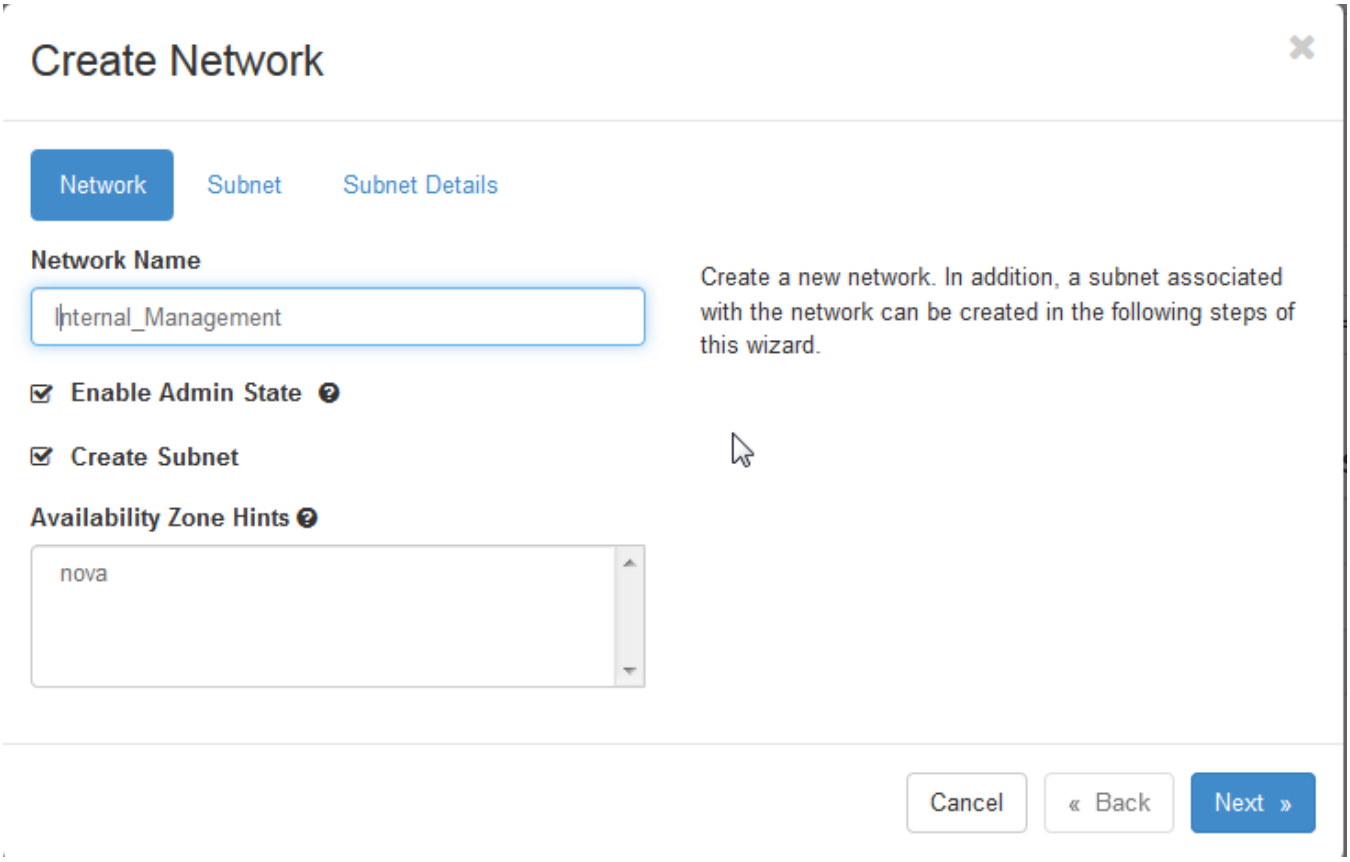
1. From the homepage, click **Project** > **Network** > **Networks**.

   The **Networks** page is displayed.

2. Click **Create Network**.

   The **Create Network** page is displayed.

   FIGURE 65 Creating an Internal Network



3. Enter the **Network Name** and click **Next**.

   The **Subnet** tab is displayed.

4. Enter the **Subnet Name**.
5. Enter the **Network Address** for the internal network and click **Next**.

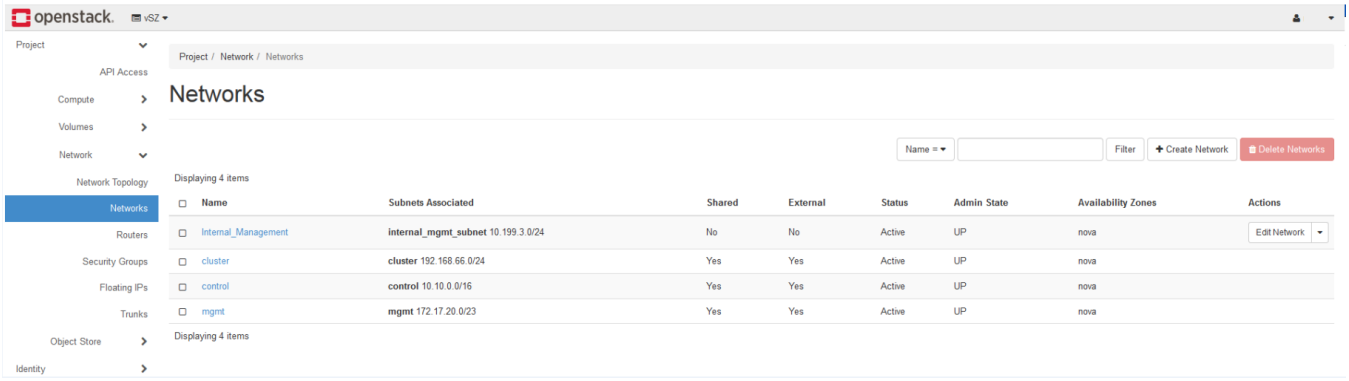
   The **Subnet Details** tab is displayed.

6. In **DNS Name Server**: enter the DNS address.

7. Click **Create**.

   The system will take few seconds to complete the action.

FIGURE 66 Internal Network

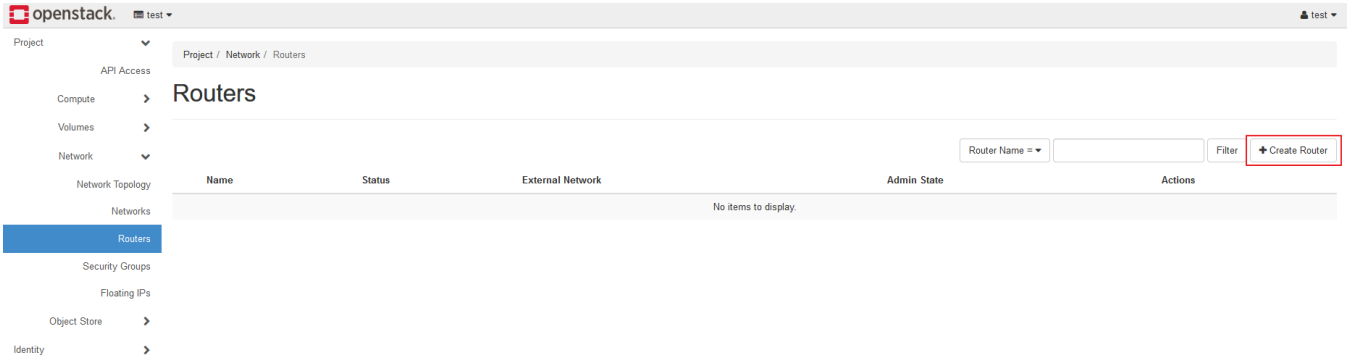


Creating Router Settings

1. From the homepage, click **Project** > **Network** > **Routers**.

   The **Routers** page is displayed.

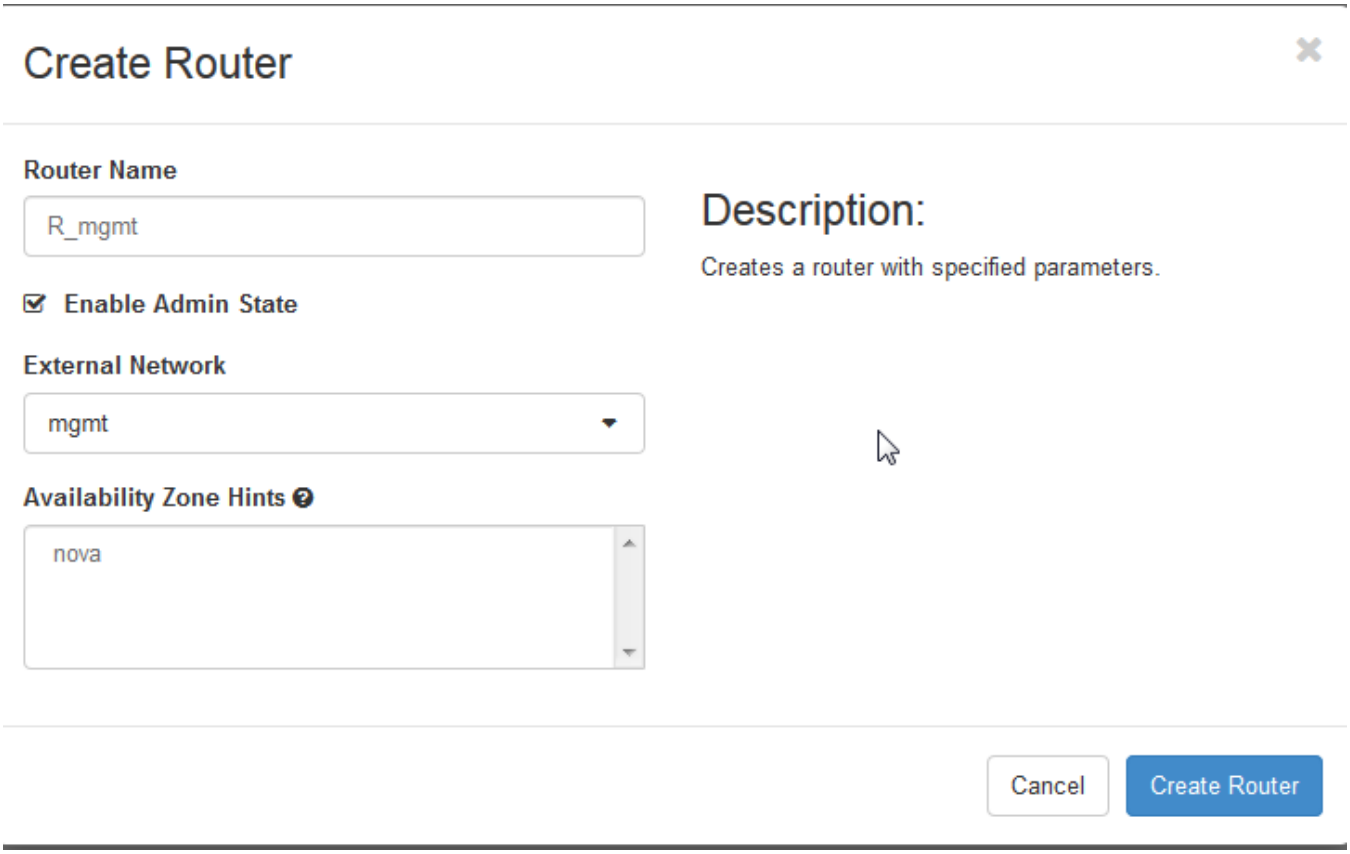
FIGURE 67 Routers Page



2. Click **Create Router**.

   The **Create Router** page is displayed.

   FIGURE 68 Create Router Page

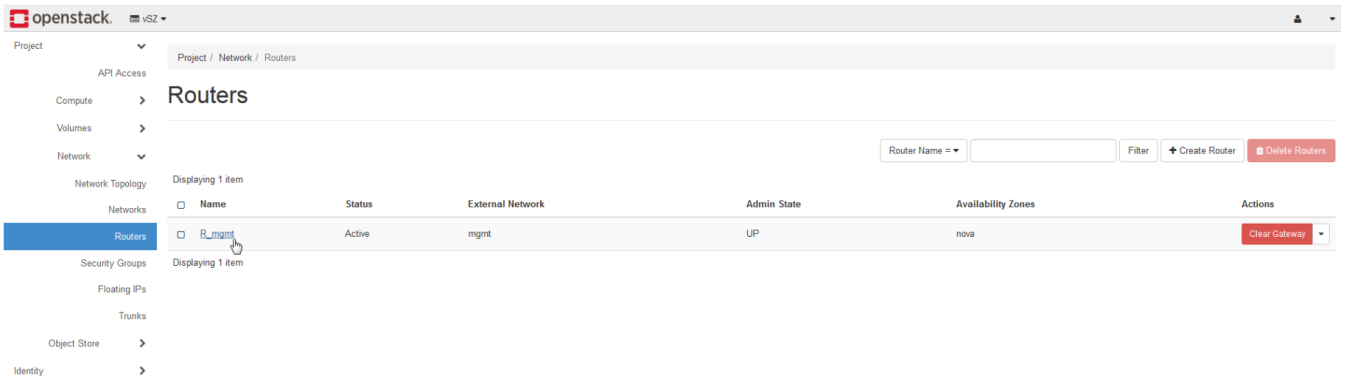


3. **Router Name**: Enter the router name.
4. **External Network**: Select the external network which must be the NAT interface.

5. Click **Create Router**.

   The newly created router is listed in the **Routers** page.

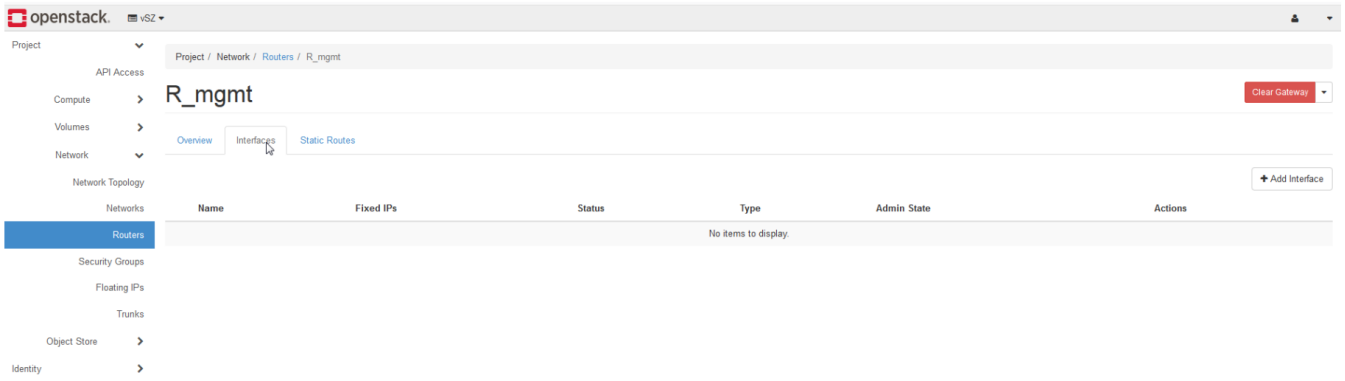
   FIGURE 69 New Router in the Routers Page



6. Select the router and click the **Interfaces** tab.

   The **Interfaces** tab page is displayed.

   FIGURE 70 Interface Tab Page



7. Click **Add Interface**.

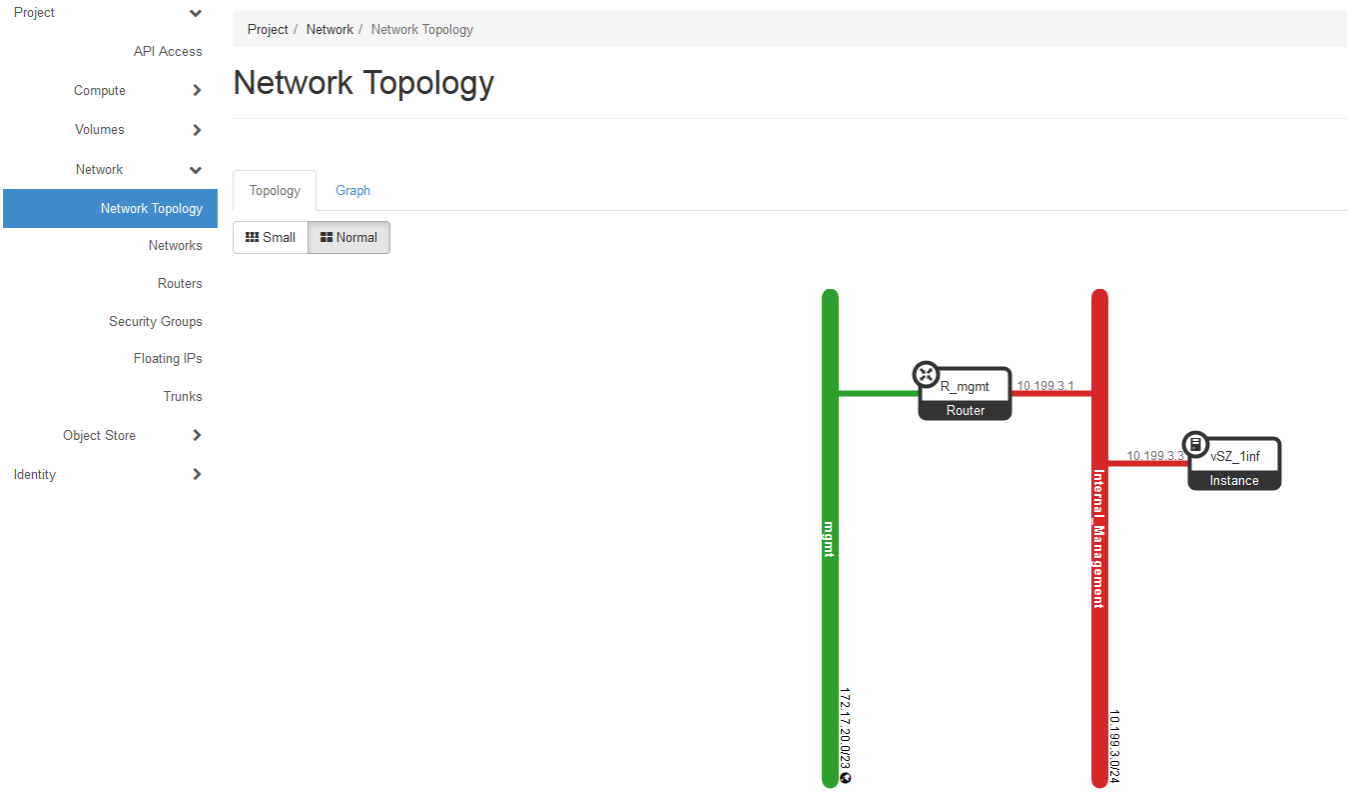
   The **Add Interface** page is displayed.

   FIGURE 71 Add Interface Page

8. **Subnet**: Select the interface that you created.
9. Click **Submit**.
10. Click **Project** > **Network** > **Network Topology**.

11. Click **Normal** mode and ensure that the router is created correctly.

FIGURE 72 Network Topology

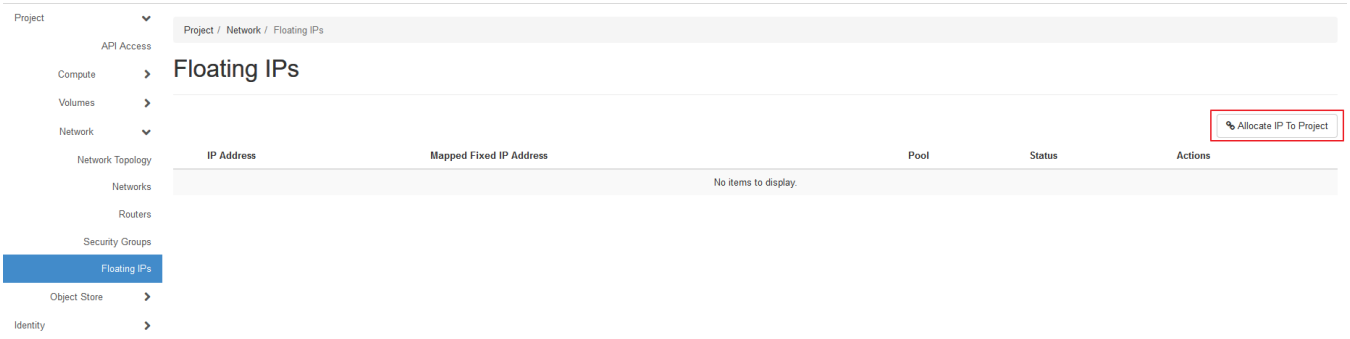


Allocating Floating IPs

1. From the homepage, click **Project** > **Network** > **Floating IPs**.

   The **Floating IPs** page is displayed.

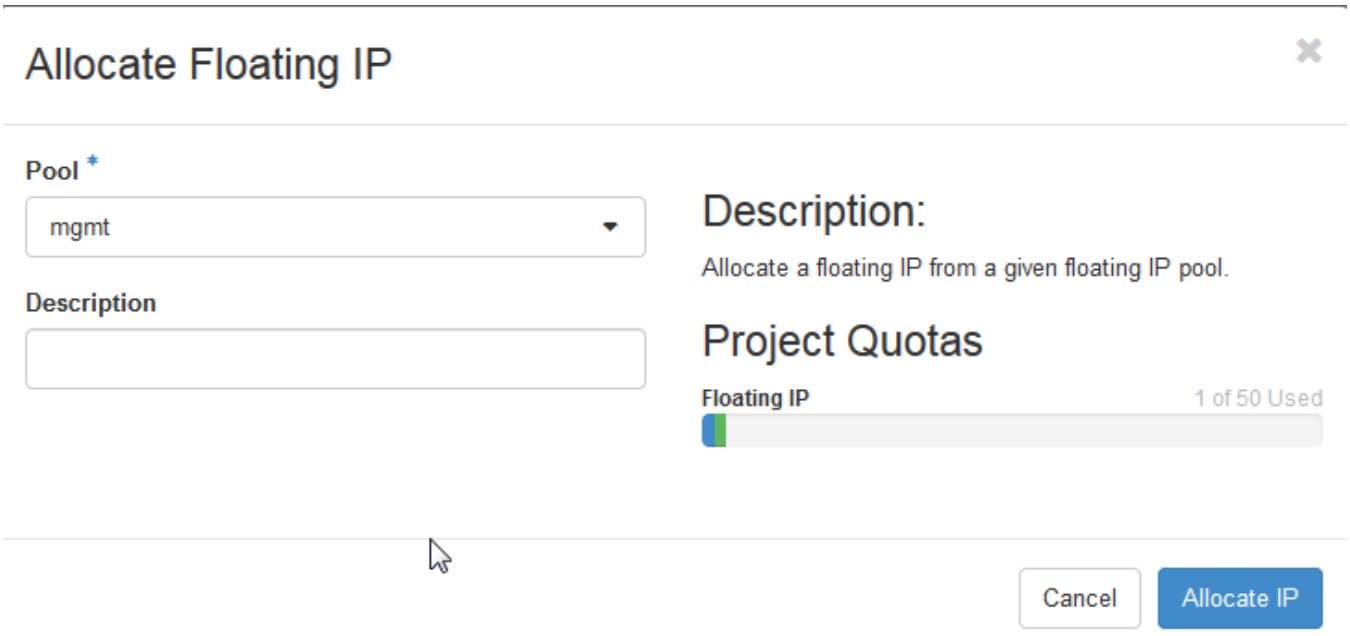
   FIGURE 73 Floating IPs Page



2. Click **Allocate IP to Project**.

   The **Allocate Floating IP** page is displayed.

   FIGURE 74 Allocate Floating IP Page

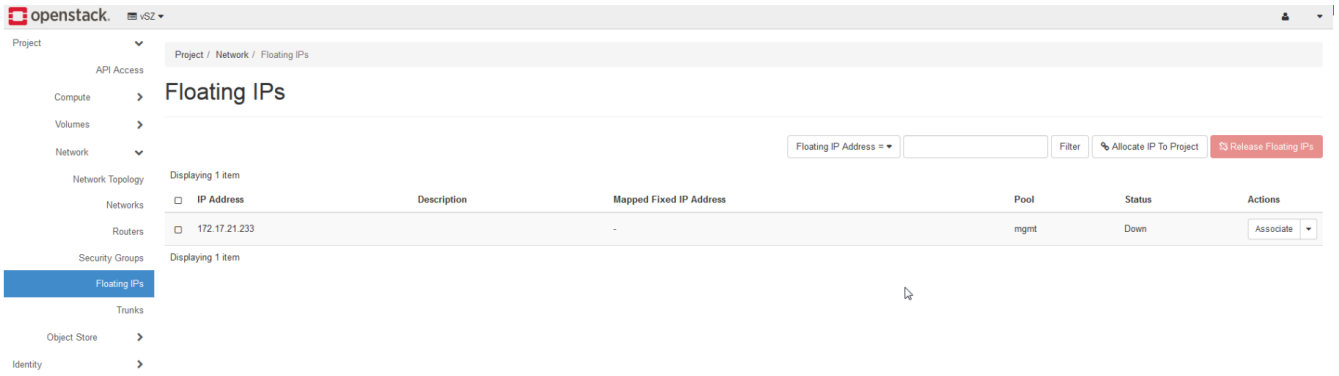


3. From the **Pool**, select the external interface.

4. Click **Allocate IP**.

   The system takes a few seconds to allocate the IP.

   FIGURE 75 Allocated Floating IP



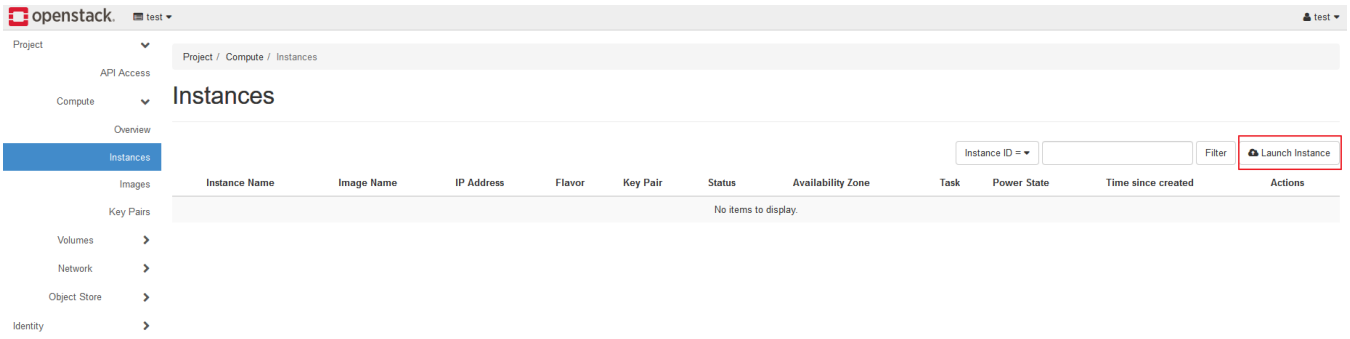
Launching an Instance for One-interface vSZ

NOTE
Login OpenStack with user account that we just created.

1. From the homepage, click **Project** > **Compute** > **Instances**.

   The **Instances** page is displayed.

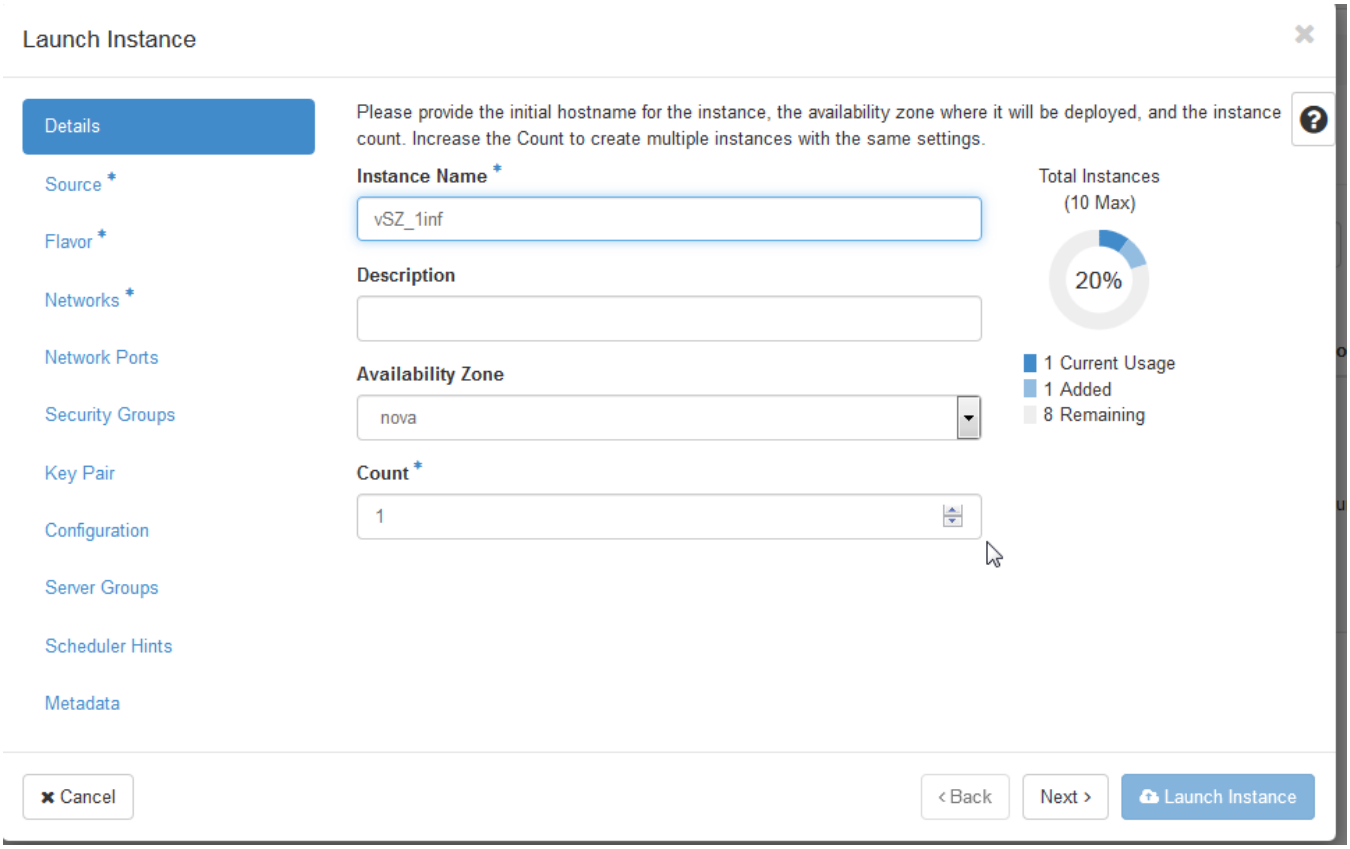
   FIGURE 76 Instances Page



2. Click **Launch Instance**.

   The **Launch Instance** page is displayed.

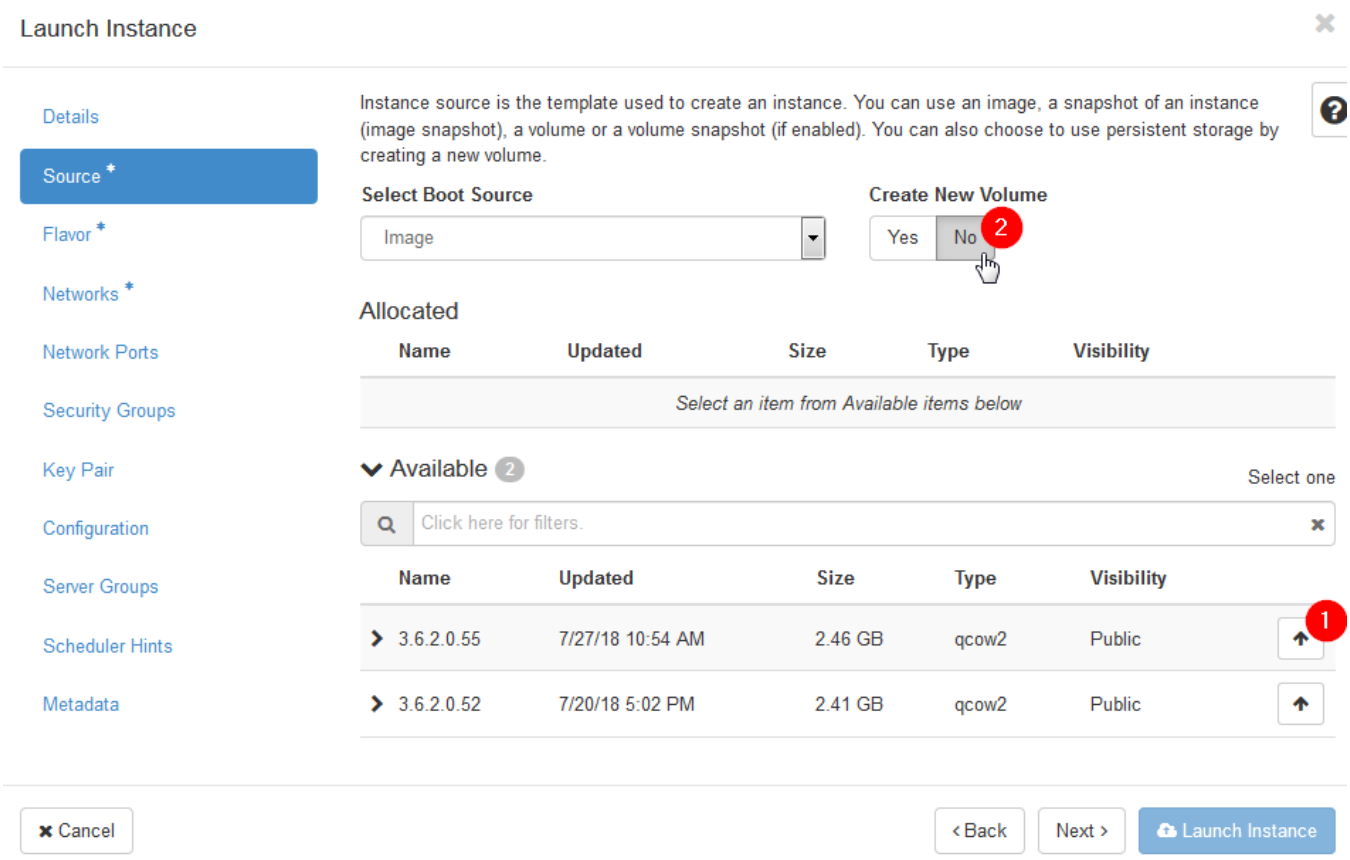
   FIGURE 77 Launch Instance Page



3. From the **Details**, enter the **Instance Name** and click **Next**.

   The **Source** tab is displayed.

FIGURE 78 Source Tab Page

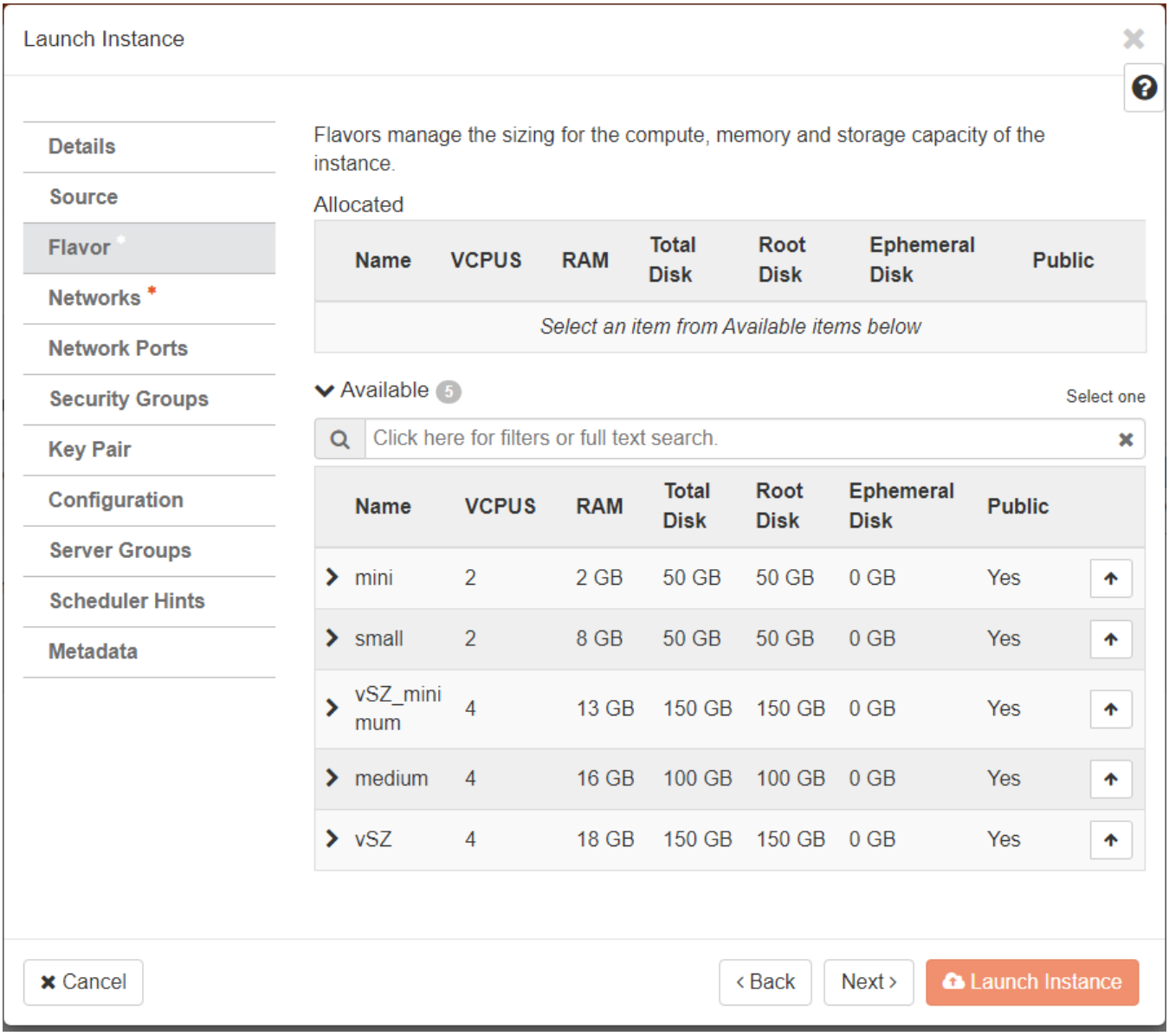


4. From the **Available** list, click **Move** to move the image to the **Allocated** list.
5. For **Create New Volume**, select **No**.

6. Click **Next**.

   The **Flavor** tab is displayed.

   FIGURE 79 Flavor Tab Page

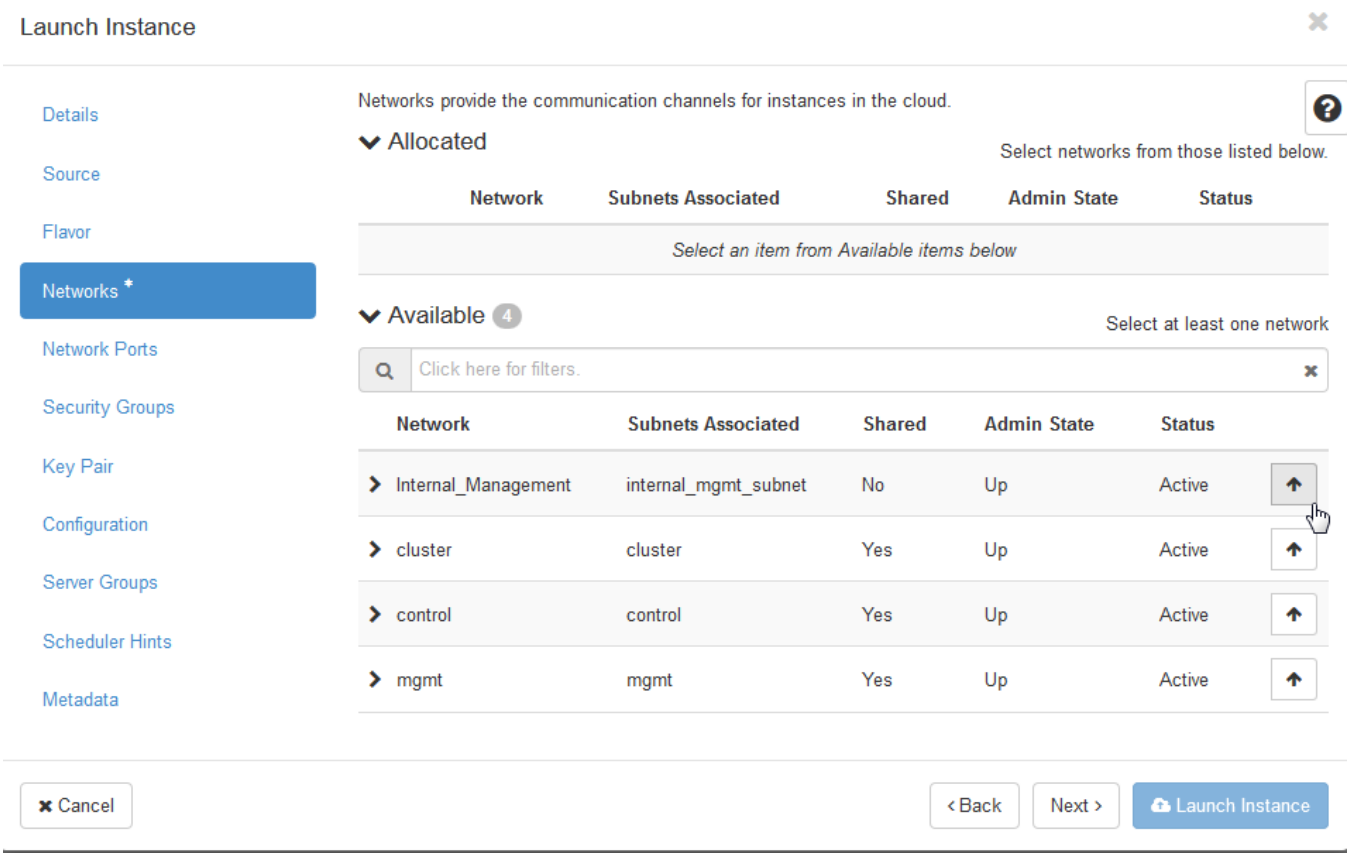


7. From the **Available** list, click **Move** to move the resource plan to the **Allocated** list.

8. Click **Next**.

   The **Networks** tab is displayed.

FIGURE 80 Networks Tab Page



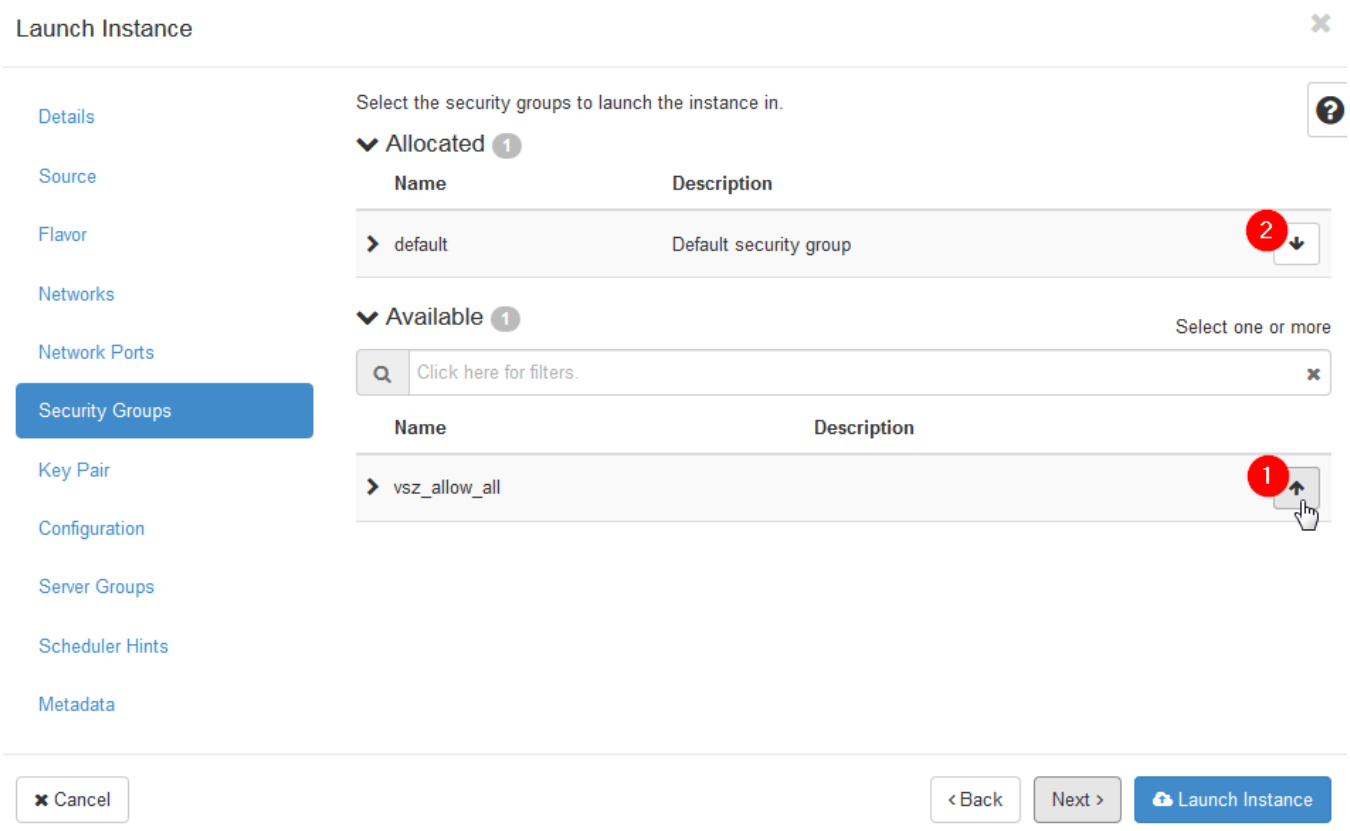
9. From the **Available** list, click **Move** to move the network interfaces to the **Allocated** list.
10. Click **Next**.

    The **Network Ports** tab is displayed.

11. Click **Next**.

    The **Security Groups** tab is displayed.

    FIGURE 81 Security Groups Tab Page



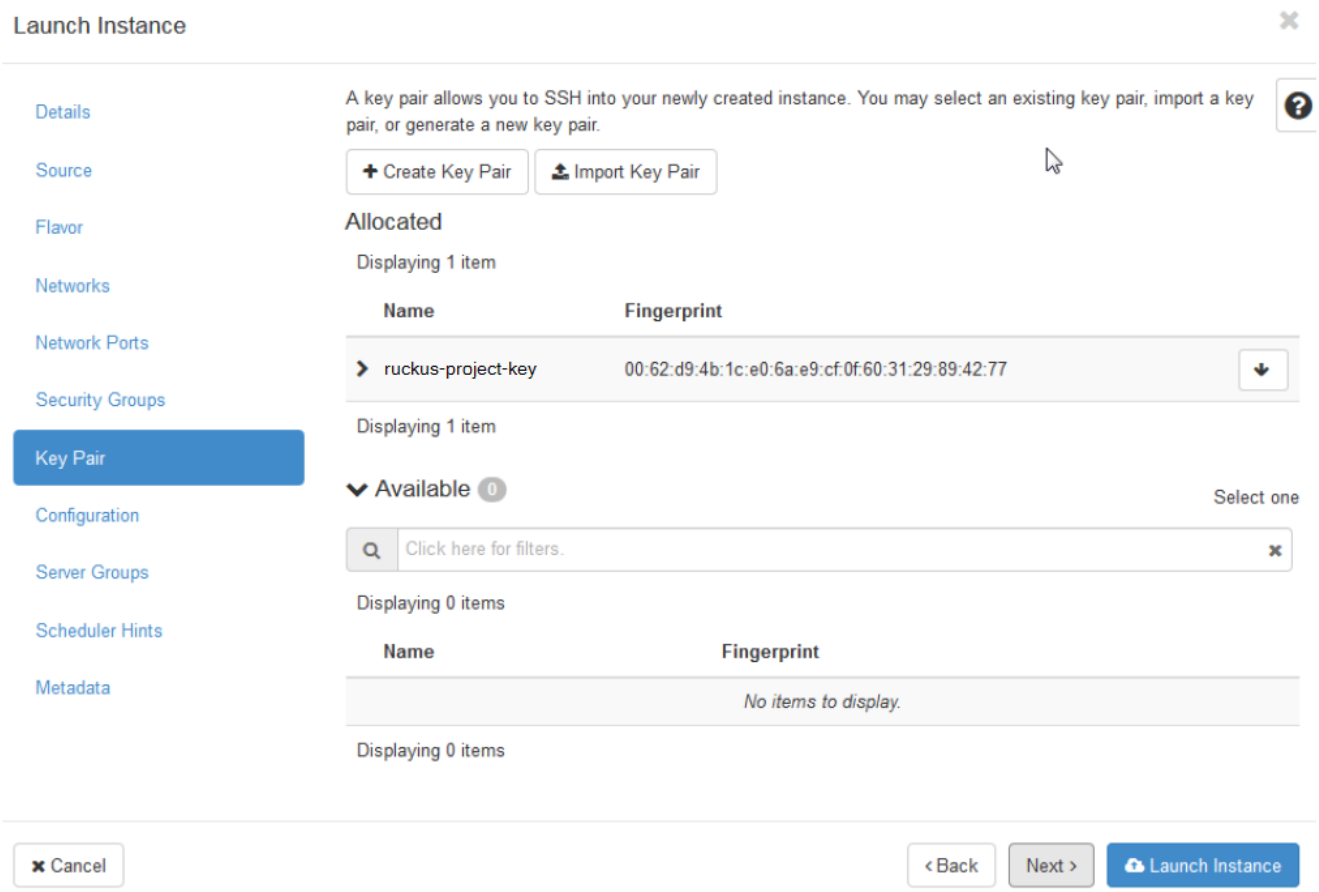
12. From the **Available** list, click **Move** to move the rule to the **Allocated** list.

13. From the **Allocated** list, click the **Remove** to delete the default rule.

14. Click **Next**.

    The **Key Pair** tab is displayed.

    FIGURE 82 Key Pair Tab Page

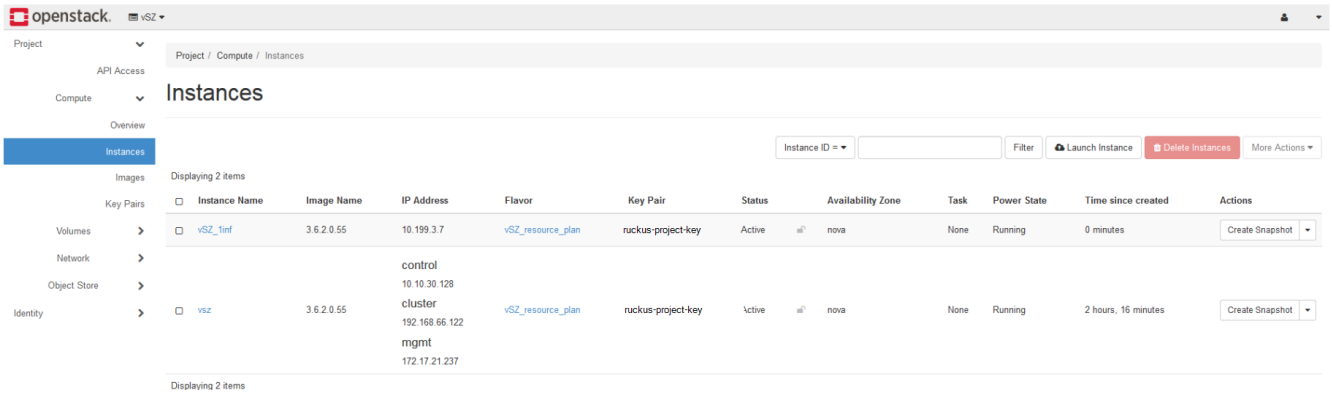


15. From the **Available** list, click **Move** to move the key pair to the **Allocated** list. If there is only one key pair, the system will automatically move it to the **Allocated** list.

16. Click **Launch Instance** to configure.

    The system will take a few minutes to complete the process. Once it is done, you can see the **Power State** change to **Running**.

    FIGURE 83 Instances Page

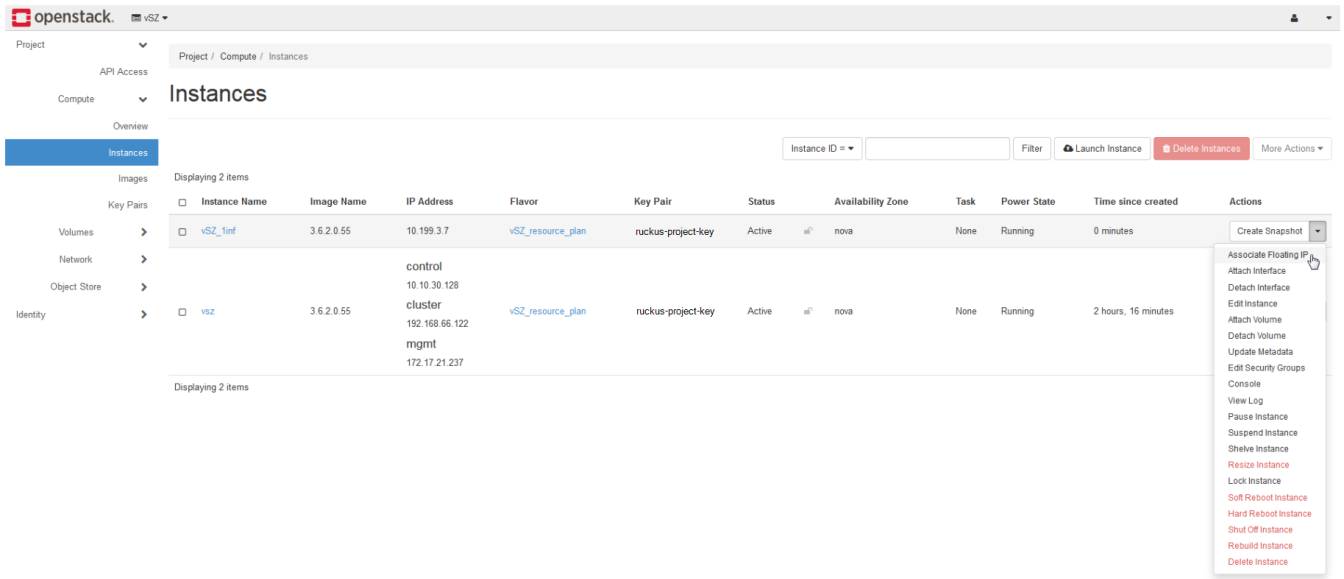


Associating Floating IPs

1. From the homepage, click **Project** > **Compute** > **Instances**.

   The **Instances** page is displayed.

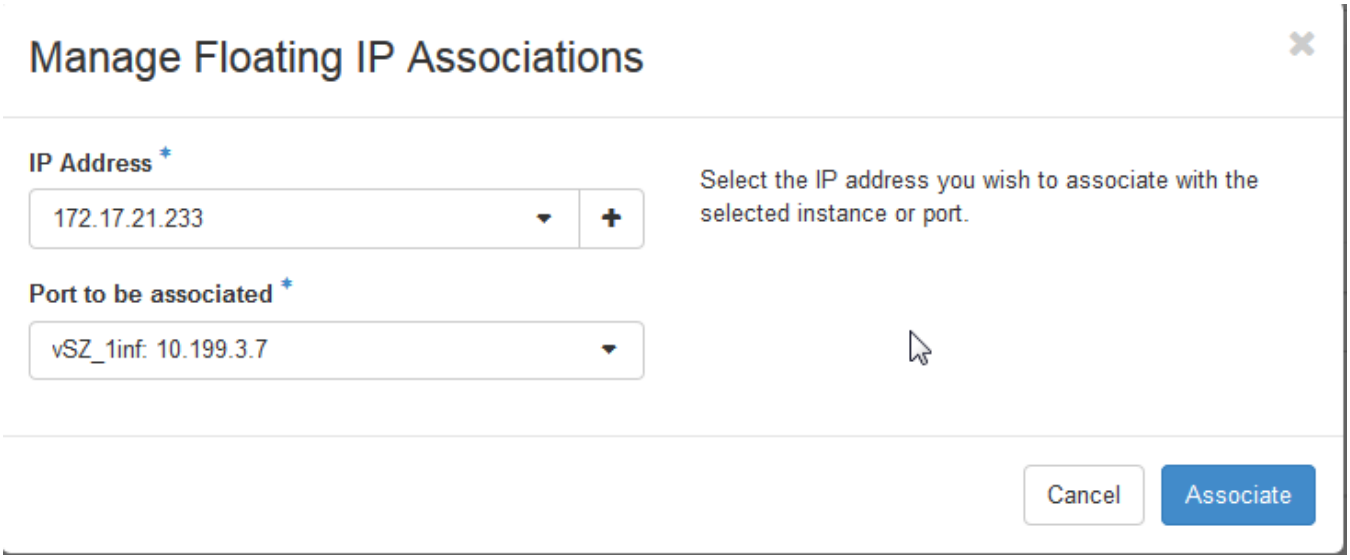
   FIGURE 84 Associating Floating IP



2. Select the drop-down by the vSZ that you want to associate the floating IP and select **Associate Floating IP**.

   The **Manage Floating IP Associations** page is displayed.

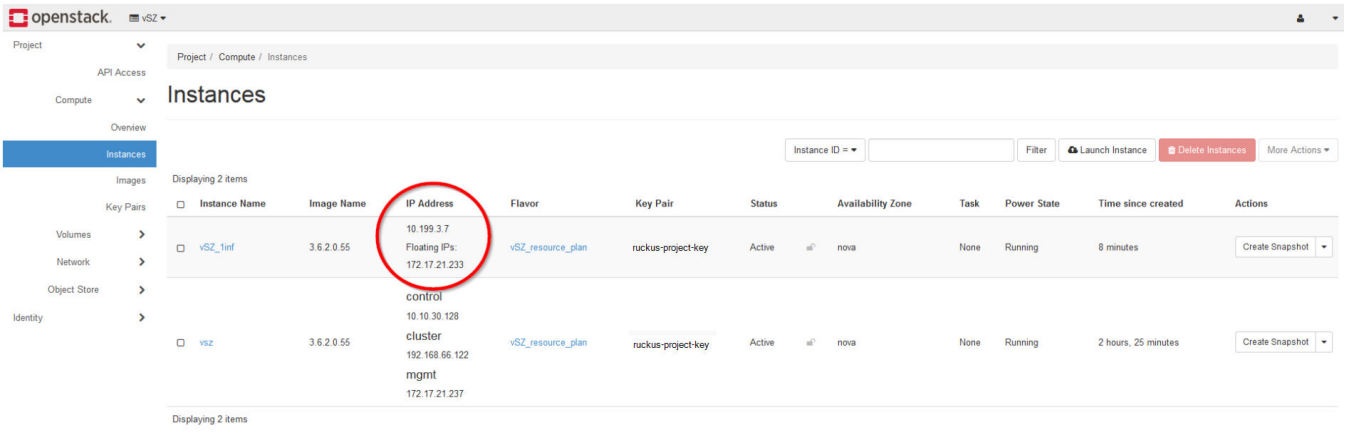
   FIGURE 85 Manage Floating IP Associations



3. From **IP Address**, select the floating IP that was reserved.
4. Click **Associate**.

   The system will take few seconds to associate the IP to the instance.

   FIGURE 86 Associated Floating IP



Setting up a vSZ Cluster

To setup a vSZ Cluster:

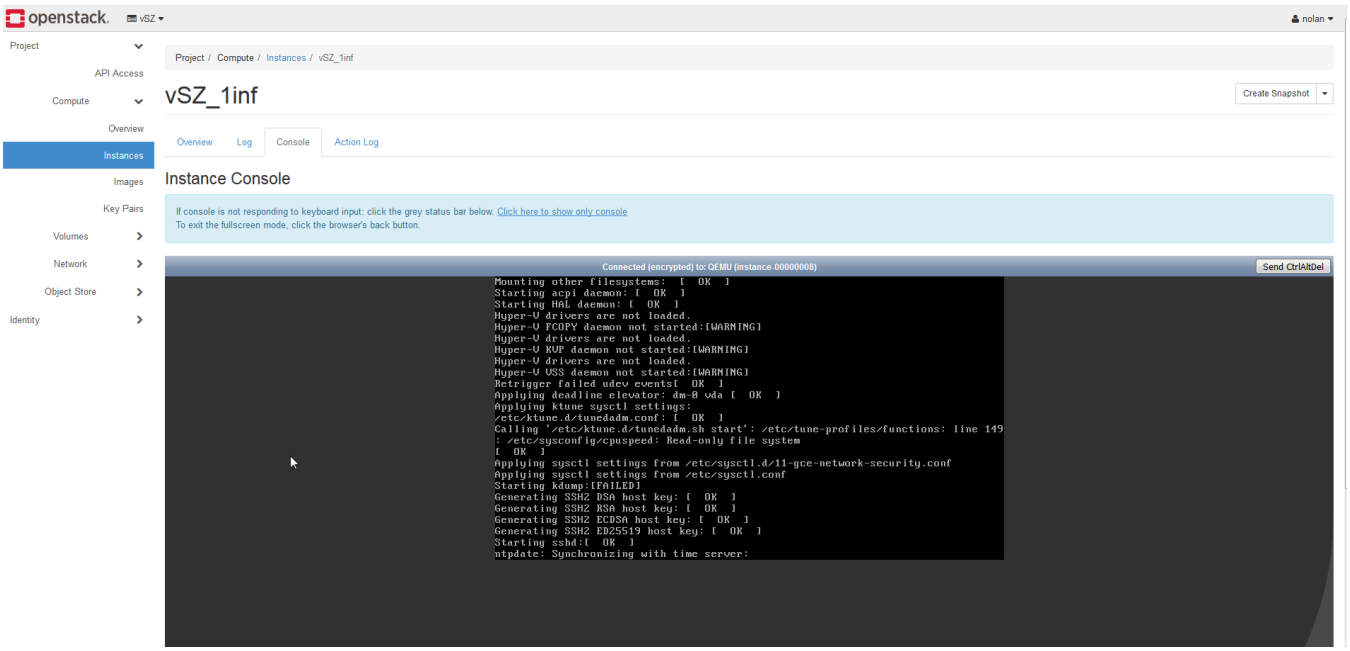
1. From the homepage, click **Project** > **Compute** > **Instances**.

   The **Instances** page is displayed.

2. Click the **Console** tab.

   The Console page is displayed.

   FIGURE 87 Console Tab Page



3. Follow the vSZ setup as explained in Using the Setup Wizard to Install vSZ on page 201.

   NOTE
   Always use DHCP in the vSZ system to avoid network issues.

Linux PC uses the private key to connect to the vSZ console.

```
ssh -i test.pem admin@192.168.66.203
The authenticity of host '192.168.66.203 (192.168.66.203)' can't be established.
ECDSA key fingerprint is SHA256:B7d9OMnrTEU6xD90pGuZ4qHWDZpqGJNQ61xt7citmkU.
ECDSA key fingerprint is MD5:85:c2:44:34:52:af:83:e1:8f:6f:af:46:6f:a8:20:97.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.66.203' (ECDSA) to the list of known hosts.
################################
#       Welcome to vSZ         #
################################
admin@192.168.66.203's password:
```

Installing the vSZ on a Nutanix Hypervisor

Hardware Requirements for Nutanix Hypervisor

NOTE
vSZ deployment on Nutanix needs more memory allocation for vSZ usage. For 10,000 AP per node either setup 24 Core CPU and 50 GB (+2GB) memory to control or lower down the AP deployment number by 25% in vSZ resource level. For example, 7500 AP in 10000 AP resource level.

TABLE 12

Component	Recommendation
CPUs	Intel CPUs with VT-x support
System Memory	16 GB minimum One Controller VM per node with optional deduplication/Compression features and additional memory for one or more user VMs.
Network Interface Card (NIC)	Intel-based NIC
Host bus adapter (HBA)	Community-Edition supports Advanced Host Control Interface (AHCI) SATA or LSI controller with: • IT mode (Nutanix testing shows better performance than IR) • IR mode with pass-through • IR mode with RAID-0
Storage Devices, All Drivers	Maximum number of SSD or HDD per node is 4
Storage Devices, cold Tier	500 GB or greater available

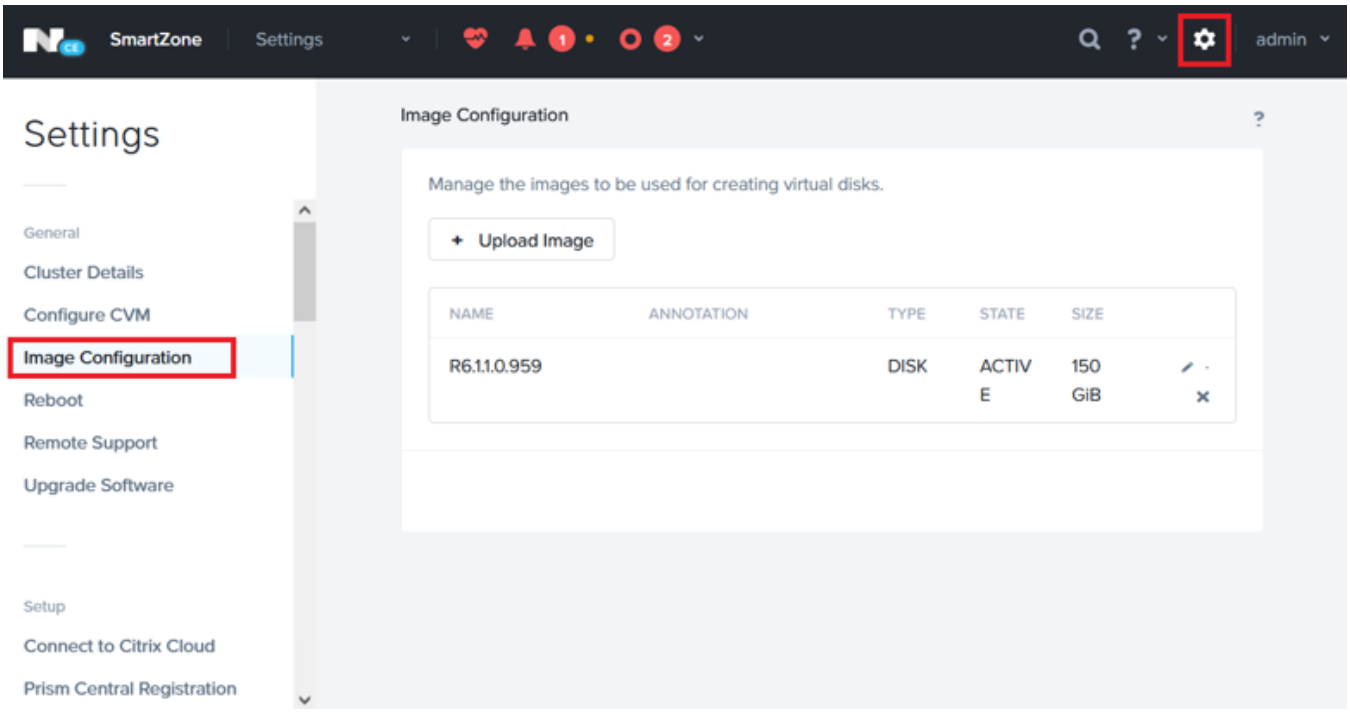
Load the vSZ Image on the Nutanix Hypervisor

1. Login the Hypervisor CVM.

   The homepage is displayed.

2. From the upper-right corner of the page, click **Settings** and select **Image Configuration** as shown in the following image.

FIGURE 88 Image Configuration



The **Image Configuration** window is displayed.

3. Click **Upload Image**. and add the vSZ image in *QCOW2* format.

For example, `vscg-6.1.1.0.959.qcow2`.

4. The default image size is 150 GB. If the image size is more than the default size, the file must be resized in the other Linux base and then uploaded.

- To resize the image file:

```
qemu-img resize <image file name>.qcow2 +500G
```

- To check the resized image:

```
qemu-img info <resized image file name>.qcow2
```

The **Create Image** window is displayed.

5. Enter the following information to add the vSZ image in *QCOW2* format:

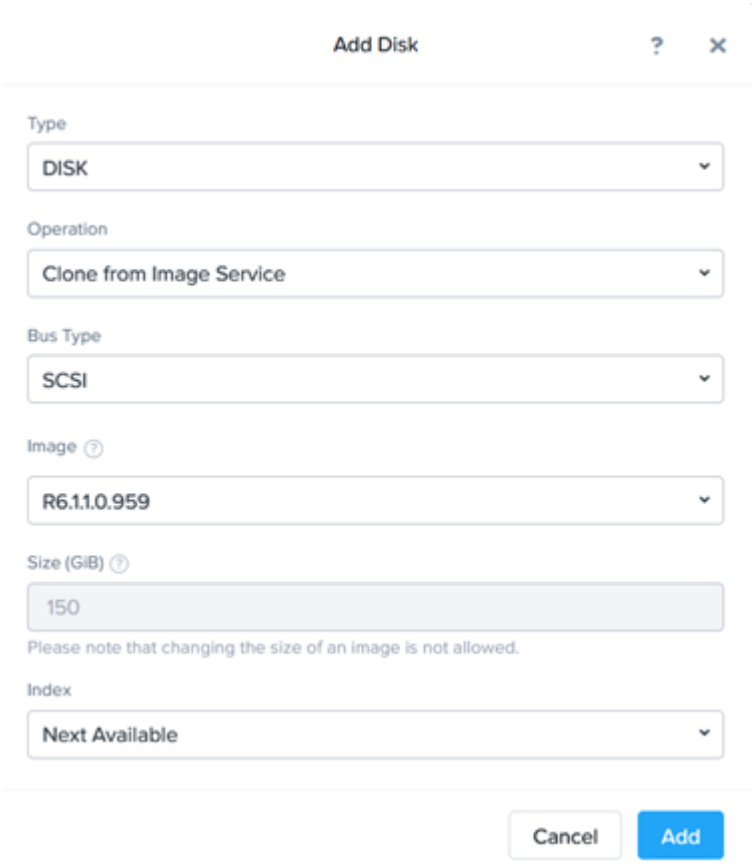
- Name
- Annotation
- Image Type
- Storage Container
- Image Source

6. Click **Save**.

Create the vSZ Image on the Nutanix Hypervisor

1. From the upper-left side of the screen, click **Home** and select **VM**.
2. On the upper-right of the screen, click **Create VM**. The **Create VM** window is displayed.
3. From the **Create VM** screen, scroll down to **Disks** area and remove CD-ROM.
4. Click **Add New Disk**, the **Add Disk** form appears.
5. From the **Operation** drop-down, select **Clone from Image Service** and click **Add** as shown in the following image.

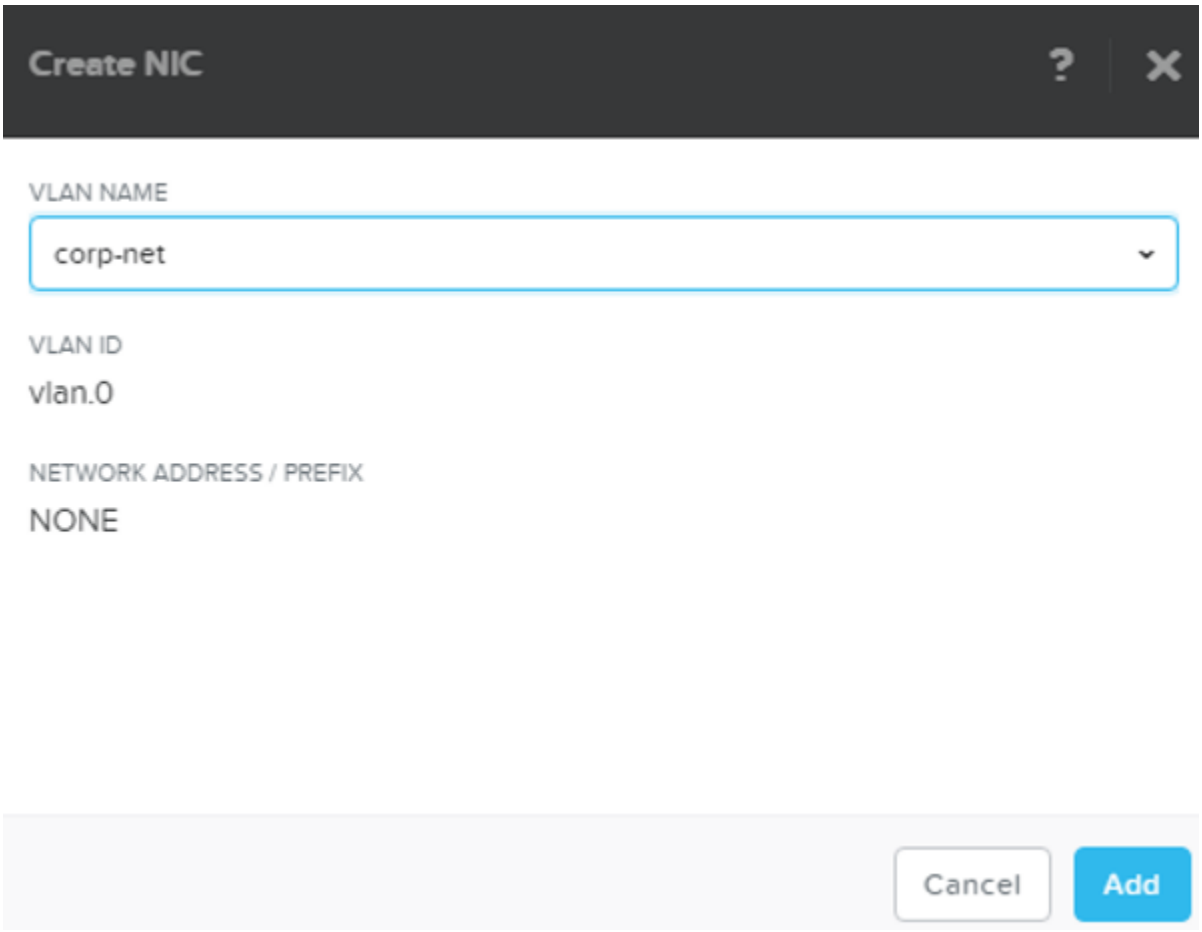
FIGURE 89 Adding First Disk



6. Click **Add**.
7. Scroll down to the **Network Adapters (NIC)** area.

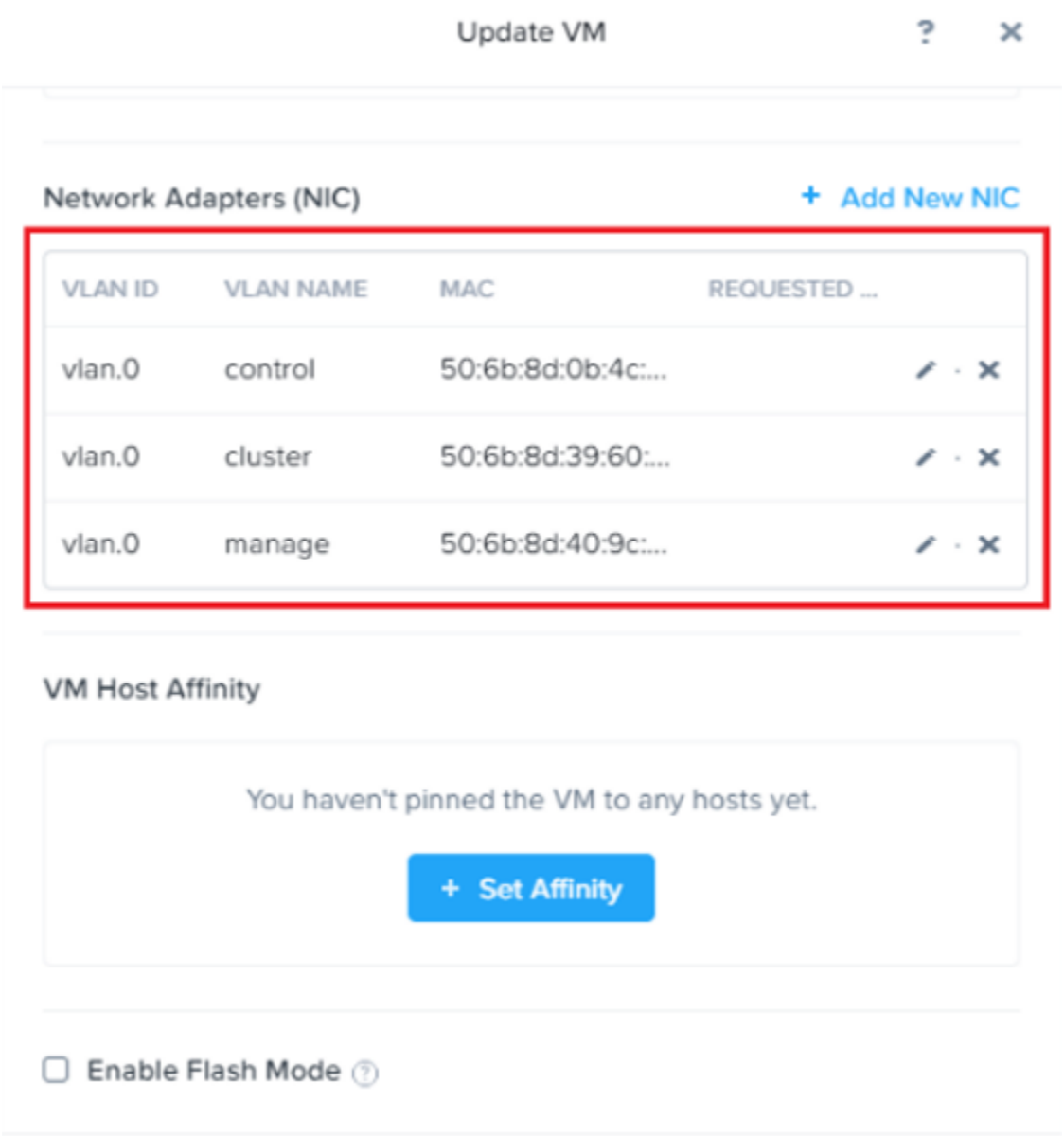
8. Select the **VLAN Name** from the drop-down and click **Add** as shown in the following image.

FIGURE 90 Creating NIC



9. In vSZ-H, create the three interfaces as follows:
   - First interface: Control Interface
   - Second interface: Cluster Interface
   - Third interface: Management Interface

FIGURE 91 Creating vSZ-H Interfaces

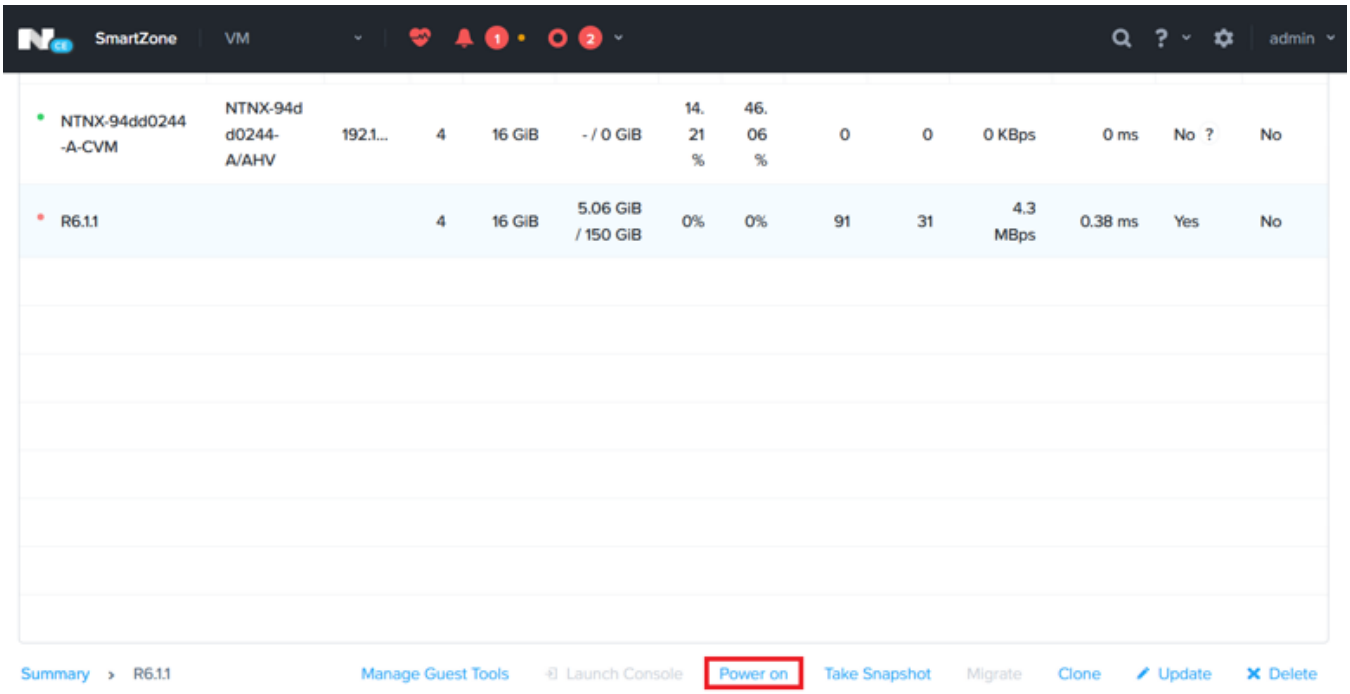


10. Click **Save**.

Power-on the vSZ Virtual Machine

From the **VM** screen, select the newly created vSZ VM and click **Power on** as shown in the following image.

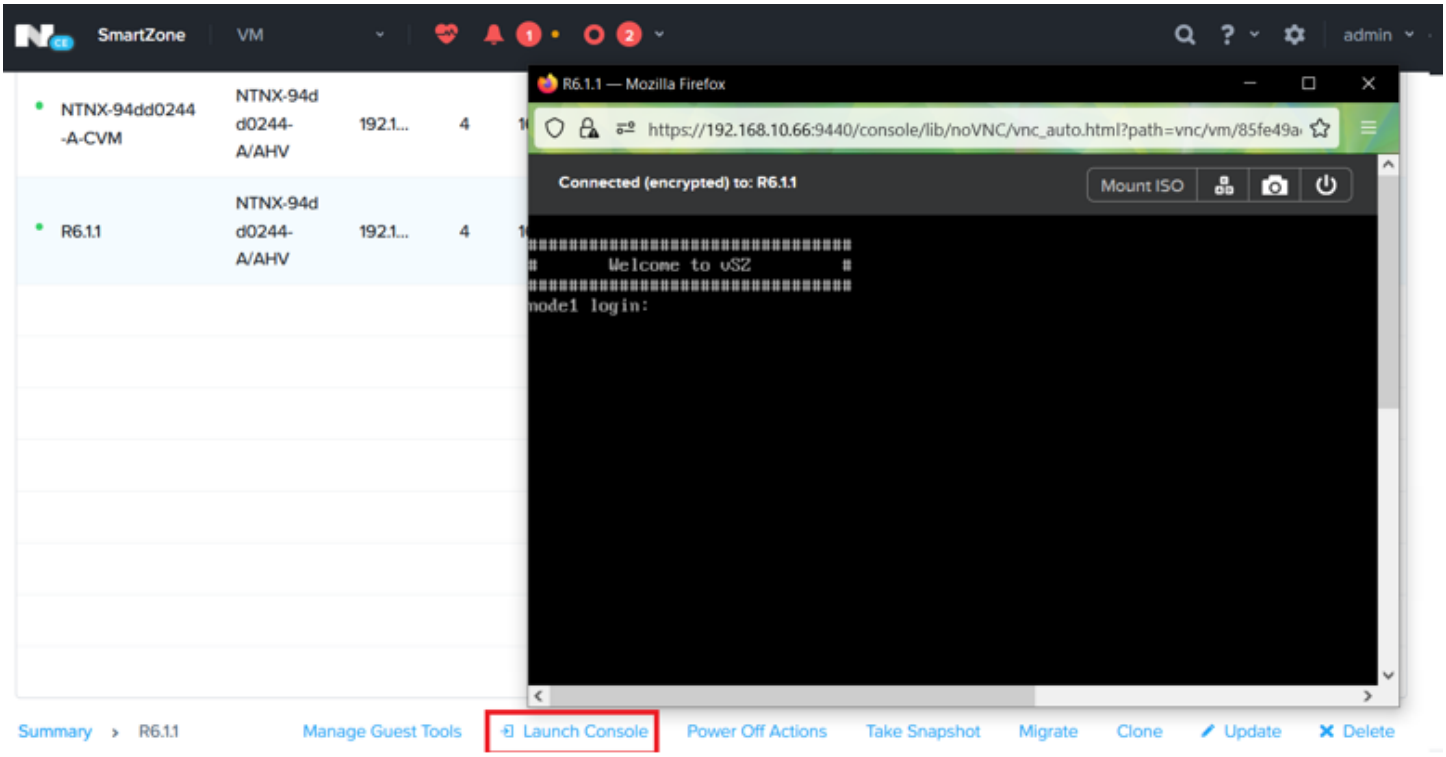
FIGURE 92 Power-on the vSZ



Launch the Console

When the vSZ virtual machine is up and running, click **Launch Console**, the console is displayed as shown in the following image.

FIGURE 93 VM Console



Installing the vSZ on Microsoft Azure

Introduction

You can install vSZ on Microsoft Azure using the procedure outlined.

> **NOTE**
> The minimum memory and CPU requirements have changed in this release. You may need to upgrade your infrastructure before upgrading. Please read carefully. This is the minimum requirement recommended. Refer to the tables in Virtual SmartZone Minimum Requirements on page 14 in the Installation Preparation chapter.

Public cloud solution resource requirement

- CPU or Memory: Minimum requirement of D series and above.

  > **NOTE**
  > Does not support A and B series

- Storage Requirement (Disk Storage): Minimum requirement of SSD 150 GB above.

  > **NOTE**
  > Any CPU with credit limitation type cannot support. For example AWS T2 instance or Azure B-series.
  > Select the proper disk size to run vSZ since disk sizes may have different disk IO performance in each cloud platform.

Logging into Microsoft Azure

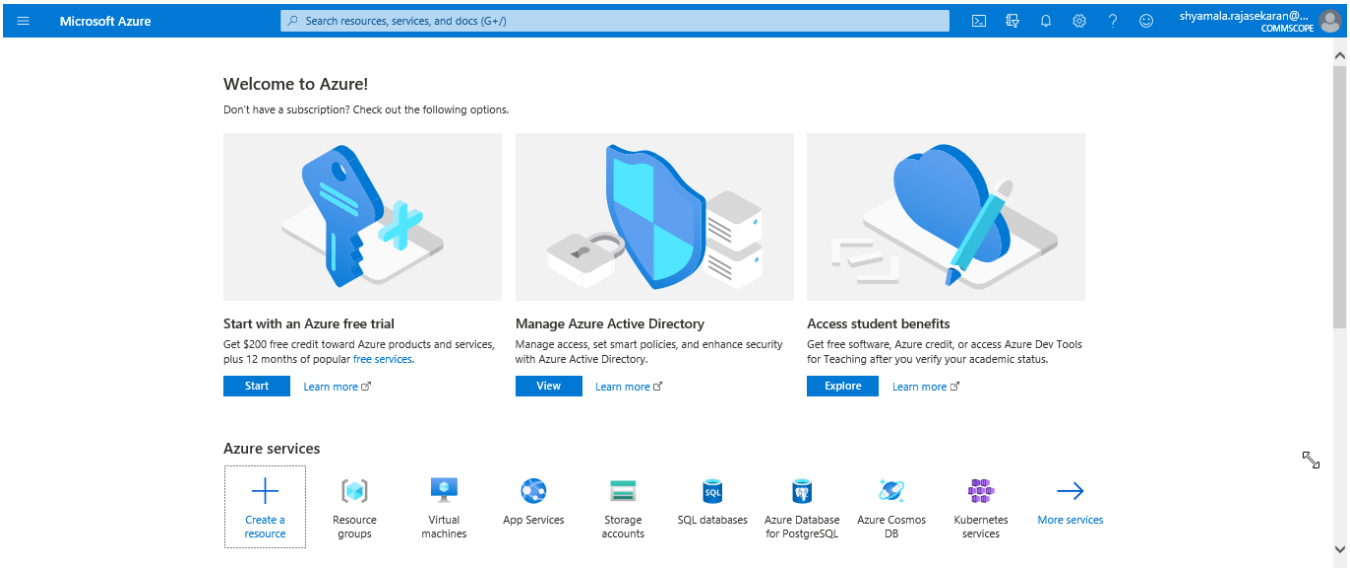
As the first step of installing vSZ on Microsoft Azure, you have to log into Microsoft Azure.

1. Click https://portal.azure.com to access the **Microsoft Azure** site.

2. Enter your login credentials.

   The Azure portal appears as shown in the following image.

FIGURE 94 Portal Tab

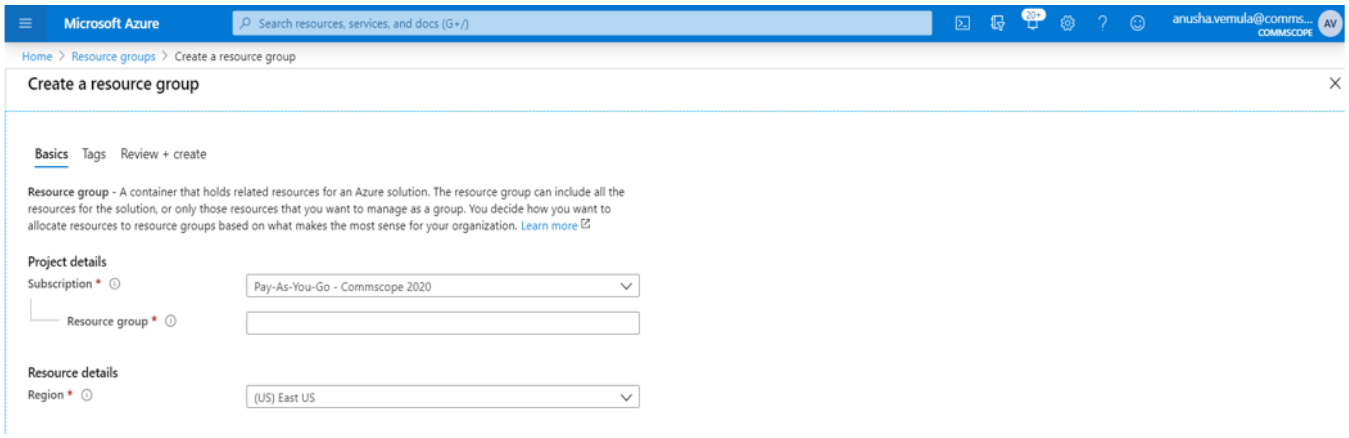


Creating a Resource Group

To create a resource group:

1. From **Azure services** section, click **Resource groups**. The **Resource groups** page is displayed.
2. Click **Add**, the **Create a resource group** is displayed as shown in the following image.

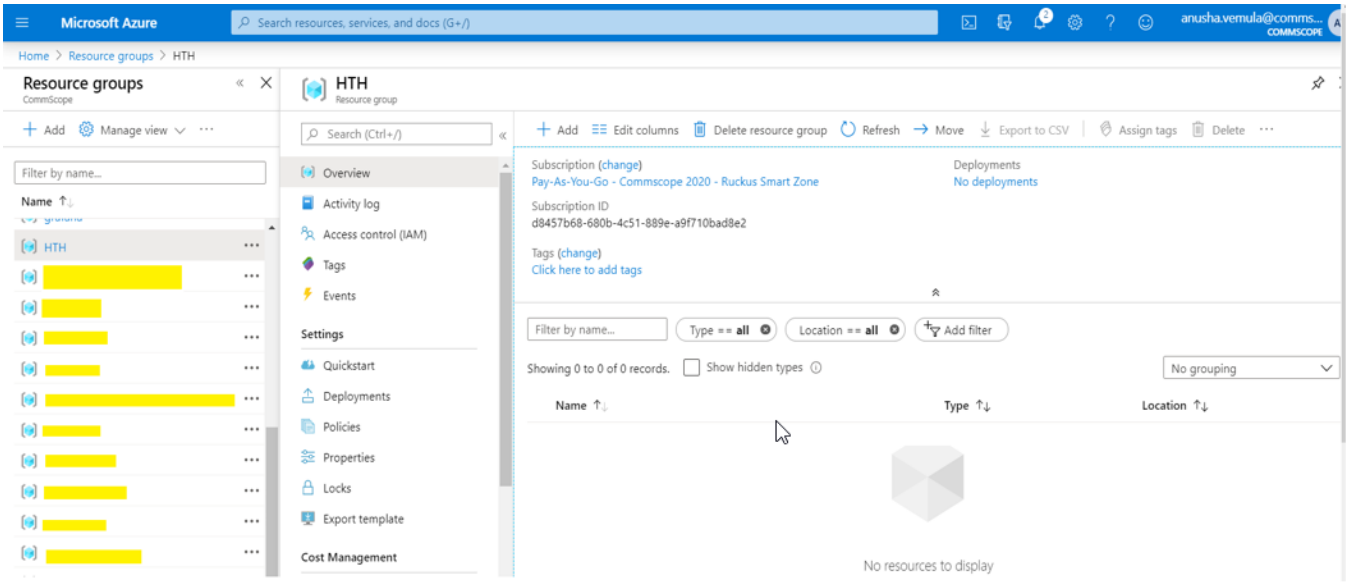
FIGURE 95 Creating a Resource Group



3. Update the following information:
   - Subscription: Select **Pay-As-You-Go**
   - Resource group: Enter a name for the resource group
   - Region: Select a region
4. Click **Create**.

   The new resource group is created.
5. Select the resource group to view its related components.

FIGURE 96 Resource Group Components

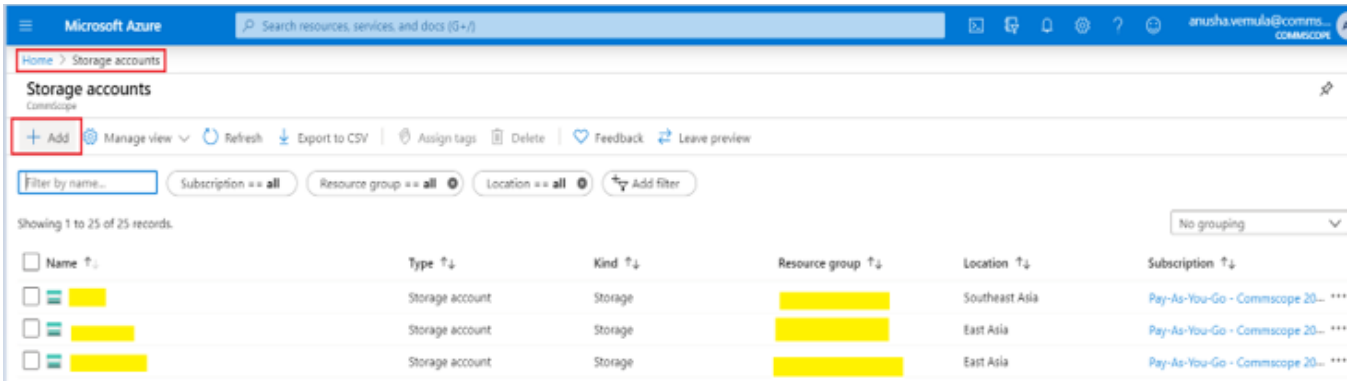


Creating a Storage Account and Container

To create a Microsoft Azure storage account, perform the steps outlined in this section.

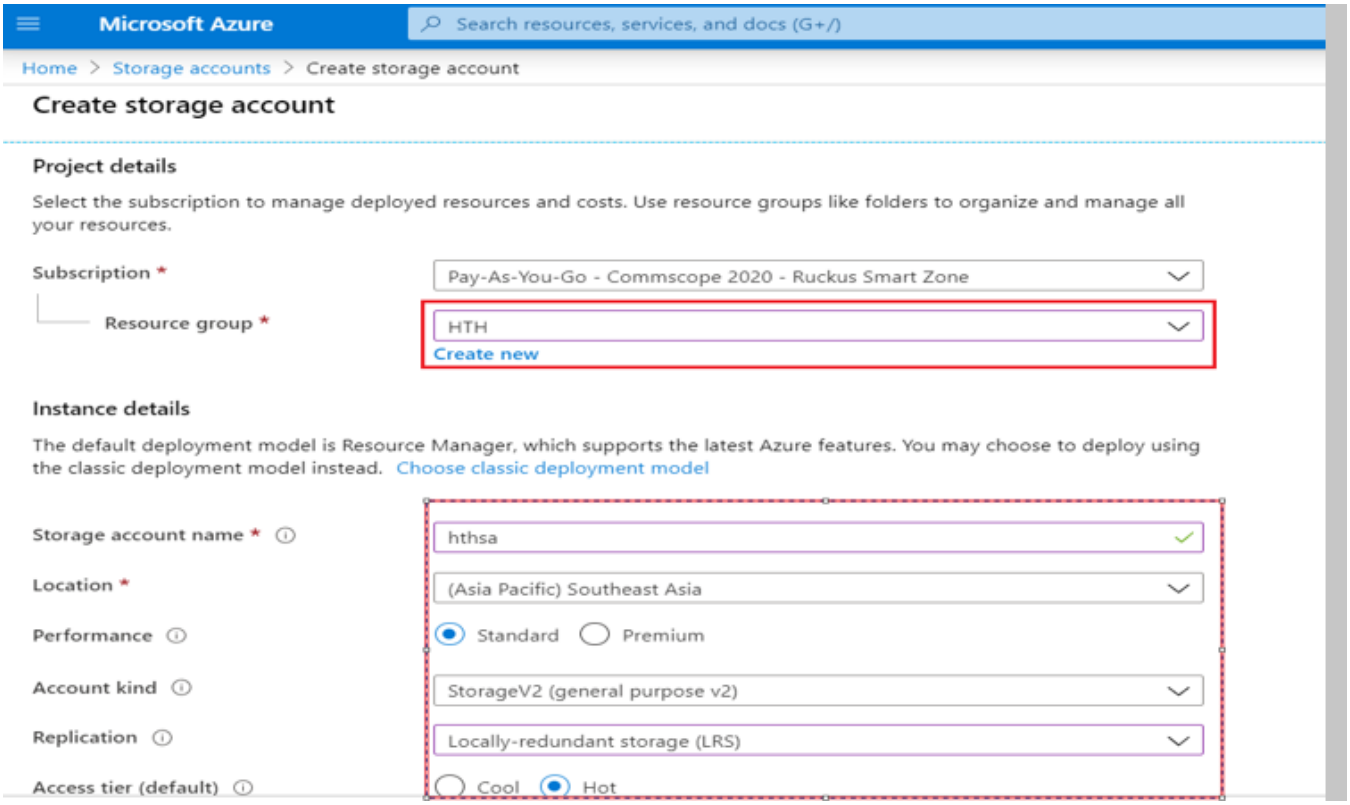
1. From the **Azure services** section, click **Storage accounts**. The **Storage accounts** screen is displayed.

   FIGURE 97 Storage account



2. Click **Add** and enter a **Name** for the storage account. The **Create Storage account** page is displayed.

   FIGURE 98 Storage Account



3. Update the following:
   - **Resource group**: Select the resource group created in the procedure.
   - **Account kind**: Select Storage v2
   - **Replication**: Select LRS

     NOTE
     All other configurations can be left default or be configured as required.

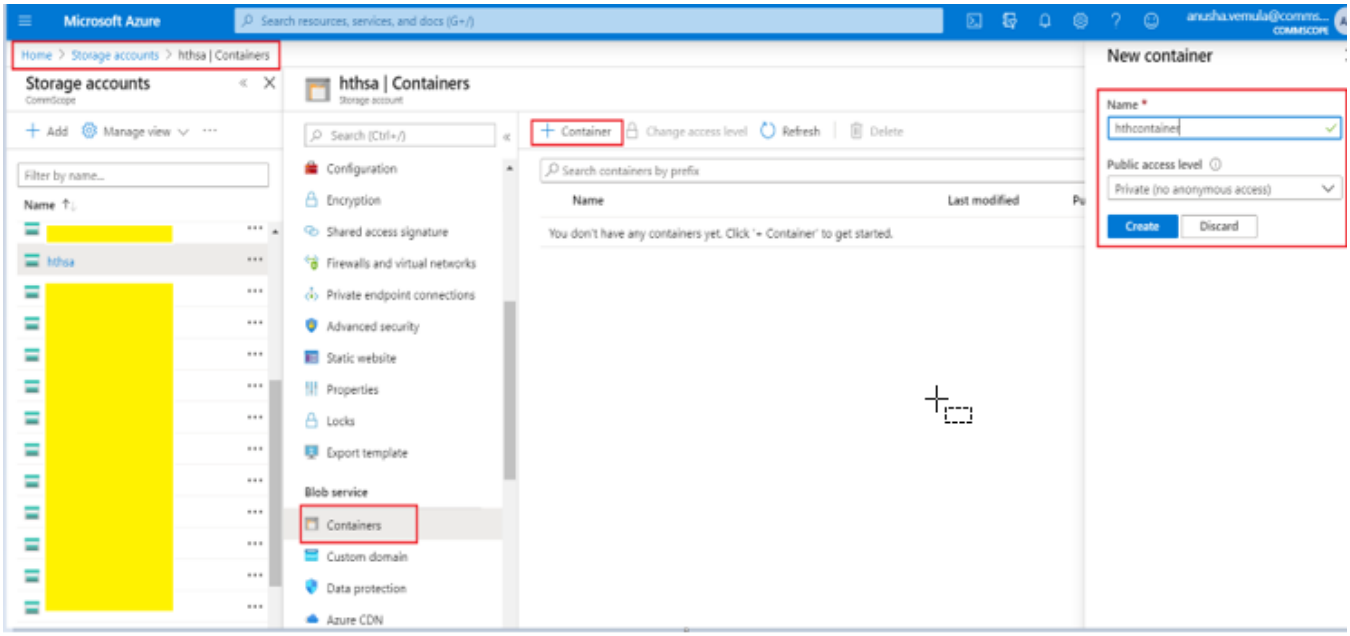
4. Click **Create**.

Creating a Container to Upload the vSZ Image to Microsoft Azure

A container must be created to upload the vSZ image to Microsoft Azure. Follow these steps outlined in this section to create a container and upload the vSZ image to Microsoft Azure.

1. Go to the storage account created in the previous procedure and select **Containers**.

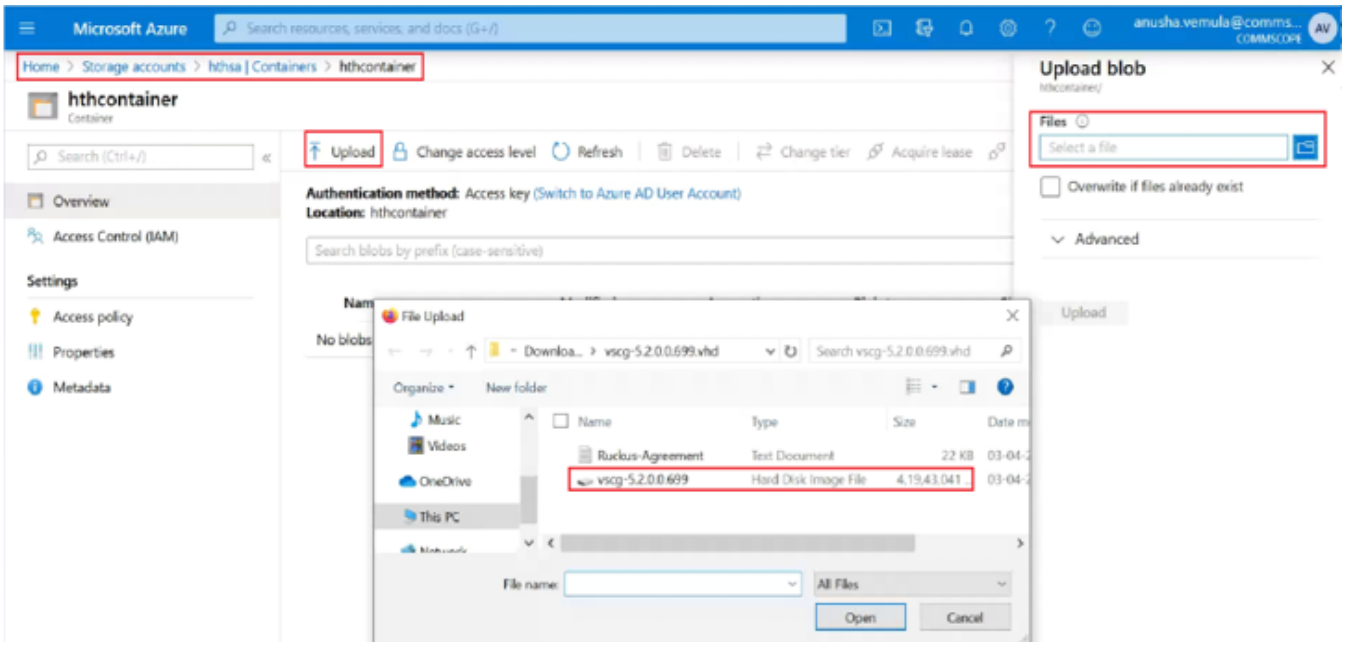
   FIGURE 99 Container creation



2. From the **Containers** page click **+ Container**.
3. In the **New Container** pane, enter a **Name** for the container and select **Public access level**.
4. Click **Create**, a new container is created.

5. Select the new container and click **Upload**.

FIGURE 100 Uploading the vSZ image file



6. Browse for the vSZ image file and click **Open**.

NOTE
Extract the software zip file downloaded from the support site and upload only the vhd image.

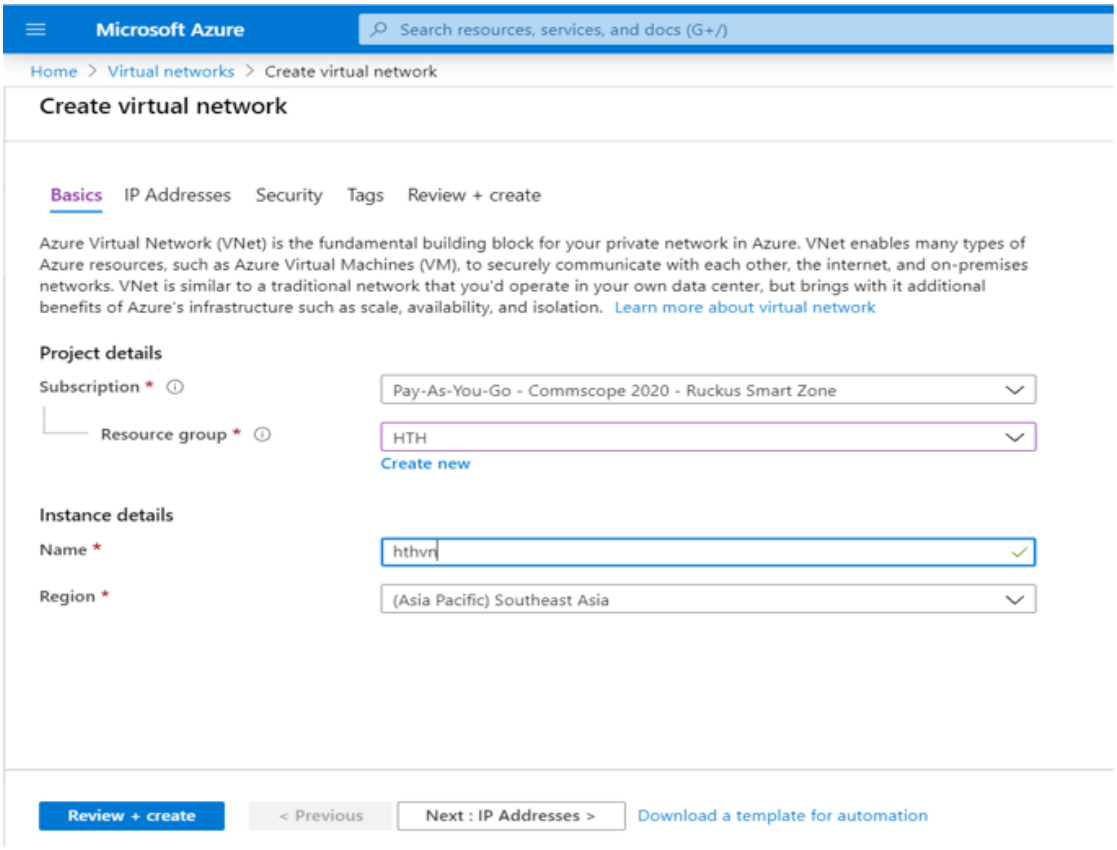
Creating a Virtual Network

Follow these steps to create a virtual network.

1. From the Azure services section, select **Virtual networks** and click **Add**.

   The **Create virtual network** page is displayed as shown in the following image.

   FIGURE 101 Creating a virtual network

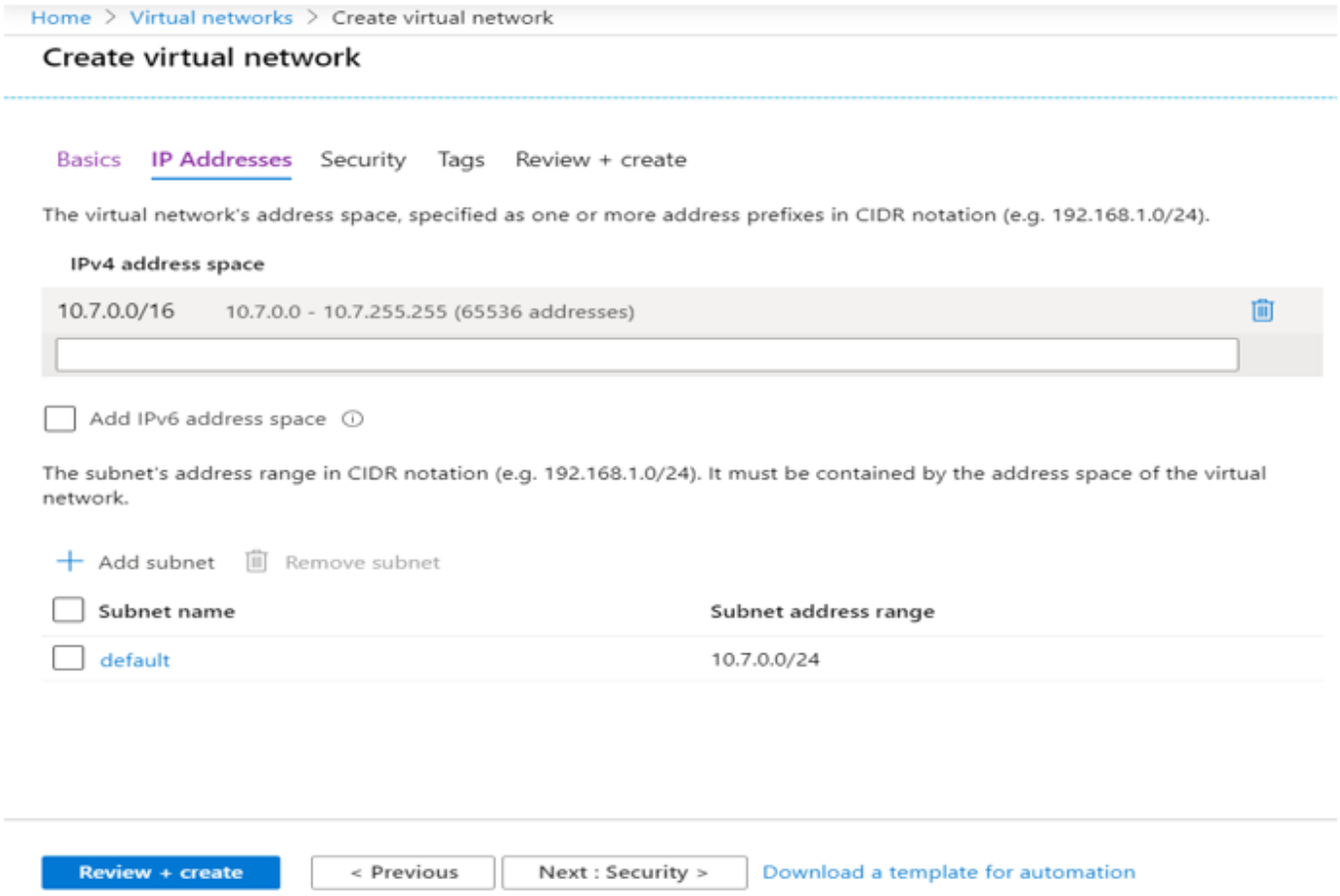


2. From the Basics tab, update the following:
   - **Resource group**: select the resource group created in the previous procedure.
   - **Name**: enter a name for the network.
   - **Region**: select a region.
3. Click **Next: IP Address**, the IP Addresses tab is displayed.

   A default IPv4 private address is displayed.

4. To create a new IPv4 address, enter the IP address in **IPv4 address space**.

   FIGURE 102 IPv4 Address



5. The **Security** and **Tags** tab can be updated or left to apply default settings.
6. Click **Review + create**.

Creating Network Security Groups

Network security group is the Azure firewall rule. You can have different firewall rules for each vSZ instance.

To create a network security group:

1. From the **Azure services** section, select **Network Security Groups** and click **Create**.

   The **Create Network Security Group** page is displayed.

2. In the **Basics** tab, udpate the following:

   - **Resource group**: select the resource group
   - **Name**: enter a name for the security group
   - **Region**: select a region to which it applies

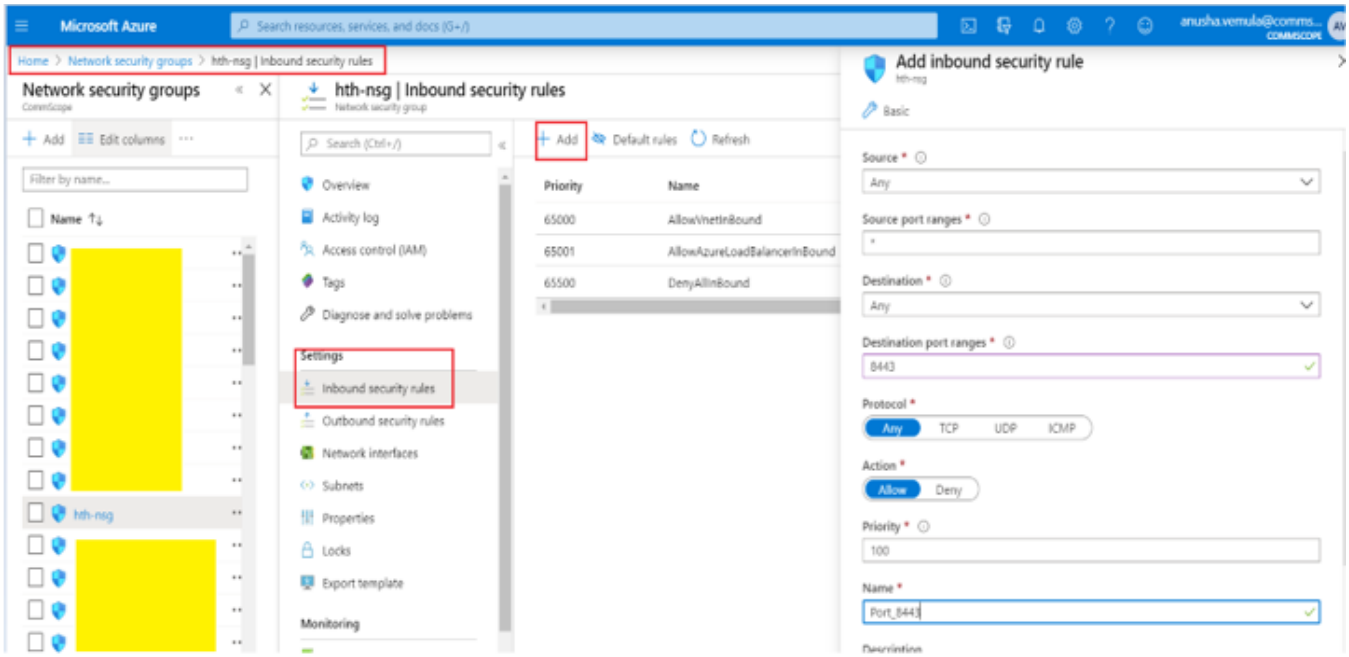
3. Click **Next: Tags** to update the tag settings or click **Review + Create** to apply the default settings.

   A new network security group is created.

4. Select the new security group and click **Settings** > **+ Add**.

   The Add inbound security rule page is displayed.

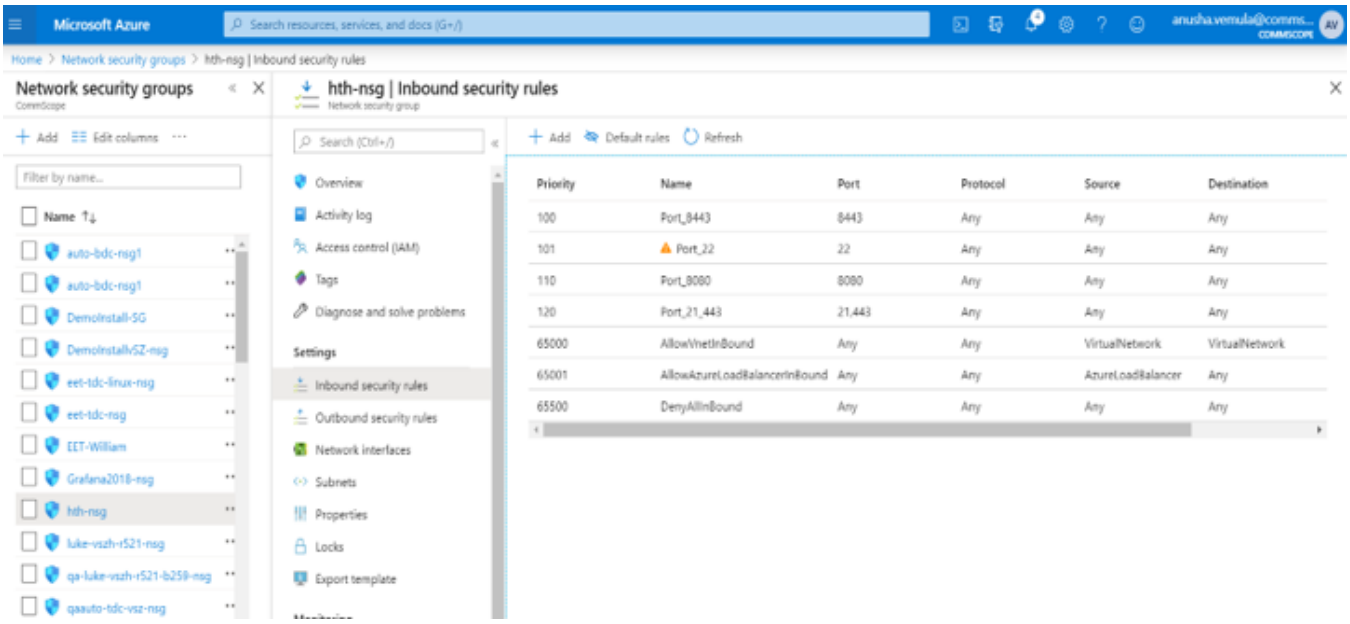
FIGURE 103 Network security groups



5. Update the following information:
   - **Source**: select the source port.
   - **Source port ranges**: enter the source port range.
   - **Destination**: select the destination port.
   - **Destination port ranges**: select the destination port ranges.
   - **Protocol**: select one of the options—Any, TCP or UDP.
   - **Action**: select Allow or Deny.
   - **Priority**: enter the rule priority number.
   - **Name**: enter a name for the rule.
   - **Description**: enter a short description about the rule.

6. Click **Add**, the new rule is added to the existing rule list as shown in the following image.

FIGURE 104 Inbound Security Rule List



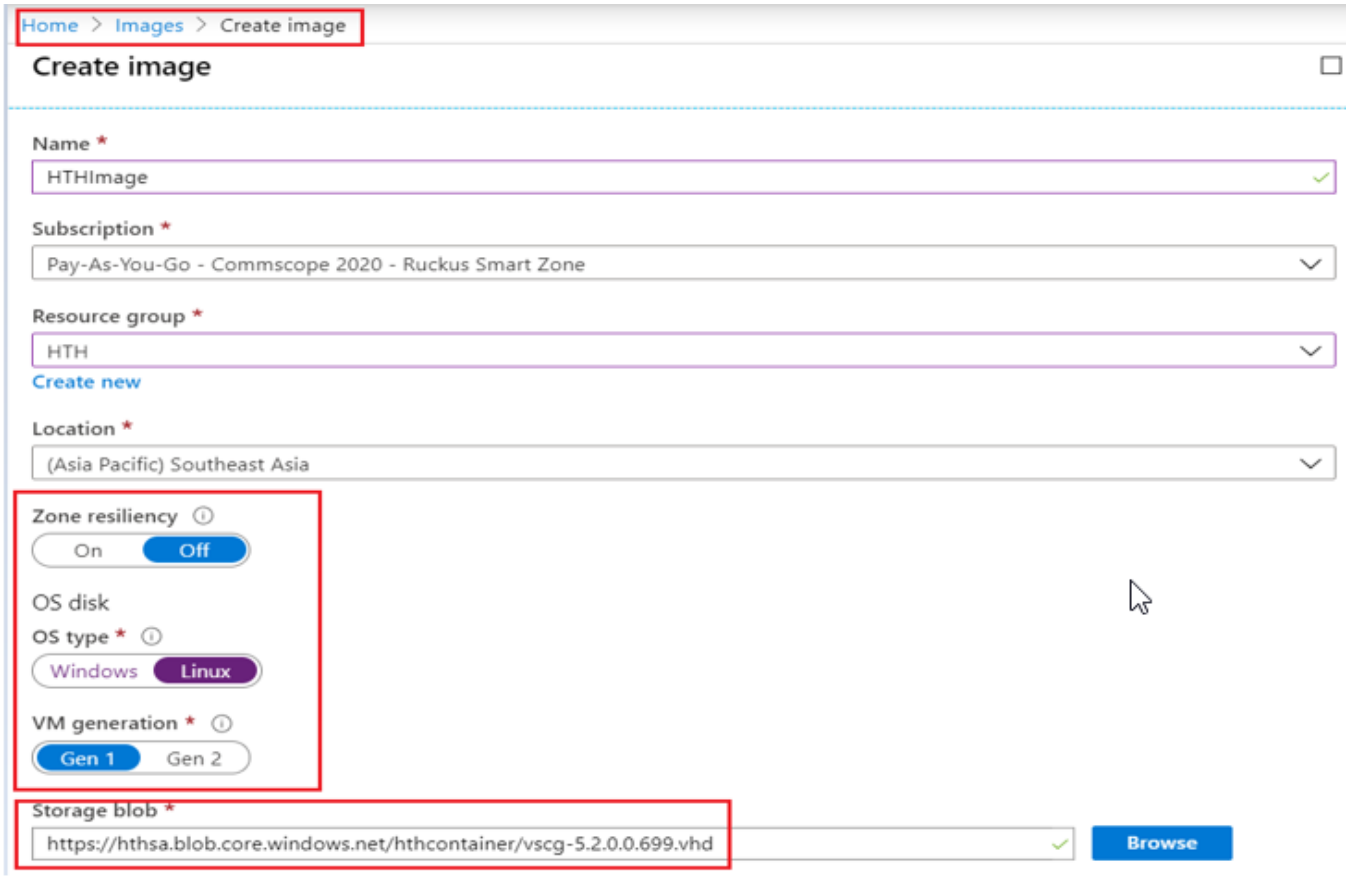
Creating a vSZ Image on Microsoft Azure

Follow these steps to create a vSZ image on Microsoft Azure:

1. From the **Azure Services** section, select **Images** and click **Create**.

   NOTE
   ssh is allowed by default, so add port 443 and 8443 for AP connection and Web access.

   FIGURE 105 Creating an image



2. Update the following fields:
   - Name: enter a name for the image
   - Resource group: select the resource group
   - Location: select the region
   - Zone resiliency: click **Off**
   - OS type: select **Linux**
   - VM generation: select **Gen 1**
   - Storage blob: click **Browse** and select the vhd image that was uploaded in the earlier procedure.
3. Click **Create**.

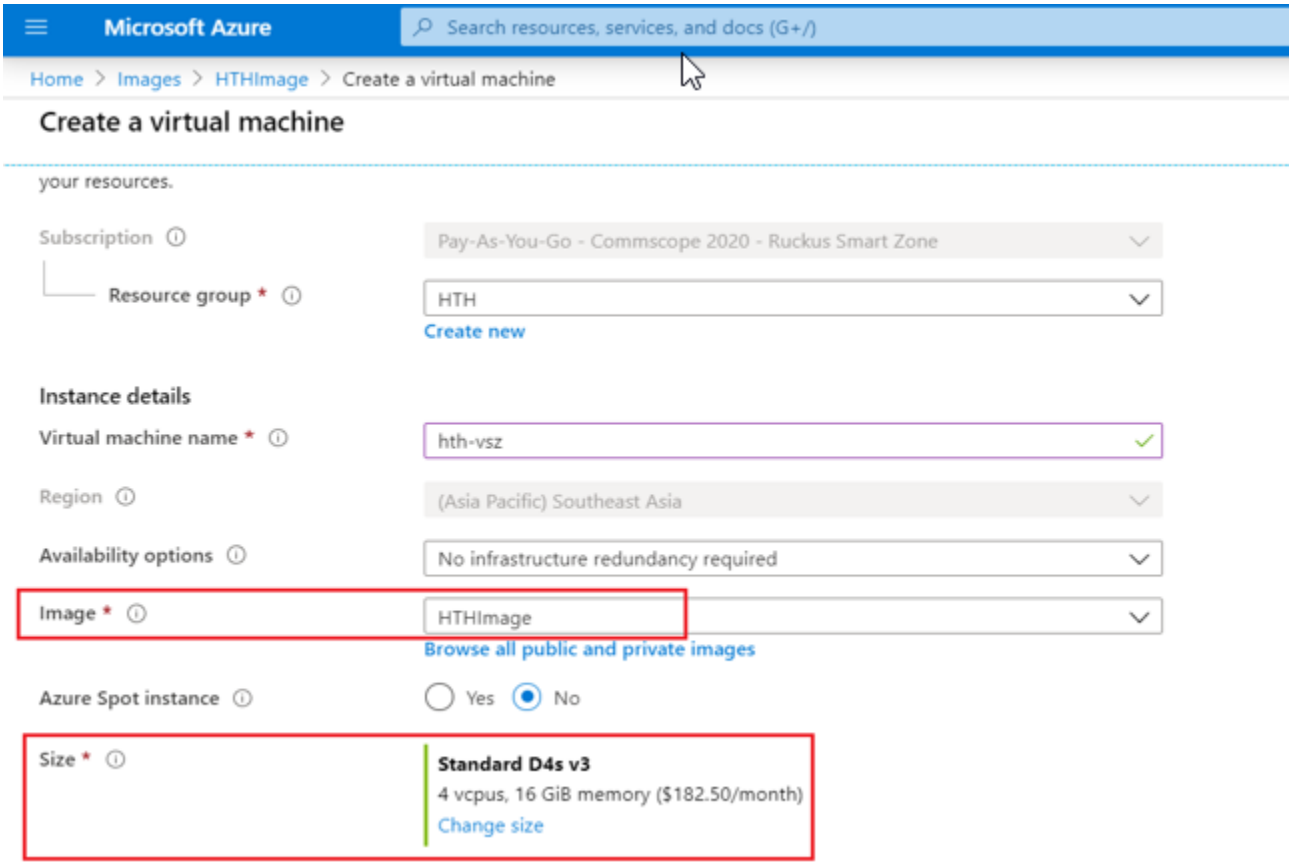
Creating a vSZ Virtual Machine

Follow these steps to create a vSZ virtual machine.

1. Select the image created in the previous procedure and click Create VM.

   The **Create a virtual manager** page is displayed.

   FIGURE 106 Basics tab



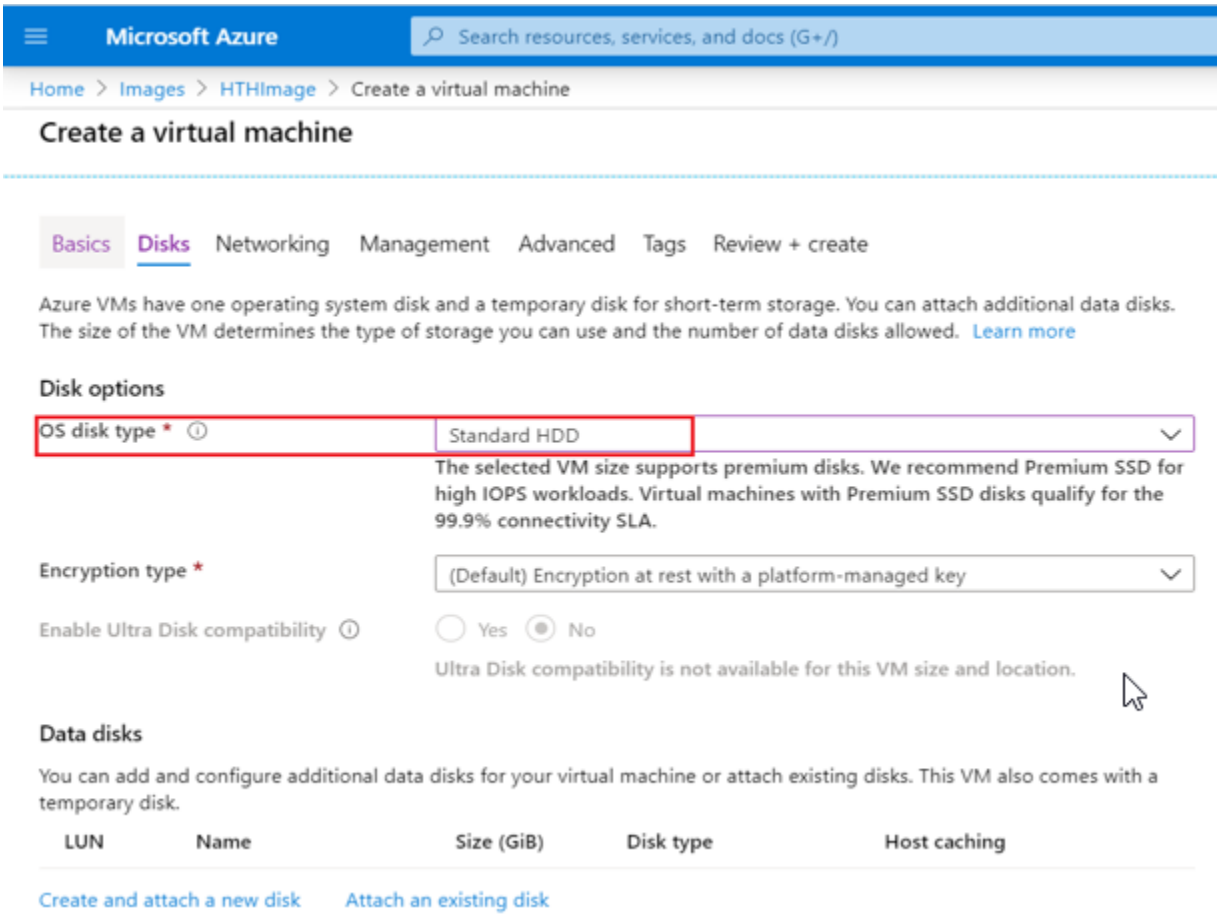
2. Update the following fields:

   - **Resource group**: select an option.
   - **Virtual machine name**: enter a name.
   - **Size**: select **D4s v3** for assigning 4 vCPUs and 16 GB memory to the vSZ.
   - **Authentication type**: select **Password**.
   - **Select inbound ports**: select all the inbound ports available. Network security group created in the previous procedure can be selected fromt the **Networking** options.

3. Click **Next Disks**.

   The **Disks** tab page is displayed.

   FIGURE 107 Disks tab

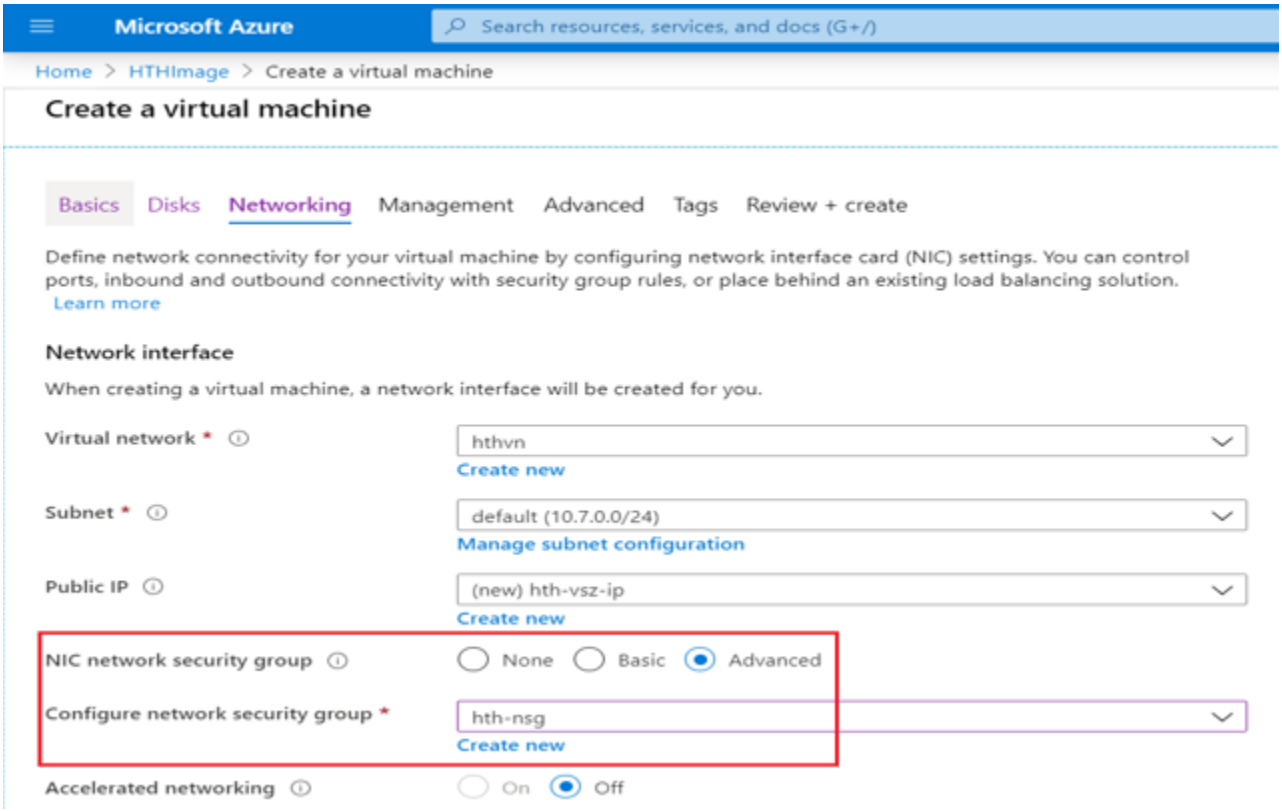


4. From **OS disk type**, select **Standard HDD**.

5. Click **Next: Networking**.

   The **Networking** tab page is displayed.

   FIGURE 108 Networking tab



6. Update the following:
   - **Virtual network**: select the virtual network created in the earlier network.
   - **Subnet**: select a subnet.
   - **NIC network security group**: select the **Advanced** option.

   Default configuration will apply to **Management**, **Advanced**, and **Tags** tab.
7. Click **Review + Create** to review the configuration.
8. Click **Create**.

Updating the Disk Size According to Resource Plan

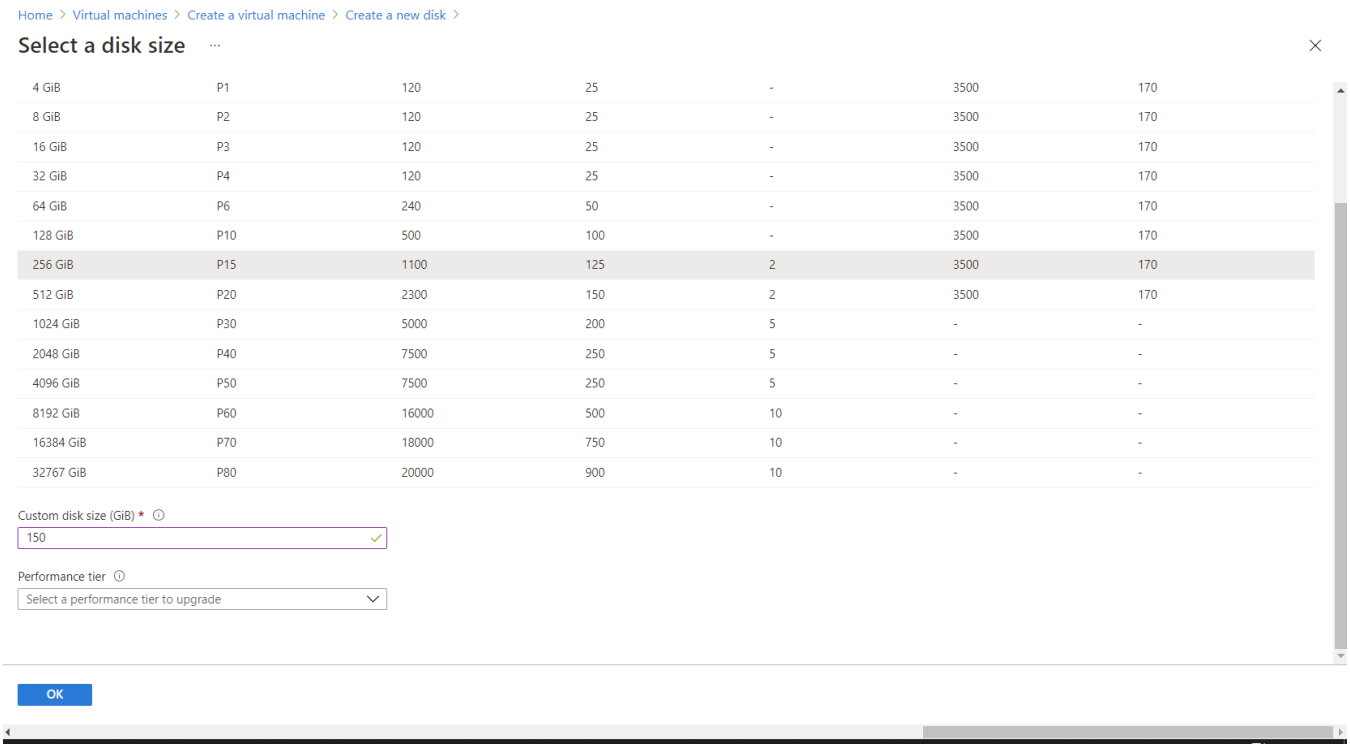
Follow these steps to update the disk size according to the resource plan:

1. From the **Virtual machines** page, select the virtual machine and click **Stop**.
2. From the **Settings** area on the left pane, select **Disks** and click **Add data disk**.

3. Go to **Data disks** > **Name** > **Create disk** for creating customised disk.

   The **Create managed disk** page is displayed.

   FIGURE 109 Creating Managed Disks



4. In **Custom disk size**, enter the minimum disk size required and click **Save**.
5. Click **Start** to apply the disk size and continue.

Setting up vSZ

1. Start PuTTY with the public IP address assigned to vSZ.

   NOTE
   Ensure port 22 to the inbound security rules for SSH access.

   NOTE
   The default credentials are as follows:

   - Username: admin
   - Password: admin
   - Enable Password: admin

2. Click **Open**. The PuTTY console appears and displays the login prompt.
3. In `login as:`, enter **admin**. The message "`Welcome to vSZ`" appears.
4. In `password`:, enter **admin**. The `vSZ>` prompt appears.

5. Enter **en** to enter the privileged mode.
6. In `password:`, enter admin. The `vSZ#` prompt appears.
7. Enter **setup**. The message "`Start vSZ setup process`" appears.
8. In `Select vSZ Profile:`, enter **1** for Essentials and **2** for Highscale.
9. In `Select address type`, enter **1** for `IPv4 only` and **2** for `IPv4 and IPv6 IP` version support.

   The next prompt asks you to choose how you want to set up the IP address.
10. Enter **1** if you want to manually assign an IP address, or enter **2** to automatically obtain an IP address from a DHCP server on the network.

    NOTE
    The vSZ Cloud setup, supports single interface configuration. The configuration applied here will be the same for control, cluster, and Management interfaces of the vSZ.

11. At the `Primary DNS` prompt, enter the IP address or host name of the primary DNS server that you want vSZ to use.

    The next prompt asks you to enter the secondary DNS server address.
12. At the `Secondary DNS` prompt, enter the IP address or host name of the secondary DNS server that you want vSZ to use.

    The next prompt asks you to confirm that you want to apply the IP address settings that you configured in the previous prompts.
13. When the prompt "`Do you want to apply the settings? (y/n)`" appears, enter **y** to confirm and continue.

    After applying the settings, the message, "`Current Network Settings (After Applying)`" is displayed.
14. At the prompt "`Accept these settings and continue? (y/n)`", enter **y** to confirm and continue.
15. Run the setup again to configure the cluster details using CLI. To configure vSZ usning the setup wizard, refer to Using the Setup Wizard to Install vSZ on page 201 for more information.

Installing vSZ on the Google Computing Engine

Introduction

You can install vSZ on the Google Computing Engine using the steps mentioned in this section.

NOTE
The minimum memory and CPU requirements have changed in this release. You may need to upgrade your infrastructure before upgrading. Please read carefully. This is the minimum requirement recommended. Refer to the tables in Virtual SmartZone Minimum Requirements on page 14 in the Installation Preparation chapter.

Public cloud solution resource requirement

- CPU or Memory: Minimum requirement of Custom Machine Type.
- Storage Requirement (Disk Storage): Minimum requirement of SSD 150 GB above

NOTE
Any CPU with credit limitation type cannot support.
Select the proper disk size to run vSZ since disk sizes may have different disk IO performance in each cloud platform.

Logging into GCE and Selecting a Project

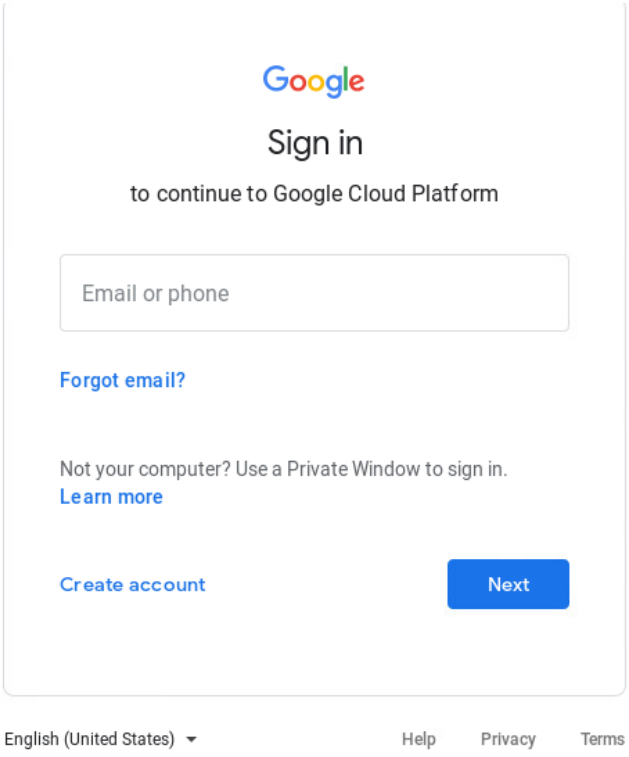
This section describes how to log into the GCE and select a project.

Ensure that you have created an account with GCE and have the login details for the same.

1. Click http://cloud.google.com to access the **Google Cloud Platform** website.

2. Log in using your user name and password.

   FIGURE 110 Login with user credentials

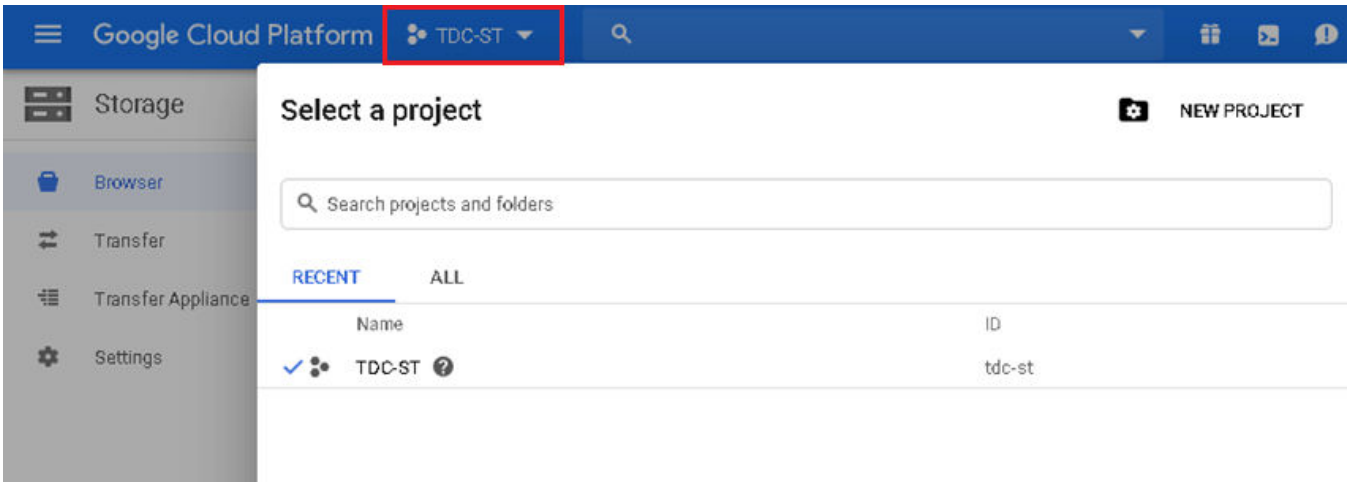


3. Select **My console** as shown.

   FIGURE 111 GCE Page - My console

4. A list of projects you created is displayed. Click to choose a project.

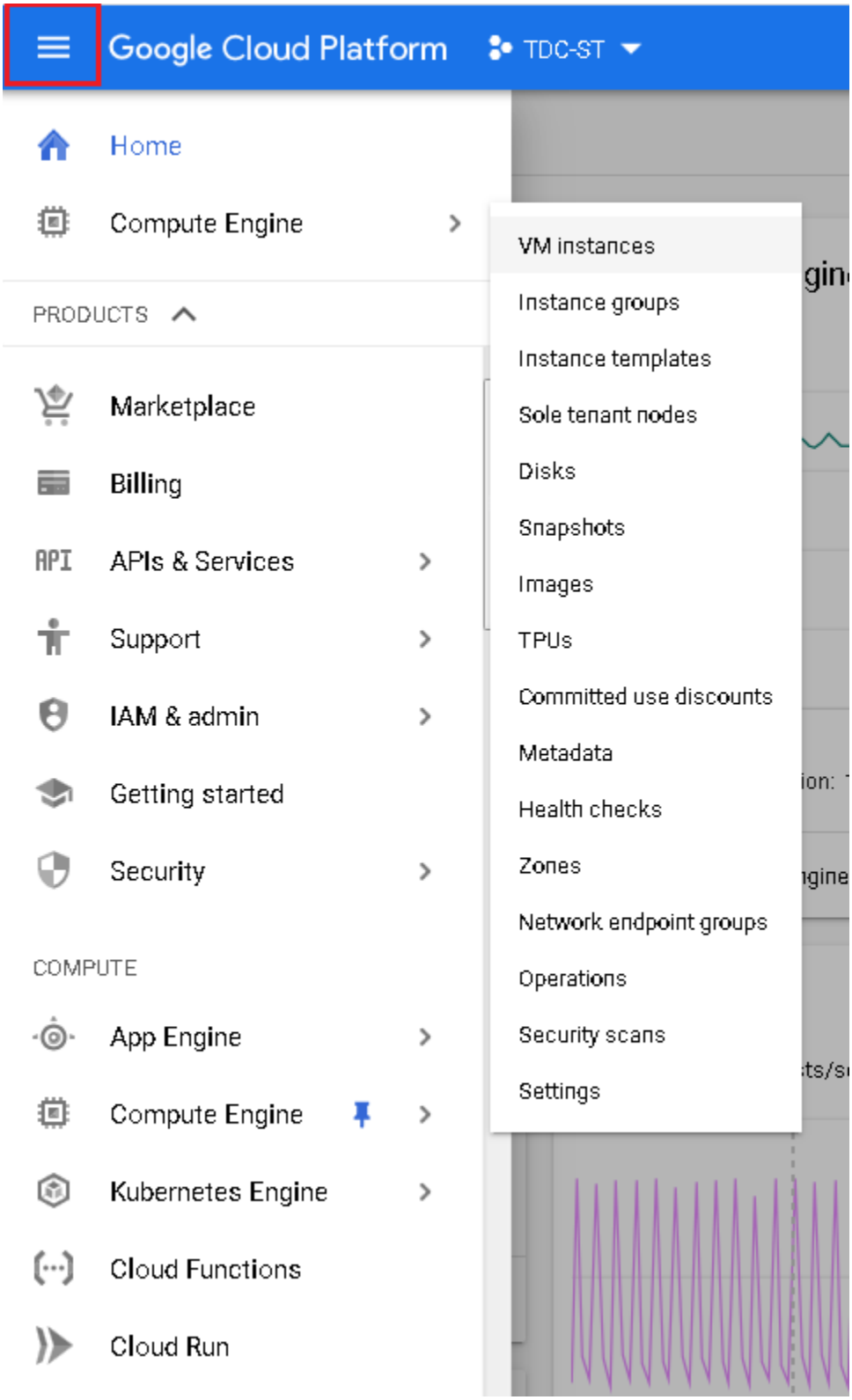
FIGURE 112 Choose the project



NOTE
You can create projects by clicking **Create a project** in the drop-down.

5. Click **Product and Services** icon to view the list of GCE services.

FIGURE 113 Selecting a Project

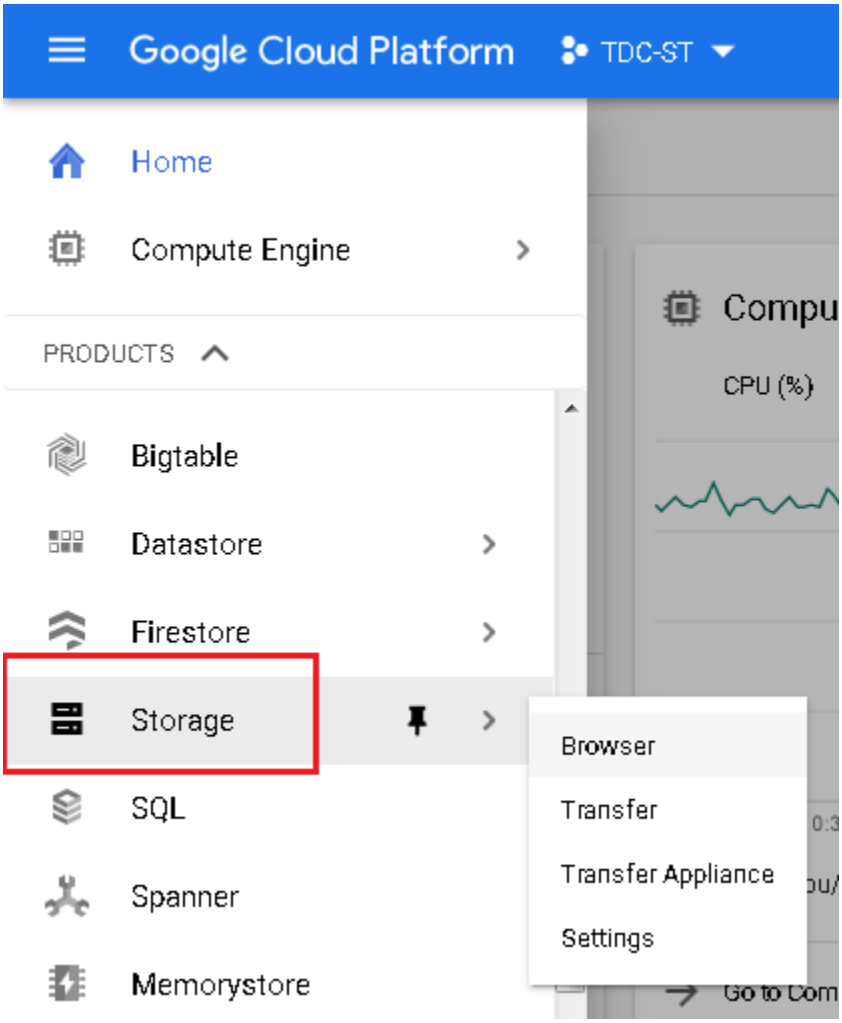


Creating a Storage Bucket

You can create storage for the objects you create. Follow these steps to create storage.

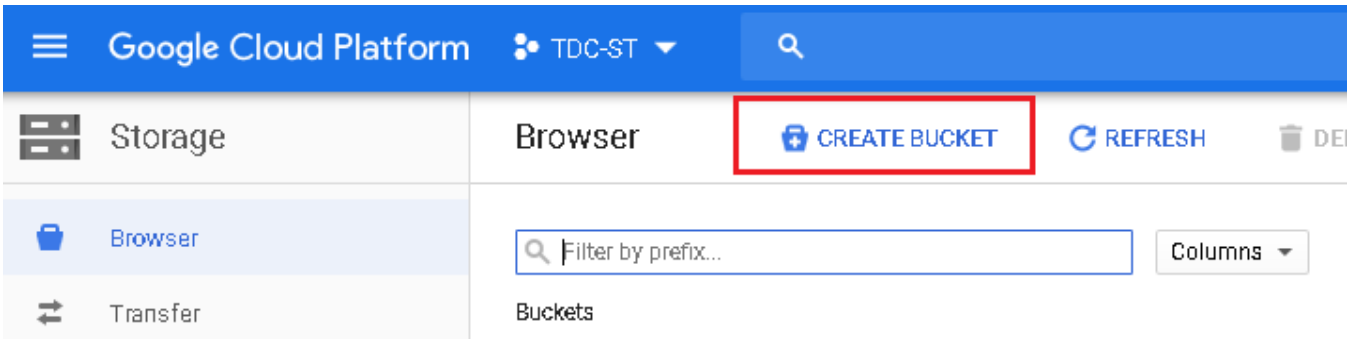
1. From **Google Developers Console**, click **Product and Services** icon > **Storage**. The **Cloud Storage Buckets** screen appears.

FIGURE 114 Storage Bucket Browser



2. Click **Create Bucket**. The New bucket screen appears.

FIGURE 115 Creating a Storage Bucket



3. Complete the following fields,
   a) In **Name**, type the name of the storage bucket
   b) In **Storage class**, select the storage class you want. You can choose from **Standard**, **Durable Reduced Availability (DRA)** or **Cloud Storage Nearline** in the drop-down list. Use the below table to compare the storage classes.
   c) In **Location**, select the location from the drop-down list.

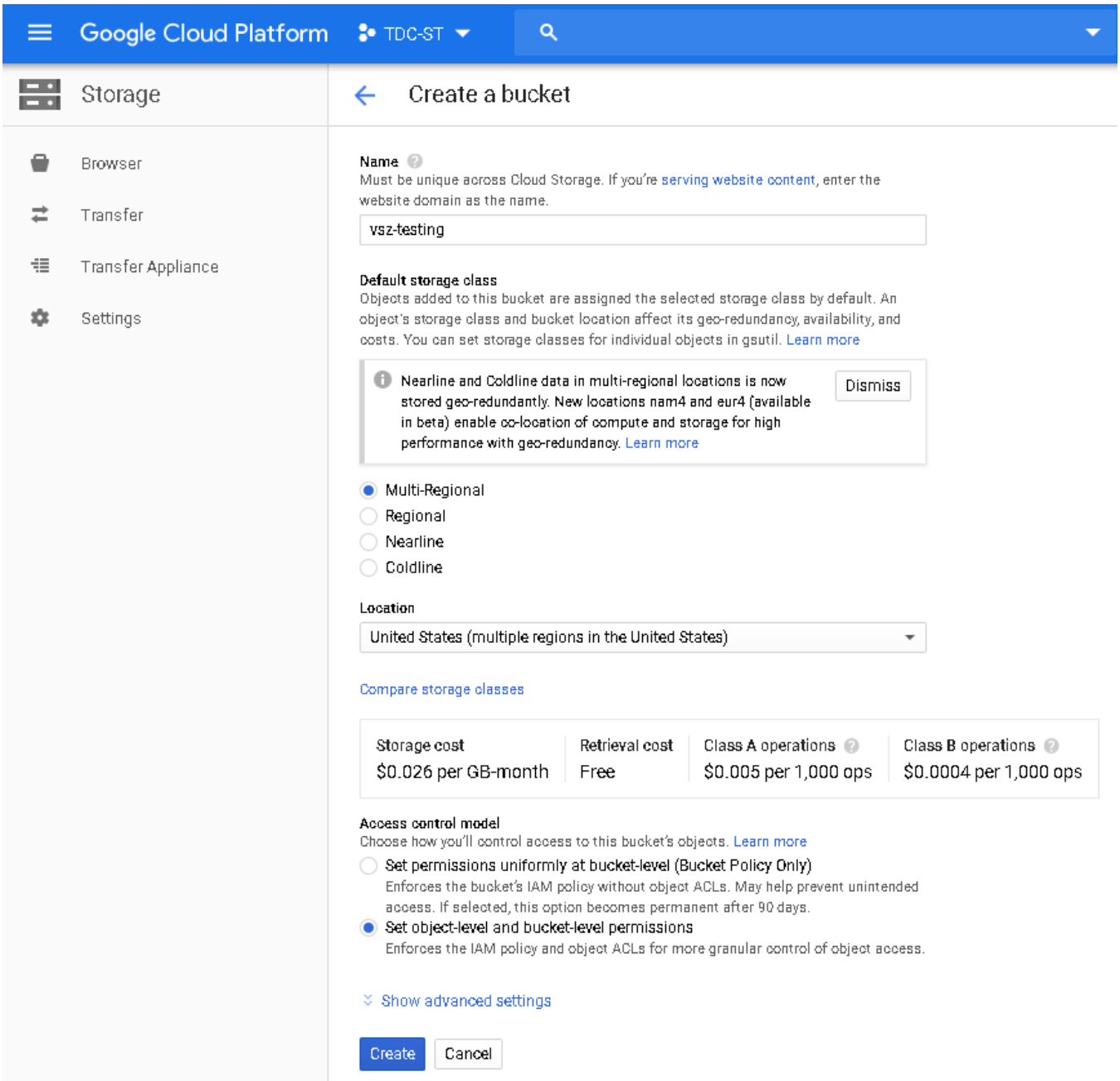
TABLE 13 Bucket Storage Location

Storage Class	Characteristics	Use Cases	Bucket Location
Standard Storage	High availability, low latency (time to first byte is typically tens of milliseconds).	Storing data that requires low latency access or data that is frequently accessed ("hot" objects), such as serving website content, interactive workloads, or gaming and mobile applications	Continental locations
Durable Reduced Availability (DRA)	Lower availability than Standard Storage and lower cost per GB stored.	Applications that are particularly cost-sensitive, or for which some unavailability is acceptable such as batch jobs and some types of data backup.	Continental and regional locations

TABLE 13 Bucket Storage Location (continued)

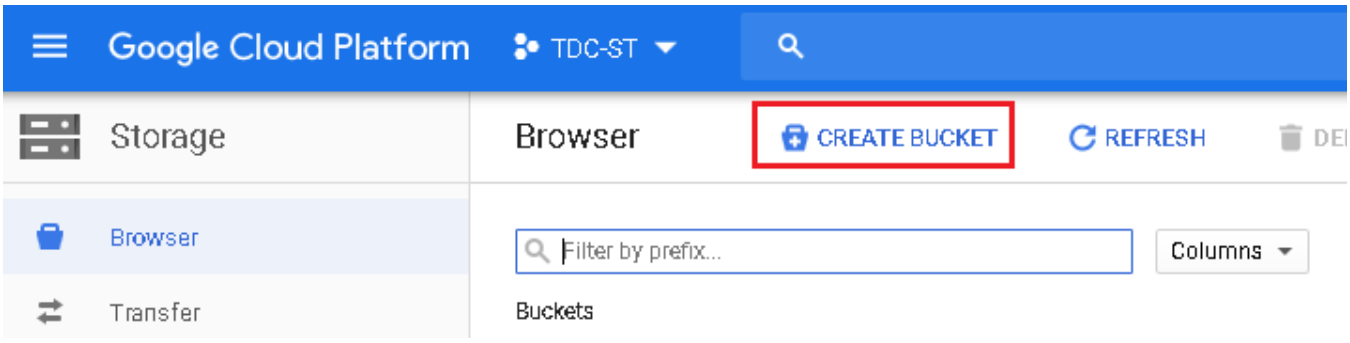
Storage Class	Characteristics	Use Cases	Bucket Location
Cloud Storage Nearline	Slightly lower availability and slightly higher latency (time to first byte is typically 2 - 5 seconds) than Standard Storage but with a lower cost.	Data you do not expect to access frequently (i.e., no more than once per month). Typically this is backup data for disaster recovery, or so called "cold" storage that is archived and may or may not be needed at some future time.	Continental locations

FIGURE 116 New Bucket Information



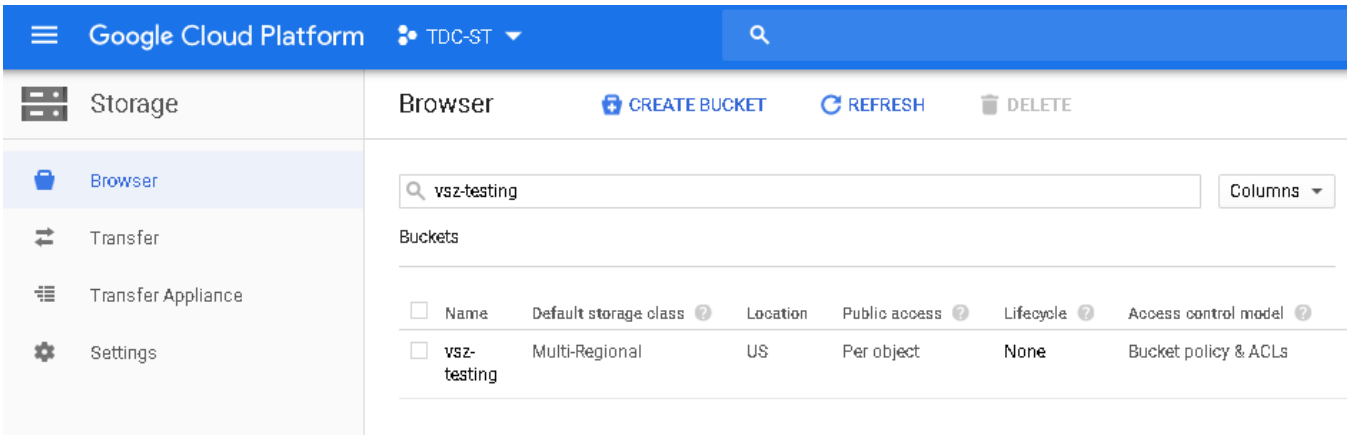
4. Click **Create**. The storage bucket you created is listed in the browser.
5. To create another storage, click **Create bucket** as shown.

FIGURE 117 Creating Another Storage Bucket



6. Verify that the storage bucket has been created.

FIGURE 118 Selecting the Storage Bucket



Uploading the vSZ Image to a Storage Bucket

Follow these steps to upload a controller image to the storage bucket you created.

1. Extract the vSZ raw.bin file that you obtained from Ruckus Networks.

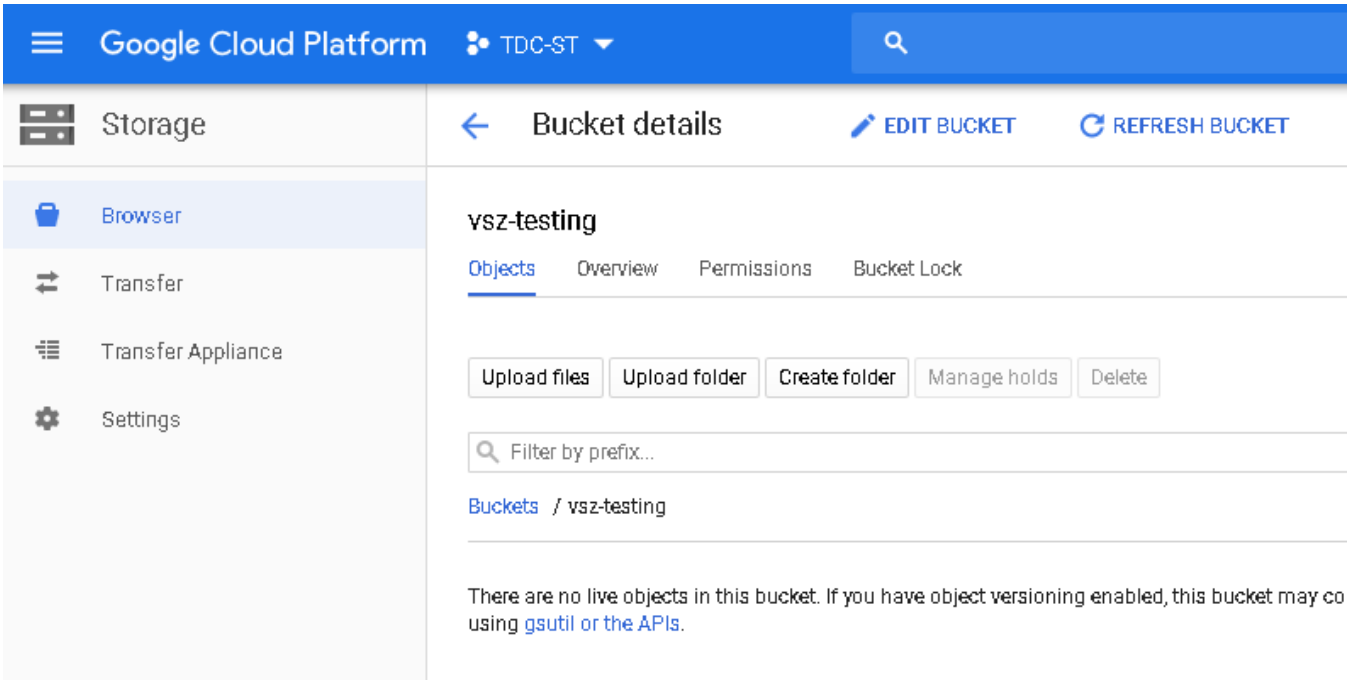
   NOTE
   - If the "`Permission denied`" error appears, execute the command "chmod +x vscg-3.5.0.0.808.raw.bin" before extracting the file.
   - If the "`uudecode: command not found`" error appears during the extraction process, install the "sharutils" package, and then try extracting the image again.

2. Read the Virtual SmartZone (vSZ) Software License agreement that appears when you extract the raw.bin file.

3. When the `Accept this agreement?` prompt appears, enter **yes** to accept the license agreement.

   When the extraction process is complete, a raw.tar.gz file appears.
4. On the GCE web interface, browse to the storage bucket where you want to upload the vSZ image file.

   FIGURE 119 Browse to the storage bucket

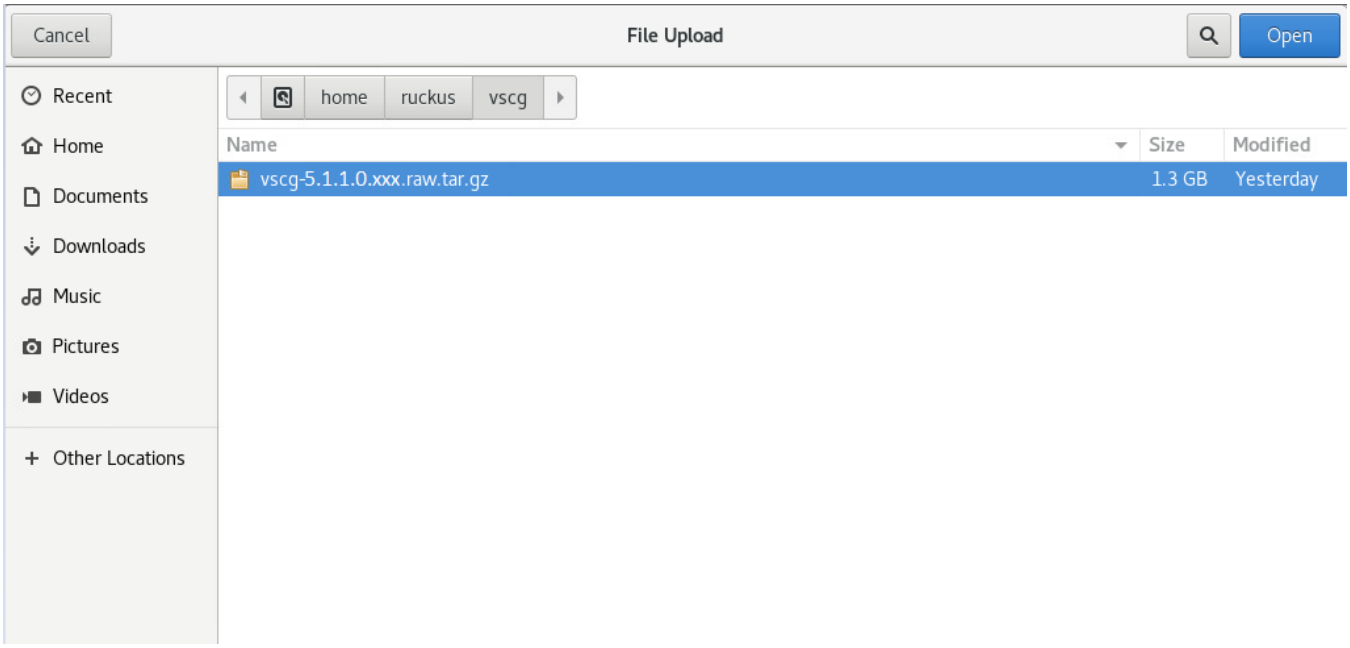


5. Click **Upload files**.

6. Browse to the location of the .raw.tar.gz image file that you extracted, and then select it.

NOTE
You can only select .raw.tar.gz files.

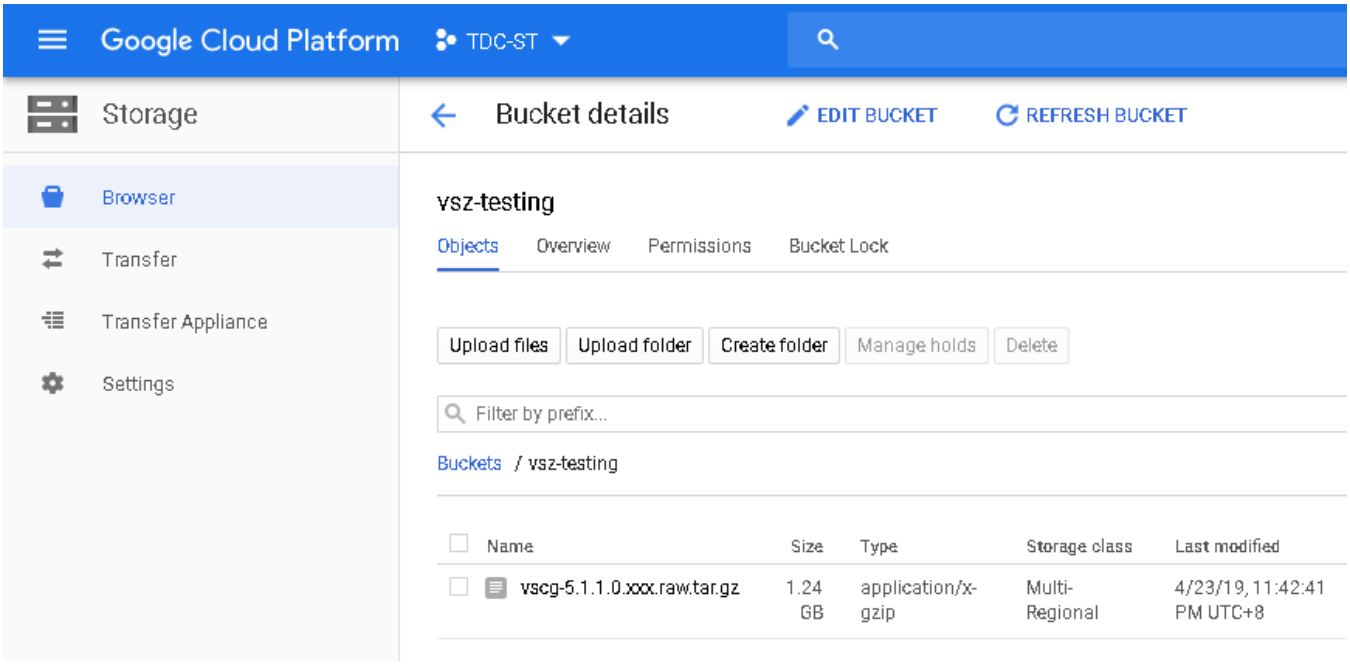
FIGURE 120 Select the .raw.tar.gz image file that you extracted



7. Click **Open** to upload the image file.

   Your browser displays the progress of the file upload process. After the upload process is complete, the image file appears in the storage bucket.

   FIGURE 121 The image file appears in the storage bucket

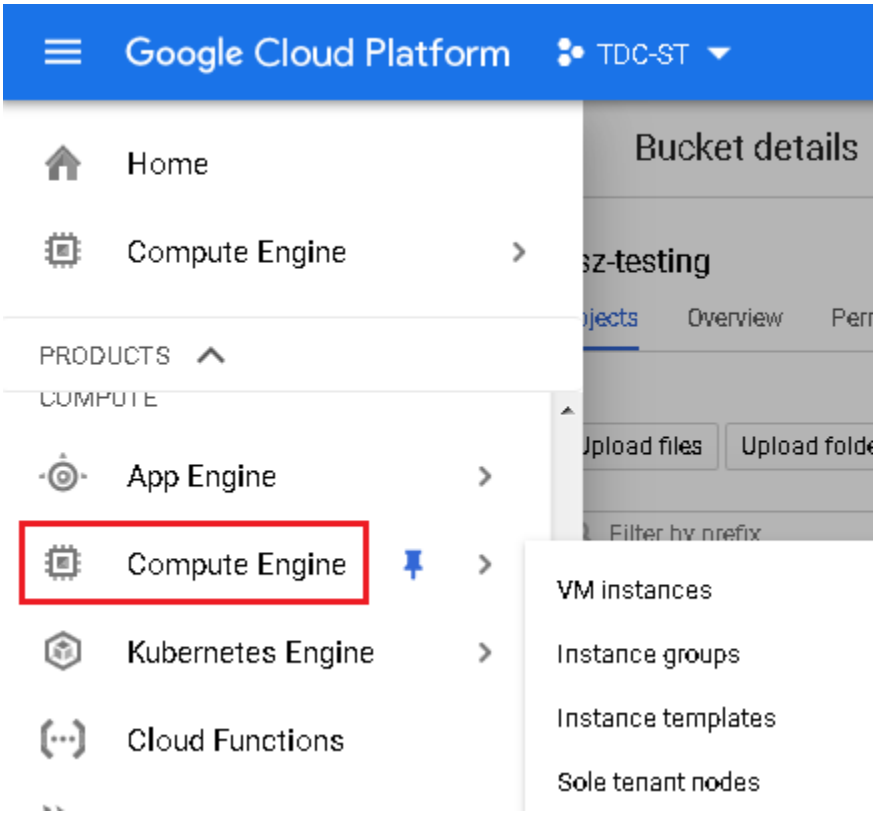


Creating a vSZ Image for Virtual Machines

Follow these steps to create a vSZ image for virtual machines.

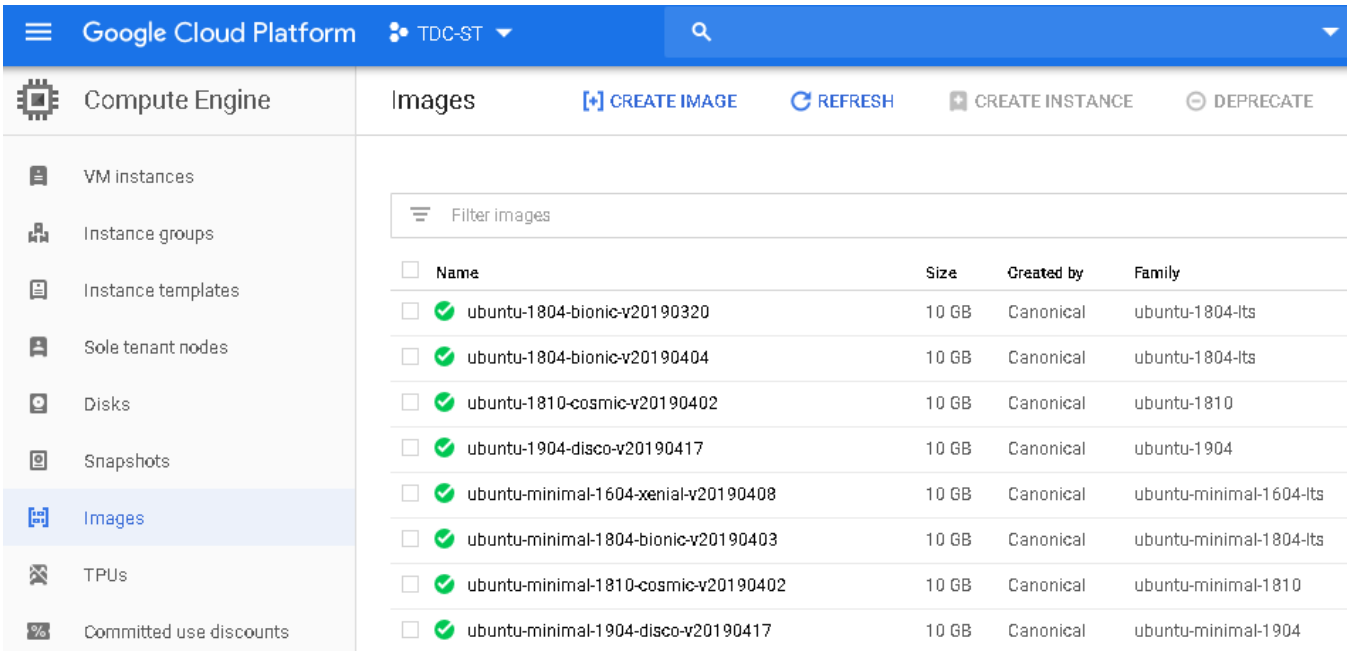
1. From **Google Developers Console**, click **Compute** > **Compute Engine**.

   FIGURE 122 Select Compute Engine



2. On the menu, click **Images**, and then cllick **Create Image**.

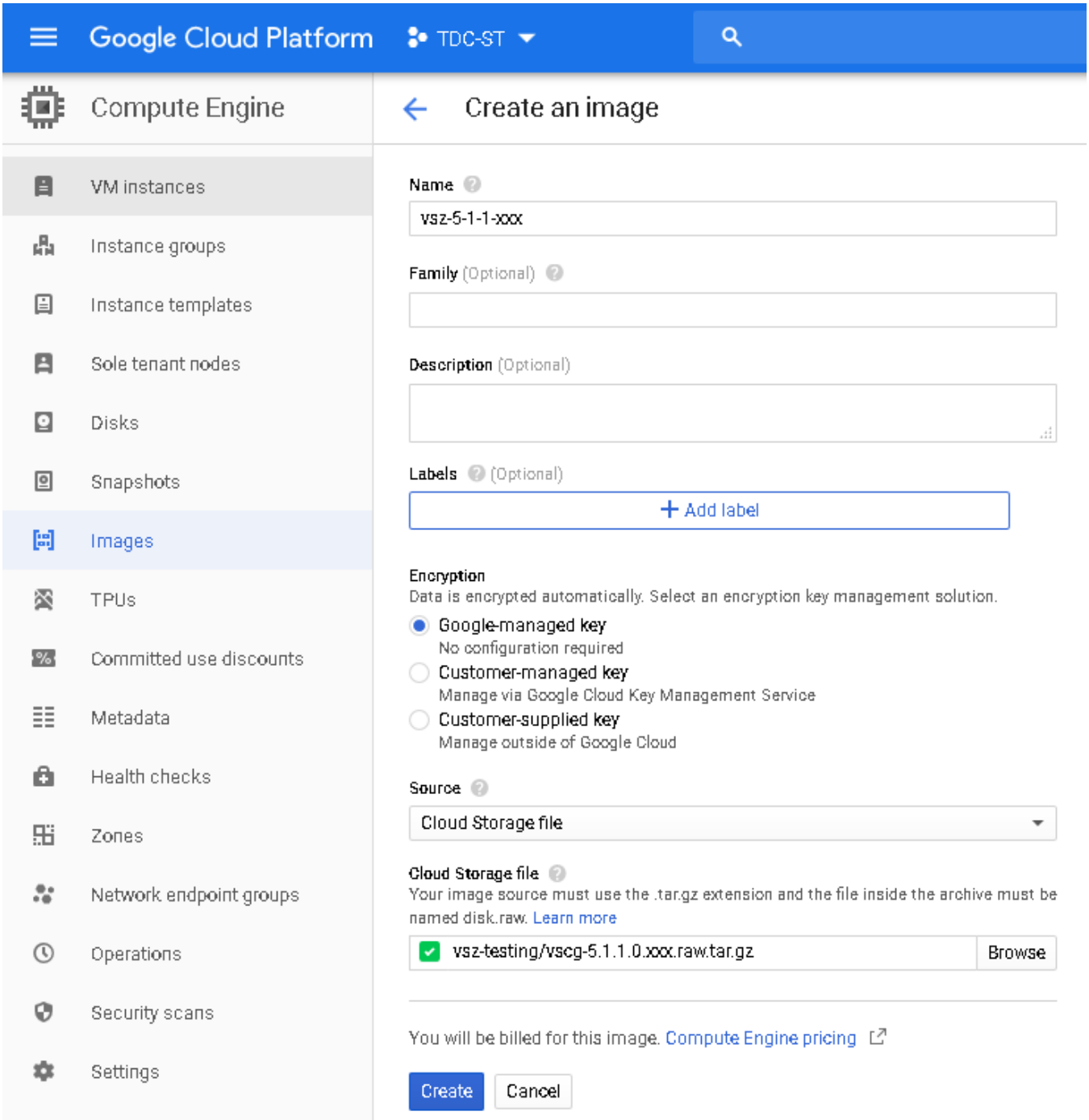
FIGURE 123 Click Create Image



The **Create an image** page appears.

3. Configure the properties of the new image by fillng out the boxes below.
   a) In **Name**, type the name of the image.
   b) In **Description**, provide a brief description about the image.
   c) In **Encryption**, select an option from the drop-down list containing Automatic (recommended) and Customer supplied.
   d) In **Source**, select **Cloud storage file**.
   e) In **Cloud Storage file**, click **Browse**, and then select the .raw.tar.gz image file that you extracted previously.

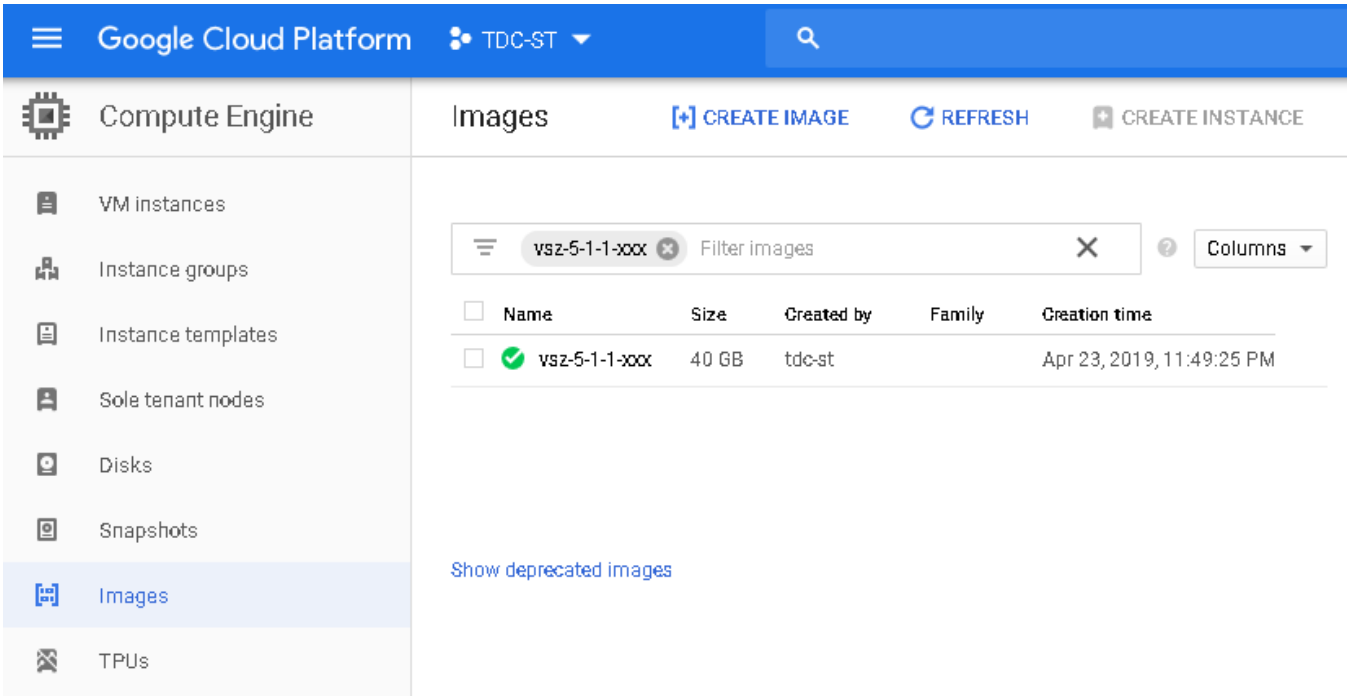
FIGURE 124 Creating an image



4. Click **Create**.The new image is listed.

   GCE creates the new image. When the process is complete, the image you created from the .raw.tar.gz image file appears on the **Images** page.

   FIGURE 125 The new image you created appears on the Images page



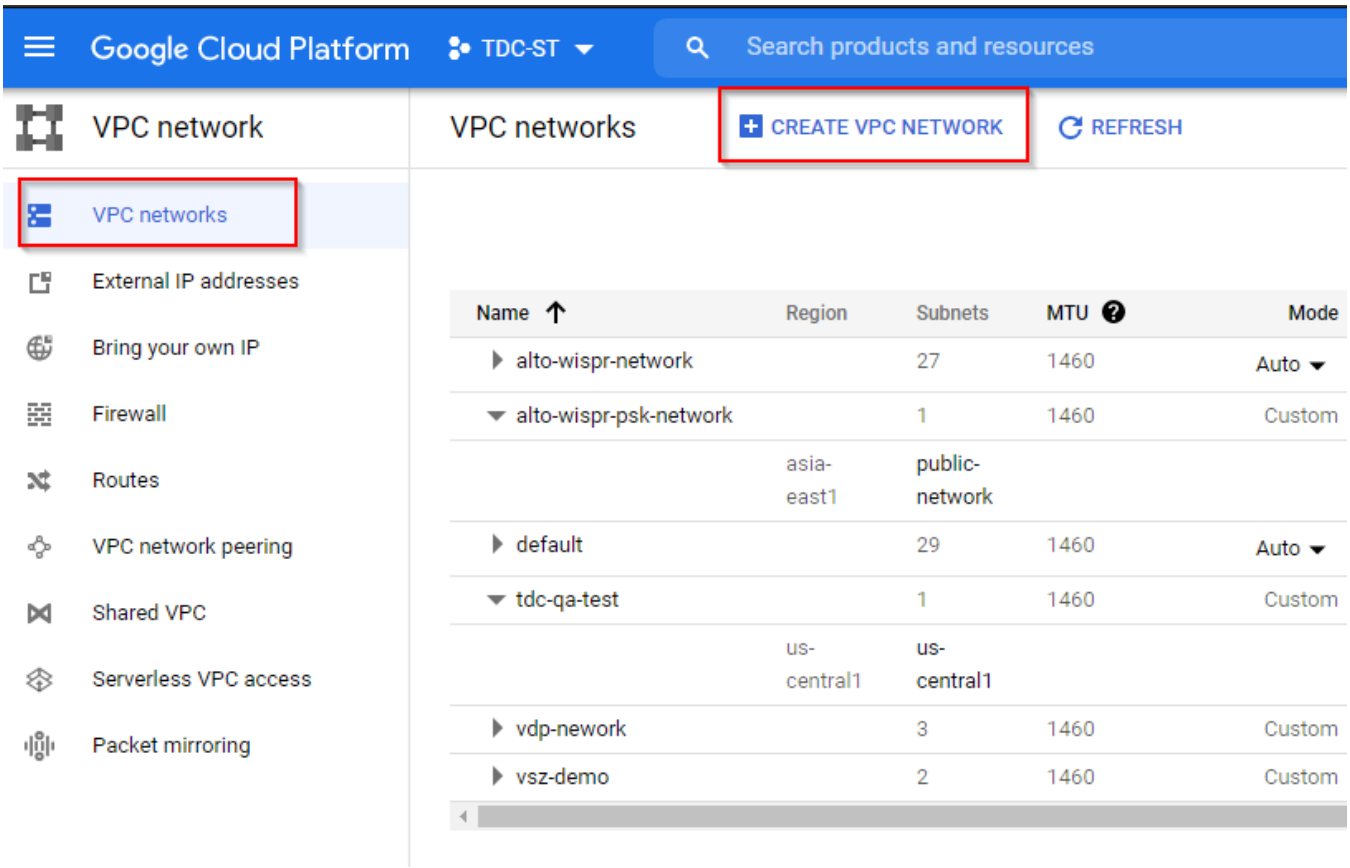
You have completed creating an image.

Creating a Network and Configuring Firewall Rules

Follow these steps to create a network and configure firewall rules for your network.

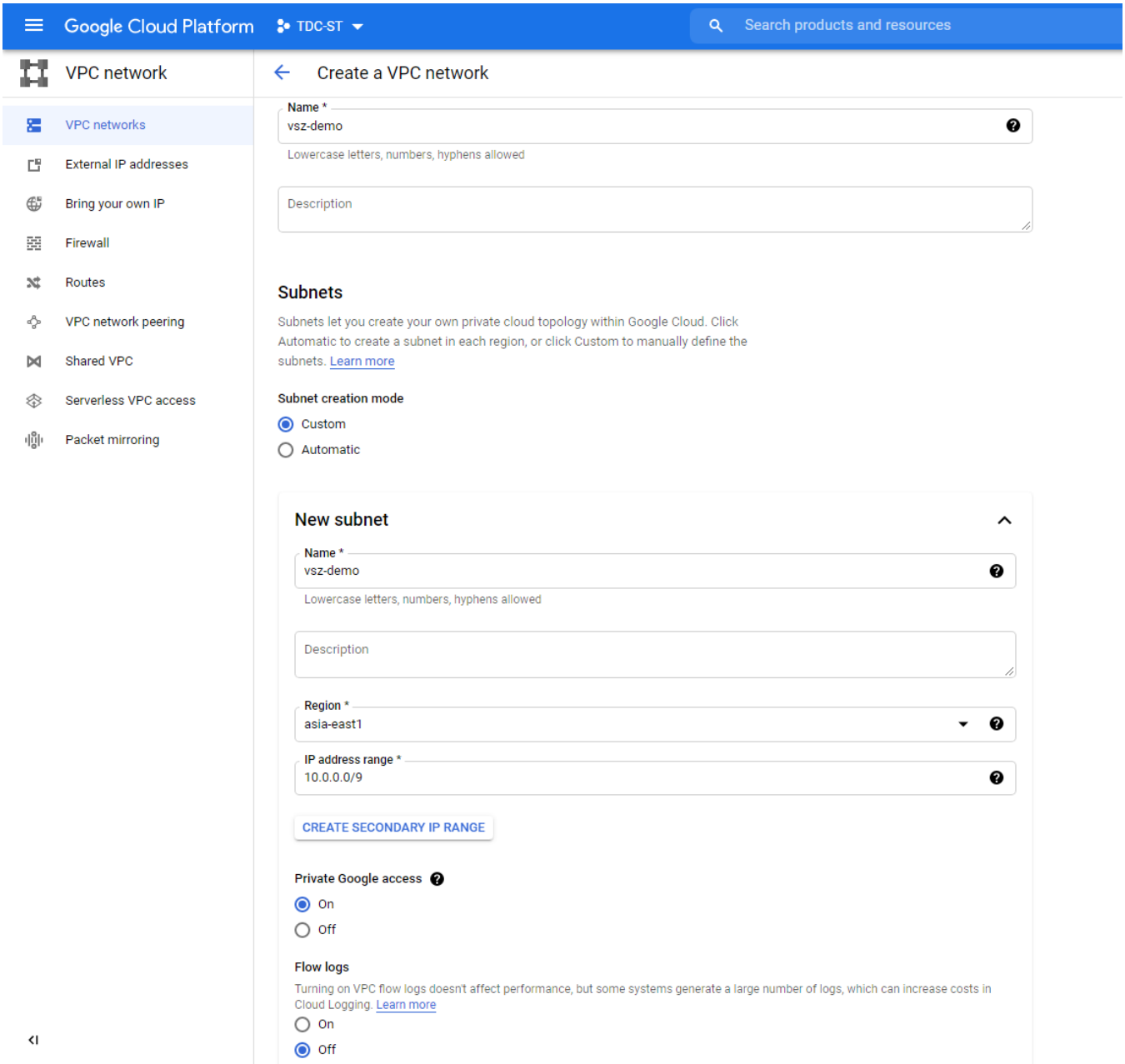
1. From **Google Developers Console**, click **Networking** > **Networks**. A page displaying a list of networks is displayed. Click on **Create VPC Network**.

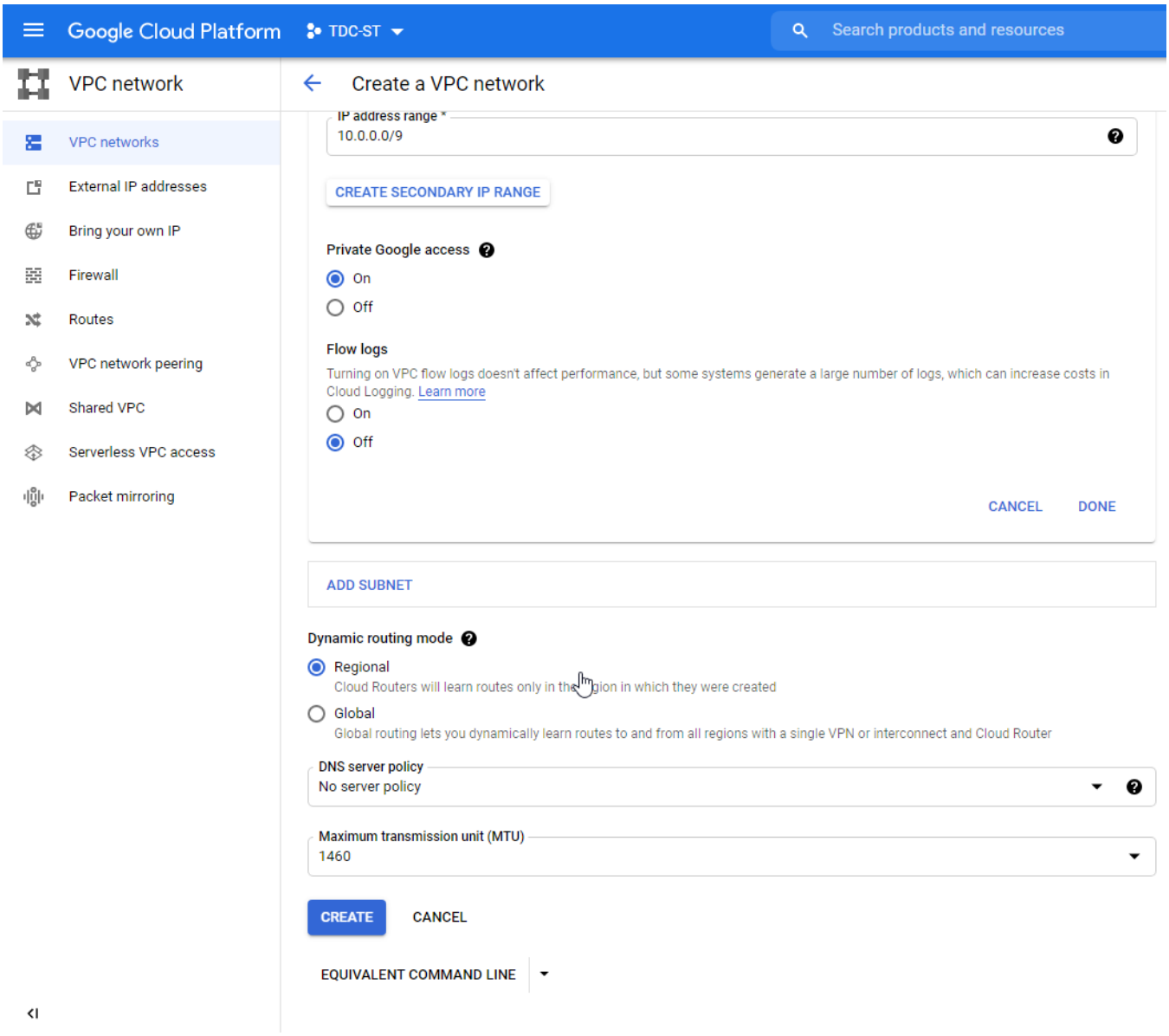
FIGURE 126 List of networks



2. In the **Create a VPC network** screen, configure the following:
   a) **Name**: enter the name of the VPC network.
   b) **Subnets**: enter a name for new subnet.
   c) **Region**: select a region from the list that is used to place the vSZ instance.
   d) **IP address range**: enter a private subnet.
   e) **Private Google access**: select **On**.

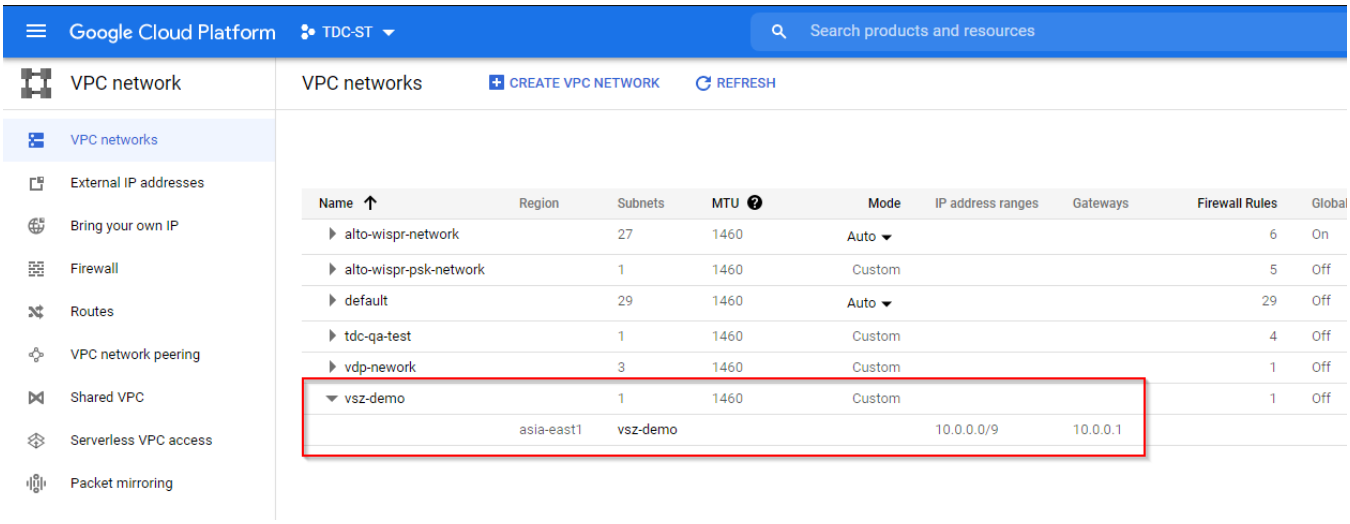
FIGURE 127 Configuring VPC network - part 1




Google Cloud Platform
TDC-ST
Search products and resources
VPC network
Create a VPC network
VPC networks
External IP addresses
Bring your own IP
Firewall
Routes
VPC network peering
Shared VPC
Serverless VPC access
Packet mirroring
IP address range *
10.0.0.0/9
CREATE SECONDARY IP RANGE
Private Google access
On
Off
Flow logs
Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Cloud Logging. Learn more
On
Off
CANCEL
DONE
ADD SUBNET
Dynamic routing mode
Regional
Cloud Routers will learn routes only in the region in which they were created
Global
Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router
DNS server policy
No server policy
Maximum transmission unit (MTU)
1460
CREATE
CANCEL
EQUIVALENT COMMAND LINE

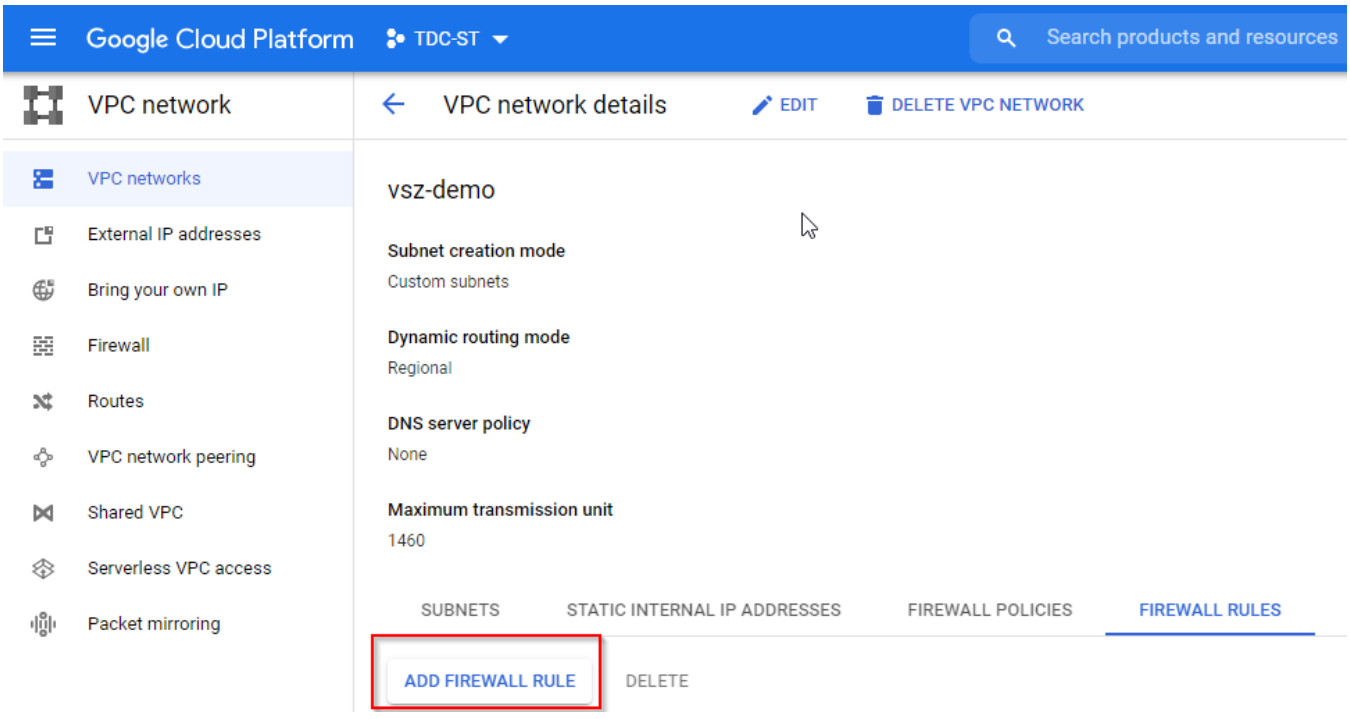
3. Click **Create**, the new VPC network entry is displayed.

FIGURE 128 VPC network entry



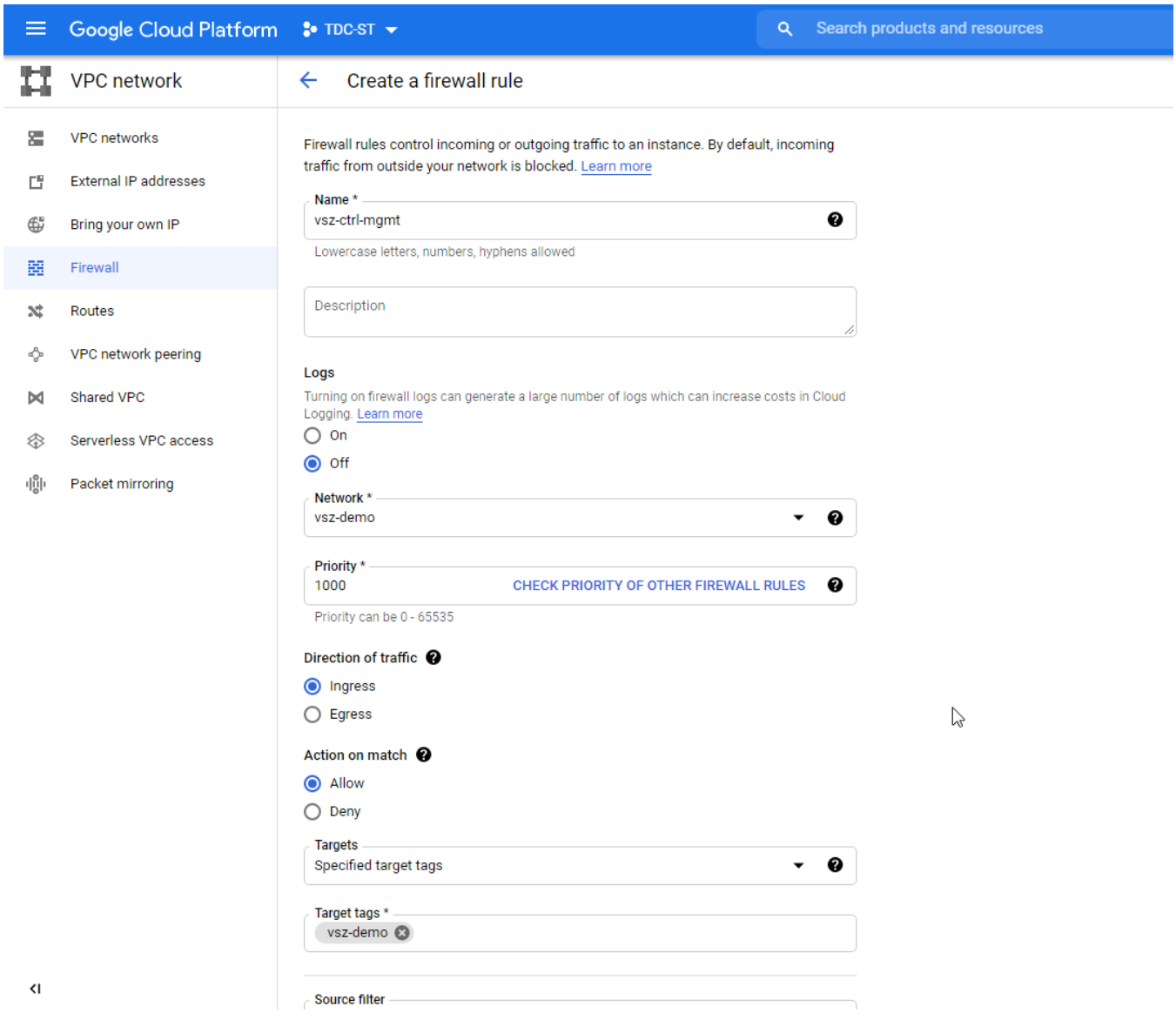
4. To create a firewall rule, click **Add a firewall rule**.

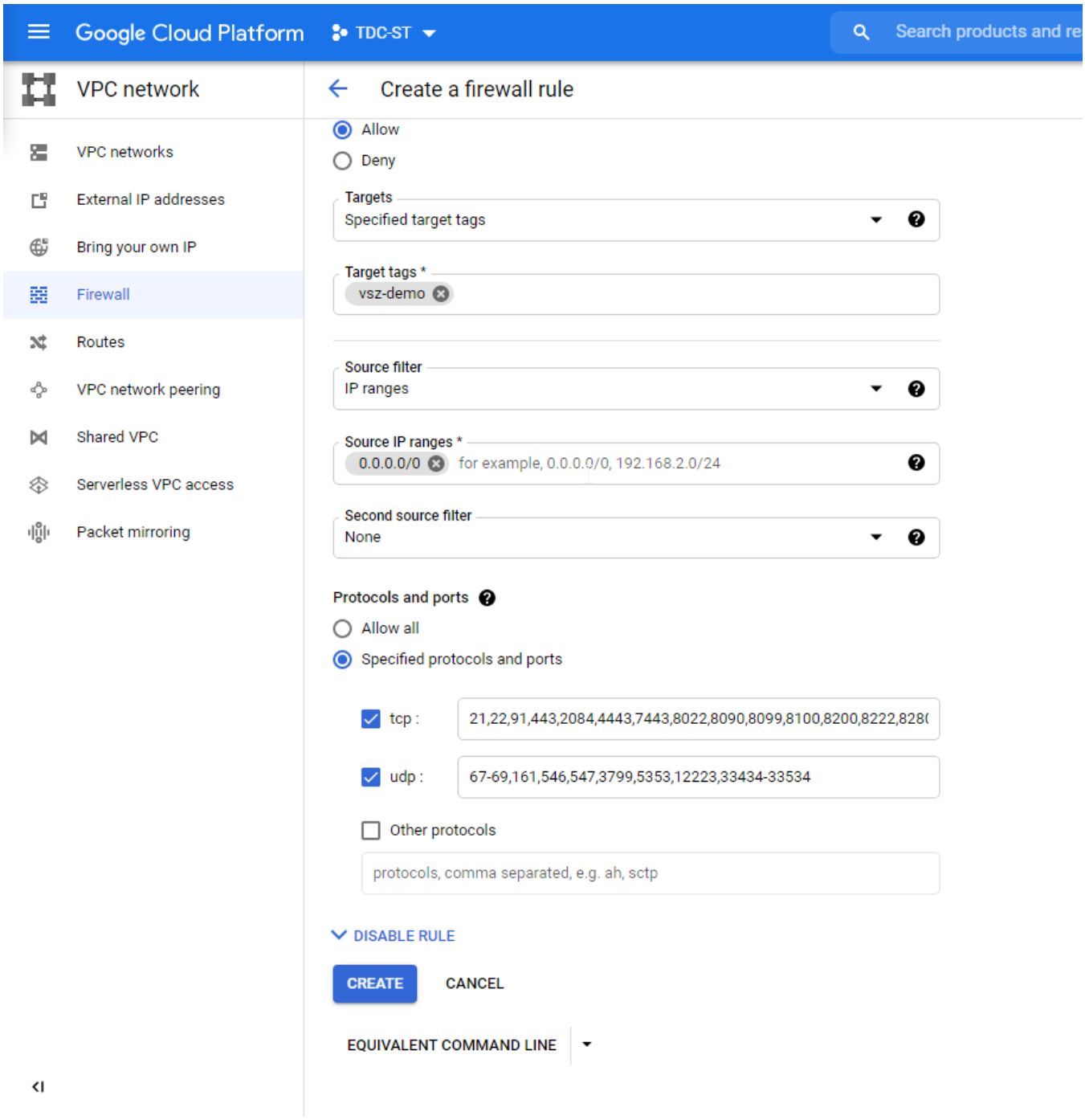
FIGURE 129 Add a Firewall Rule



5. In the **Create a firewall rule** screen, configure the following:
   a) **Name**, enter the name of the rule
   b) **Description**, provide a brief description about the rule.
   c) **Network**, enter the network address.
   d) **Source filter**, select **Allow from any source**.
   e) **Source IP ranges**, enter the range.
   f) **Allowed protocols and ports**, enter the protocols and ports that will be allowed. Refer to the *RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide*, for details of required open ports for control and management interface.
   g) In **Target tags**, specify a tag name. It is recommended that you provide a tag as all network instances with this tag will adhere to the firewall rule.

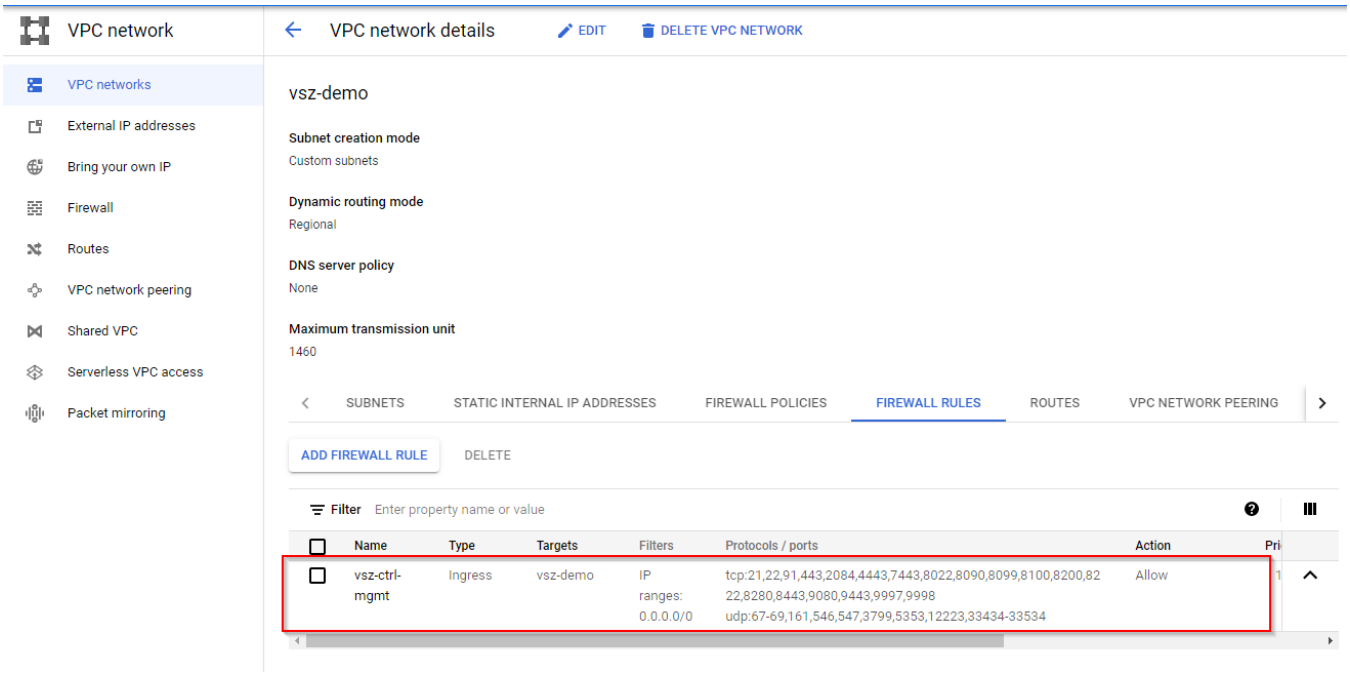
FIGURE 130 Creating a Firewall Rule



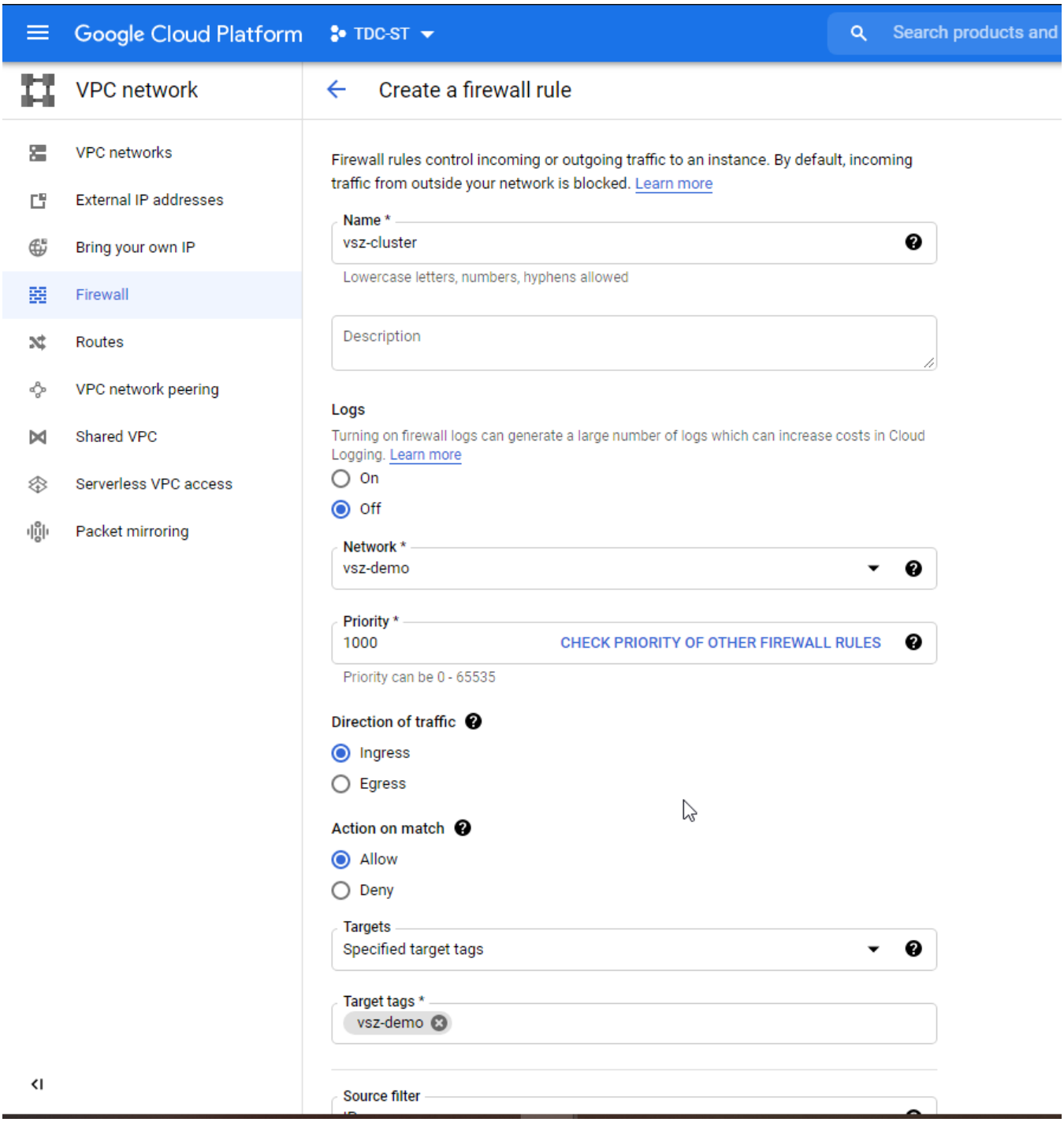

Google Cloud Platform
TDC-ST
Search products and re
VPC network
Create a firewall rule
VPC networks
External IP addresses
Bring your own IP
Firewall
Routes
VPC network peering
Shared VPC
Serverless VPC access
Packet mirroring
Allow
Deny
Targets
Specified target tags
Target tags *
vsz-demo
Source filter
IP ranges
Source IP ranges *
0.0.0.0/0
for example, 0.0.0.0/0, 192.168.2.0/24
Second source filter
None
Protocols and ports
Allow all
Specified protocols and ports
tcp :
21,22,91,443,2084,4443,7443,8022,8090,8099,8100,8200,8222,828(
udp :
67-69,161,546,547,3799,5353,12223,33434-33534
Other protocols
protocols, comma separated, e.g. ah, sctp
DISABLE RULE
CREATE
CANCEL
EQUIVALENT COMMAND LINE

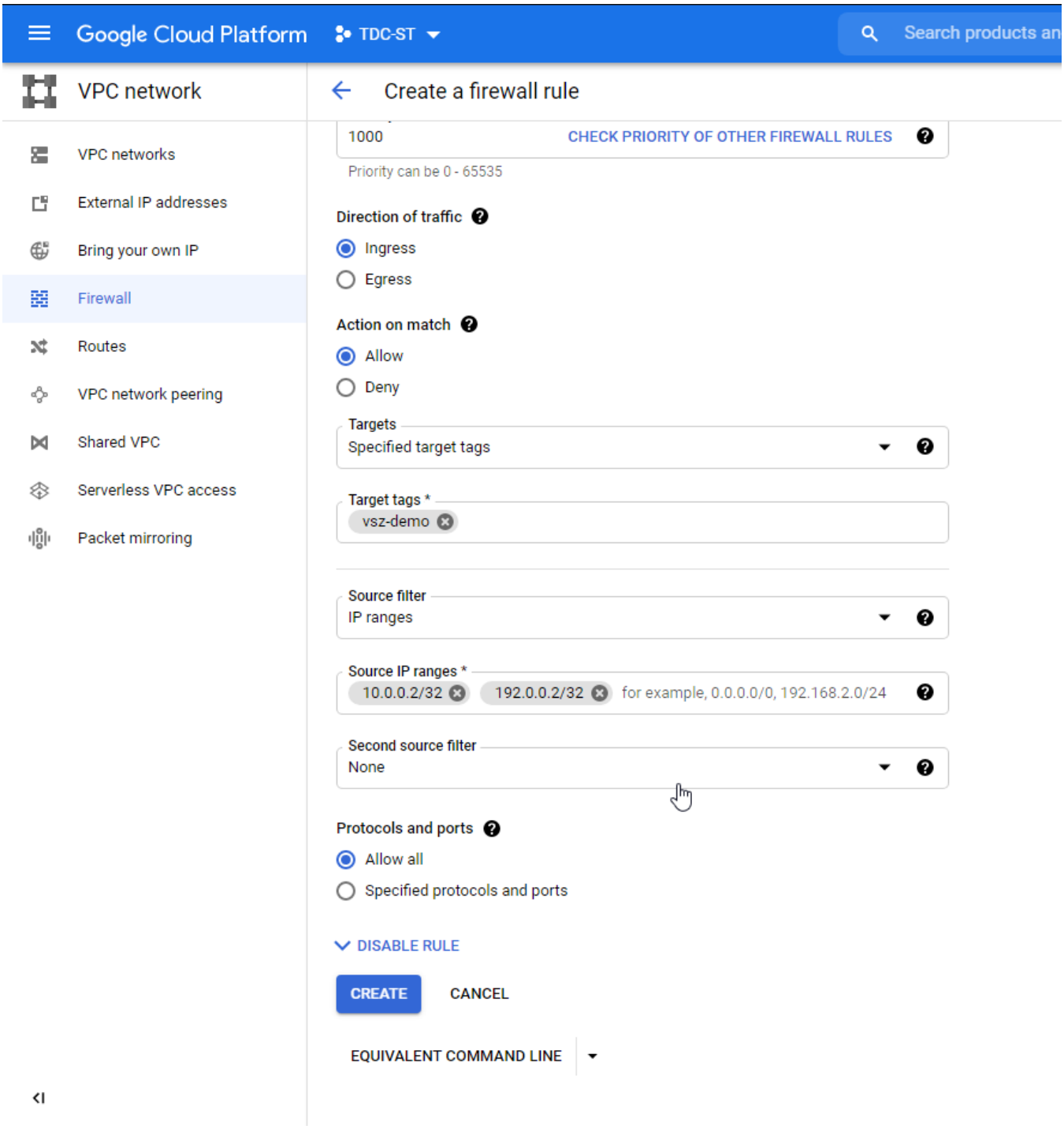
6. Click **Create**. A page displaying the new firewall rule appears.

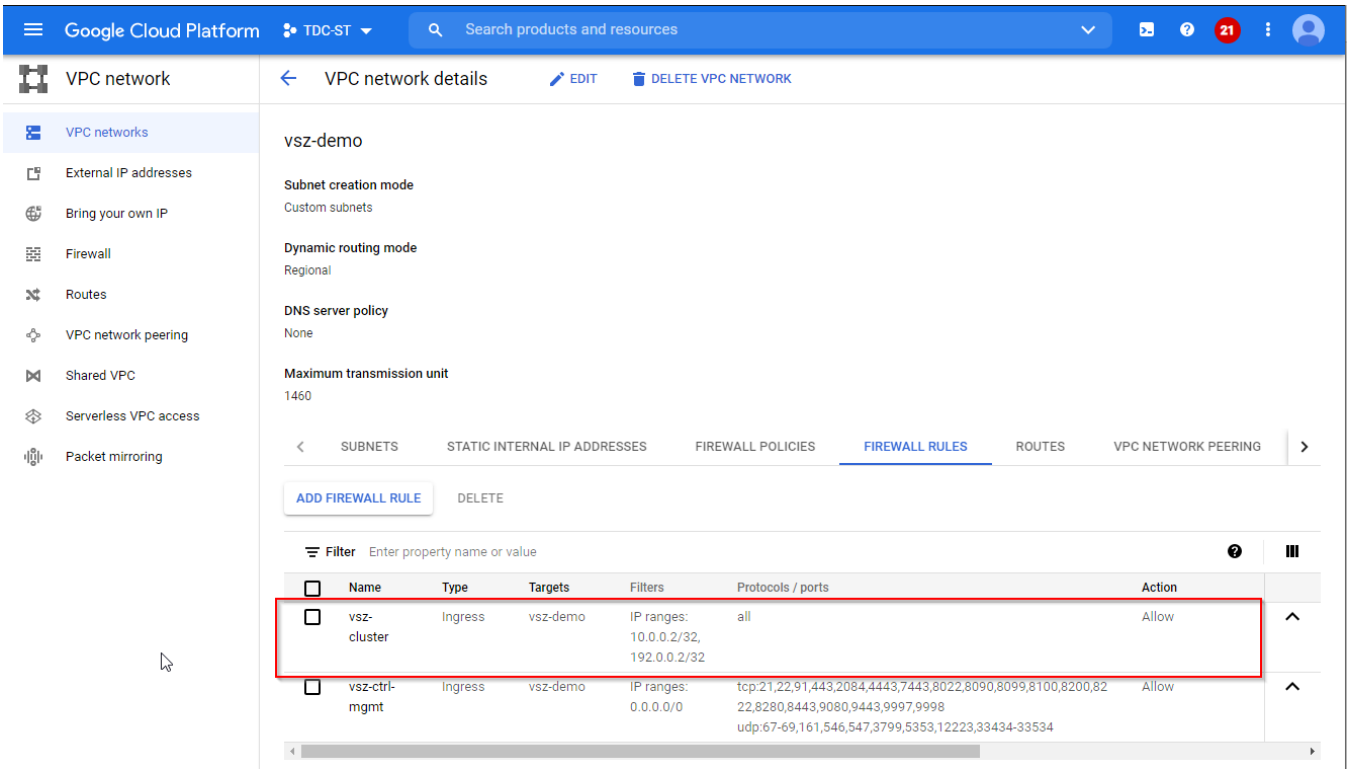
FIGURE 131 Adding Firewall Rules



7. For building up a 2-4 node cluster, create another firewall rule that allows all traffic on internal interface of all your vSZ instances.




Google Cloud Platform
TDC-ST
Search products an
VPC network
Create a firewall rule
VPC networks
External IP addresses
Bring your own IP
Firewall
Routes
VPC network peering
Shared VPC
Serverless VPC access
Packet mirroring
1000
CHECK PRIORITY OF OTHER FIREWALL RULES
Priority can be 0 - 65535
Direction of traffic
Ingress
Egress
Action on match
Allow
Deny
Targets
Specified target tags
Target tags *
vsz-demo
Source filter
IP ranges
Source IP ranges *
10.0.0.2/32
192.0.0.2/32
for example, 0.0.0.0/0, 192.168.2.0/24
Second source filter
None
Protocols and ports
Allow all
Specified protocols and ports
DISABLE RULE
CREATE
CANCEL
EQUIVALENT COMMAND LINE



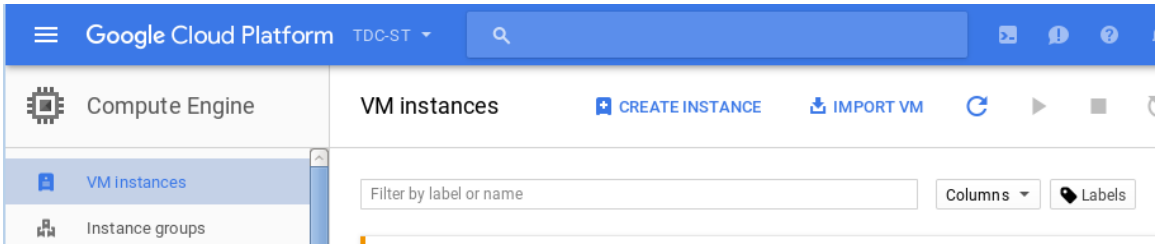
Creating a Virtual Machine Instance

Follow these steps to create a new virtual machine (VM_ instance).

1. From **Google Developers Console**, click **Compute** > **Compute Engine** > **VM instances**.

   The **VM instances** page appears.

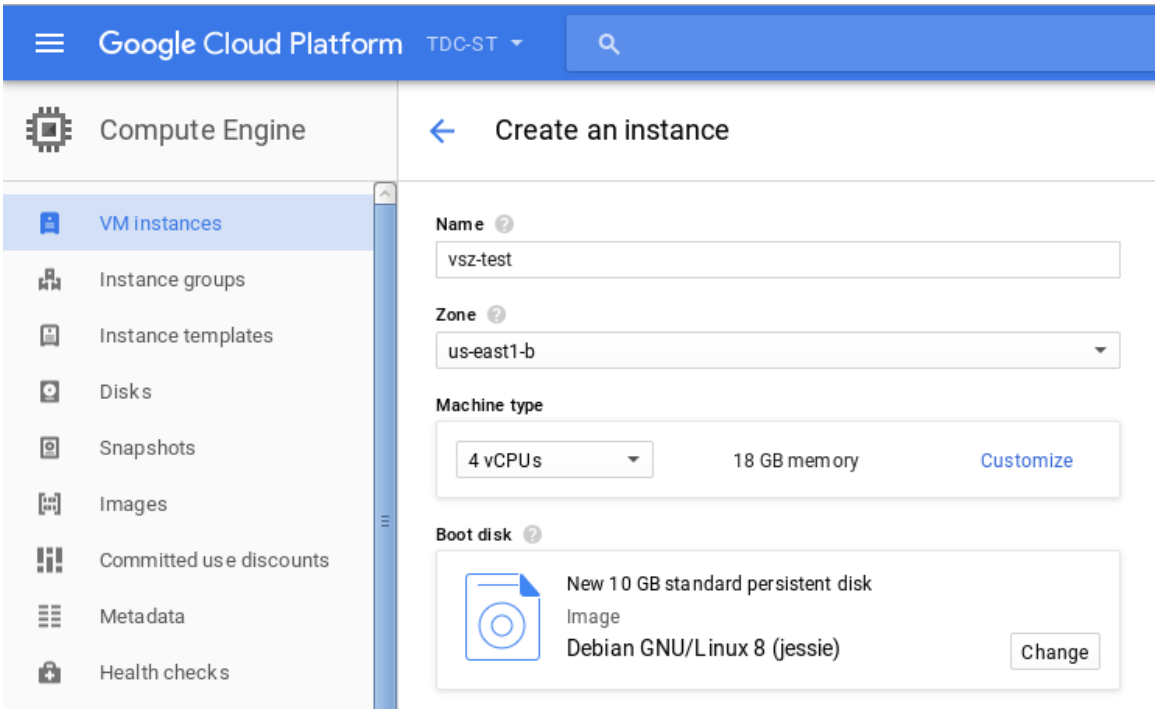
   FIGURE 132 The VM instances page



2. Click **Create Instance**.

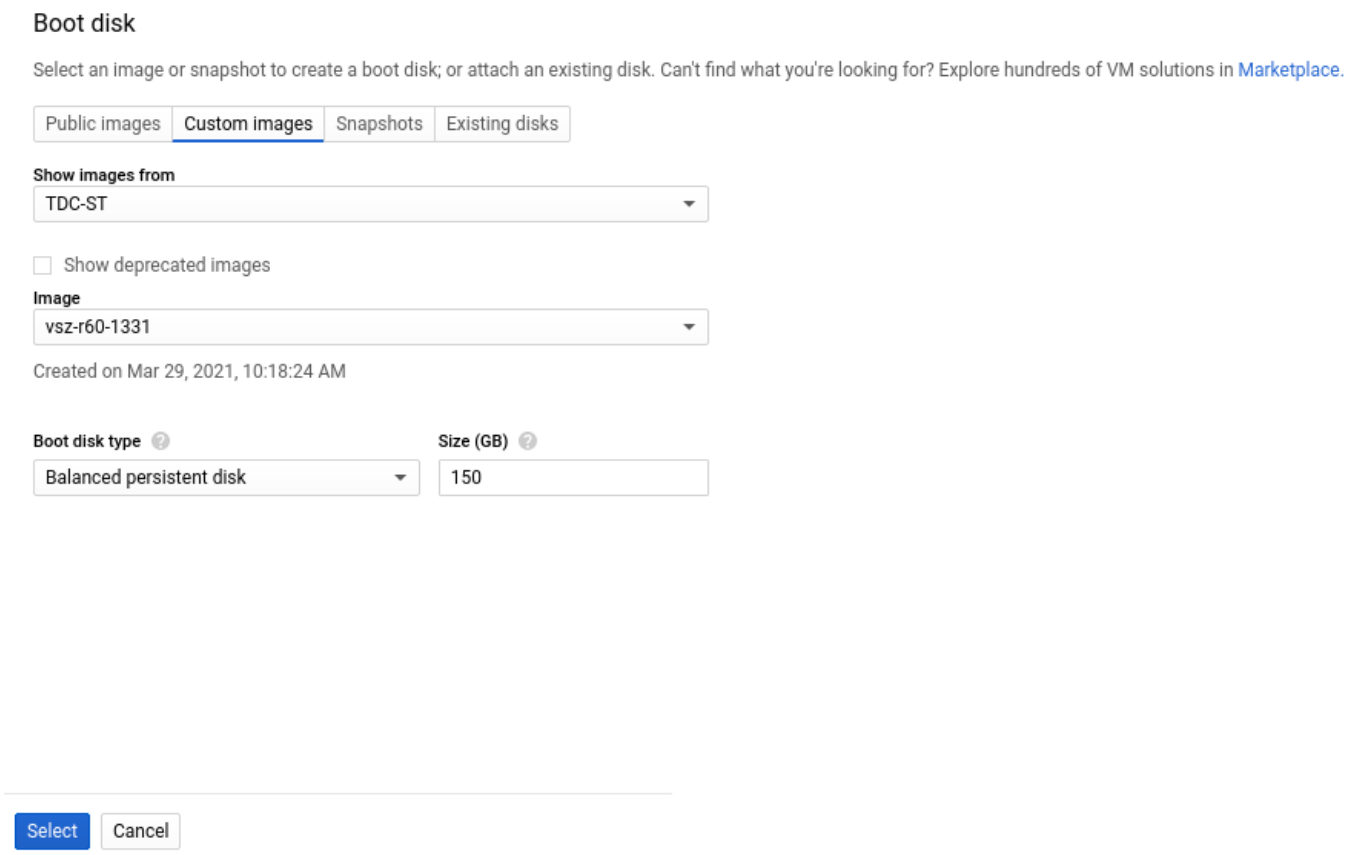
   The **Create an instance** page appears.

   FIGURE 133 The Create an instance page



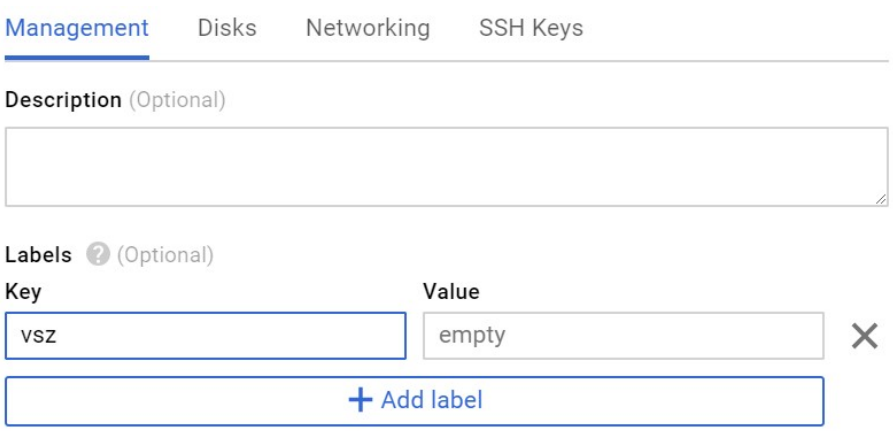
3. Configure the new VM instance that you are creating by filling out the boxes below.
   a) In **Name**, type the name of the VM instance.
   b) In **Zone**, select a zone from the drop-down list.
   c) In **Machine type**, accept or modify the default values for **vCPUs** and **Memory**.
   d) Under **Boot disk**, click **Change**. The **Boot disk** page appears. Click **Custom images**.In **Show images from**, select the storage bucket where you uploaded the controller image, and then select the image. Click **Select**.
   e) In **Project access**, allow API access as appropriate.

   FIGURE 134 Creating a new VM instance



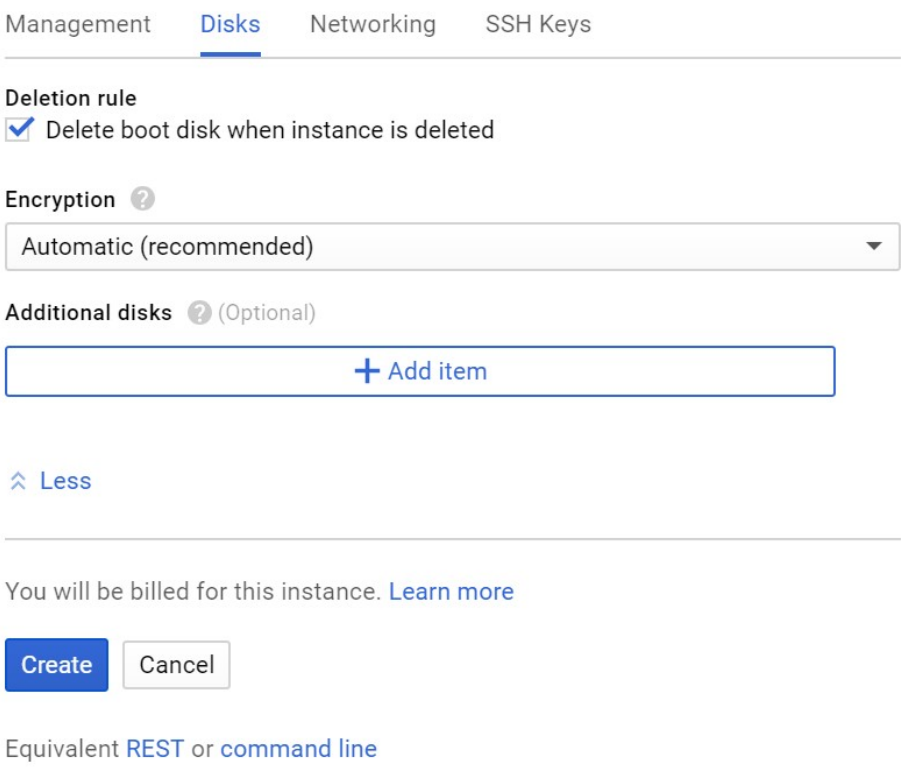
   f) In **Firewall**, select the options as appropriate.
   g) In **Project access**, allow API access as appropriate.
   h) In **Management**, ensure that the tag provided is the same as the one provided while creating a firewall rule. This ensures port mapping happens correctly.

FIGURE 135 Management Tab



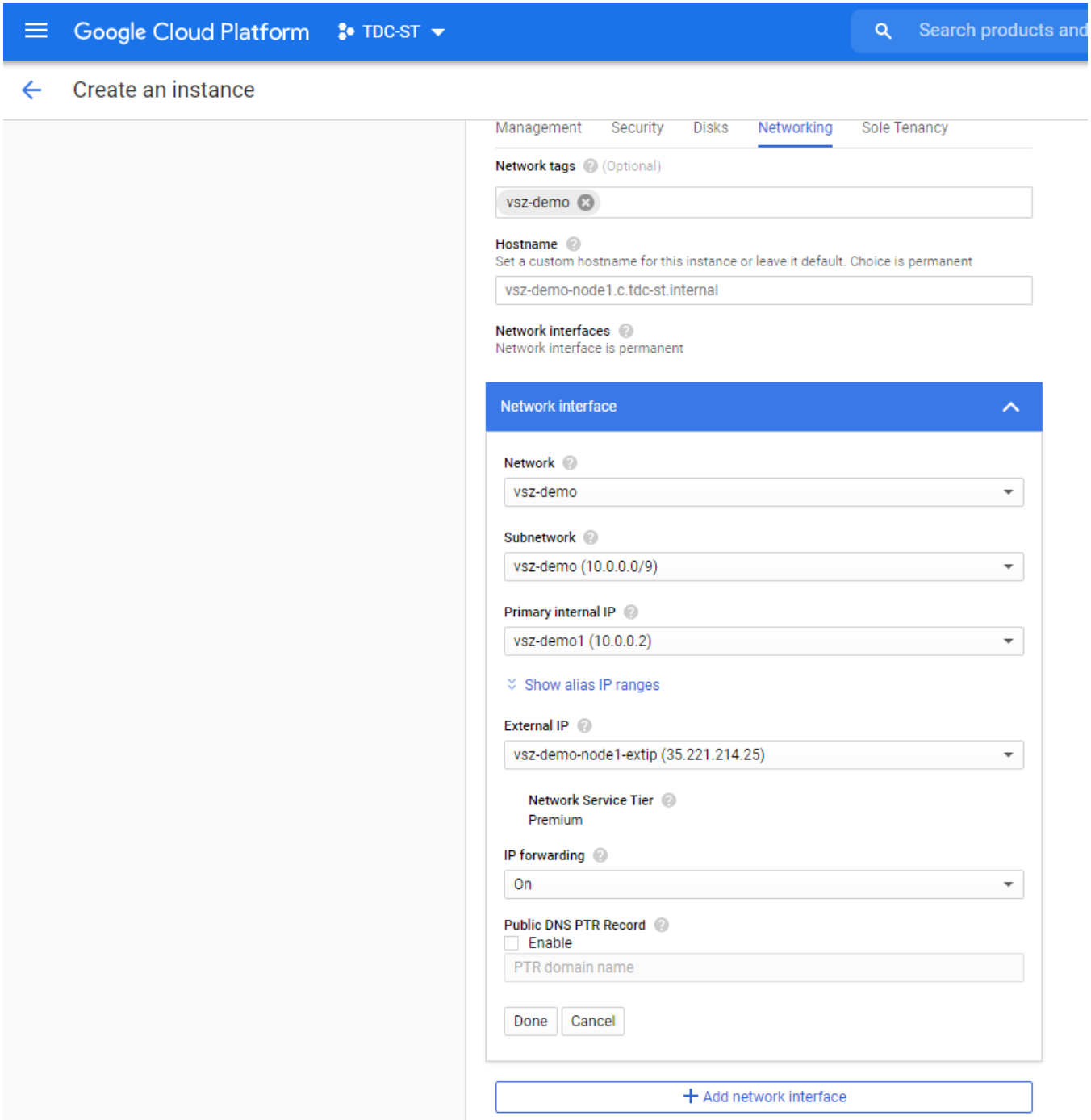
i) In **Disk**, select the options as appropriate.

FIGURE 136 VM Disk Configuration



j) In **Networking**, select the external options as per the following table.

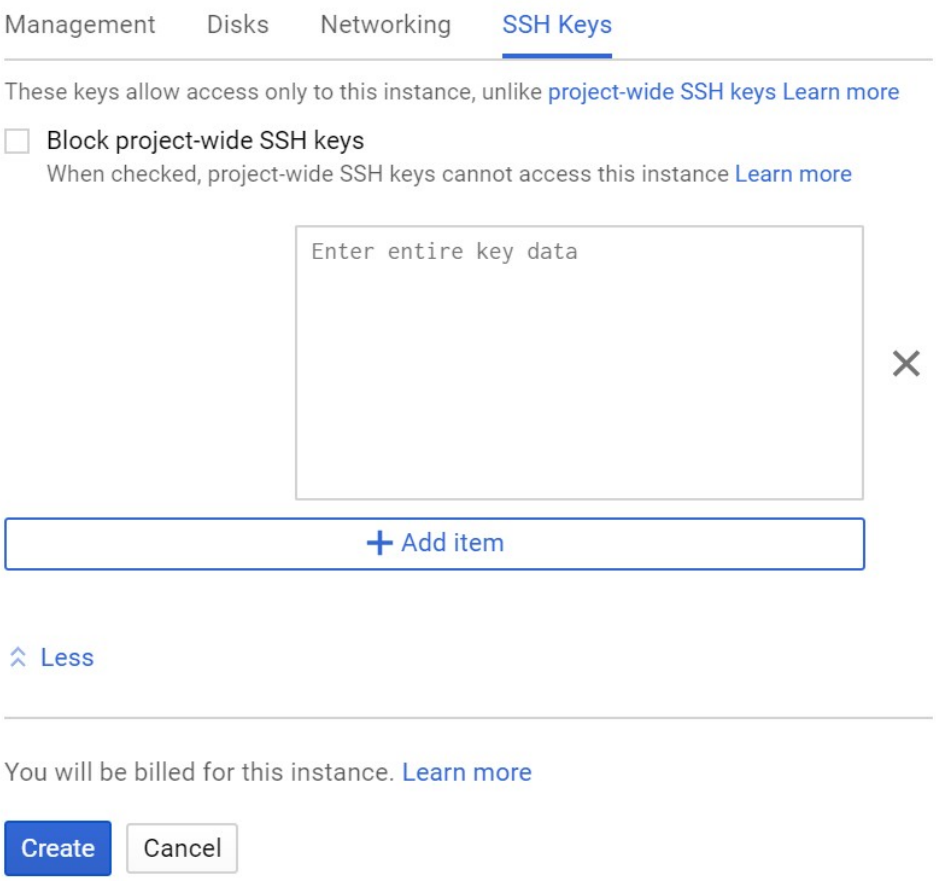
FIGURE 137 Networking



External IP Options	Description
Ephemeral	The VM is assigned a dynamic public IP address
None	The VM instance is not assigned an external IP address
New static IP address	The VM is assigned a static public IP address

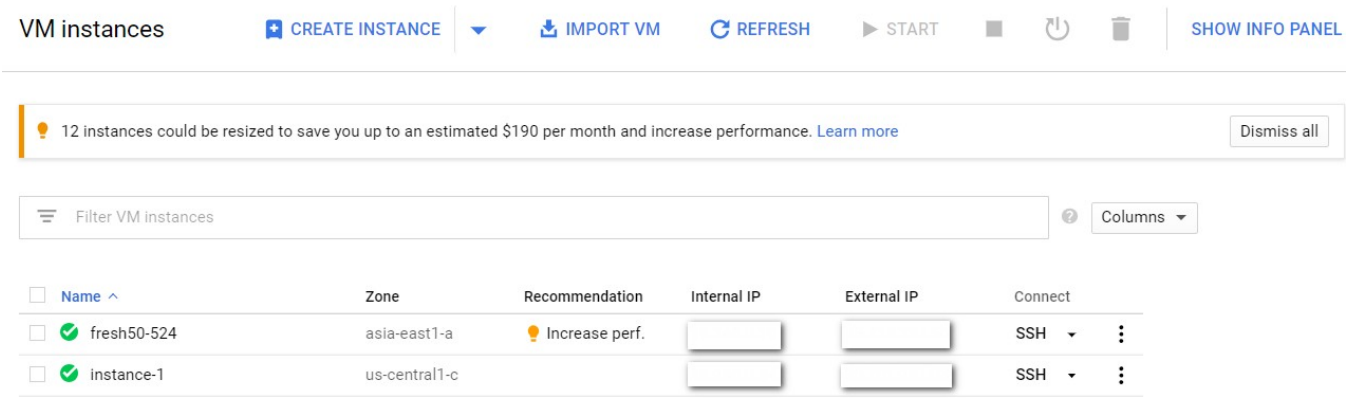
k) In **SSH Keys**, select the options as appropriate.

FIGURE 138 SSH Keys



l) Click **Create**. The **VM instances** page appears listing the new VM that is created.

FIGURE 139 The new VM appears on the list of VMs



You have completed creating a virtual machine instance.

Installing vSZ on Amazon Web Services

Installing AWS CLI

Public cloud solution resource requirement

- CPU or Memory: Minimum requirement of c4, c5 types and above.

  NOTE
  Does not support a1, t2, t3 types

- Storage Requirement (Disk Storage): Minimum requirement of SSD - GP2 150 GB above

  NOTE
  Any CPU with credit limitation type cannot support.
  Select the proper disk size to run vSZ since disk sizes may have different disk IO performance in each cloud platform.

Ensure that you have created an account with AWS and have the login details for the same.

NOTE
All the commands must be run on the host computer.

1. Install pip by running the command

   ```
   # curl -O https://bootstrap.pypa.io/get-pip.py
   # sudo python27 get-pip.py
   ```

2. Install AWS CLI using pip:**# pip install**
3. Test the installation by using the command: **# aws help**
4. To set up AWS CLI you need to get your access and secret key identifier. Follow the instructions and find your identifier keys.
5. Use the following command to configure CLI:

   ```
   # aws configure
   AWS Access Key ID [None]: xxx
   AWS Secret Access Key [None]: xxx
   Default region name [None]: us-west-2
   Default output format [None]: json
   ```

6. The default region should be the same as the bucket region. Refer to Table for the mapping details. In addition refer to you can also refer to latest version.

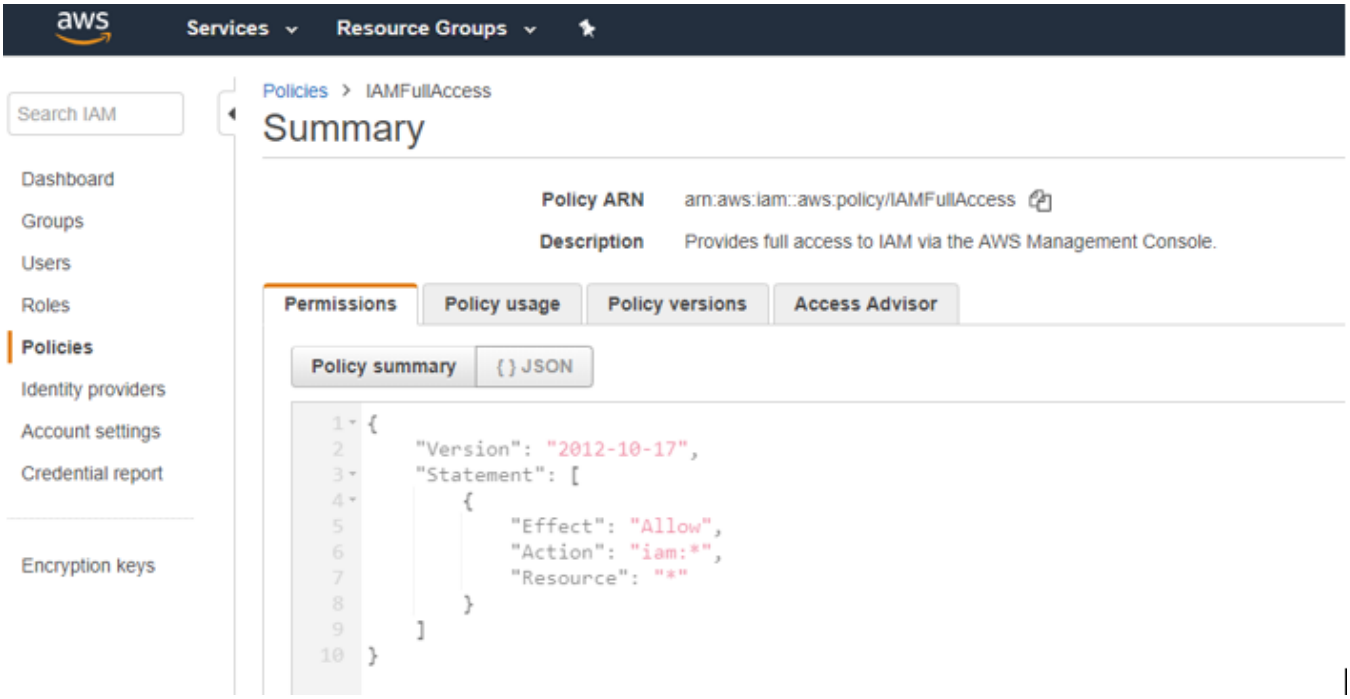
Region Name	Region
US East (Ohio)	us-east-2
US East (N. Virginia)	us-east-1
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Osaka-Local)	ap-northeast-3
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
China (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1
EU (Frankfurt)	eu-central-1
EU (Ireland)	eu-west-1
EU (London)	eu-west-2
EU (Paris)	eu-west-3
EU (Stockholm)	eu-north-1
South America (São Paulo)	sa-east-1
AWS GovCloud (US-East)	us-gov-east-1
AWS GovCloud (US)	us-gov-west-1

Creating a VM Import Service Role

1. In the AWS web interface navigate to **AWS dashboard** > **Identity & Access Management**.

2. Check your account permission by navigating to **Users** > **select your Username** > **Permissions**. Your account should have the permission - *IAMFullAccess*.

FIGURE 140 Account Permission



3. Create a JSON file called trust-policy.json using the following commands:

```
{   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"",
         "Effect":"Allow",
         "Principal":{            "Service":"vmie.amazonaws.com"
         },
         "Action":"sts:AssumeRole",
         "Condition":{
            "StringEquals":{
               "sts:ExternalId":"vmimport"
            }
         }
      }
   ]
}
```

4. Use the following command to create a role. Specify the name as vmimport and give the option VM Import/Export access.

```
# aws iam create-role --role-name vmimport --assume-role-policy-document file://trust-policy.json
```

5. Create a policy for the service role by creating a JSON file called role-policy.json using the following commands. Replace the bucket name with the storage bucket name that you created.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource":[
            "arn:aws:s3:::<bucket-name>"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3:::<bucket-name>/*"
         ]
      }
```

6. Run the following command to attach the policy to the service role created. `# aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document file://role-policy.json`

Installing vSZ on AWS

Follow the steps to install vSZ using the AWS web user interface.

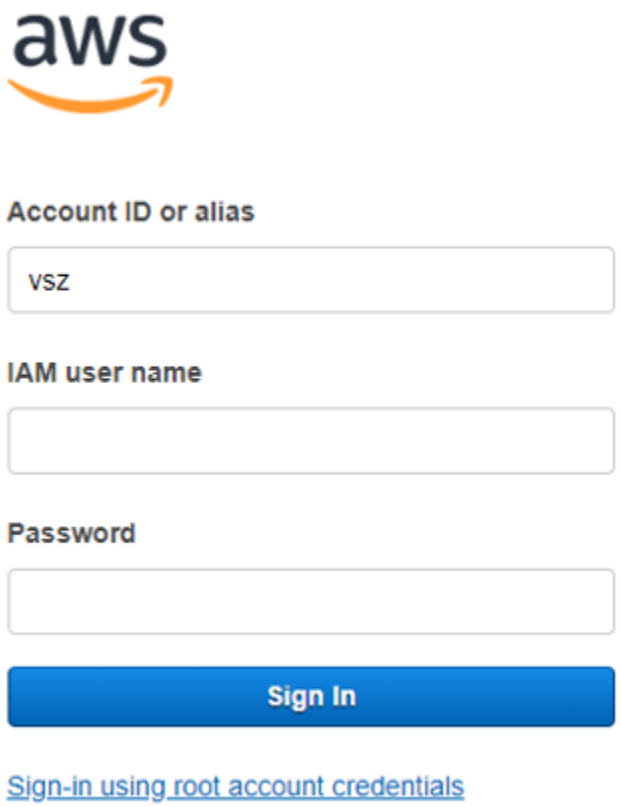
Logging into AWS

Follow these steps to login to the AWS site.

1. Click https://aws.amazon.com, to access the **Amazon Web Services** website.

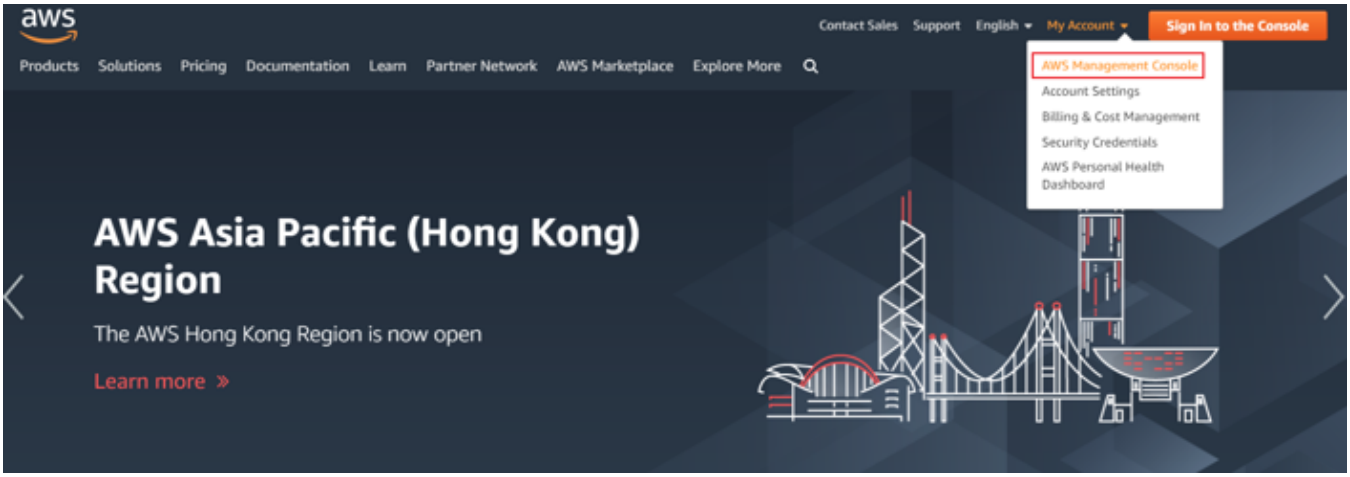
2. Login with your user credentials of user name and password.

FIGURE 141 Login with user credentials



3. Select **My Account** > **AWS Management Console** as shown.

FIGURE 142 AWS management console

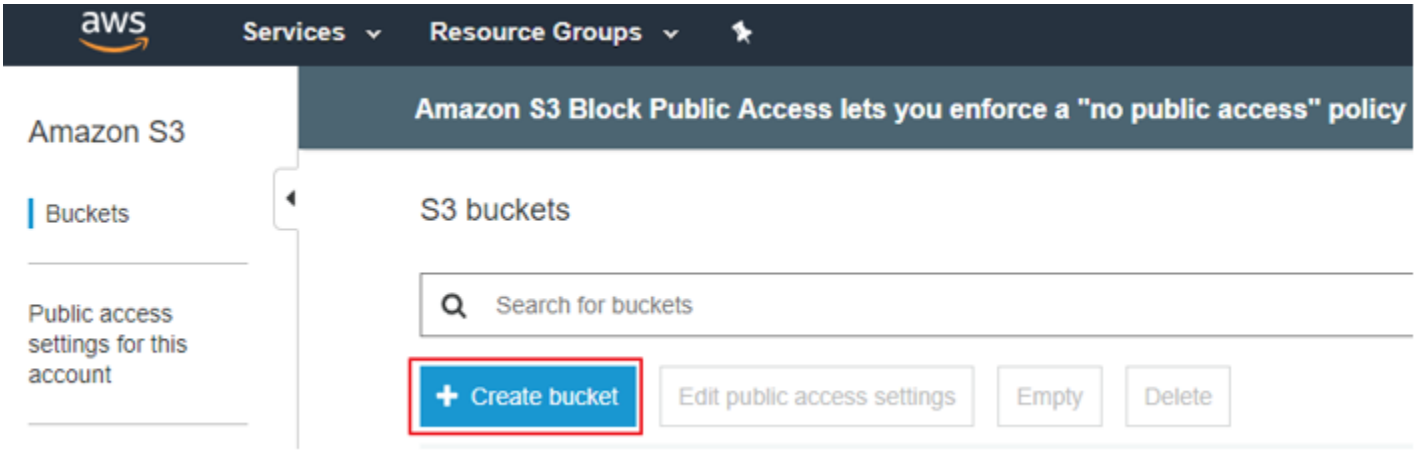


Creating a Storage Bucket

Create storage for the objects you create. Follow these steps to create storage.

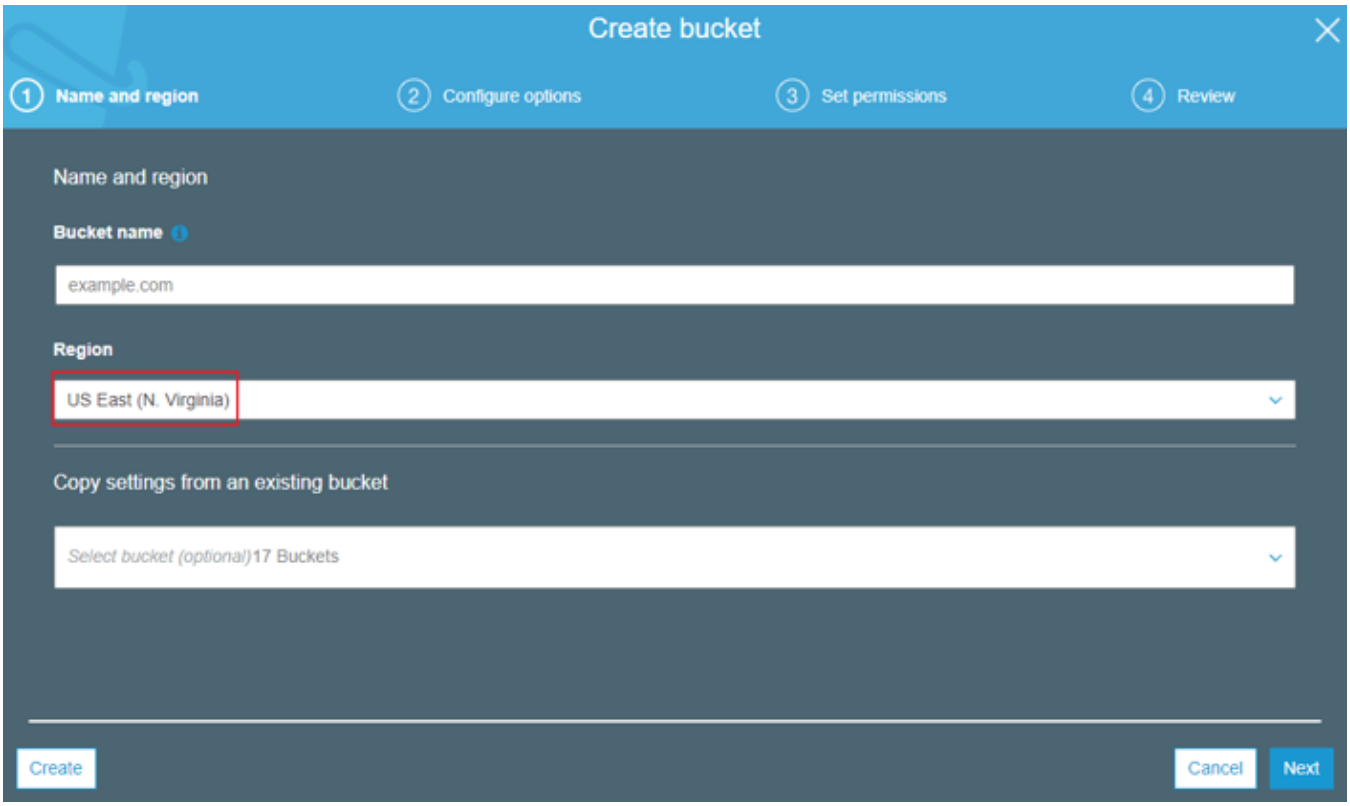
1. Navigate to **Amazon Web Services** > **Storage and Content Delivery** > **S3**, click **Create Bucket** as shown.

   FIGURE 143 Create Bucket



2. Type the name of the storage bucket and select a suitable regional endpoint to reduce data latency.

   FIGURE 144 Selecting regional endpoint



3. Click **Create**. The storage bucket you created is listed in the browser.
4. Check the storage bucket has been created.

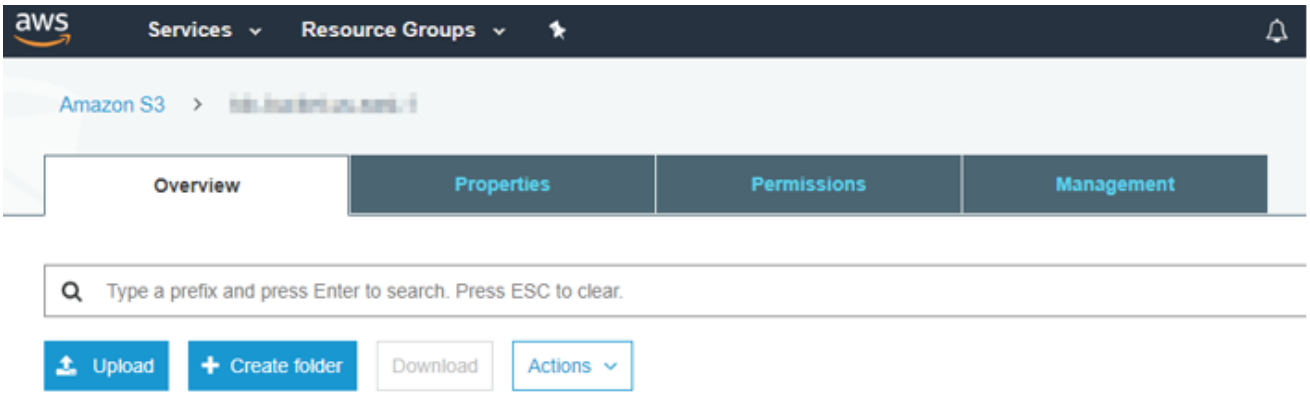
Uploading vSZ Image to a Storage

Follow these steps to upload a vSZ image to the storage bucket you created.

1. Select the storage bucket to upload the vSZ image.

2. Click **Upload** as shown.

FIGURE 145 Selecting the Storage

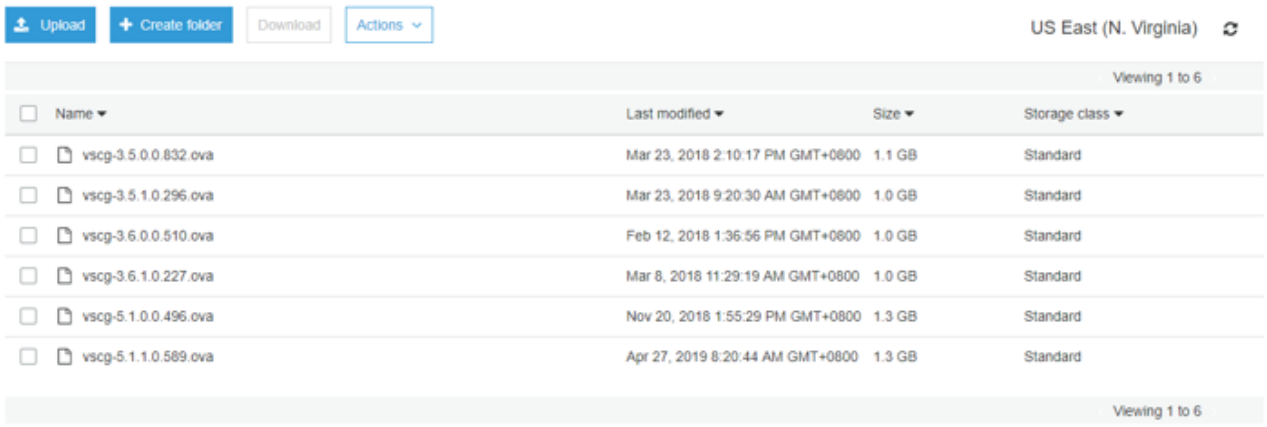


3. Browse to the location of the vSZ image and select vSZ image file.

   Only images with file-type *.raw or .ova or vmdk can be selected.

4. Click **Start Upload** to upload the file. The upload process is displayed.
5. The image is listed in the storage bucket after the image is uploaded.

FIGURE 146 vSZ Image Uploaded to Storage Bucket



NOTE
The vSZ image should be in the Bucket, which has Region information. Example: **Test_bucket**

AWS Service Policy

VM Import uses a role in your AWS account to perform certain operations (for example, downloading disk images from an Amazon S3 bucket). You must create a role with the name vmimport with the following policy and trusted entities.

1. Install the AWS CLI by following the instructions at http://docs.aws.amazon.com/cli/latest/userguide/installing.html
2. Enter the following command in the AWS CLI **#sudo pip install awscli**.

3. Get the access key for the AWS CLI by following the instructions on the AWS website.
4. Add the access key details to the AWS CLI using the following commands

```
# aws
        configureAWS Access Key ID [None]:
        AWS Secret Access Key
        [None]: Default region name [None]:
        us-west-2Default output format
        [None]: json
```

5. Create a file named role-policy.json with the following policy:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetBucketLocation"
         ],
         "Resource":[
            "arn:aws:s3:::<disk-image-file-bucket>"
         ]
      },
      {
        "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3:::<disk-image-file-bucket>/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:ModifySnapshotAttribute",
            "ec2:CopySnapshot",
            "ec2:RegisterImage",
            "ec2:Describe*"
         ],
         "Resource":"*"
      }
   ]
}
```

6. Replace <*disk-image-file-bucket*> with the appropriate Amazon S3 bucket where the disk files are stored. Run the following command to attach the policy to the role created above:
7. Replace <*disk-image-file-bucket*> with the appropriate Amazon S3 bucket where the disk files are stored. Run the following command to attach the policy to the role created above **aws iam put-role-policy --role-name vmimport --policy-name vsz34-policy --policy-document file://role-policy.json**

Importing the vSZ Image

Follow these steps to import the vSZ image into AWS shared AMI.

1. Create a JSON file called import.json using the following commands. Replace the bucket name with the storage bucket name that you created. In this example, the vSZ image file name is **vscg-3.4.0.0.750.ova**.

```
{
    "Description": "Import vSZ",
    "DiskContainers": [
        {
            "Description": "vSZ 3.4.0.0.750",
            "UserBucket":{
                "S3Bucket": "<bucket-name>",
                "S3Key": "vscg-3.4.0.0.750.ova"
            }
        }
    ]
}
```

2. Run the following command to attach the policy to the role created. **# aws ec2 import-image --cli-input-json file://import.json**
3. The system displays the below response.

```
{
    "Status": "active",
    "Description": "Import vSZ",
    "Progress": "2",
    "SnapshotDetails": [
        {
            "UserBucket": {
                "S3Bucket": "<bucket-name>",                "S3Key": "vscg-3.4.0.0.750.ova"
            },
            "DiskImageSize": 0.0
        }
    ],
    "StatusMessage": "pending",
    "ImportTaskId": "import-ami-ffgof9w1"
}
```

4. Check the status of the import vSZ image by running the following command. Ensure to enter the correct import task identifier.**# aws ec2 describe-import-image-tasks --import-task-ids "import-ami-ffgof9w1"**
5. You will see the following converting status response. Check the status until the converting is complete. The estimated time for conversion is 30 minutes.

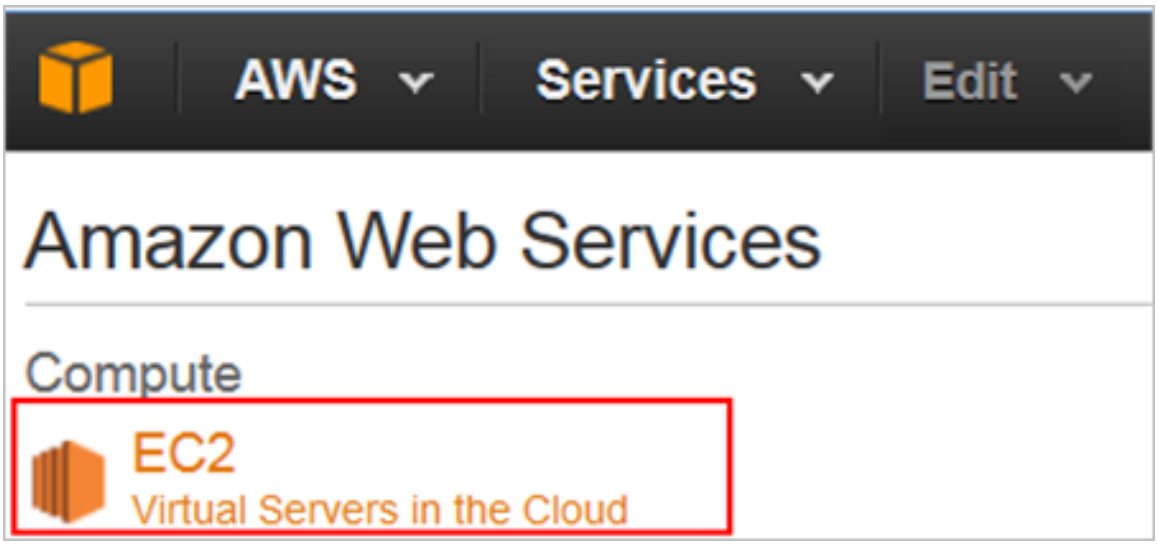
```
{
    "ImportImageTasks": [
        {
            "Status": "active",
            "Description": "vSZ test",
            "Progress": "28",
            "SnapshotDetails": [
                {
                    "UserBucket": {
                        "S3Bucket": "<bucket-name>",
                        "S3Key": "vscg-3.4.0.0.750.ova"
                    },
                    "DiskImageSize": 964430848.0,
                    "Format": "VMDK"
                }
            ],
            "StatusMessage": "converting",
            "ImportTaskId": "import-ami-ffgof9w1"
        }
    ]
}
```

Creating the vSZ Instance

Follow these steps to create a vSZ instance on AWS.

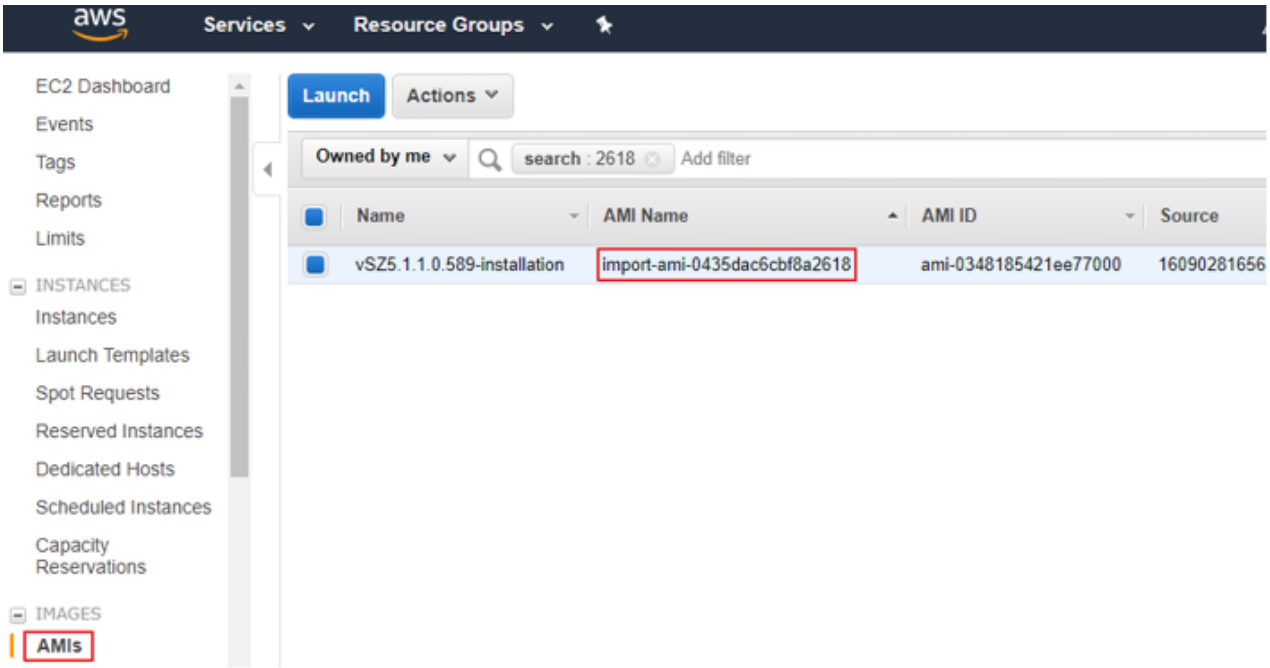
1. From **Amazon Web Service**, click **Compute** > **EC2**.

FIGURE 147 Select EC2



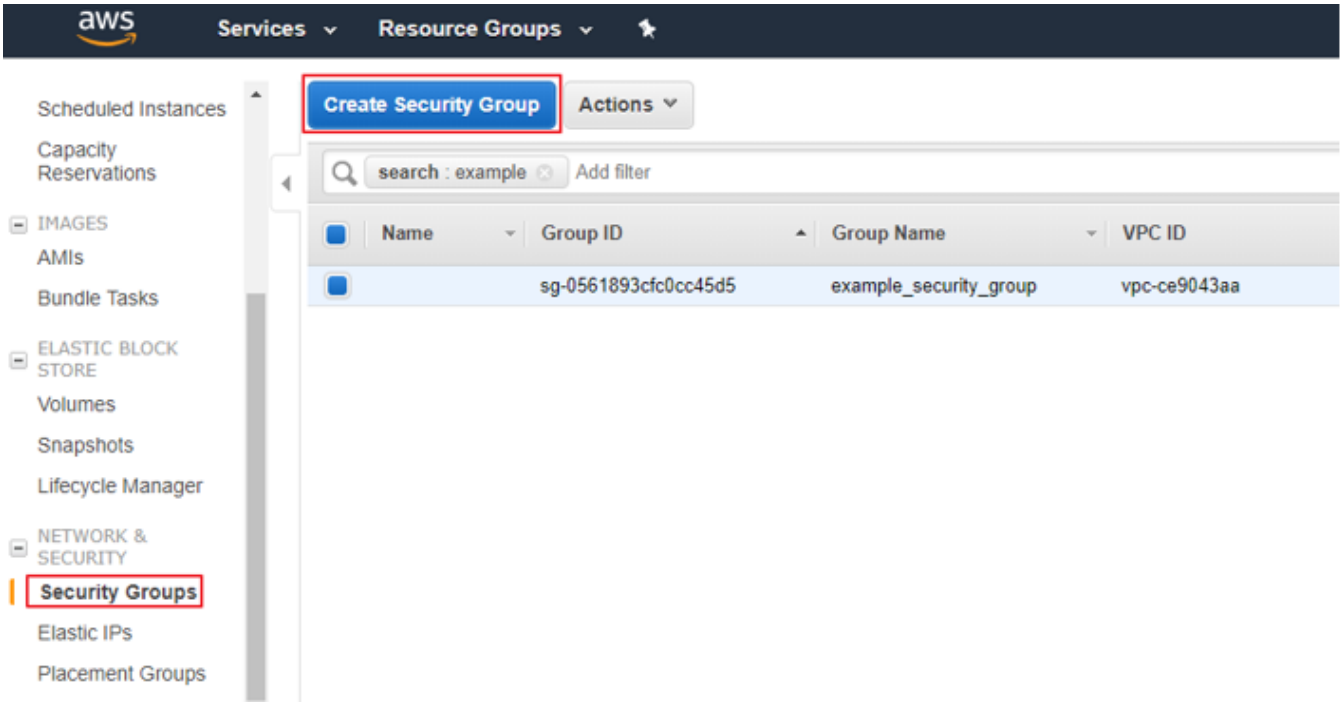
2. Navigate to **Images** > **AMIs** to ensure that the imported **Amazon Machine Image (AMI)** exists. In this example the AMI file is **import-ami-ffgof9w1**.

FIGURE 148 Select AMI



3. Navigate to **Network & Security** > **Security Groups** > **Create Security Group**. Security group acts as a virtual firewall that controls the traffic for one or more instances.

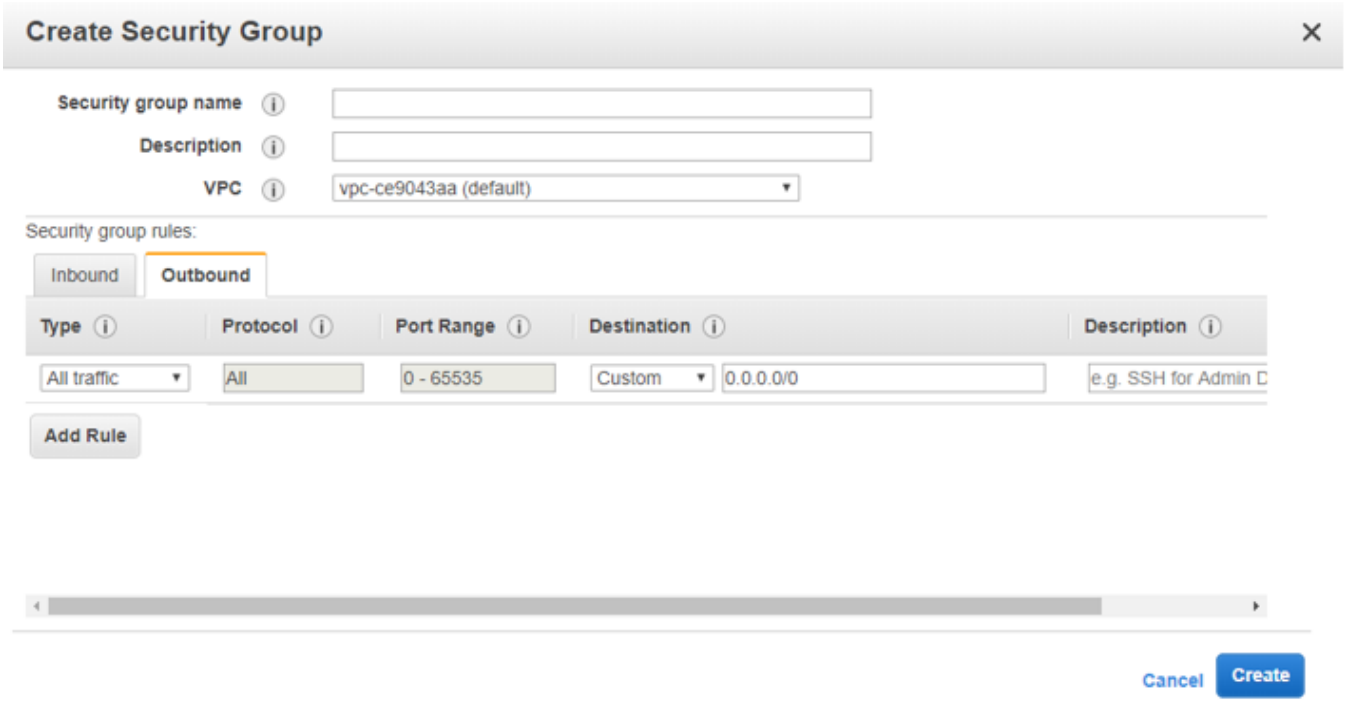
FIGURE 149 Create Security Group



4. Define the setup group name, description, ports and the firewall rule. The table lists the common service ports. For more information, see Ports to open for AP-vSZ communication.

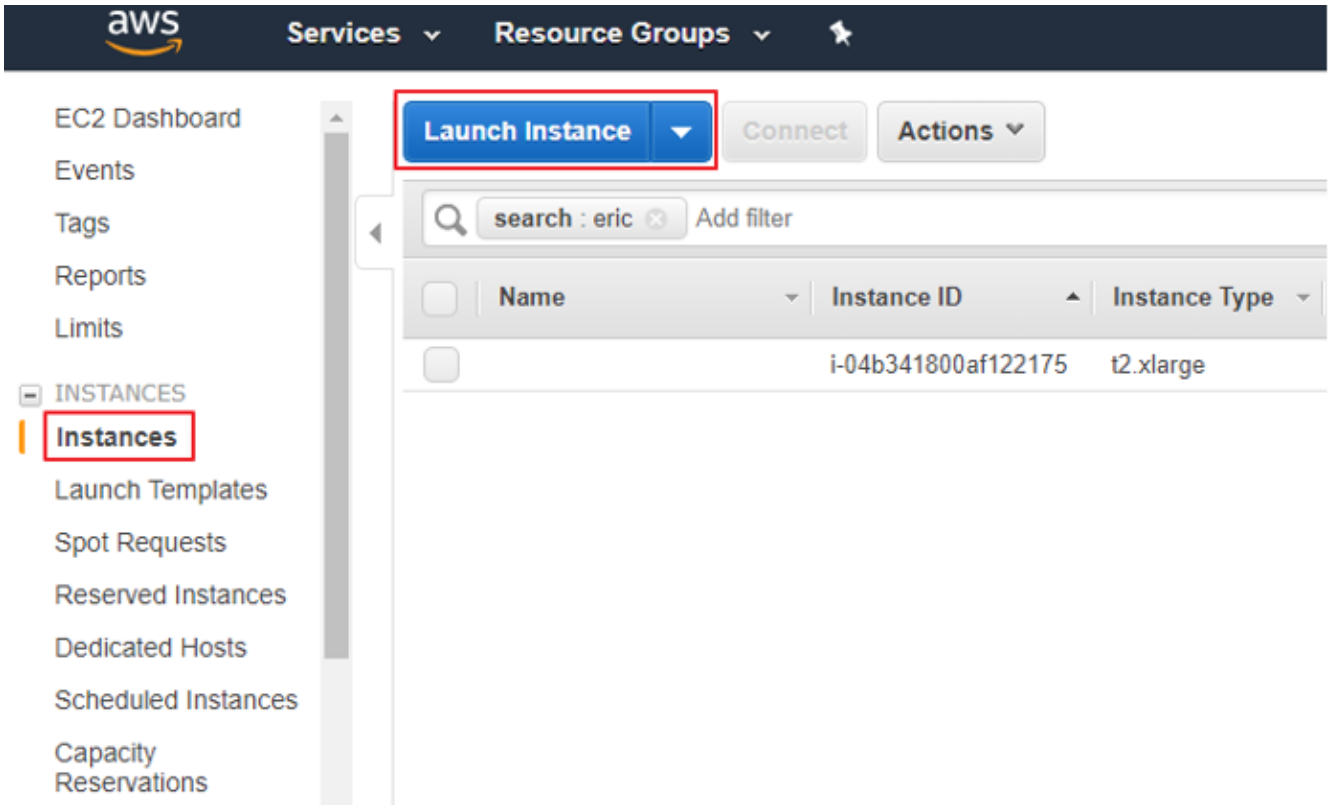
Port Number	Description
UDP	
161	SNMP
12223	ZD AP forward update using FTP (control connection)
TCP	
21	ZD AP forward update using FTP (control connection)
22	AP SSH
91	AP forward update using HTTP
443	Allows AP get SSH private key and do AP FW udpate via HTTPs
7443	Public API
8022	SSH for management (mgmt-acl is enabled on 1 nic vSZ)
8080	vSZ setup wizard using the web user interface (User will be redirected to the port 8443)
8443	vSZ web user interface
8090, 8099	WISPr for non-web-proxy user equipment
8100	WISPr for web-proxy user equipment
9998	Tomcat for WISPr (internal WISPr portal uses the port 9998)
9080, 9443	Northbound API (NBI)
16384-65000	ZD AP forward update using FTP (data connection)

FIGURE 150 Define Security Group



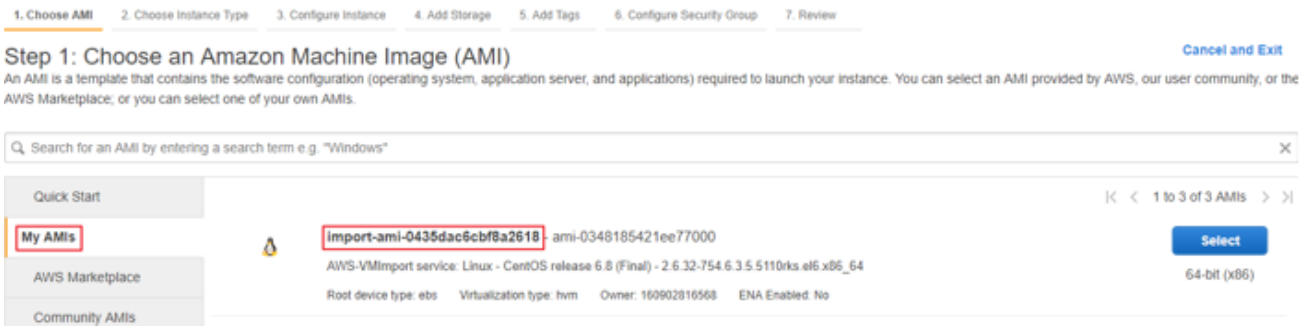
5. Navigate to **Instances** and click on **Launch Instances**. Follow these steps.
   a) Launch Instance

FIGURE 151 Launch instances



   b) Navigate to **My AMIs** and choose the **Amazon Machine Image (AMI)** that you imported previously.

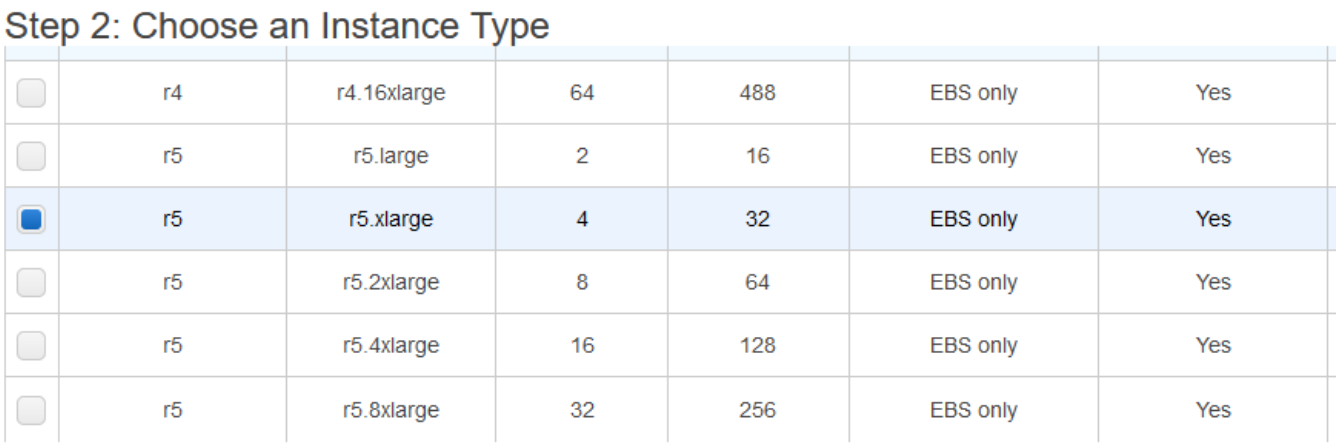
FIGURE 152 Choose the imported AMI



   c) Click **Next**.
   d) Choose a suitable instance type. In this example the instance type is *m4.xlarge*. Based on the number of APs and client counts, select the instance type to fit the recommended system resources.

   The minimum memory and CPU requirements have changed in this release. You may need to upgrade your infrastructure before upgrading. Please read carefully. This is the minimum requirement recommended. Refer to Table 5 and Table 6 in the chapter Preparing to Install the vSZ.

FIGURE 153 Choose the instance type

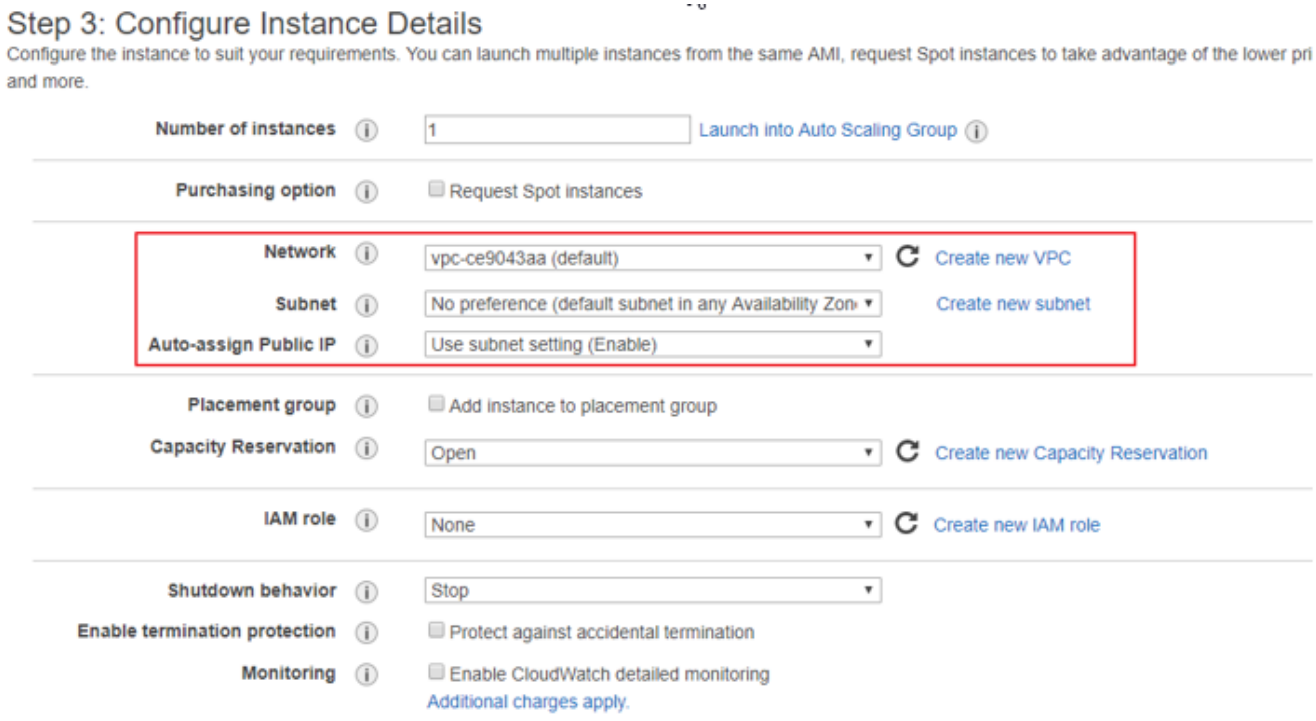


e) Click **Next**.

f) Select the required network, subnet, and private IP address.

The private IP address cannot be changed once the vSZ image is launched.

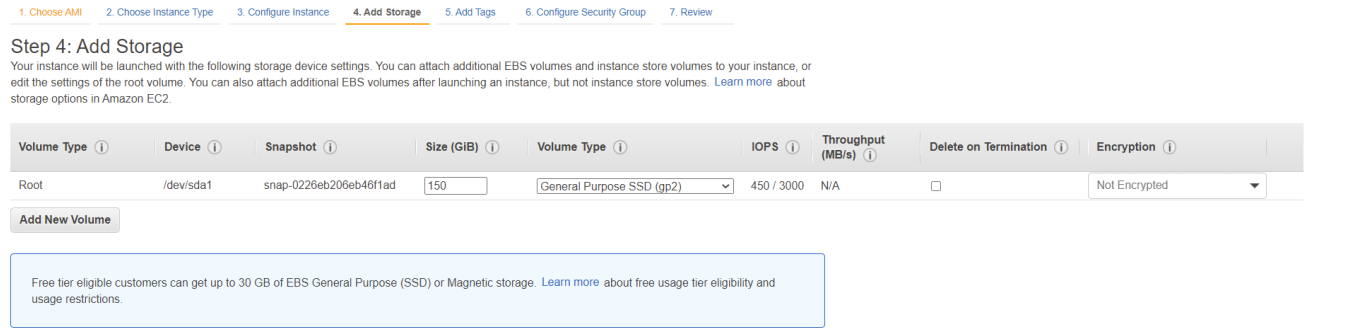
FIGURE 154 Configure the instance



g) Click **Next**.

h) Change the size of storage as required.

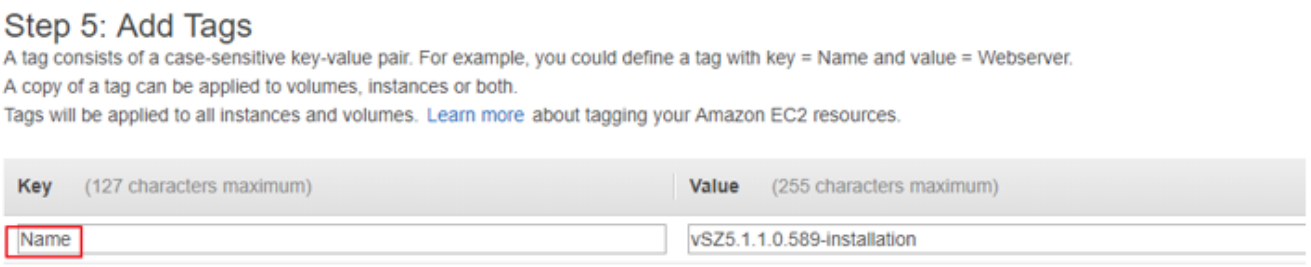
FIGURE 155 Change the storage size



i) Click **Next**.

j) Specify the vSZ instance by giving it a name.

FIGURE 156 Specify the vSZ instance



k) Click **Next**.

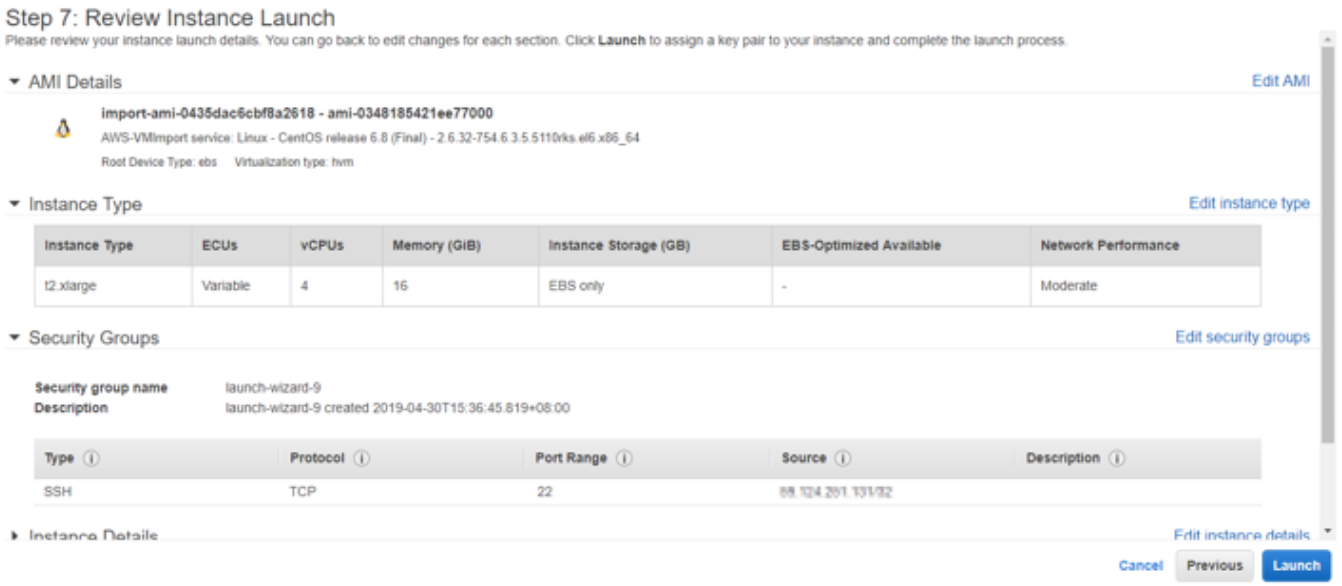
l) Create a new security group or select an existing group. Configure the rules if required.

FIGURE 157 Specify the security group

m) Click **Next**.

n) Review the configuration settings.

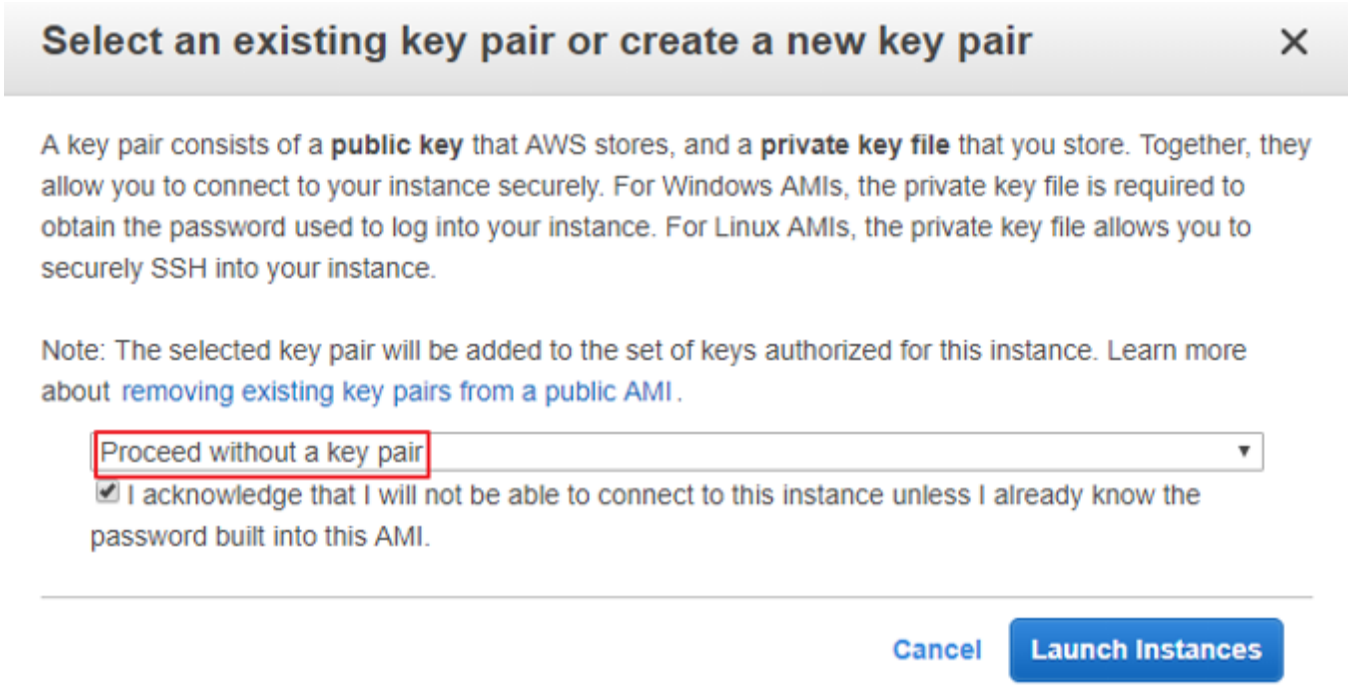
FIGURE 158 Review the configuration settings



o) Click **Launch**

p) Select the **Proceed without a key pair** for vSZ instance.

FIGURE 159 Select existing key pair



q) Verify that the vSZ instance is running. Connect the vSZ instance with the selected key pair using the SSH interface.

Configuring AWS for a vSZ Instance

Follow these steps to configure AWS for creating and launching a vSZ instance.

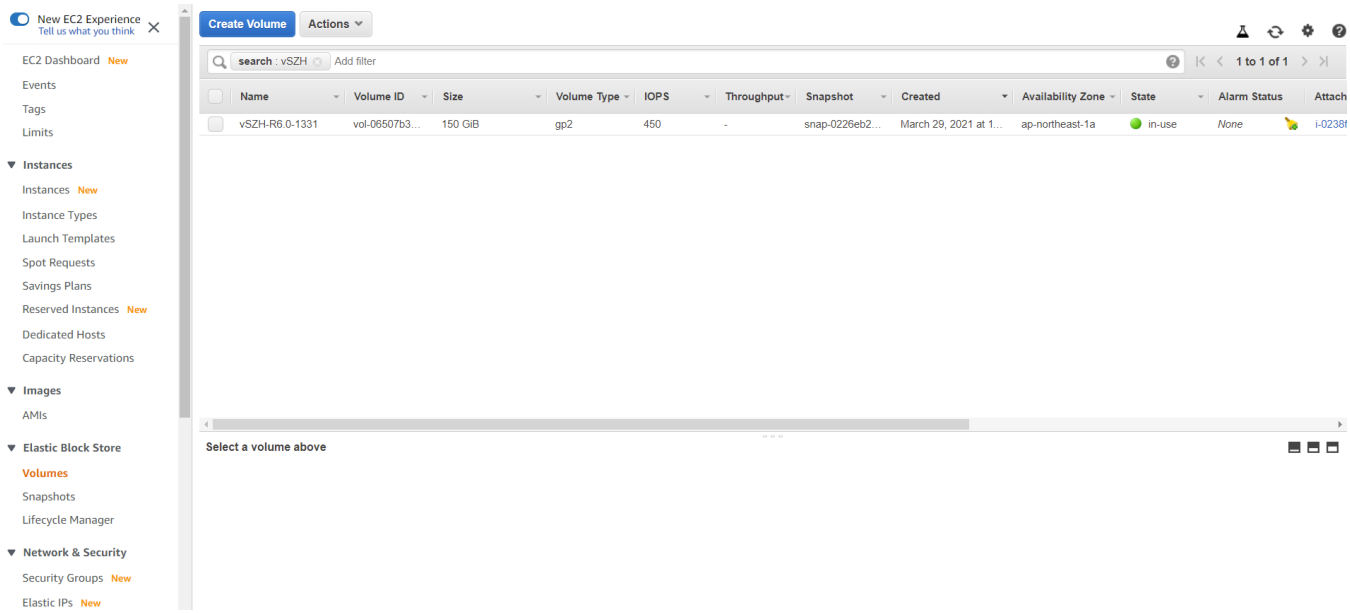
NOTE
When vSZ nodes are on two different AWS zones, ensure that the VPC peering is configured on AWS.

Attach a New Disk Volume

Follow these steps to add a new disk volume.

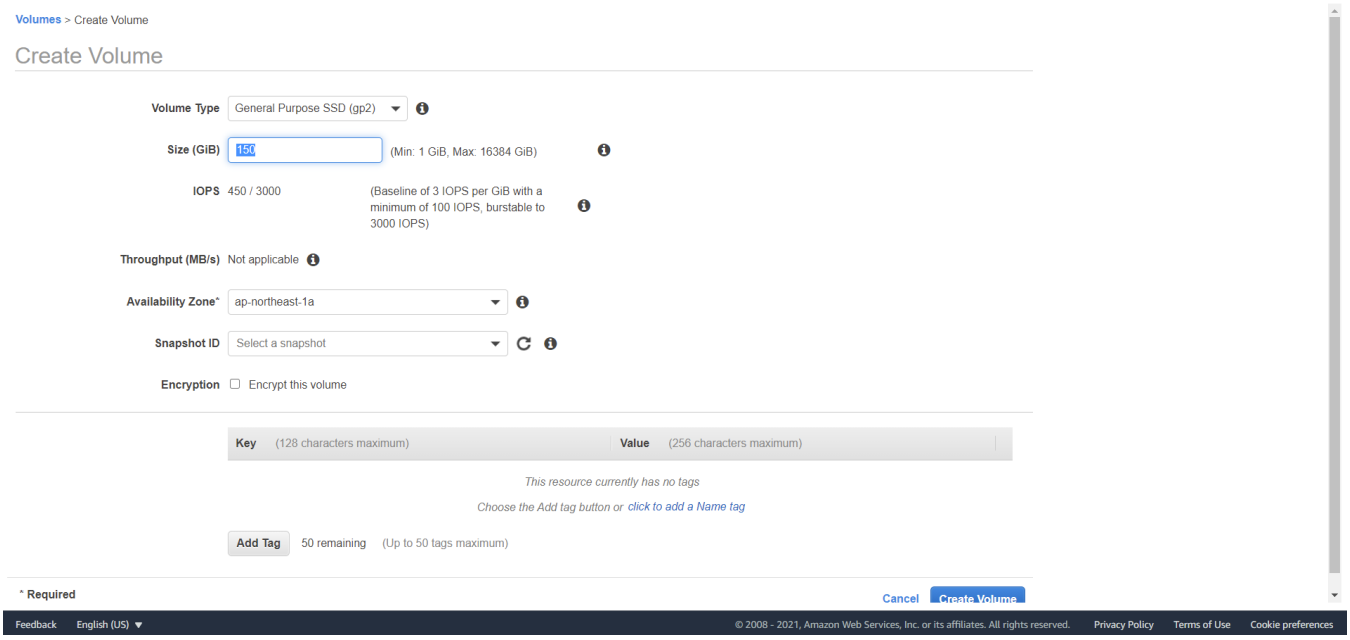
1. Navigate to **EC2 Dashboard** > **Elastic Block Store** > **Volumes** and click **Create Volume** as shown.

FIGURE 160 Create Volume



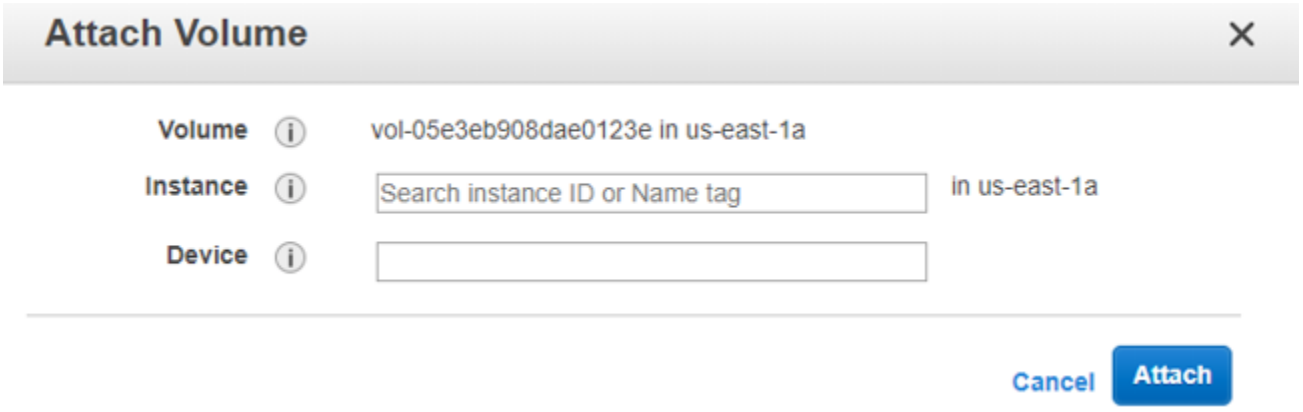
2. Enter the required disk type, size and availability zone.

FIGURE 161 Create Volume



3. Click **Create**.
4. Right click on the newly created disk and select **Attach Volume**. Enter the instance identifier and the desired device name.

FIGURE 162 Attach Volume



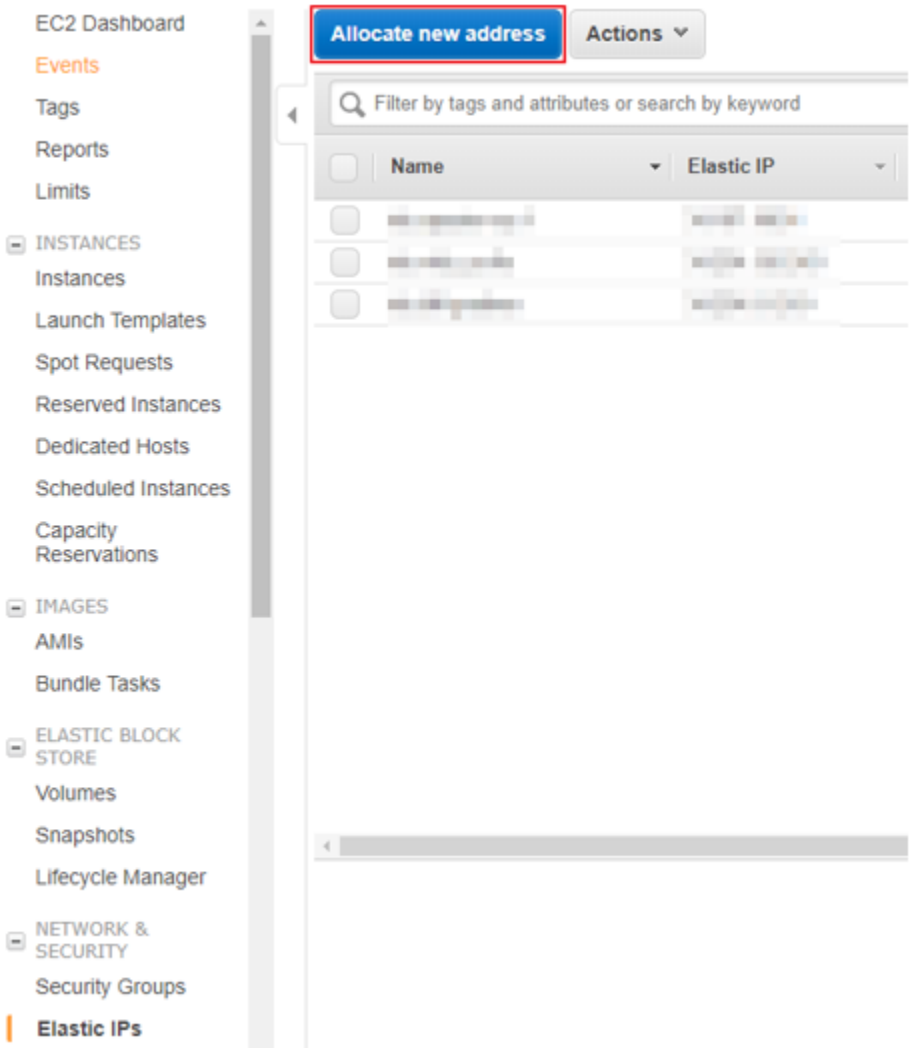
5. Click **Attach**.

Allocate a Public IP Address

Follow these steps to allocate a public IP address.

1. Navigate to **EC2 Dashboard** > **Network & Security** > **Elastic IPs.** Click **Allocate New Address** as shown.

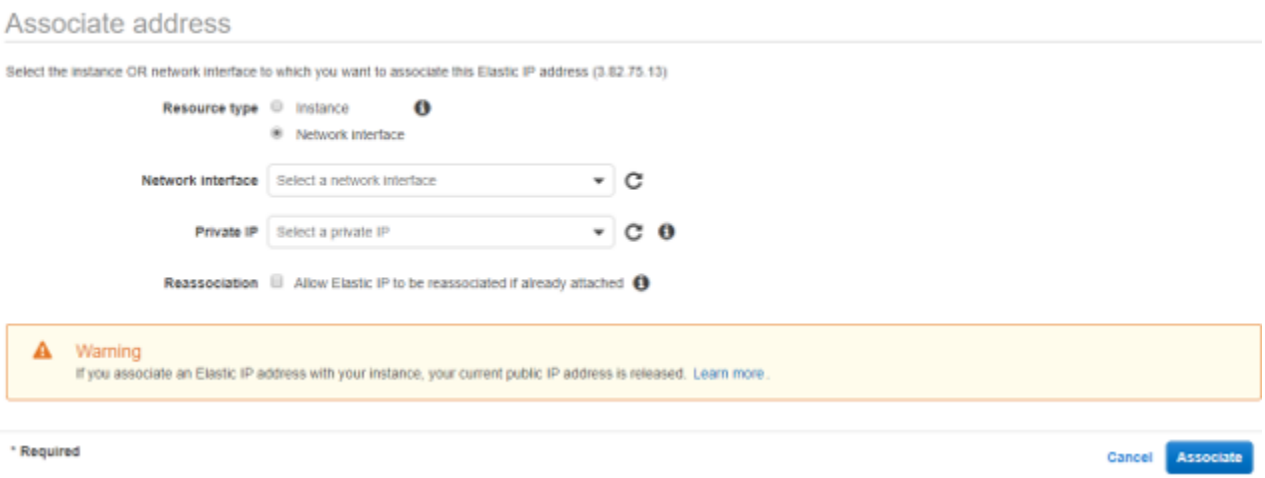
   FIGURE 163 Allocate New IP Address



2. Click **Create**.

3. Right click on the newly created IP address and select **Associate Address**. Enter the instance identifier or network interface and the desired device name.

   FIGURE 164 Associate Address



4. Click **Associate**.

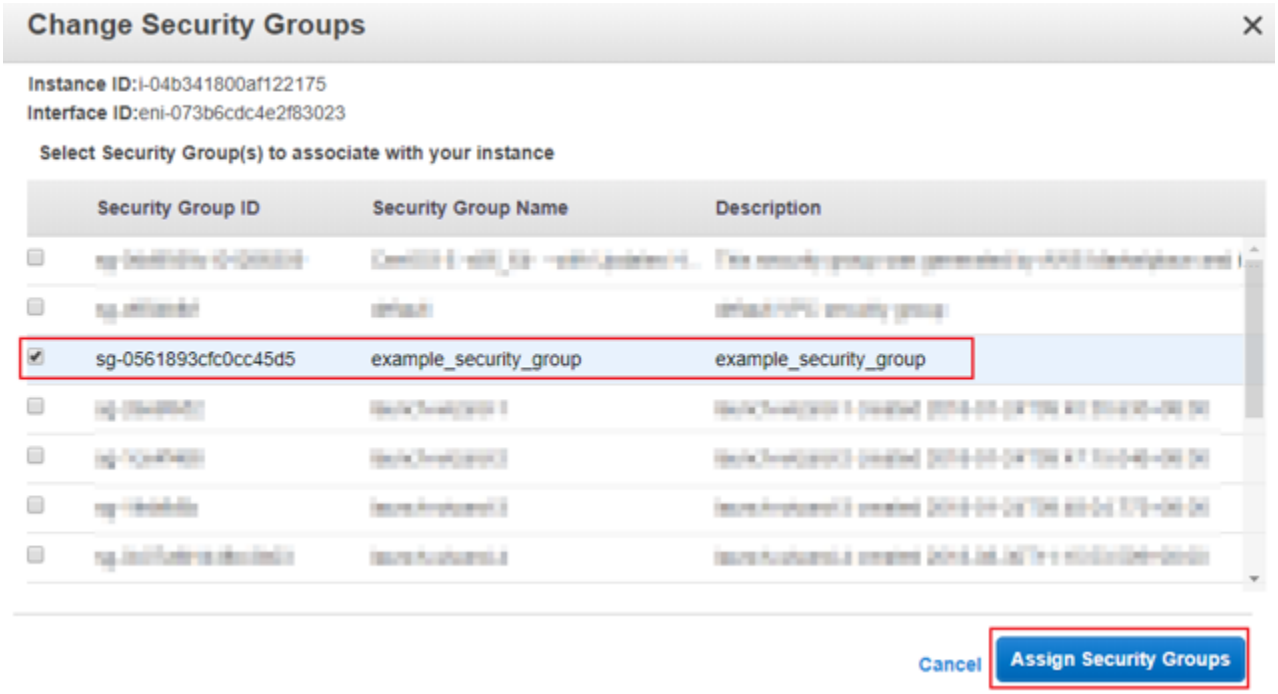
Change Security Group

Follow these steps to change the security group.

1. Navigate to Instances and right click the target instance.
2. Select **Network** > **Change Security Group**.

3. Select the security groups.

FIGURE 165 Allocate New IP Address



4. Click **Assign Security Groups**.

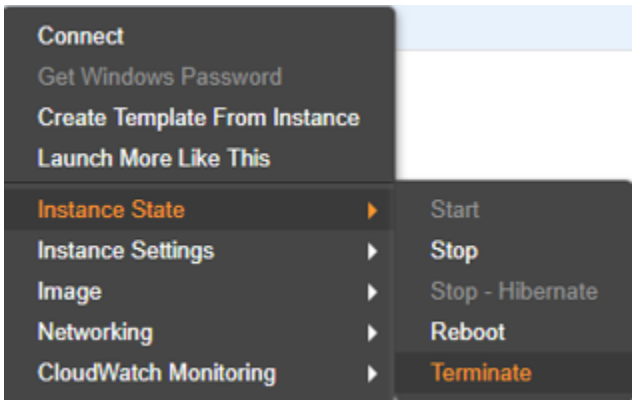
Deleting a vSZ Instance

Follow these steps to delete a vSZ instance on AWS.

1. Navigate to Instances and right click to select the vSZ instance that you want to delete.

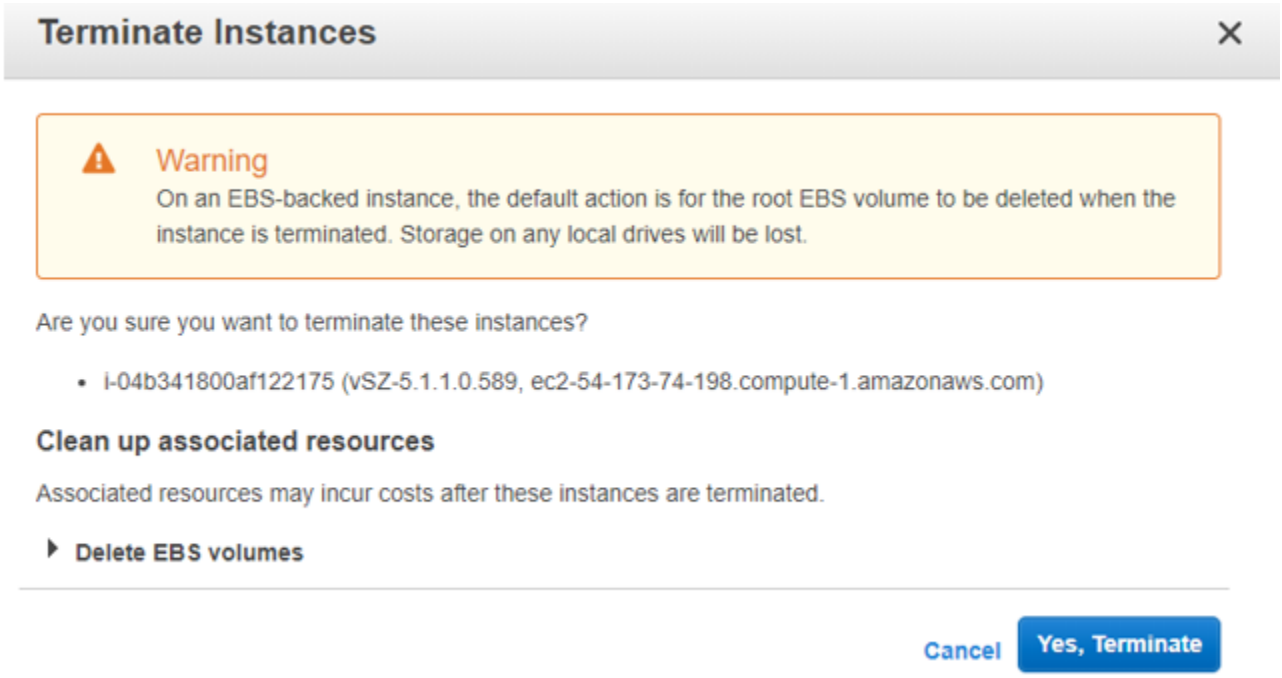
2. Select **Instance State** > **Terminate**.

FIGURE 166 Select terminate



3. Confirm deletion of the vSZ instance by clicking on **Yes, Terminate**. The vSZ instance is deleted from AWS.

FIGURE 167 Confirm termination of vSZ instance



Configuring the Virtual Machine Interfaces

Configuring the Virtual Machine Interfaces

The vSZ comes with the option to operate with either one (1) network interface or three (3) network interfaces. Therefore the procedure for setting up the vSZ interface depends on the number of interfaces that it has.

Follow the procedure below that corresponds to the number of interfaces that the vSZ you are installing has:

- Setting Up the vSZ with One Interface on page 185
- Setting Up the vSZ with Three Interfaces on page 198

NOTE
By default, the VMWare ESXi package comes with three network interfaces. If you want to deploy the vSZ with only one interface, you can edit the virtual machine settings to remove the extra interfaces. The KVM package, on the other hand, comes with a single interface. If you want to deploy the vSZ with three interfaces, edit the virtual machine settings to create two additional interfaces.

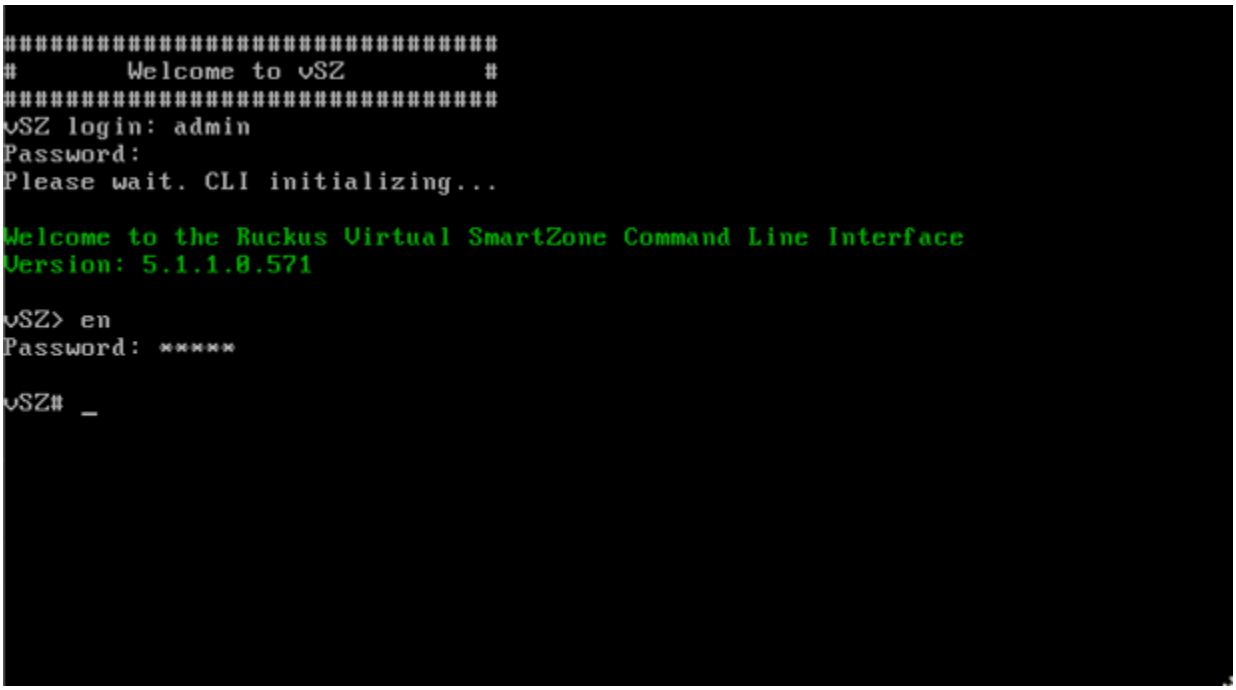
Setting Up the vSZ with One Interface

Follow these steps to set up the vSZ with a single network interface

1. Log on to the console using; **User name: admin Password**: **admin**
2. At the **vSZ>** prompt, enter **en** to enable privileged mode.

3. At the **Password** prompt, enter **admin**. The **vSZ#** prompt appears.

   FIGURE 168 At the vSZ> prompt, enter setup

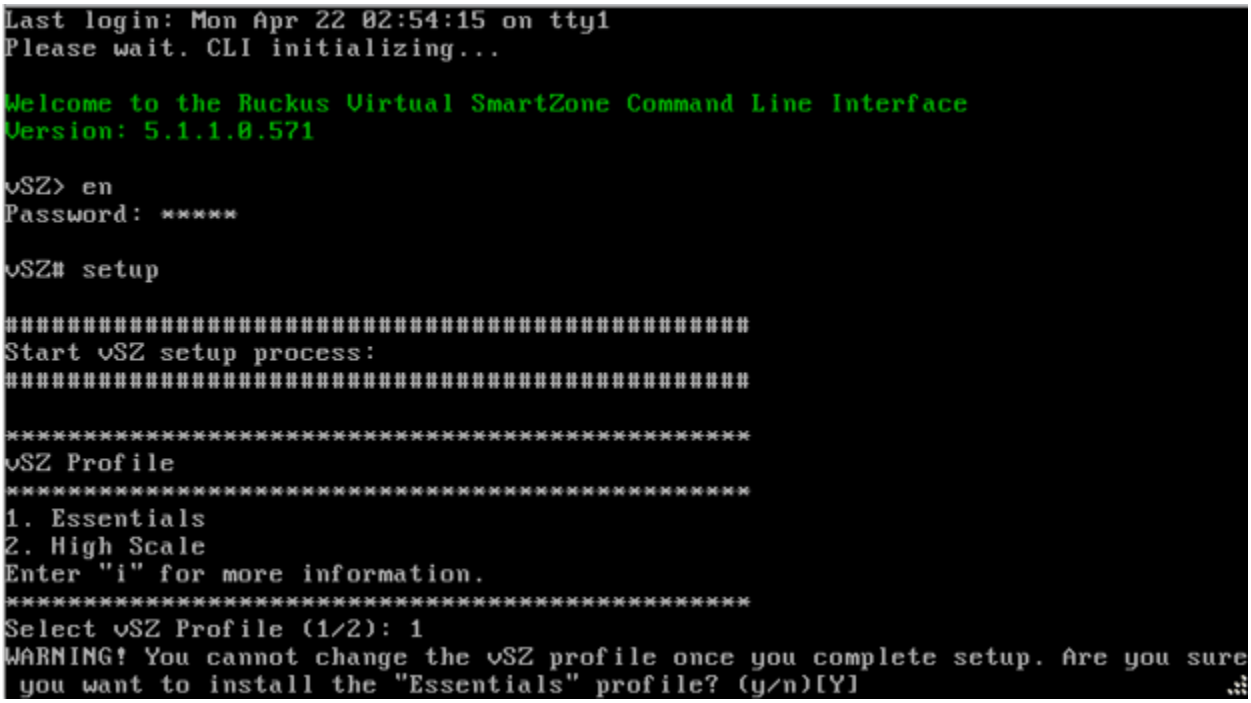


4. Enter **setup**. The console displays the current network settings (if any), and then displays the following prompt: **Do you want to setup network? [YES/no]**
5. Enter **YES**. The next screen prompts you to select the profile configuration that you want to use for this instance of vSZ. The options include: **(1) High-Scale(2) Essentials**

6. Enter the number that corresponds to the profile configuration that you want to deploy.

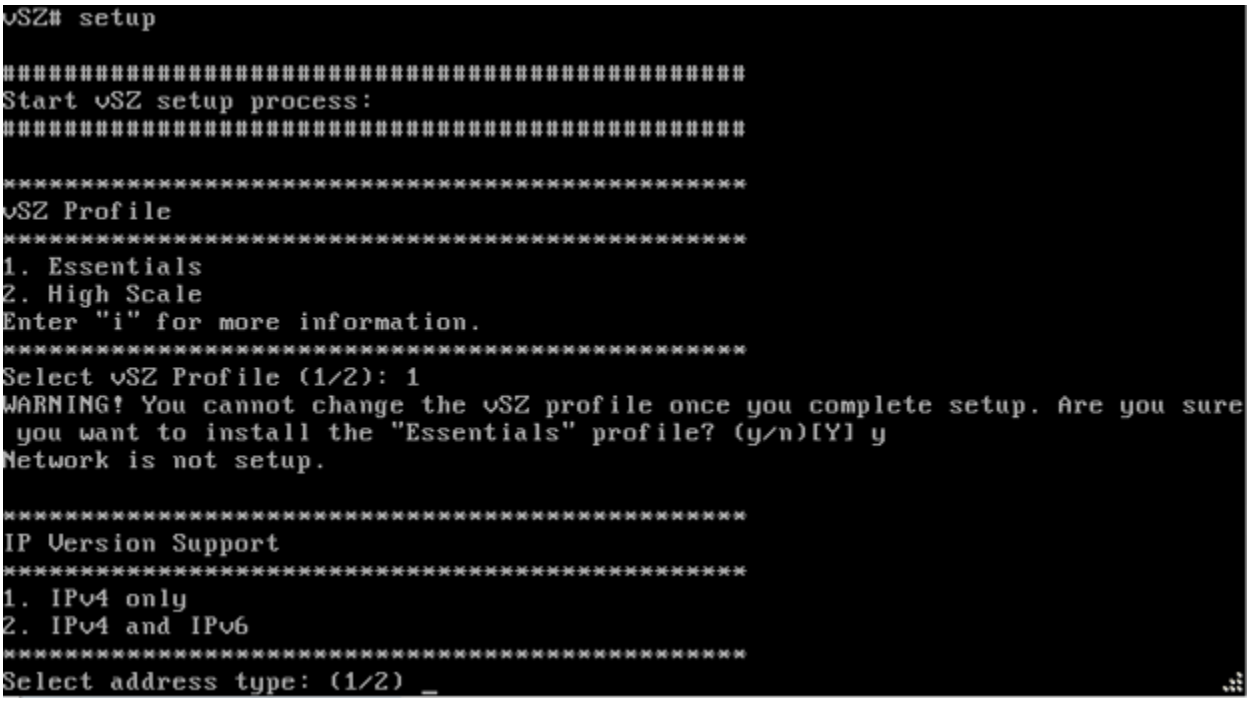
   If you selected Essentials and the virtual machine has insufficient memory resources available (for example, the VM has only 8GB of RAM when the minimum RAM requirement is 12GB), you will be unable to continue with the setup process.

   FIGURE 169 Enter the number that corresponds to the profile that you want to deploy



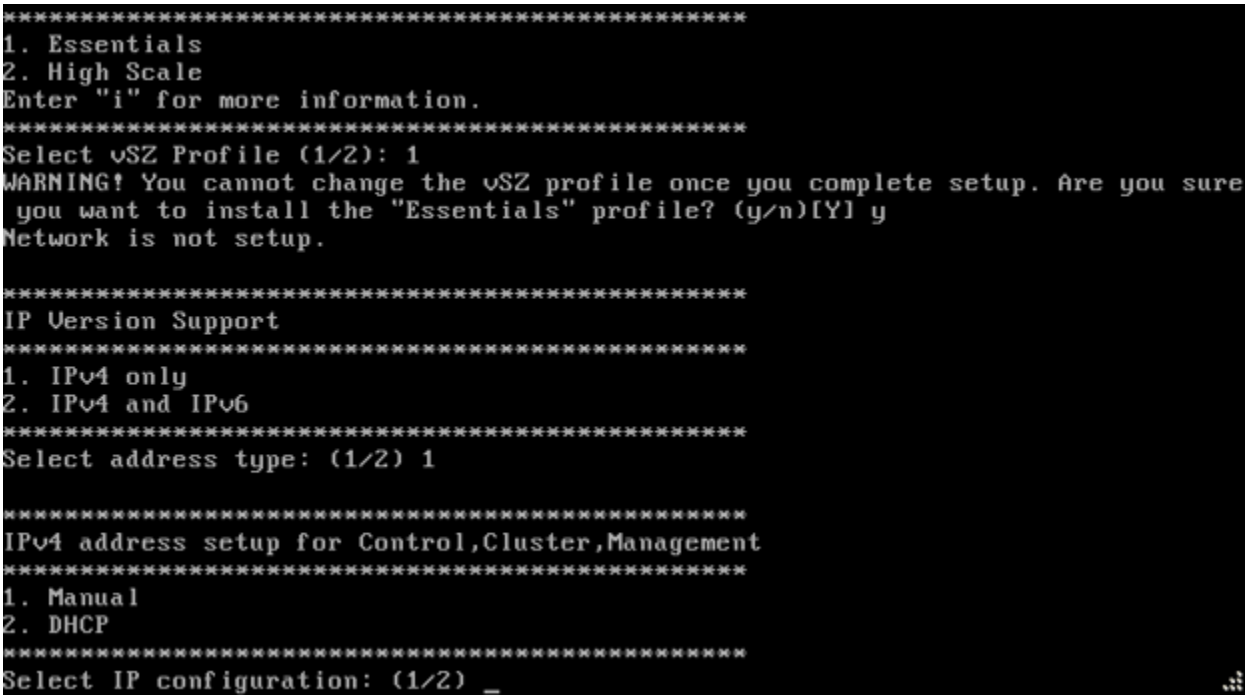
7. Enter **Y** for confirmation. At the **IP Version Support** prompt, enter one of the following options: **1: IPv4 Only2: IPv4 and IPv6**.

FIGURE 170 Configure the IP address settings of the single interface



8. The **IPv4 address setup for Control, Cluster, Management** option appears. At the **Select IP configuration** prompt, enter **1** for Manual and **2** for DHCP.

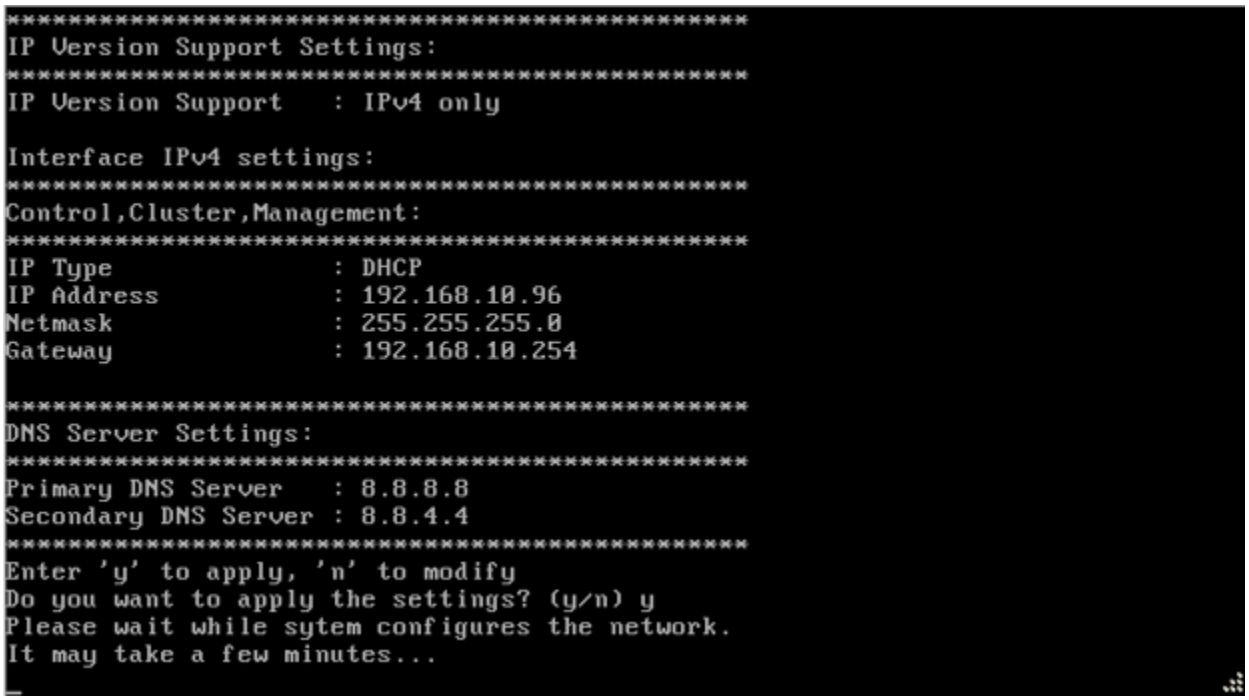
   FIGURE 171 Configure the IP version setup



9. At the **Primary DNS Server** prompt, enter the primary DNS server on the network.
10. At the **Secondary DNS Server** prompt, enter the secondary DNS server (if any) on the network.

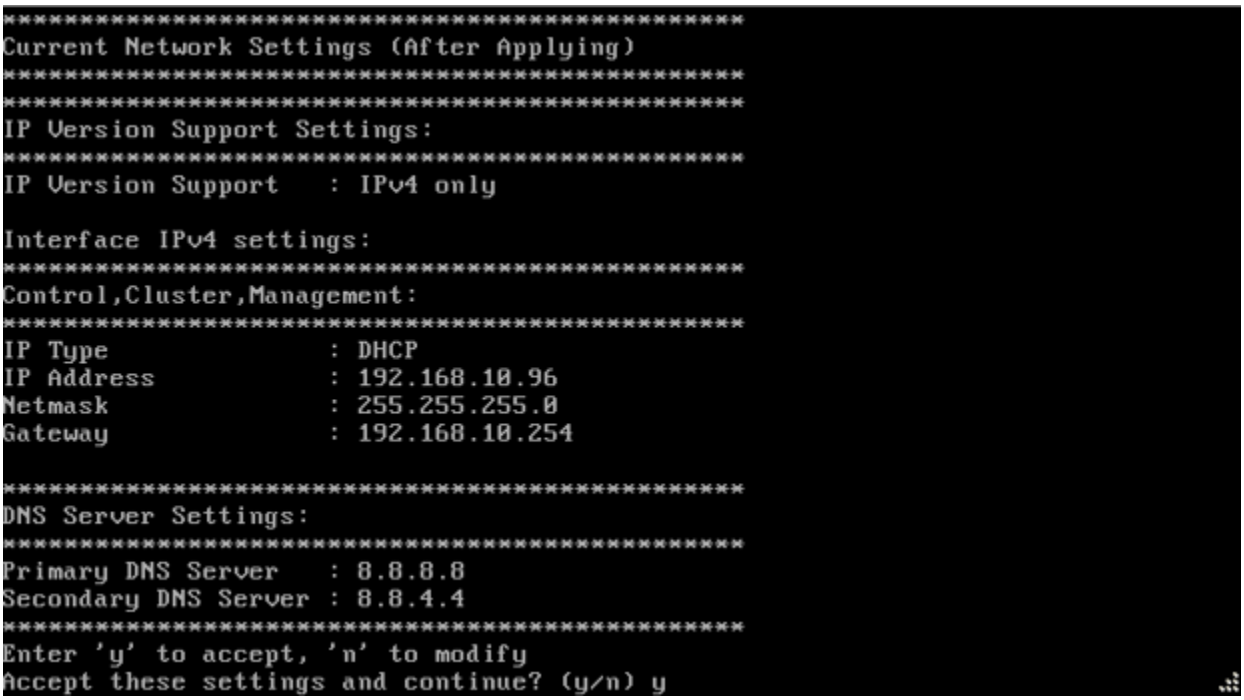
11. Enter **y** to apply settings.

FIGURE 172 Apply Settings



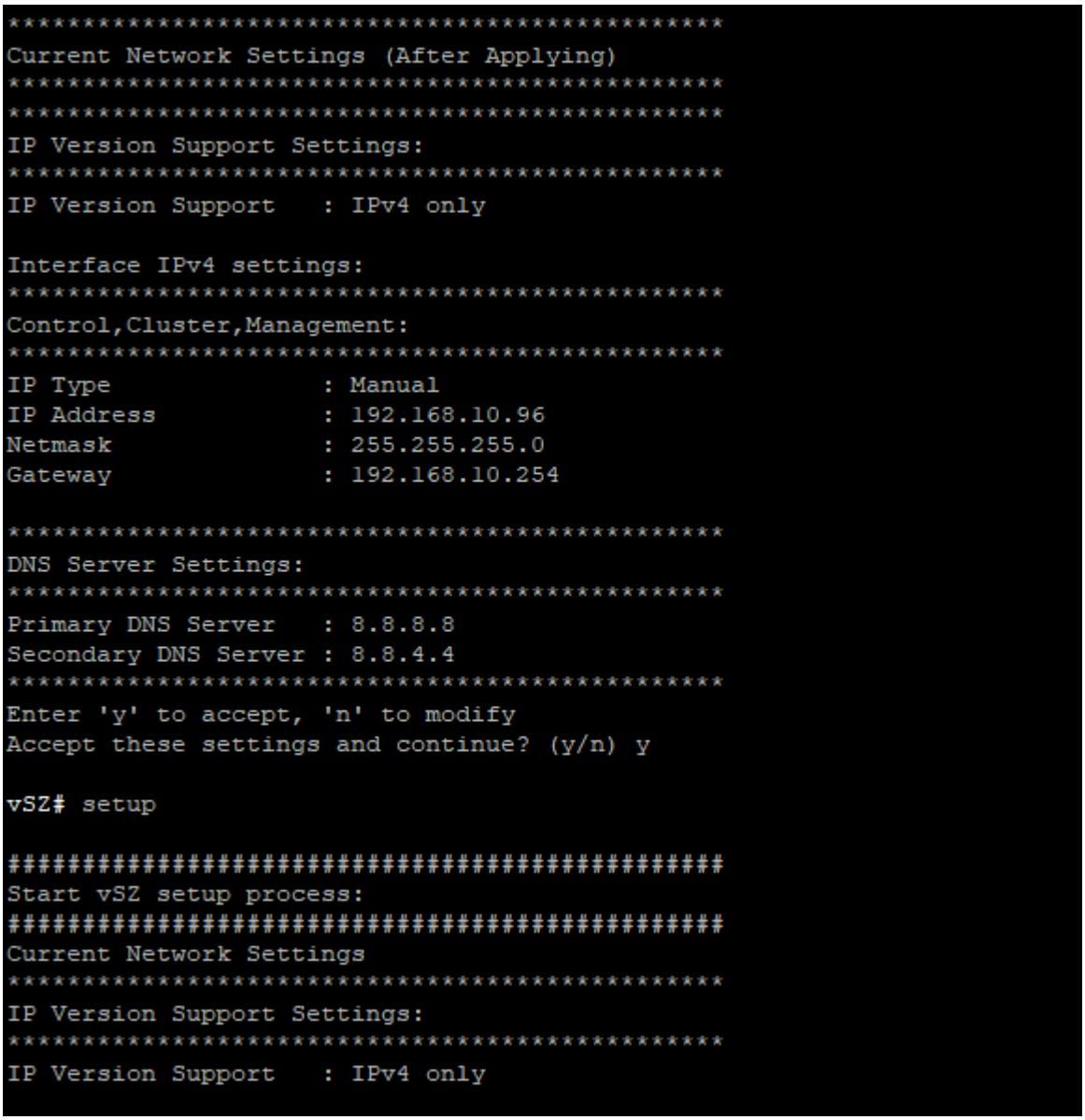
12. To accept settings enter **y**. Else, enter **n**

FIGURE 173 Accept Settings



13. To setup a network, enter **y**. Else, enter **n**.

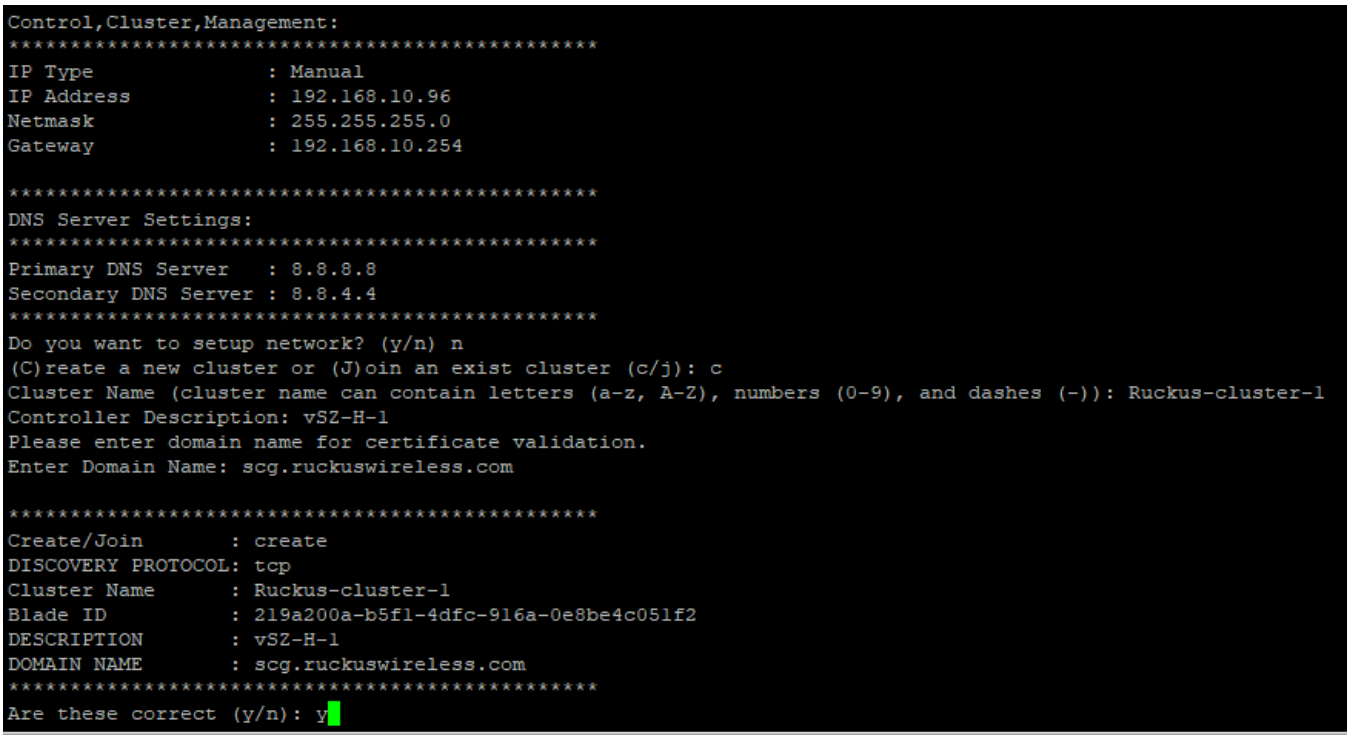
FIGURE 174 Network Setup



14. To start cluster setup, enter **setup** at the prompt.

15. Choose the option for cluster setup. Enter **c** to create a new cluster or **j** to join an existing cluster.

FIGURE 175 Cluster Setup



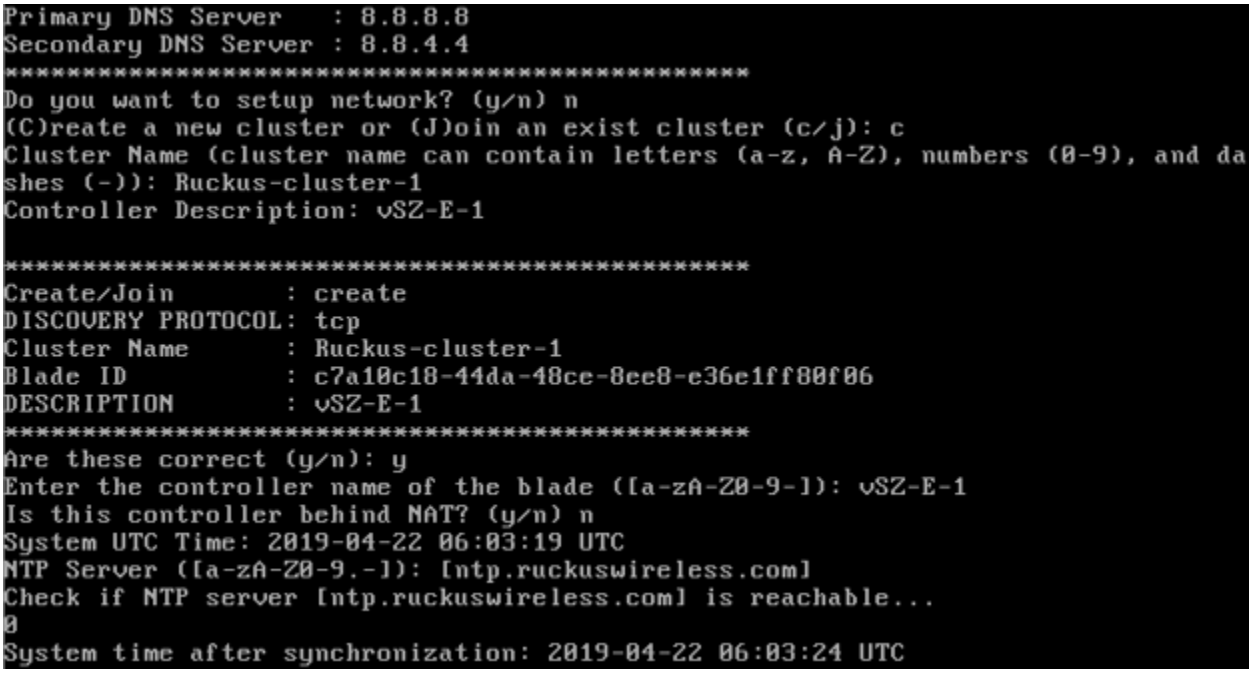
16. Enter the following information:

- **Cluster Name**
- **Controller Description**
- **Enter Domain Name**

Create/Join cluster, **DISCOVERY PROTOCOL**, **Cluster Name**, **Blade ID**, and **DESCRIPTION** are created by the system.

17. When the prompt **Are these correct? (y/n)** appears, enter **y** to confirm the cluster setup. Enter the controller name of the blade and enter **y** to specify if the controller is behind NAT. Else, enter **n**.

FIGURE 176 Configure Cluster Setup



18. To Convert ZoneDirector APs in factory settings to vSZ APs to vSZ APs automatically, enter **y**, else enter **n**.

FIGURE 177 Converting Factory Settings to vSZ Settingsl

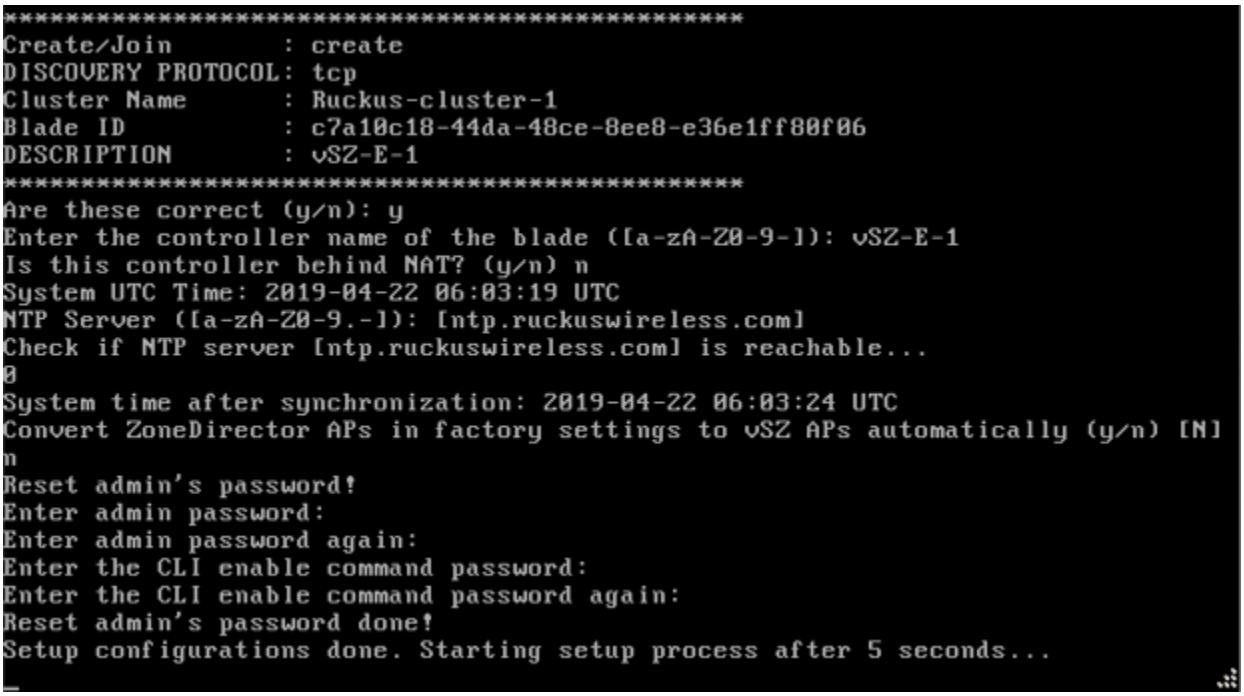
```
shes (-)): Ruckus-cluster-1
Controller Description: vSZ-E-1

************************************************
Create/Join       : create
DISCOVERY PROTOCOL: tcp
Cluster Name      : Ruckus-cluster-1
Blade ID          : c7a10c18-44da-48ce-8ee8-e36e1ff80f06
DESCRIPTION       : vSZ-E-1
************************************************
Are these correct (y/n): y
Enter the controller name of the blade ([a-zA-Z0-9-]): vSZ-E-1
Is this controller behind NAT? (y/n) n
System UTC Time: 2019-04-22 06:03:19 UTC
NTP Server ([a-zA-Z0-9.-]): [ntp.ruckuswireless.com]
Check if NTP server [ntp.ruckuswireless.com] is reachable...
0
System time after synchronization: 2019-04-22 06:03:24 UTC
Convert ZoneDirector APs in factory settings to vSZ APs automatically (y/n) [N]
n
Reset admin's password!
Enter admin password:
Enter admin password again:
Enter the CLI enable command password:
Enter the CLI enable command password again:
```

19. In **Reset admin's password**, press **<Enter>**.

20. Enter the following information:
    - **Enter the admin password**
    - **Enter the admin password again**
    - **Enter the CLI enable command password**
    - **Enter the CLI enable command password again**

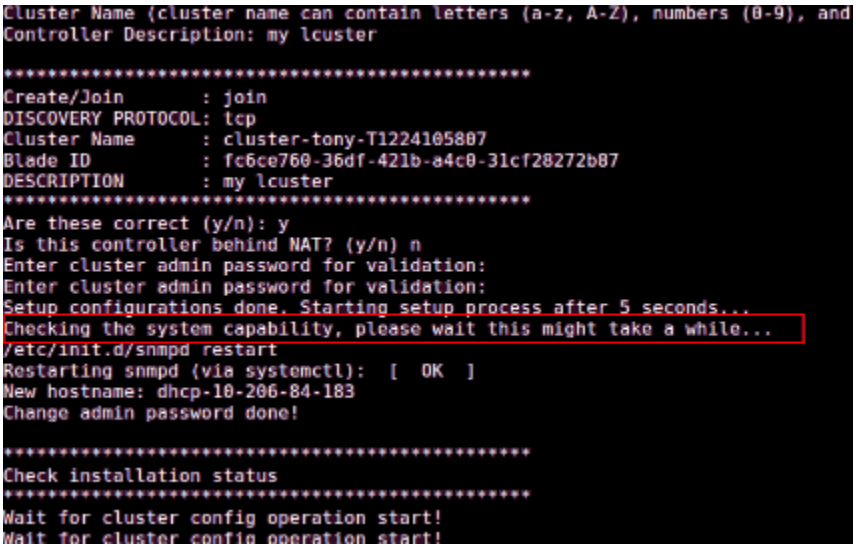
    The password reset confirmation appears and starts setup process.

    FIGURE 178 Admin Password Reset



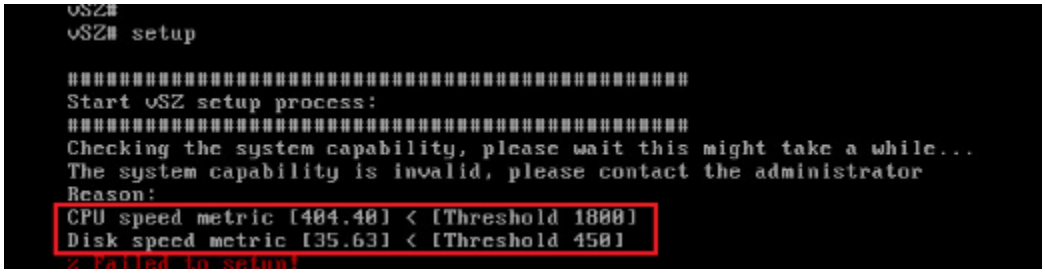
21. The setup process begins and checks for system capabilities.

FIGURE 179 Checking System Capabilities



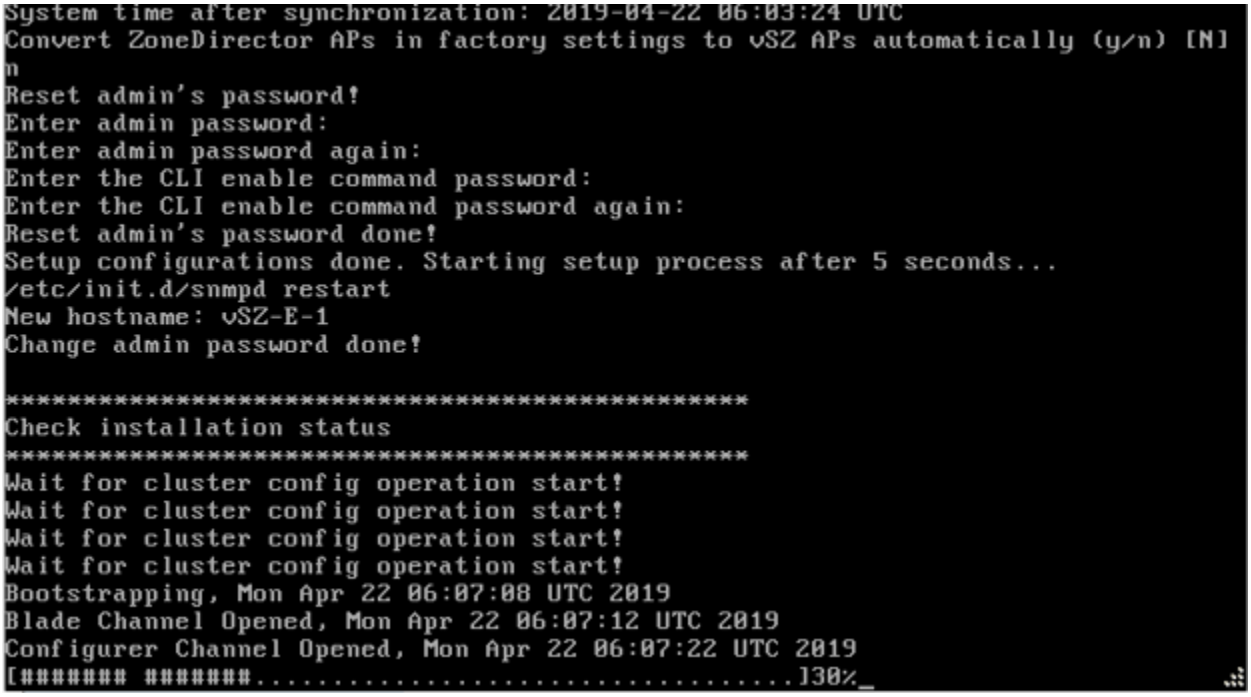
- If the system capability is invalid an error message appears.

FIGURE 180 System Capability Error Message



- If the system capability is within the threshold the setup process begins

FIGURE 181 Setup Process Begins



You have completed configuring the vSZ interfaces. You are now ready to run the vSZ Setup Wizard. See Using the Setup Wizard to Install vSZ on page 201.

Setting Up the vSZ with Three Interfaces

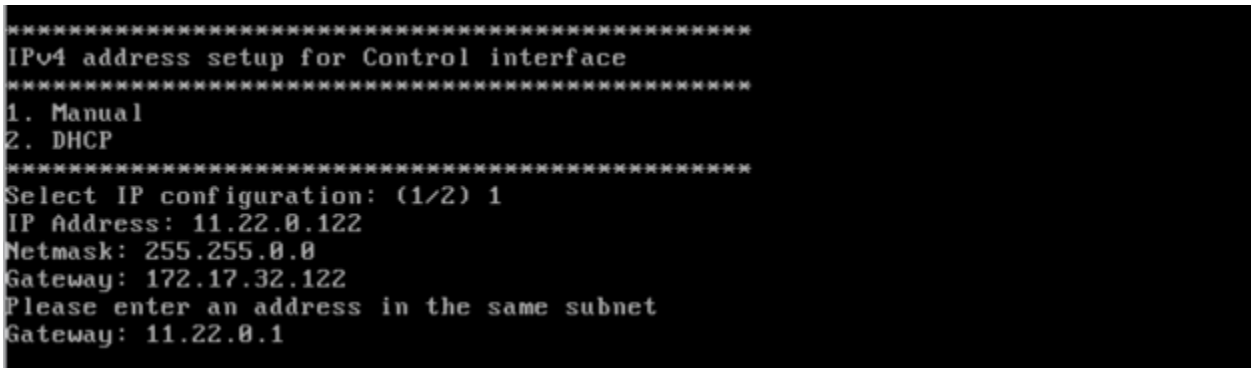
1. Log on to the console using the following credentials: **User name: admin Password: admin**
2. At the **vSZ>** prompt, enter **en** to enable privileged mode.
3. At the **Password** prompt, enter **admin**. The **vSZ#** prompt appears.

4. Enter **setup**. The console displays the current network settings (if any), and then displays the prompt: **Choose IP Version Support (either 1. IPv4 only or 2. IPv4 and IPv6)**

   FIGURE 182 At the vSZ> prompt, enter setup

5. At the **Select IP configuration** prompt, enter **1** to set up the *control interface* manually.
6. Configure the IP address, netmask, and gateway of the control interface, and the press **<Enter>**.

   FIGURE 183 Configure the IP address settings of the control interface



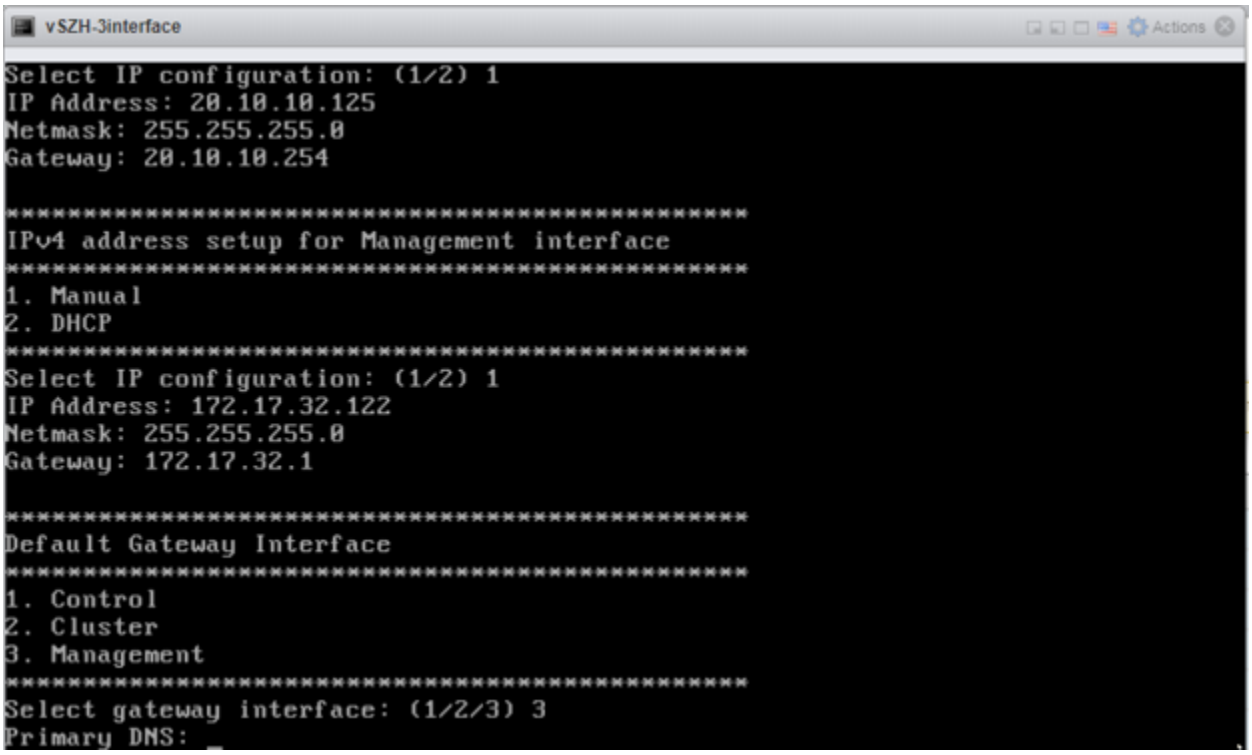
7. At the **Select IP configuration** prompt, enter **1** to set up the cluster interface manually.
8. Configure the IP address, netmask, and gateway of the *cluster interface*, and then press **<Enter>**.
9. At the **Select IP configuration** prompt, enter **1** to set up the management interface manually.
10. Configure the IP address, netmask, and gateway of the management interface, and the press **<Enter>**.

    Take note of the IP address that you assign to the management interface – you will use this IP address to log on to the vSZ web interface.

11. When the message **Select system default gateway (Control, Cluster, Management)?**, enter **Control** or **Management**, depending on your network topology (see Important Notes About Selecting the System Default Gateway on page 200).

    This entry is case-sensitive. Make sure you enter the system default gateway exactly as shown at the prompt.

    FIGURE 184 When prompted for the system default gateway, enter either Management or Control (depending on your network design)



12. When prompted, enter the primary and secondary DNS server IP addresses.
13. Enter **restart network**.

You have completed configuring the vSZ interfaces. You are now ready to run the vSZ Setup Wizard. See Using the Setup Wizard to Install vSZ on page 201.

Important Notes About Selecting the System Default Gateway

Depending on your network topology, you may select either the Management or Control interface as the system default gateway.

- If all of the managed APs are located in different locations on the Internet, the vSZ may not know all of the IP subnets of these APs. In this case, the control interface should be set as the default gateway for the vSZ and you will need to add a static route to reach the management network.
- If all of the managed APs belong to a single subnet or to multiple subnets on which you can set the route statically, then you can set the management interface as the default gateway users can set default gateway for the vSZ and set static routes for the vSZ to reach all of its managed APs.

Using the Setup Wizard to Install vSZ

Before You Begin

The Setup Wizard helps you perform the initial configuration of the vSZ by presenting the vSZ configuration options in a set of easy-to-complete screens.

The Setup Wizard will prompt you to select one of the two available profile configurations (High-Scale profile and Essentials profile). You must select the profile configuration that corresponds to the vSZ license that you purchased. Before you start the Setup Wizard, make sure you know the profile configuration that you need to select. If you are unsure which profile configuration you need to select, contact Ruckus Networks Support.

Follow these steps to run and complete the vSZ Setup Wizard:

- Start the Setup Wizard and Set the Language
- Select the Profile Configuration That Corresponds to Your vSZ License
- Configure the Management IP Address Settings
- Configure Dual Mode IP Address Settings Using CLI
- Configure the Cluster Settings
- Set the Administrator Password
- Verify the Settings

NOTE
This guide describes the Setup Wizard screens that appear when you select the High-Scale profile configuration. If you select the Essentials profile configuration, the screens that appear may be slightly different.

Step 1: Start the Setup Wizard and Set the Language

1. Start your web browser, and then enter the following in the address bar: **https://{management-IP-address}:8443**, where management-IP-address is the address you assigned to the management interface. The vSZ Setup Wizard appears, displaying the **Language** page.

FIGURE 185 The Language page

2. Select your preferred language for the vSZ web interface. Available options include:
   - English
   - Traditional Chinese
   - Simplified Chinese
3. Click **Next**. The **Profile** page appears.

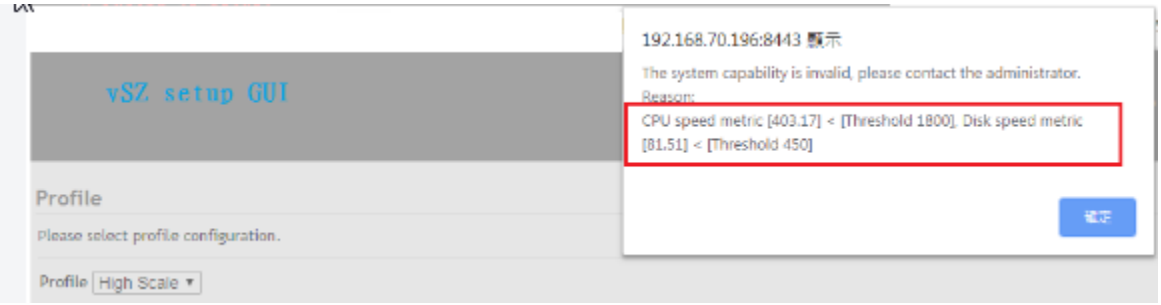
Step 2: Select the Profile Configuration That Corresponds to Your vSZ License

1. Select the profile configuration that corresponds to the vSZ license that you purchased. Available profile configurations include:
   - High Scale
   - Essentials

FIGURE 186 Select a profile configuration that matches your vSZ license

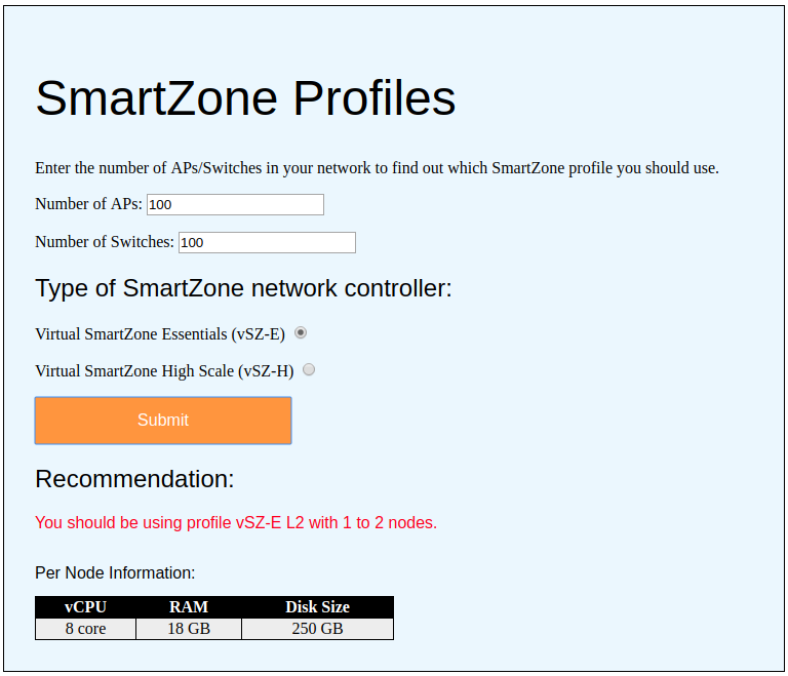
2. Under **Profile Tool**, click **Use Tool** to configure a SmartZone profile. The system capability is checked and an error message is displayed if it is invalid.

   FIGURE 187 System Capability Invalid



3. In the **SmartZone Profiles** page, enter the number of APs and switches, type of SmartZone network controller, and click **Submit**.

   The following is an example to configure a SmartZone profile.



4. Click **Next**. The Confirmation message appears. Once you accept the confirmation, the **Management IP** page is displayed.

Step 3: Configure the Management IP Address Settings

While installing vSZ on Cloud, always use DHCP.

The vSZ comes in either a single network interface or three network interfaces (one interface each for Control (AP), Cluster, and Management (Web) traffic). The following procedure assumes that the vSZ you are installing uses a single network interface.

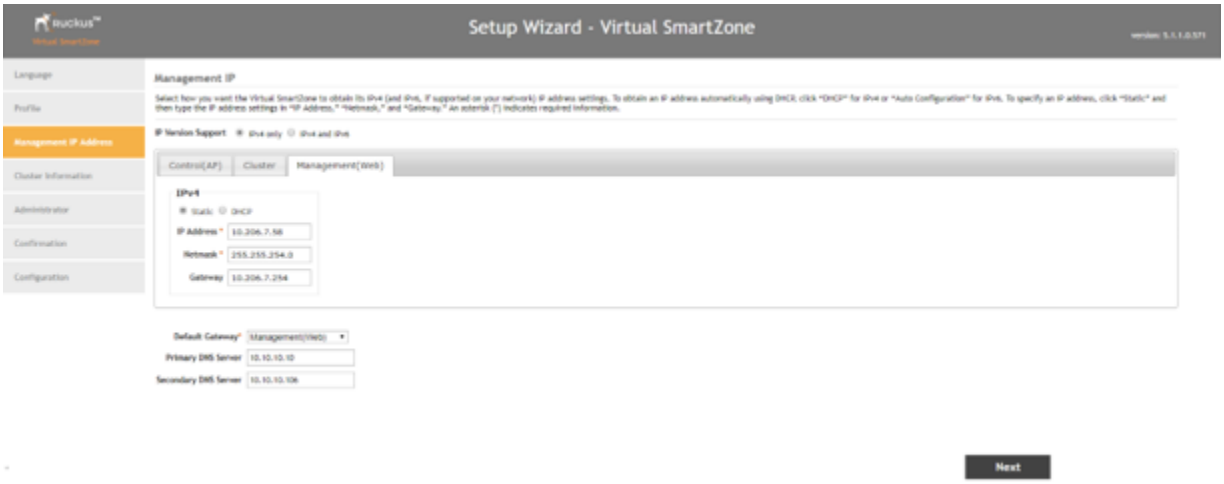
If the vSZ that you are installing comes with three network interfaces, you must configure each of the three interfaces to be on three different subnets. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

1. In *IP Version* Support, select one of the following options:

   IPv4 Only: Click this option if you want the controller to obtain an IPv4 address from a DHCP server on the network.

   IPv4 and IPv6: Click this option if you want the controller to obtain both IPv4 and IPv6 addresses from DHCP and DHCPv6 servers on the network. Refer to Step 4: Configure Dual Mode IP Address Settings Using CLI for configuring dual setup using CLI. This is an alternative method for configuring IPv4 and IPv6 manually if the DHCP server is not available on the network.

   FIGURE 188 Select the IP version support

2. Configure the IP address settings of the *Management* interface.
   a) Under the **IPv4** section, click **Static**, and then enter the network settings that you want to assign to the AP/DataPlane interface, through which client traffic and configuration data are sent and received.

      Although it is possible to use DHCP to assign IP address settings to the Control interface automatically, Ruckus Networks strongly recommends assigning a static IP address to this interface.The following network settings are required (others are optional):

      - IP address
      - Netmask
      - Gateway

   a) If you clicked IPv4 and IPv6 at the beginning of this procedure, under the IPv6 section, click **Auto Configuration** if you want the controller to obtain its IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network. If you want to manually assign the IPv6 network address, click **Static**, and then set the values for the following: IP address (IPv6): Enter an IPv6 address (global only) with a prefix length (for example, **1234::5678:0:C12/123)**. Link-local addresses are unsupported. Gateway: Enter an IPv6 address (global or link-local) without a prefix length. Here are examples:

      Global address without a prefix length: **1234::5678:0:C12**

      Link-local address without a prefix length: **fe80::5678:0:C12**

3. At the bottom of the screen, select the interface that you want to set as the default system gateways for IPv4 and IPv6 (if enabled), and then type the **Default Gateway**, **Primary DNS Server** address and **Secondary DNS Server** Address.

   The appropriate interface to use as the default system gateway depends on the topology of your network. See Important Notes About Selecting the System Default Gateway on page 200 for more information.

4. Check the network settings that you have configured.

5. Click the **Next** to continue. The controller validates and applies the network settings that you have configured. Continue to Step 5: Configure the Cluster Settings on page 210

Important Notes About Selecting the System Default Gateway

Depending on your network topology, you may select either the Management or Control interface as the system default gateway.

- If all of the managed APs are located in different locations on the Internet, the vSZ may not know all of the IP subnets of these APs. In this case, the control interface should be set as the default gateway for the vSZ and you will need to add a static route to reach the management network.
- If all of the managed APs belong to a single subnet or to multiple subnets on which you can set the route statically, then you can set the management interface as the default gateway users can set default gateway for the vSZ and set static routes for the vSZ to reach all of its managed APs.

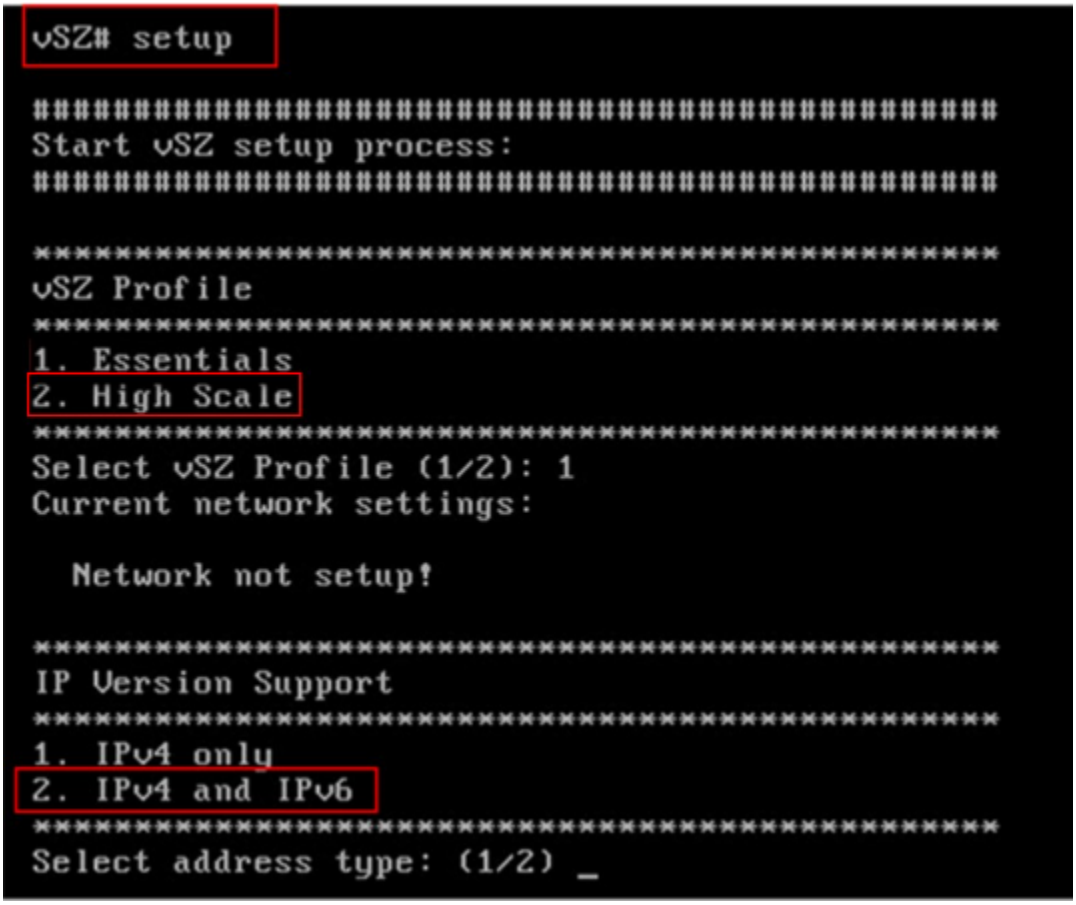
Step 4: Configure Dual Mode IP Address Settings Using CLI

The following are the steps to configure the dual setup using CLI. This is an alternative method of configuring IPv4 and IPv6 manually if the DHCP server is not available on the network.

1. Using CLI execute the setup command: **vSZ# setup**
2. In **vSZ Profile,** choose either **1. Essentials** or **2. High Scale**.

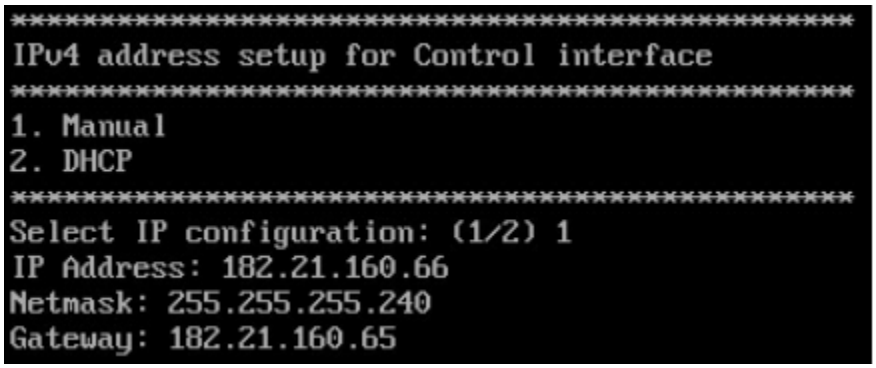
3. In **IP Version Support**, choose **2. IPv4 and IPv6**.

FIGURE 189 Choose **2. IPv4 and IPv6** to use dual mode IP addresses



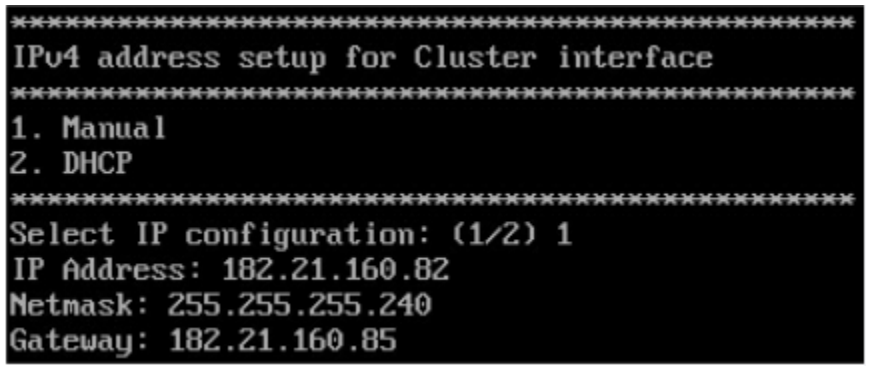
4. Configure the IPv4 address settings that you want to assign to the AP/DataPlane interface, through which client traffic and configuration data are sent and received.
   a) Enter the setup for **Control** as either:
      1. Manual
      2. DHCP
   b) Enter the IP configuration as 2 (DHCP).
   c) Enter following network settings as required:
      - IP address
      - Netmask
      - Default gateway
   d) Save the networking configuration of **Control** settings.

FIGURE 190 IPv4 Control Settings



   e) Enter the setup for Cluster as either: **1. Manual 2. DHCP**
   f) Enter the IP configuration as 1 (Manual)
   g) Enter following network settings as required: **IP address**, **Netmask**, and **Default gateway**
   h) Save the networking configuration of **Cluster** settings.

FIGURE 191 IPv4 Cluster Settings

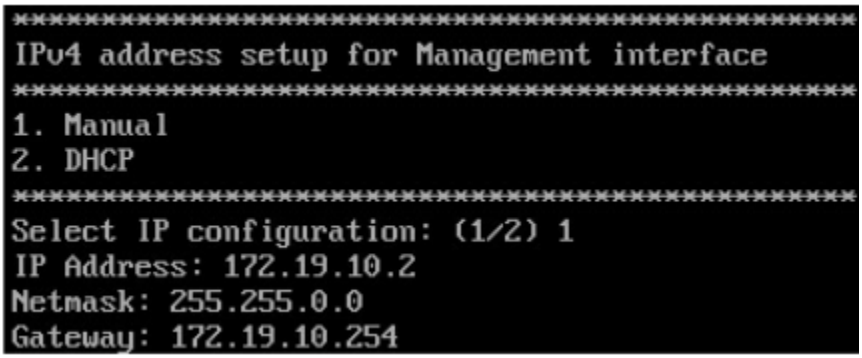


   i) Enter the setup for Management as either: **1. Manual 2. DHCP**
   j) Enter the IP configuration as **2** (DHCP)
   k) Enter following network settings as required:

- IP Address
- Netmask
- Gateway

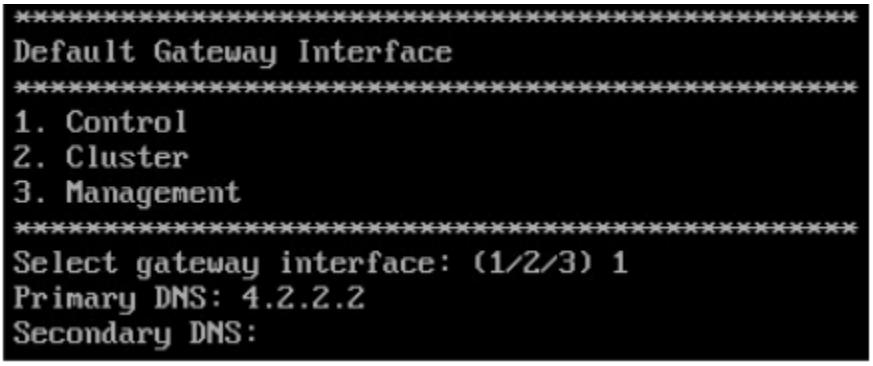
l) Save the networking configuration of **Management** settings

FIGURE 192 IPv4 Management Settings



The available gateway for Control, Cluster and Management will be displayed. You can select the system default gateway.

FIGURE 193 Default Gateway Settings

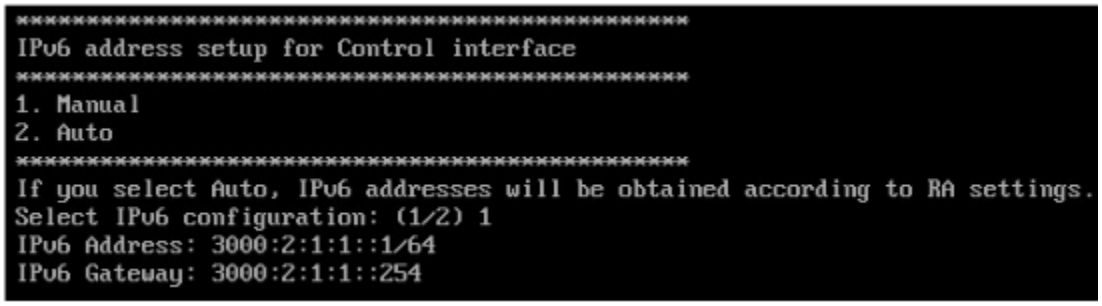


5. Configure the IPv6 address settings that you want to assign to the AP/Data Plane interface, through which client traffic and configuration data are sent and received.

   NOTE
   The cluster interface setting does not support IPv6 addresses.

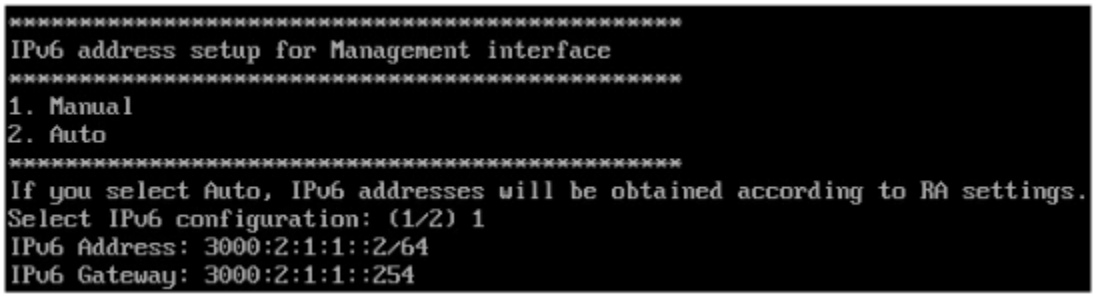
   a) Enter the setup for Control as either: **1. Manual2. Auto Configuration**
   b) Enter the IP configuration as **1** (Manual).
   c) Enter following network settings as required:
      - IPv6 Address
      - Gateway
   d) Save the networking configuration of **Control** settings.

   FIGURE 194 IPv6 Control Settings



   e) Enter the setup for Management as either: 1. Manual2. Auto Configuration
   f) Enter the IP configuration as **1** (Manual)
   g) Enter following network settings as required: IP address Default gateway
   h) Save the networking configuration of **Management** settings.

   FIGURE 195 IPv6 Management Settings

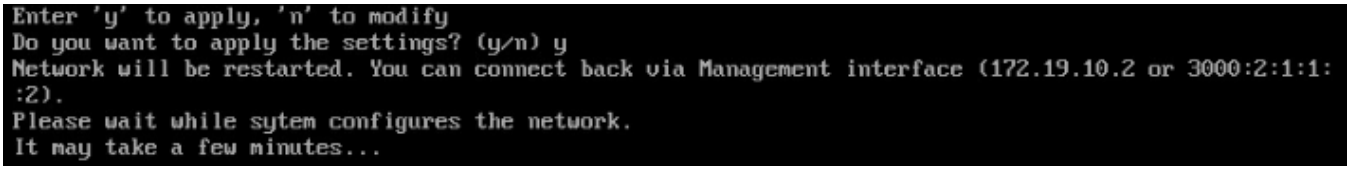


   The available gateway for Control and Management will be displayed. You can select the system default gateway.

FIGURE 196 Default Gateway Settings

6. To apply the settings, press **Y**. The system takes a while to configure the network.

FIGURE 197 Network Configuration



7. Verify that the Control Plane network settings display the IPv4 and IPv6 addresses that you configured.
8. Continue to Step 5: Configure the Cluster Settings on page 210

Step 5: Configure the Cluster Settings

The next step is to configure the vSZ cluster settings. The actions that you need to perform in this step depend on whether you are creating a new cluster (with this vSZ as the first node) or you are setting up this vSZ to join an existing cluster.

- If This vSZ Is Forming a New Cluster on page 211
- If This vSZ Is Joining an Existing Cluster on page 212

FIGURE 198 The Cluster Information page, showing the New Cluster option

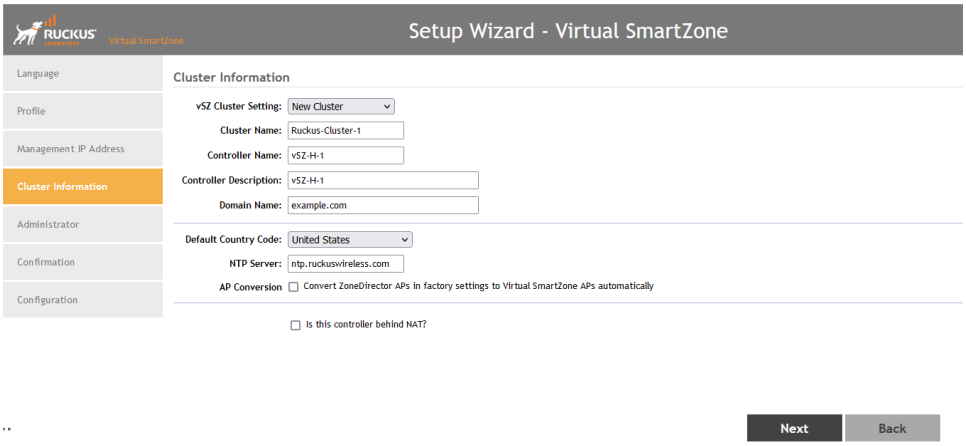
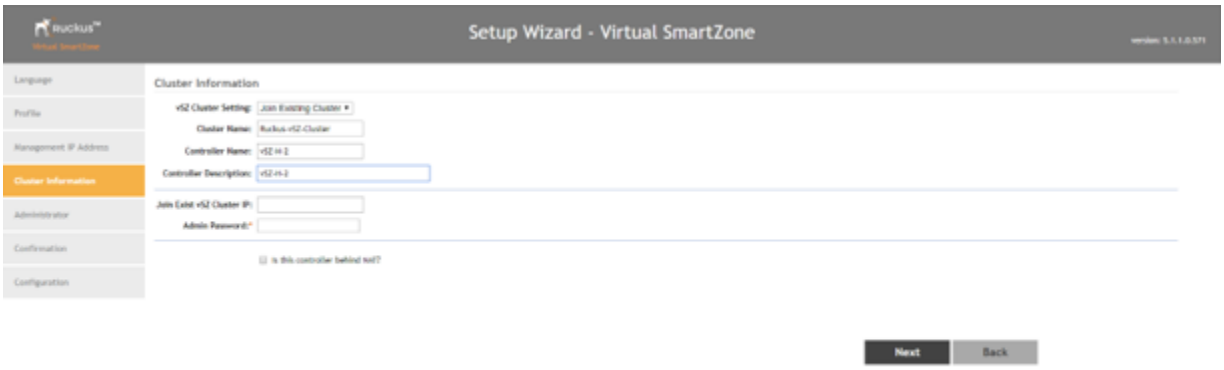


FIGURE 199 The Cluster Information page, showing the Join Existing Cluster option



If This vSZ Is Forming a New Cluster

Follow these steps if you want to use this vSZ to create a new cluster.

On the **Cluster Information** page, configure the following settings:

1. In **vSZ Cluster Setting**, select **New Cluster**.
2. In **Cluster Name**, type a name for the new cluster that you are creating.

   NOTE
   The **Cluster Name** and **Controller Name** boxes only accept alphanumeric characters, hyphens (-), and underscores (_). They do not accept the space character or other special characters (for example, $, *, #, !).

3. In **Controller Name**, type a name for the vSZ controller in this new cluster.
4. In **Controller Description**, type a brief description for the vSZ controller.
5. In **Domain Name**, enter a name for the domain.
6. In **Default Country Code**, select the country.
7. In **NTP Server**, type the address of the NTP server from which members of the cluster will obtain and synchronize time. The default NTP server is **ntp.ruckuswireless.com**

8. If you want ZoneDirector APs that are in factory default settings to be converted to SmartZone APs automatically, select the **AP Conversion** check box.
9. If the controller is behind NAT, select the check box and enter the **Controller NAT IP**.
10. Click **Next** to continue to the **Administrator** page.

If This vSZ Is Joining an Existing Cluster

If this is not the first vSZ cluster on the network, you can set up this vSZ virtual appliance to join an existing cluster.

NOTE

- A vSZ cluster supports a maximum of four nodes. If you are building a vSZ-E cluster with more than two nodes, two (2) additional cores must be added to each node to support the added search and replication capabilities.
- For vSZ deployments, the node that you are joining into an existing cluster must have identical virtual machine resources (CPU, memory, and disk size) as the existing nodes in the cluster.
- Use the AP Rebalance feature to distribute AP load evenly between the existing and new cluster nodes, and the Dataplanes in appliance SZ models.
- There is no impact or downtime on existing cluster node operations when a new node joins the cluster.

To add this vSZ to an existing cluster, the entire target cluster must be in a healthy state (no node must be in “out of service” state). If any member node is out of service, the join request will fail. You will need to remove any out-of-service node from the cluster before you can add a new node successfully.

NOTE
When adding a new node into an existing cluster, any ARC signature files, AP or switch firmware, and AP patches on the existing cluster will be synchronised onto the new node.
Kernel Space Program (KSP) patches must be independently uploaded to the new node. Refer to the KSP documentation to ensure whether the KSP patches are applied per node and whether the cluster needs to be reloaded.

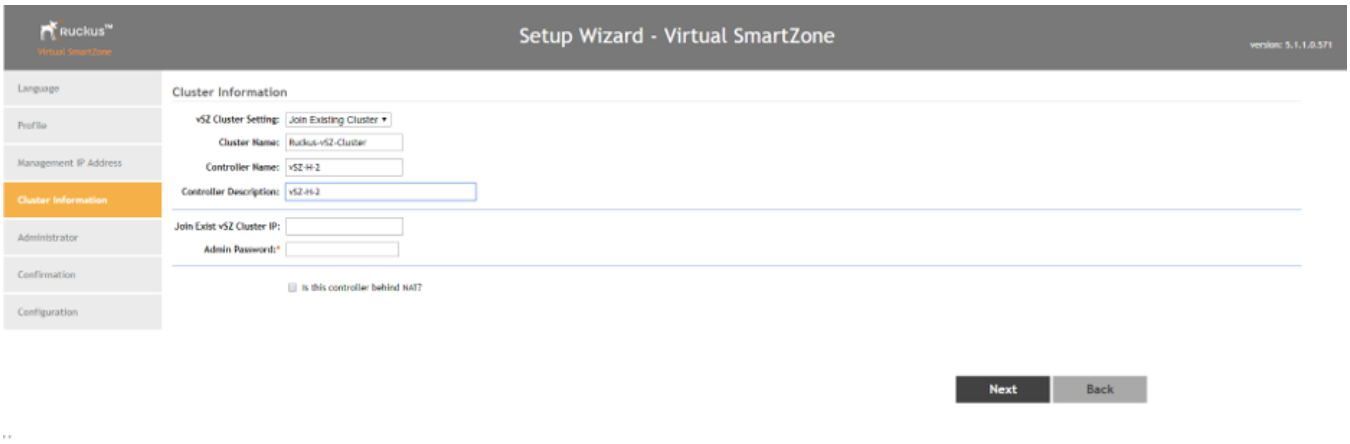
Follow these steps to configure this to join an existing cluster.

1. In **vSZ Cluster Setting**, select **Join Existing Cluster**.
2. In **Cluster Name**, type the name of the cluster that this vSZ is joining.

   The **Cluster Name** and **Controller Name** boxes only accept alphanumeric characters, hyphens (-), and underscores (_). They do not accept the space character or other special characters (for example, $, *, #, !).
3. In **Controller Name (optional)**, type a name that you want to assign to this new controller.
4. In **Controller Description**, type a description for this new controller.
5. In **Join Exist vSZ Cluster IP**, type the IP address of the leader in the existing cluster.
6. In **Admin Password**, type the administrator password to the web interface of the leader node.

7. Click **Next** to continue to the **Administrator** page. See Step 6: Set the Administrator Password on page 213.

FIGURE 200 The Cluster Information page, showing the Join Existing Cluster option



If the firmware version on this vSZ (shown in the bottom-left area of the **Cluster Information** page) does not match the firmware version of the cluster, a message appears and prompts you to upgrade the vSZ firmware. Click **Upgrade**, and then follow the prompts to perform the upgrade.

Step 6: Set the Administrator Password

Set the administrator passwords for the web interface and command line interface (CLI).

Follow these steps to set the web interface and CLI passwords.

NOTE
The web interface and CLI passwords must be at least eight (8) characters in length and must include one number, one letter, and one special character (for example, $, *, #, !).

1. In **Admin Pasword**, type a password that you want to use to access the web interface.
2. In **Confirm Password**, retype the password above to confirm.
3. In **Enable Password**, type a password that you want to use to enable CLI access to the vSZ.
4. In **Confirm Password**, retype the password above to confirm.
5. Click **Next** to continue. The **Confirmation** page appears and displays all the controller settings that you have configured using the Setup Wizard.

FIGURE 201 Set the web interface and CLI passwords

Step 7: Verify the Settings

After you complete setting the web interface and CLI passwords, check the **Confirmation** page and review all of the controller settings that you have configured using the Setup Wizard.

Follow these steps to verify the controller settings that you have configured.

1. Verify that all the settings displayed on the **Confirmation** page are correct.
2. If they are all correct, click **Finish** to apply the settings and activate the controller on the network.

FIGURE 202 The Confirmation page

NOTE
If you find an incorrect setting, click the **Back** button until you reach the related page, and then edit the settings. When you finish editing the settings, click the **Next** button until you reach the **Confirmation** page again.

A progress bar appears and displays the progress of applying the settings, starting the vSZ services, and activating the vSZ on the network.

When the process is complete, the progress bar shows the message `100% Done`. The page also shows the IP address through which you can access the vSZ web interface to manage the controller.

FIGURE 203 Setup is complete when the progress bar shows “100% Done”

Congratulations! You have completed the Setup Wizard. You are now ready to log on to the web interface. Go to **https://{management-IP-adddress}:8443**, and then log on with the user name and password that you assigned to the web interface.

Logging On to the Web Interface

You can access the web interface from any computer that is on the same subnet as the management (web) interface. Follow these steps to log on to the vSZ web interface.

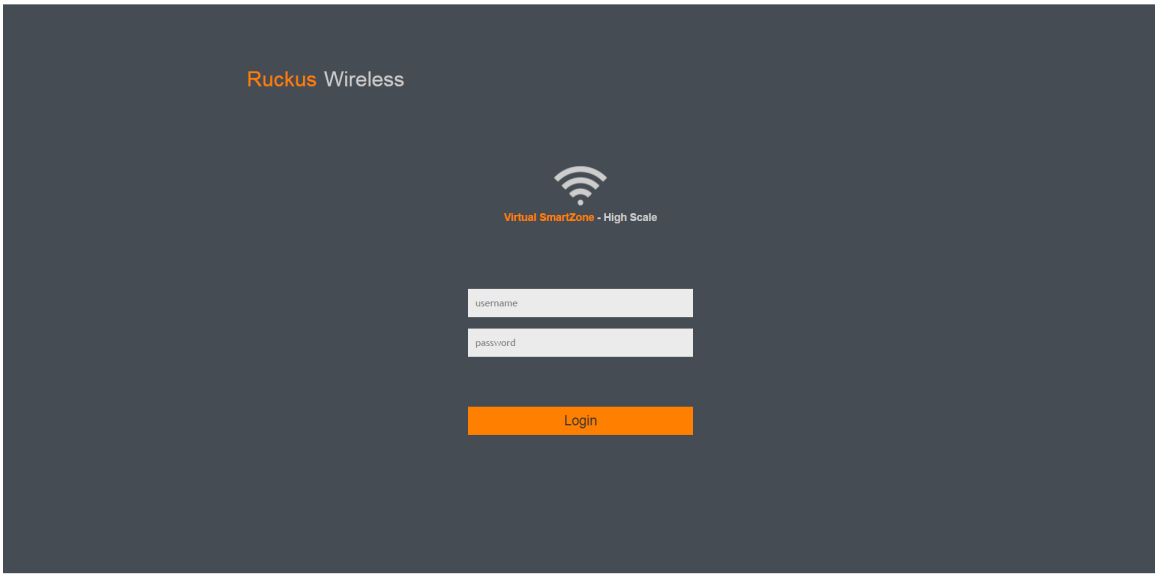
1. On a computer that is on the same subnet as the Management (Web) interface, start a web browser.
2. In the address bar, enter the IP address that you assigned to the Management (Web) interface and append a colon and 8443 (vSZ management port number) at the end of the address. The vSZ web interface logon page appears.

   If the IP address that you assigned to the Management (Web) interface is 10.10.101.1, then you should enter:

   ```
   https://10.10.101.1:8443
   ```

   The vSZ logon page appears.

   FIGURE 204 The vSZ logon page



3. In **User Name**, type **admin**.
4. In **Password**, type the administrator password that you assigned to the web interface earlier.
5. Click **Log On**. The web interface refreshes, and then displays the vSZ dashboard page, which indicates that you have logged on successfully.

You are now ready to configure the controller. For information on how to configure the controller, refer to the **Administrator Guide** for the controller platform that you have installed.

Deployment of vSZ

Deploy vSZ on ESXi Server

Hardware Requirement and Prerequisite for ESXi Server

The following are the hardware and prerequisite for deploying vSZ on ESXi 5.5 or later version.

Hardware Requirement

1. DELL Inc. PowerEdge R530
2. ESXi Server License 5.5 or later version
3. Broadcom NetXtreme BCM5720 Gigabit Ethernet 4 Ports
4. Intel Ethernet 10G 2P X520
5. CPU minimum 8 cores
6. vSphere ESXi Server 5.5 or later version
7. 1 or 3 vNICs
8. 16 GB memory
9. 256 GB Hard disk

Prerequisite

- A hypervisor on ESXi to install vSZ. Recommended version is ESXi 5.5 or later version.
- Download the vSZ package (.OVA file) from Ruckus support .
- The IP addresses, netmask, gateway, DNS, DHCP and NAT support for vSZ.
- Ensure that the vSZ license that you have, is a high-capacity mode or an essential mode.
- Ensure the number of physical network interfaces. Choose the interface group, 3 or 1, that would be used implement for vSZ. vSZ-E mode supports only 1 interface group. vSZ-H mode supports both 3 and 1 interface groups.
- Before you power on vSZ, ensure that the networking is configured on ESXi.
- Recommended to use static network addresses that are assigned to vSZ during setup.

  NOTE
  Due to different servers and NIC, the deployment procedure mentioned in this section is for reference.

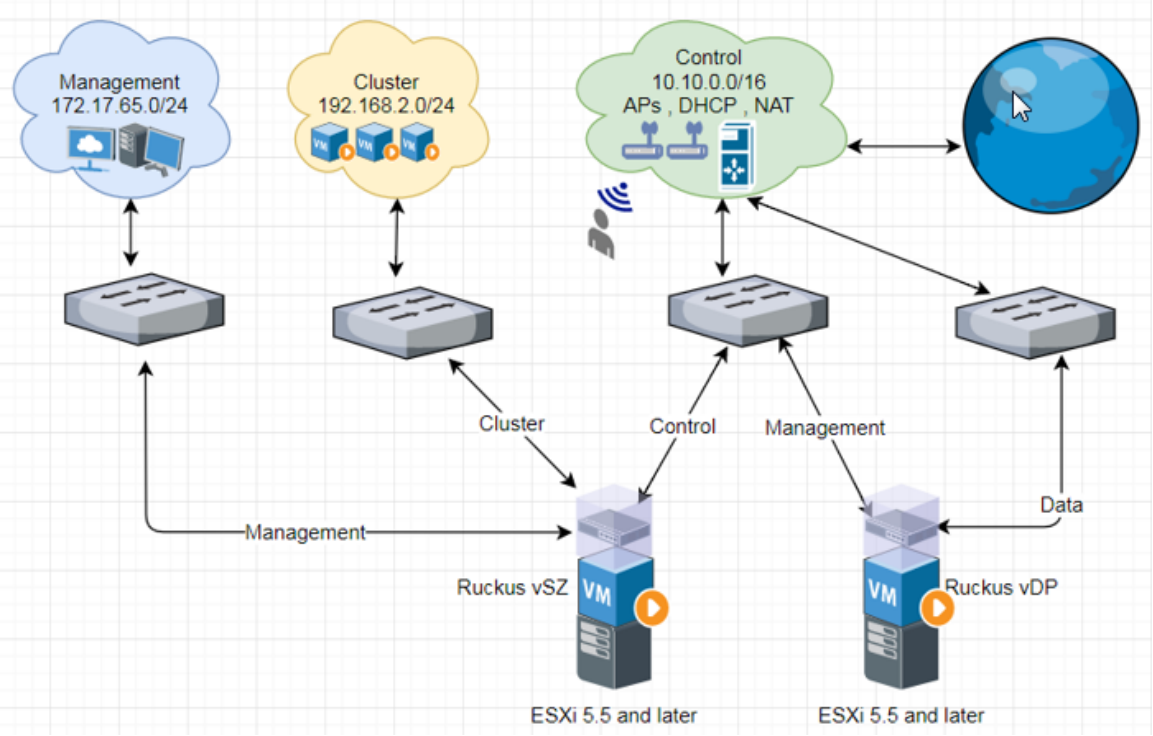
Topology for vSZ Deployment on ESXi 5.5 Server

The network topologies for vSZ deployment on ESXi 5.5 server.

The following are basic topologies for setting up vSZ. Based on your requirement you can choose any of the alternatives for deployment.

- High-Scale mode with three group interfaces.

  FIGURE 205 vSZ-H with Three Group Interfaces



- Essentials mode with one group interface.

FIGURE 206 Example 1: vSZ-E with one Group Interface

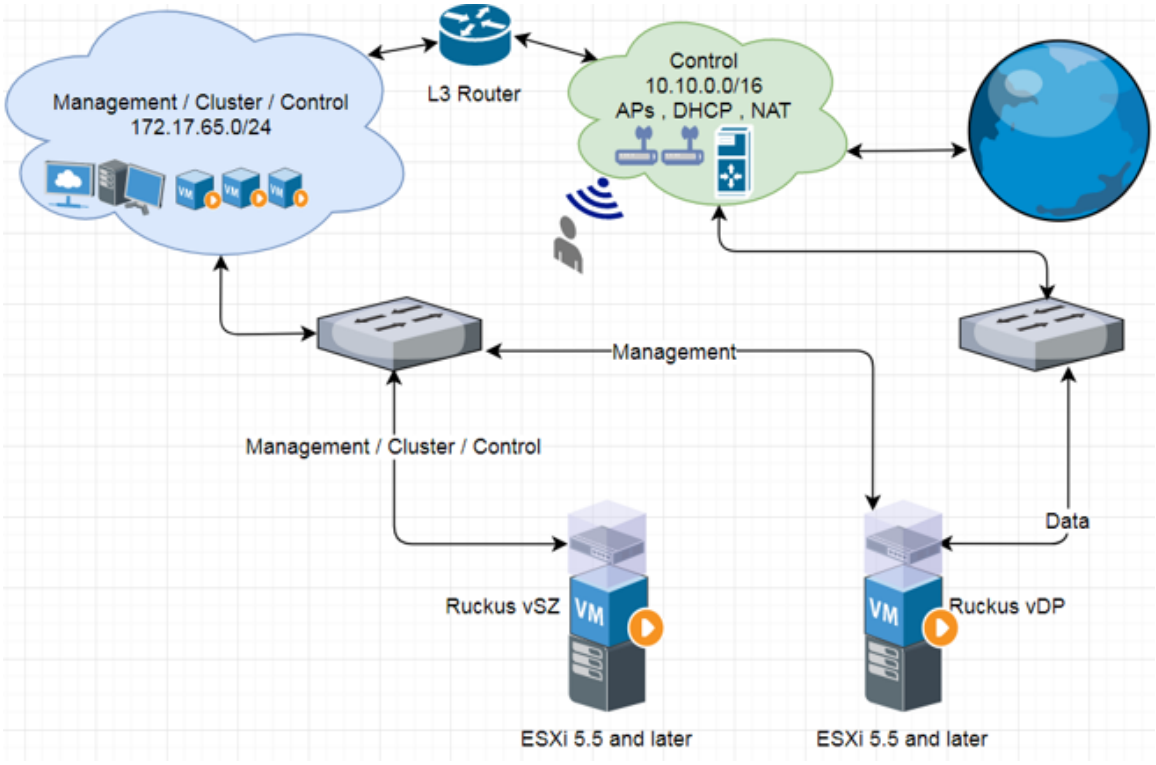
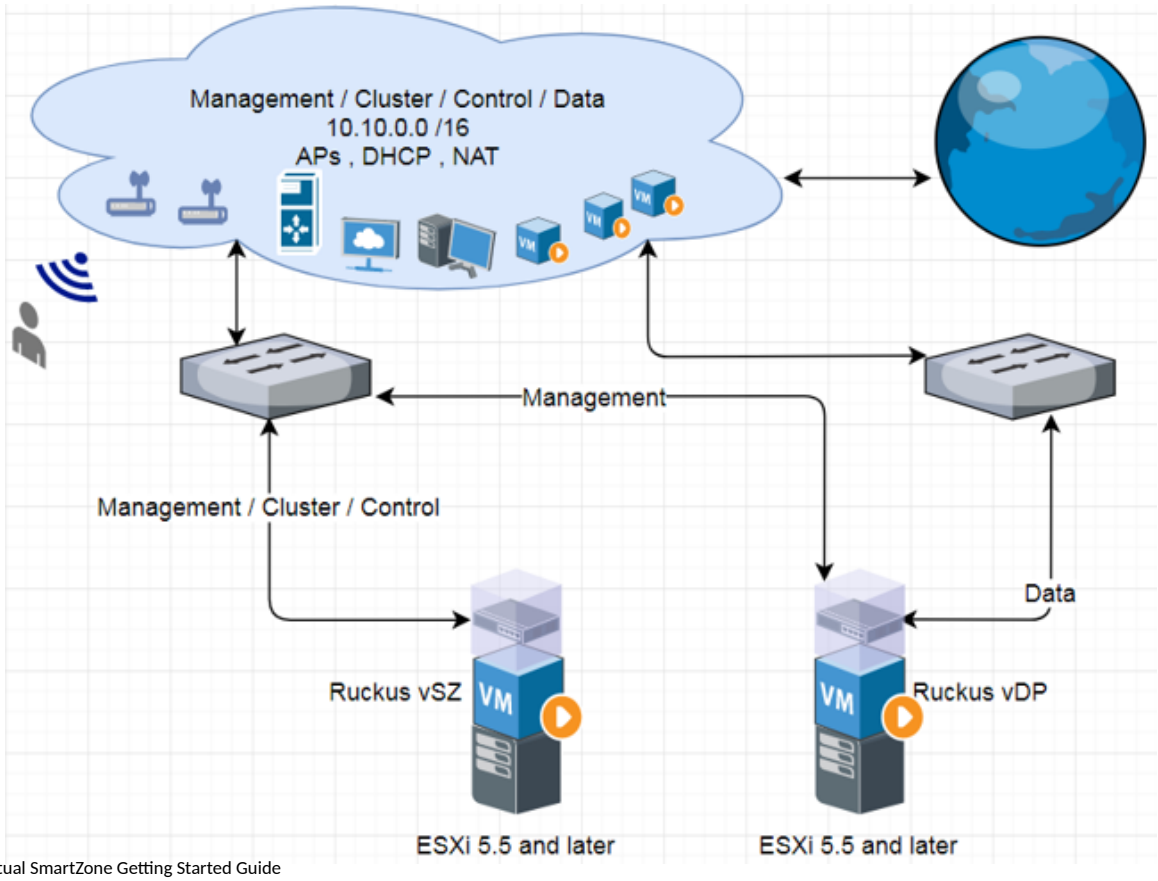


FIGURE 207 Example 2: vSZ-E with one Group Interface



Deployment Procedure on the ESXi Server

The following are basic instructions for setting up vSZ on the ESXi server.

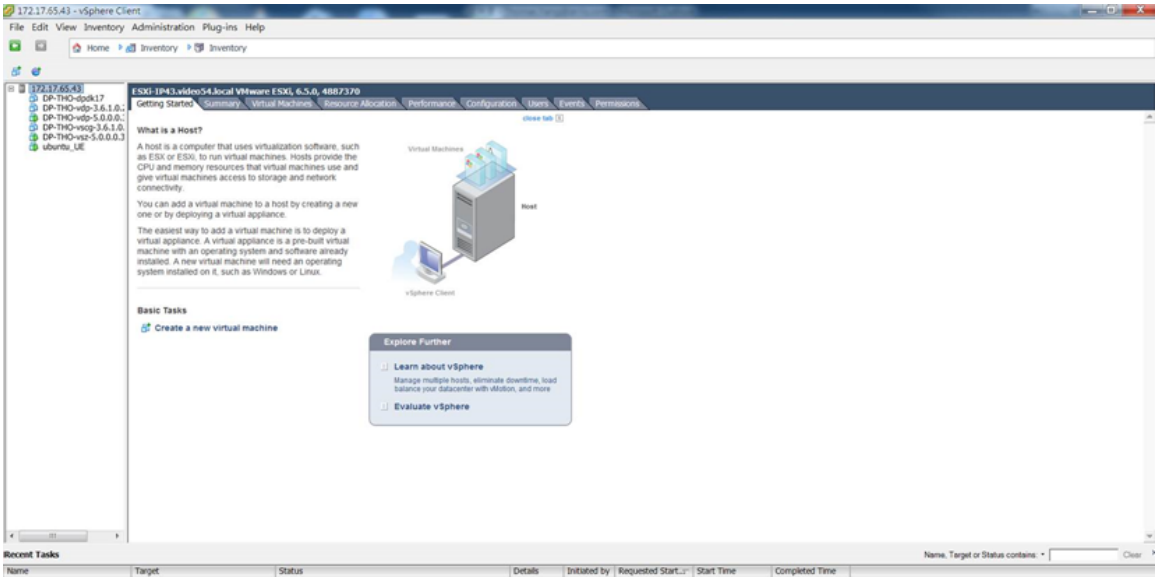
VMware ESXi 5.5 is installed and working.

1. Login to the server through vSphere client tool as seen below.

FIGURE 208 Login to vSphere

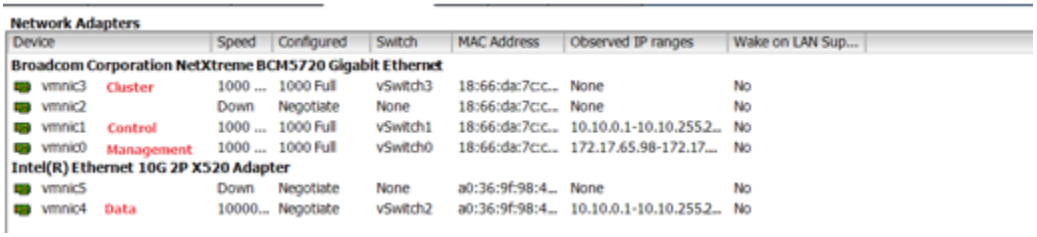
The vSphere Client management page appears as shown in the following figure.

FIGURE 209 vSphere Client management page



2. Navigate to **Configuration** > **Network Adapters**. Ensure the physical ports are linked to the correct port speed as seen below.

FIGURE 210 Define network adapters

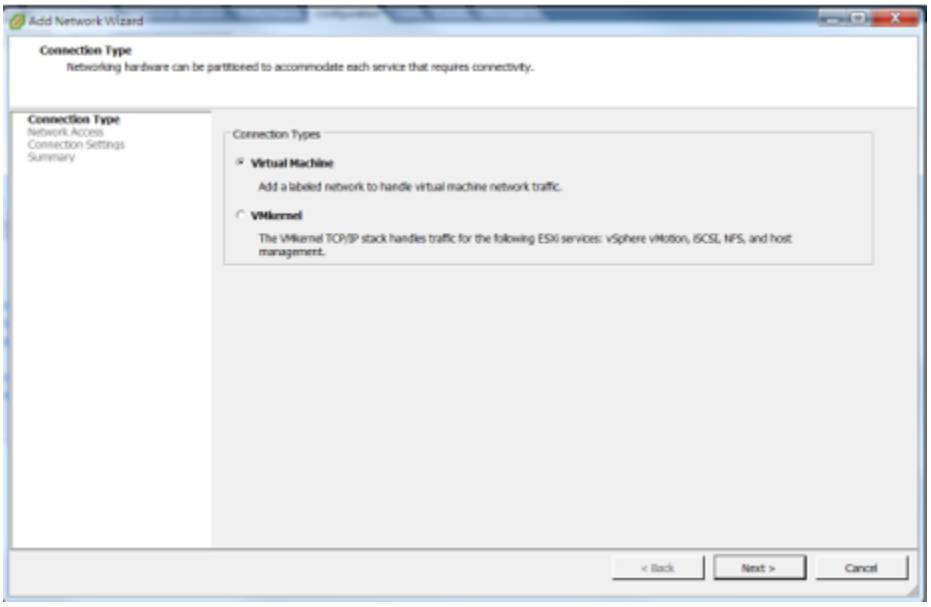


Network Adapters

Device	Speed	Configured	Switch	MAC Address	Observed IP ranges	Wake on LAN Sup...
Broadcom Corporation NetXtreme BCM5720 Gigabit Ethernet						
vmnic3 Cluster	1000 ...	1000 Full	vSwitch3	18:66:da:7c:c...	None	No
vmnic2	Down	Negotiate	None	18:66:da:7c:c...	None	No
vmnic1 Control	1000 ...	1000 Full	vSwitch1	18:66:da:7c:c...	10.10.0.1-10.10.255.2...	No
vmnic0 Management	1000 ...	1000 Full	vSwitch0	18:66:da:7c:c...	172.17.65.98-172.17....	No
Intel(R) Ethernet 10G 2P X520 Adapter						
vmnic5	Down	Negotiate	None	a0:36:9f:98:4...	None	No
vmnic4 Data	10000...	Negotiate	vSwitch2	a0:36:9f:98:4...	10.10.0.1-10.10.255.2...	No

3. Create each vSphere standard switch (vSwitch) using the physical network adapters since vSZ requires three interfaces for management, cluster, and control. Navigate to **Configuration** > **Networking** > **Add Networking**. Select the option **Virtual Machine** to choose the connection type.

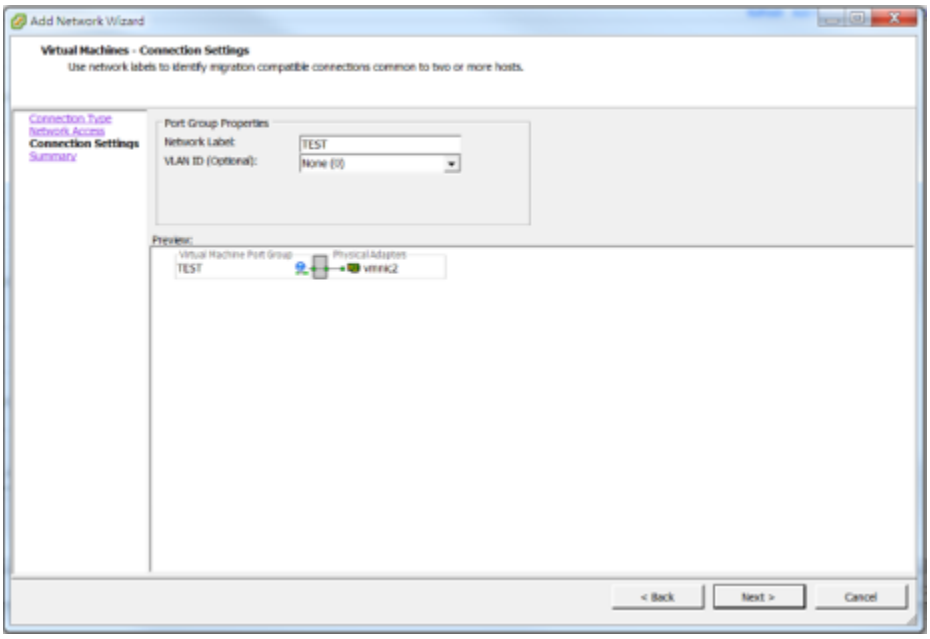
FIGURE 211 Define connection type



4. Click **Next.**
5. Select the Network Adapter from the list and click **Next**.

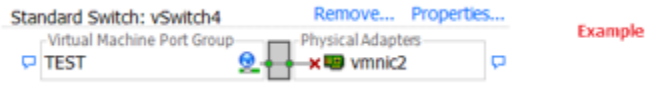
6. Enter the **Network Label** and click **Next** as shown in the following figure.

FIGURE 212 Define the Network Adapter



7. Click **Finish**.
8. View the created vSwitch as seen below.

FIGURE 213 View created vSwtich

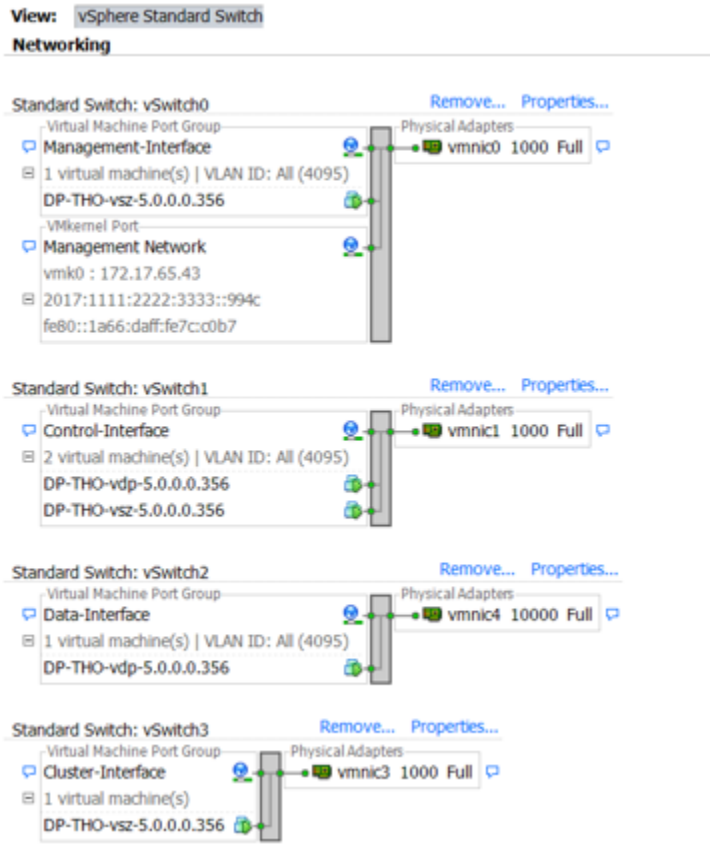


Example

9. Repeat step 3 to step 6 to create three vSwitch for vSZ. View the created vSwitch as seen below.

   NOTE
   vSZ management interface is associated to the Control-IP-Domain.

FIGURE 214 View vSwitch for management and data interfaces

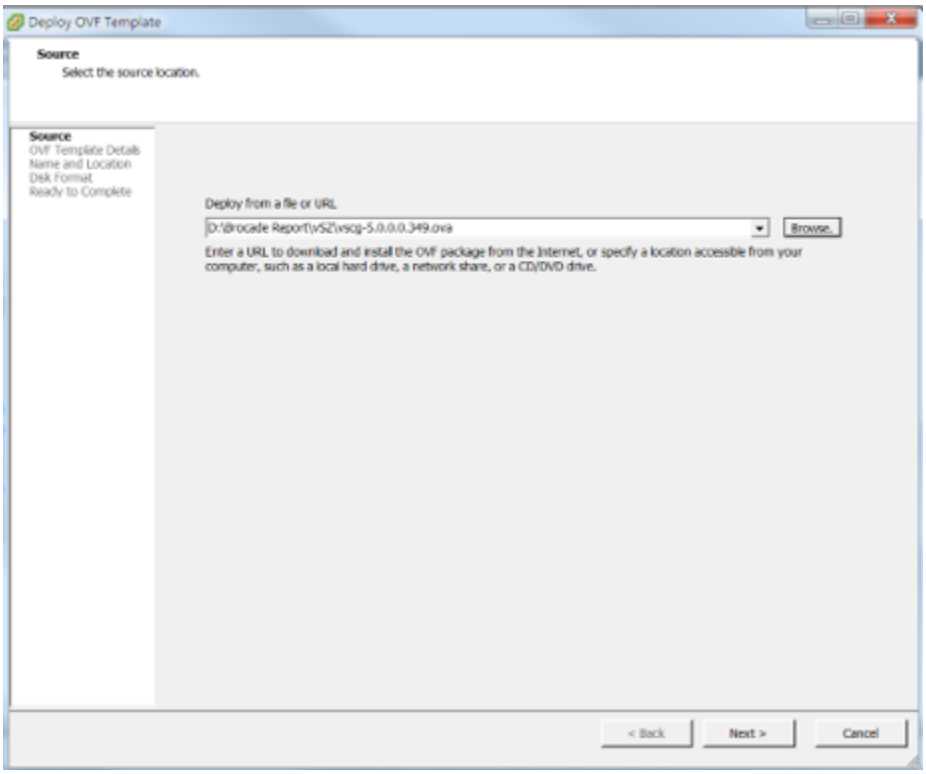


10. Download the vSZ (.ova file) from the Ruckus Website.
11. Click **File** > **Deploy OVF Template**.

    The Deploy OVF Template form appears.

12. Click **Browse** to select the source location to install the OVF package as shown in the following figure.

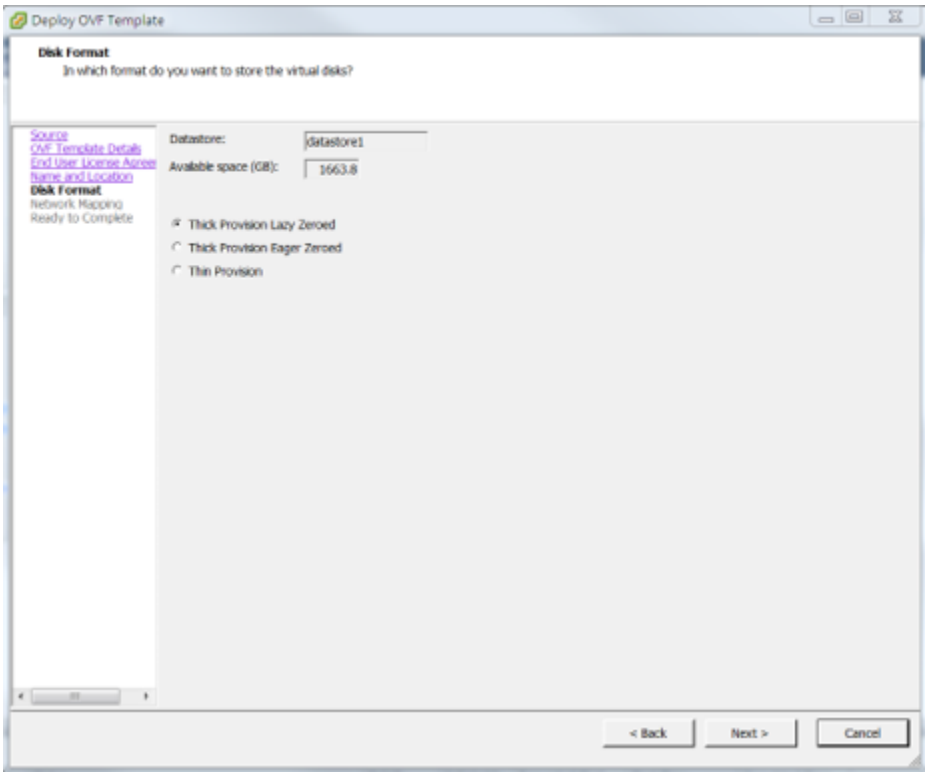
FIGURE 215 Deploy the file



13. Click **Next.**

14. Enter the vSZ datastore name and choose the disk format as seen below.

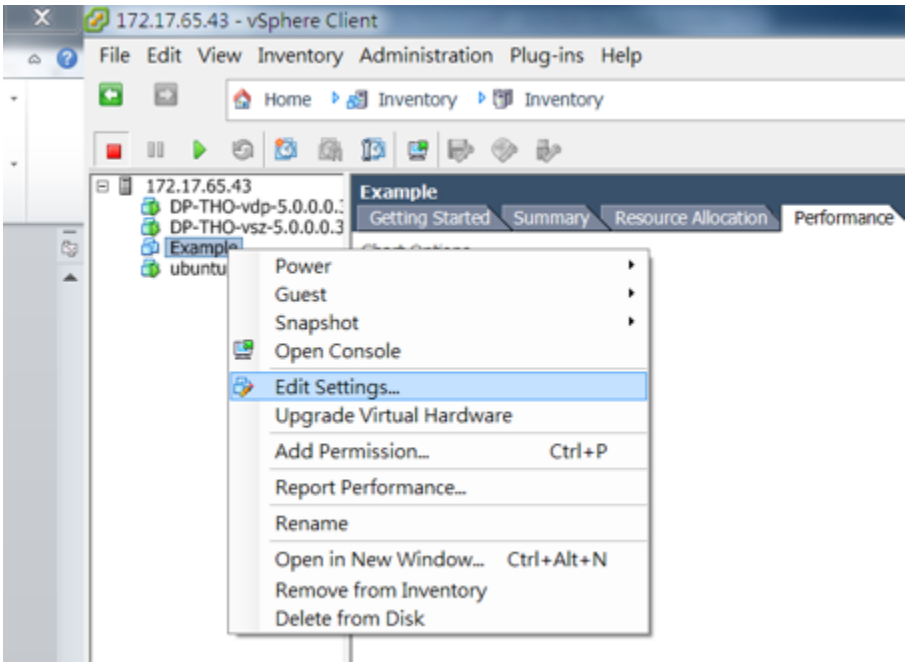
FIGURE 216 Choose the disk format



15. Click **Next** and wait for deploying.

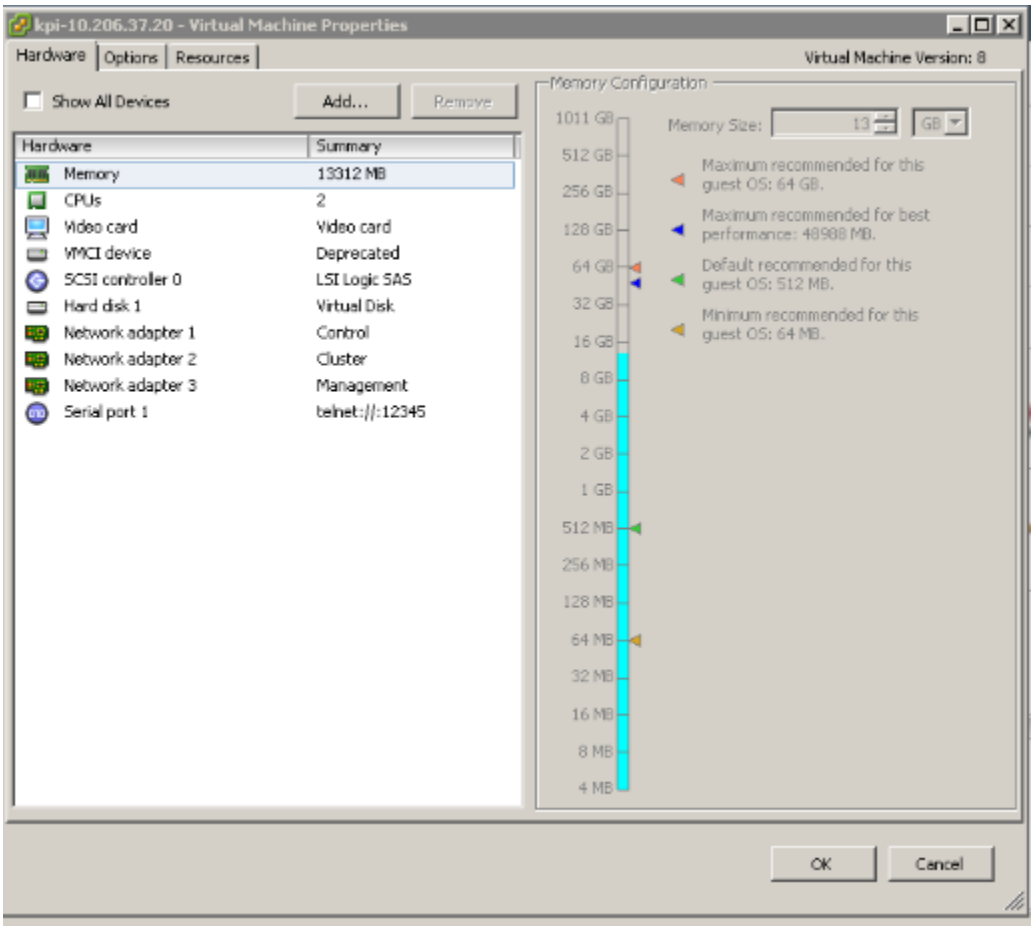
16. From the vSphere client, select **Edit Settings** to change network interface settings for vSZ-H and vSZ-E as shown in the following figure.

FIGURE 217 vSphere Client Settings



17. By default, vSZ supports three network interfaces as shown in the figure.

FIGURE 218 vSphere Setting



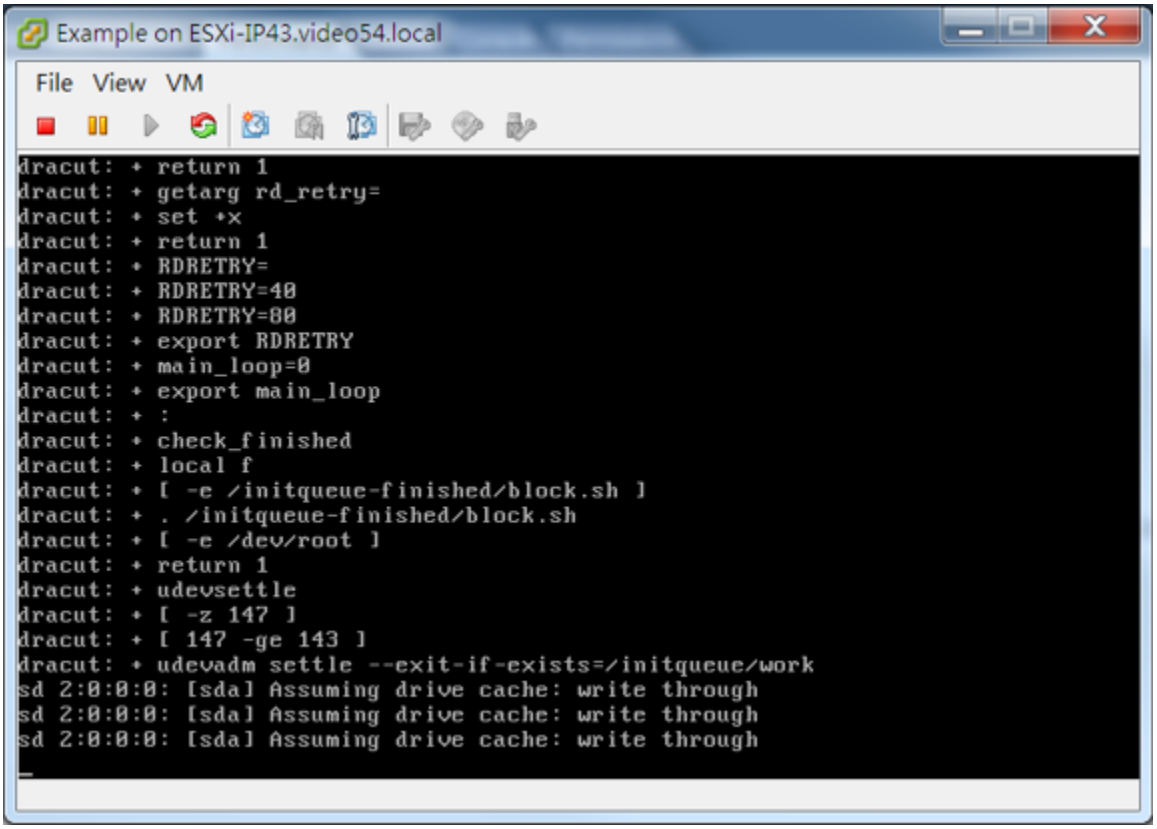
NOTE
If your vSZ is running as Essential mode, select the two interfaces and click **Remove**.

Connect to vSZ Using CLI on ESXi Server

Follow the below procedures to connect to vSZ.

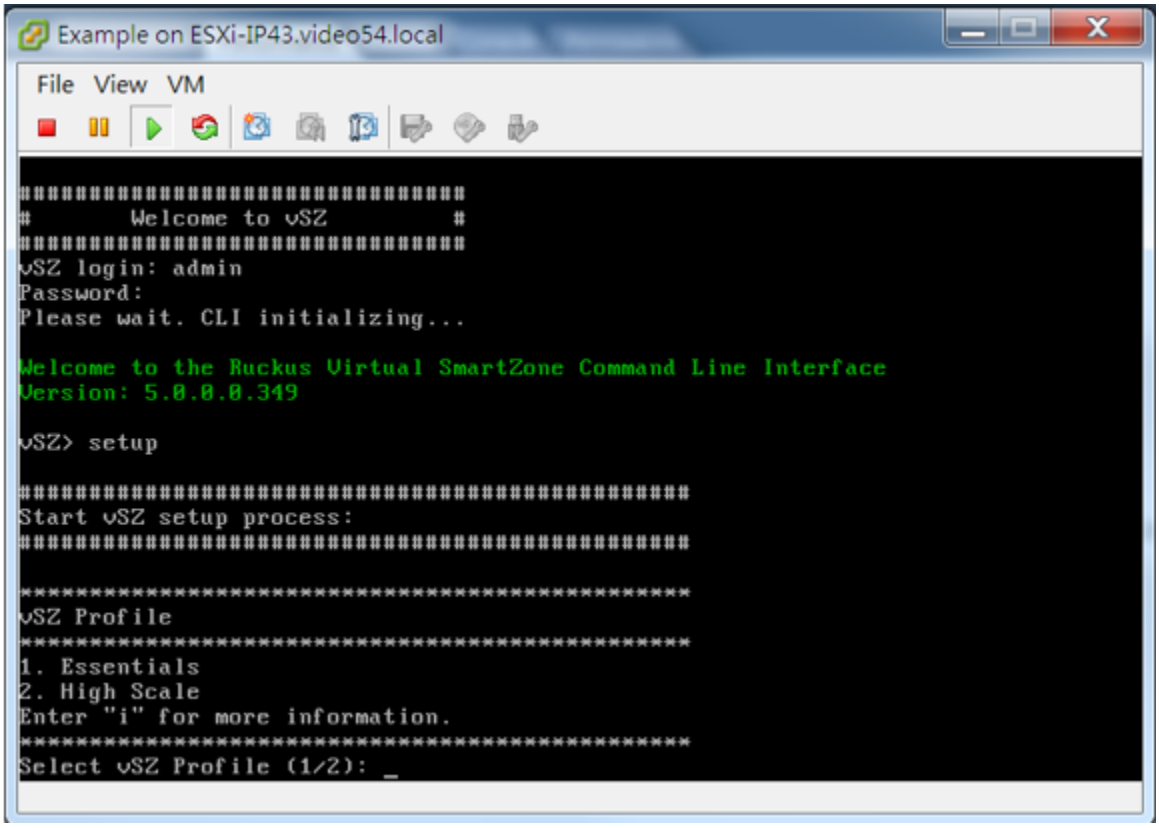
Open a CLI console window to run the deployed vSZ.

FIGURE 219 Run vSZ on the console



1. At the login prompt, login using **administrator** credentials of username and password. Run the **setup** command to initialize vSZ as shown in the figure below.

FIGURE 220 Login and Privileged mode

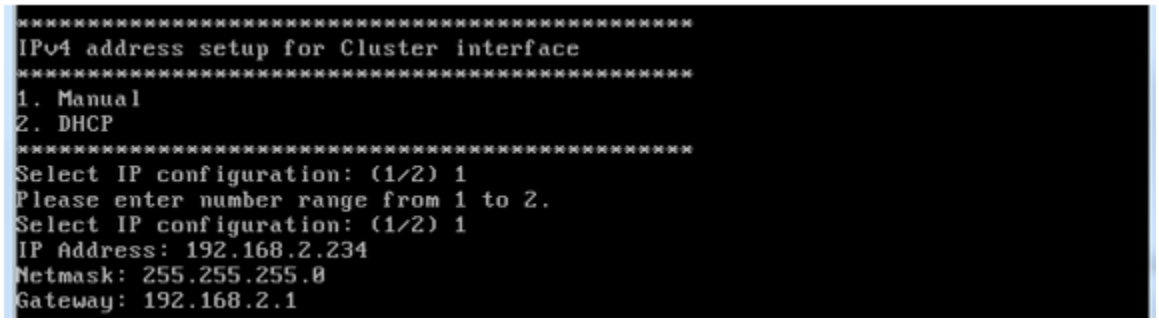


2. Enter **2** for High-Scale mode and press **Y** to continue.
3. Enter static IP address for control interface as shown in the figure below.

FIGURE 221 Static IP Address for Control Interface

4. Enter static IP address for cluster interface as shown in the figure below.

   FIGURE 222 Static IP Address for Cluster Interface



5. Enter static IP address for management interface as shown in the figure below.

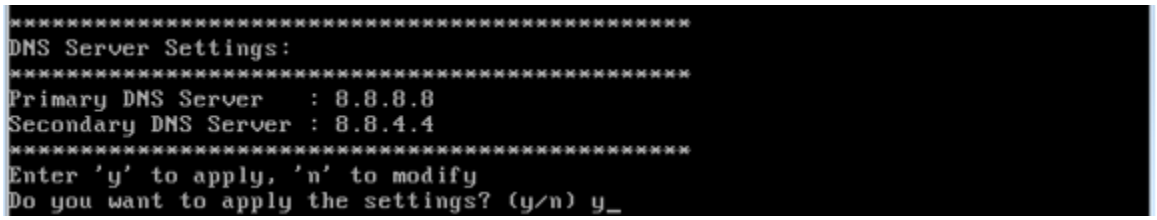
   FIGURE 223 Static IP Address for Management Interface

6. Select the default gateway interface. Enter **1** for control interface, **2** for cluster interface, and **3** for management interface as shown in the figure below.

   FIGURE 224 Default Gateway Interface

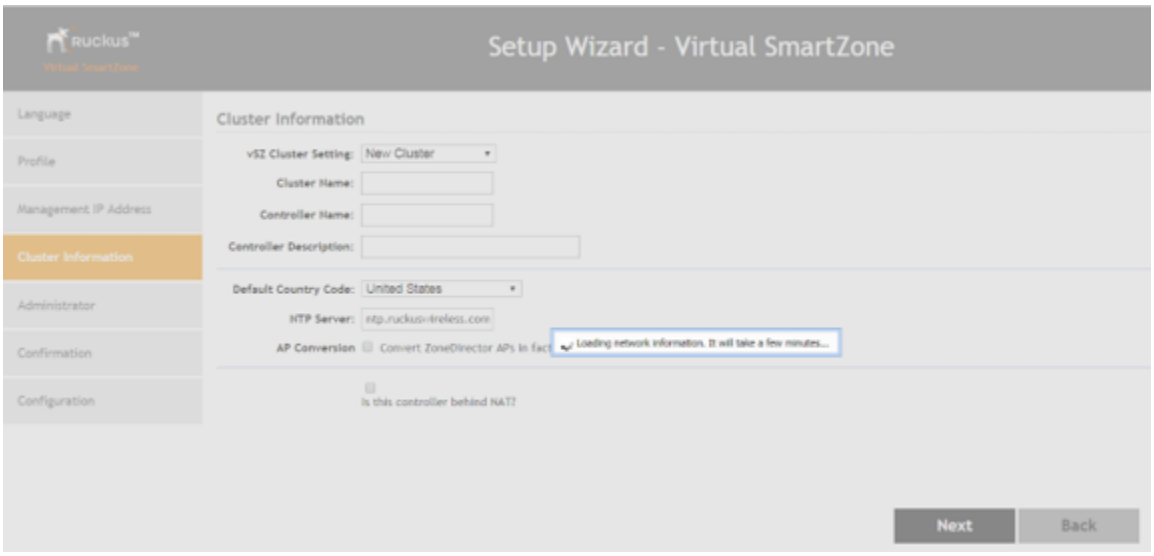
7. Enter the DNS server setting and press **Y** to apply all setting.

FIGURE 225 DNS Server Settings



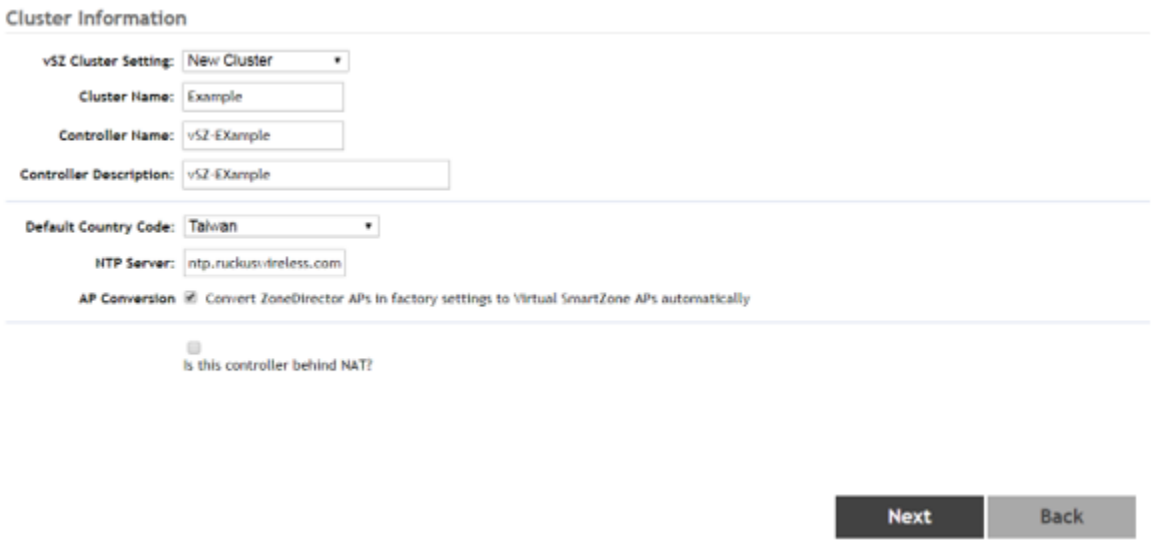
8. Access the web link http://172.17.65.234:8443 to continue other setting as shown in the figure below.

FIGURE 226 vSZ Web UI



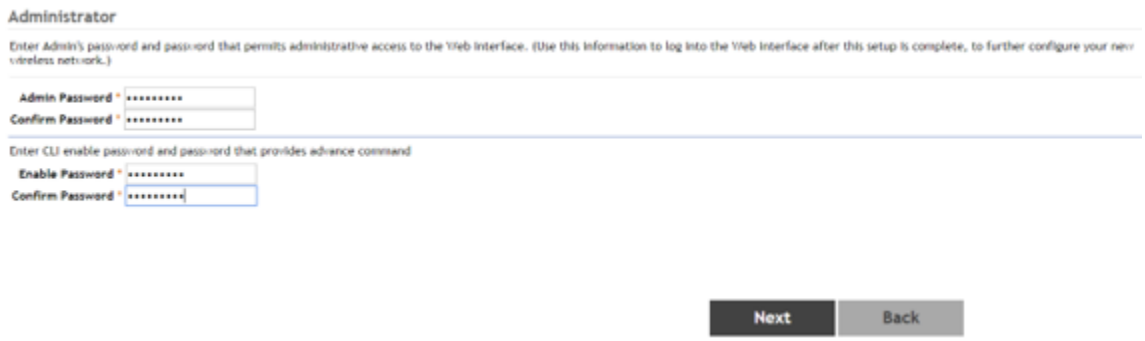
9. Enter your **Cluster Information** and click **Next** as shown in the following figure.

FIGURE 227 Cluster Information



10. Enter your vSZ Administrator password requirements and click **Next** as shown in the following figure.

FIGURE 228 vSZ Administrator Password

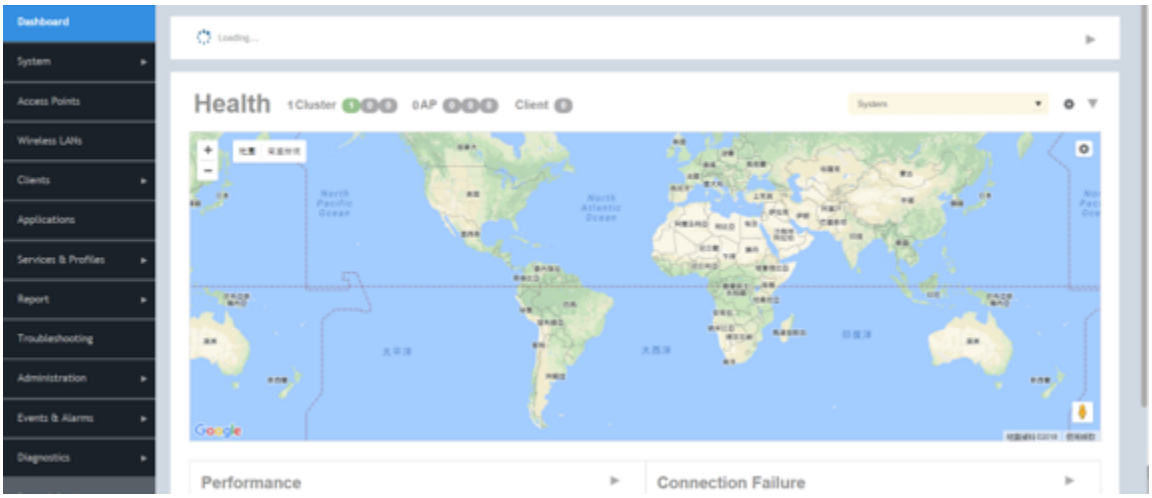


11. Click **Finish** and wait until vSZ is configured.
12. After vSZ is configured, reconnect to vSZ web as shown in the following figure.

FIGURE 229 vSZ Configuration

13. Enter **Username** and **Password** to access vSZ as shown in the following figure.

FIGURE 230 vSZ Homepage



Deploy vSZ on Linux Server

Hardware Requirement and Prerequisite for LINUX CentOS 7

The following are the hardware and prerequisite for deploying vSZ on LINUX CentOS 7.

Hardware Requirement

1. DELL Inc. PowerEdge R320
2. Linux CentOS 7
3. Broadcom NetXtreme BCM5720 Gigabit Ethernet 2 Ports
4. Intel Ethernet 10G 2P X520

Prerequisite

- A Linux host enabled KVM which to install vSZ VM. Prefer CentOS 7 and later.
- Download the vSZ package (.qcow2 file) from Ruckus support .
- The IP addresses, netmask, gateway, DNS, DHCP and NAT support for vSZ.
- Ensure if the vSZ license that you have, is a high-capacity mode or an essential mode.
- 1Ensure the number of physical network interfaces. Choose the interface group, 3 or 1, that would be used implement for vSZ. vSZ-E mode supports only 1 interface group. vSZ-H mode supports both 3 and 1 interface groups.
- Before you power on vSZ, ensure that the networking is configured on LINUX.
- Recommended to use static network addresses that are assigned to vSZ during setup.
- Using CentOS 7, install KVM package with the **yum** command.

```
root@localhost ruckusvnc]# yum -y install qemu-kvm qemu-img virt-manager virt-viewer virt-install
libvirt libvirt-phthon libvirt-client
```

- Ensure KVM is active and running the following command.

```
[root@localhost ruckusvnc]# systemctl status libvirtd
```

- Edit the following commands and file.

```
sudo yum install grub2-common

gedit /etc/default/grub
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=centos/root rd.lvm.lv=centos/swap rhgb quiet
intel_iommu=on"
GRUB_DISABLE_RECOVERY="true"

sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

- Reboot Linux host.

NOTE
Due to different servers and NIC, the deployment procedure mentioned in this section is for reference.

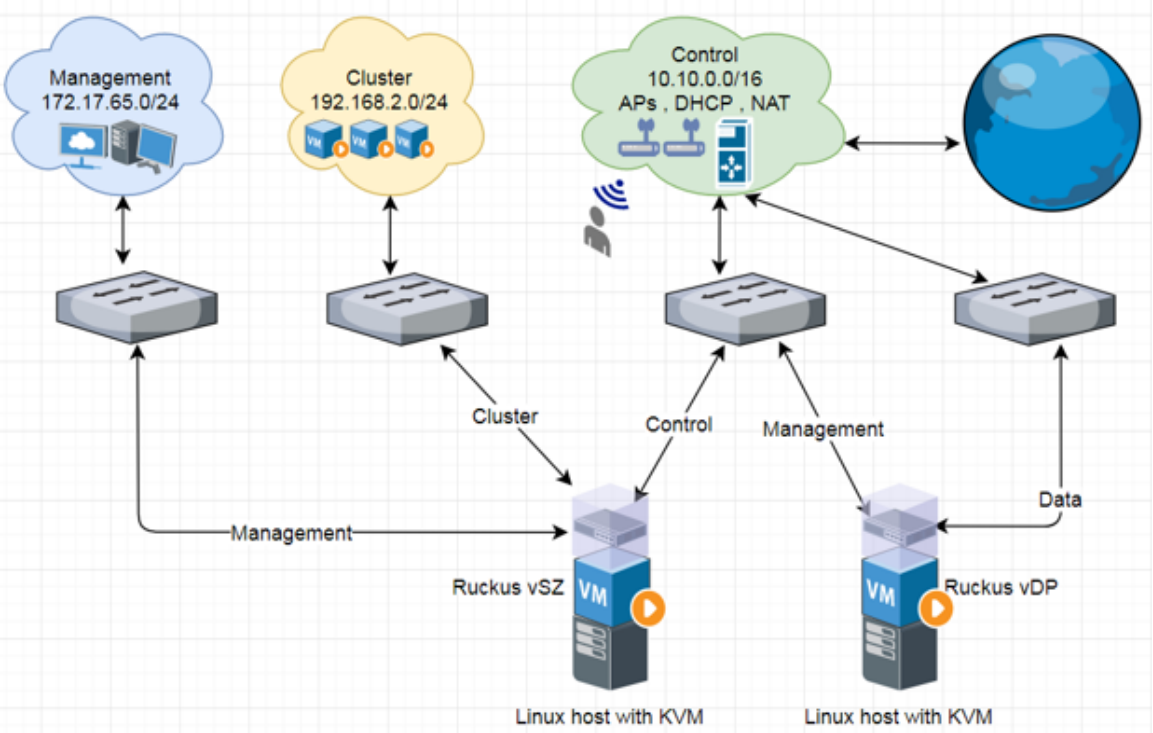
Topology for vSZ Deployment on LINUX CentOS7

The network topologies for vSZ deployment on LINUX CentOS 7.

The following are basic topologies for setting up vSZ. Based on your requirement you can choose any of the alternatives for deployment.

- High-Scale mode with three group interfaces.

FIGURE 231 vSZ-H with Three Group Interfaces



- Essentials mode with one group interface.

FIGURE 232 Example 1: vSZ-E with one Group Interface

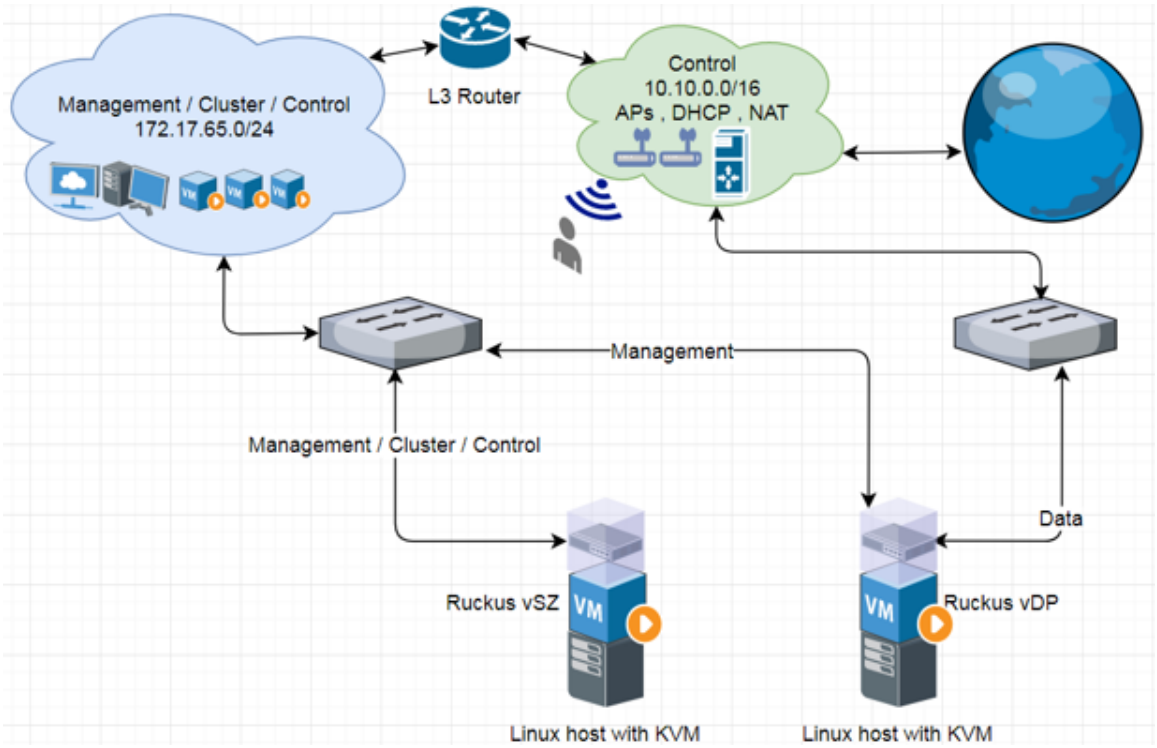
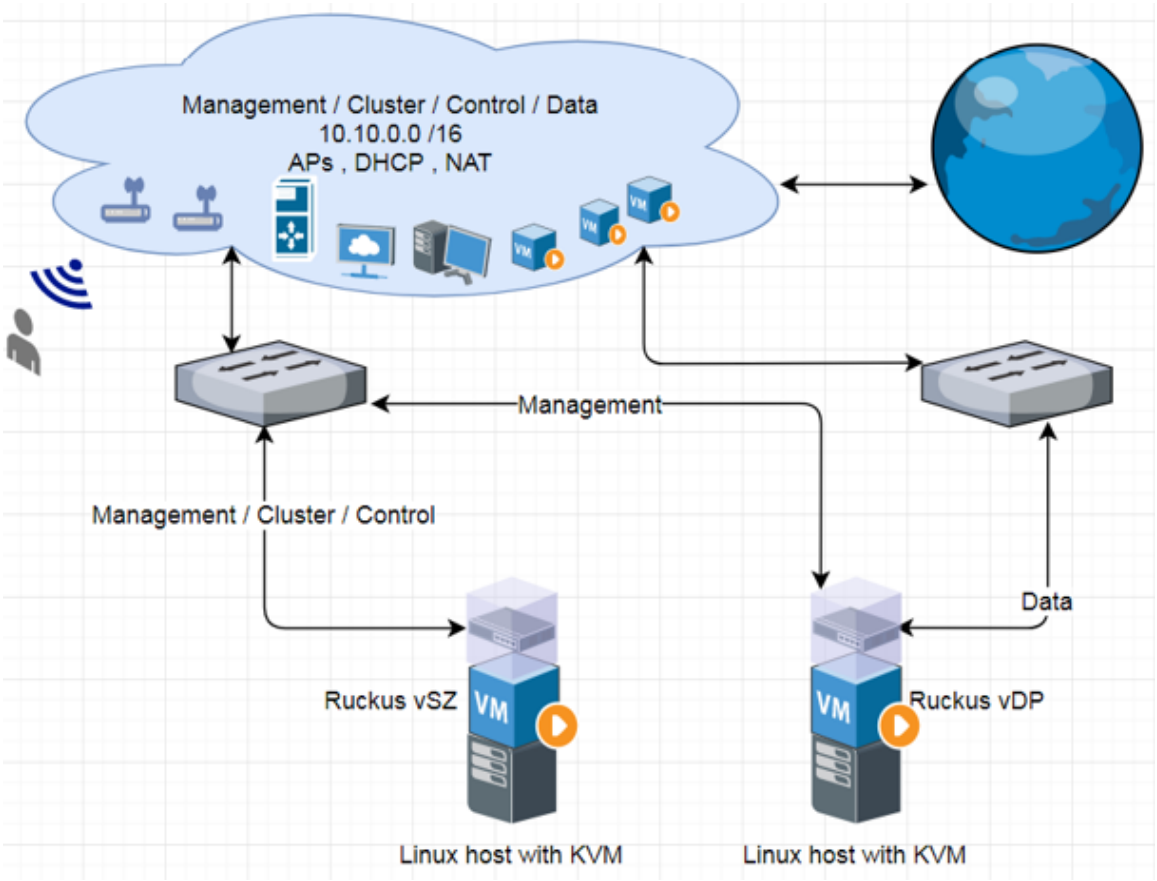


FIGURE 233 Example 2: vSZ-E with one Group Interface



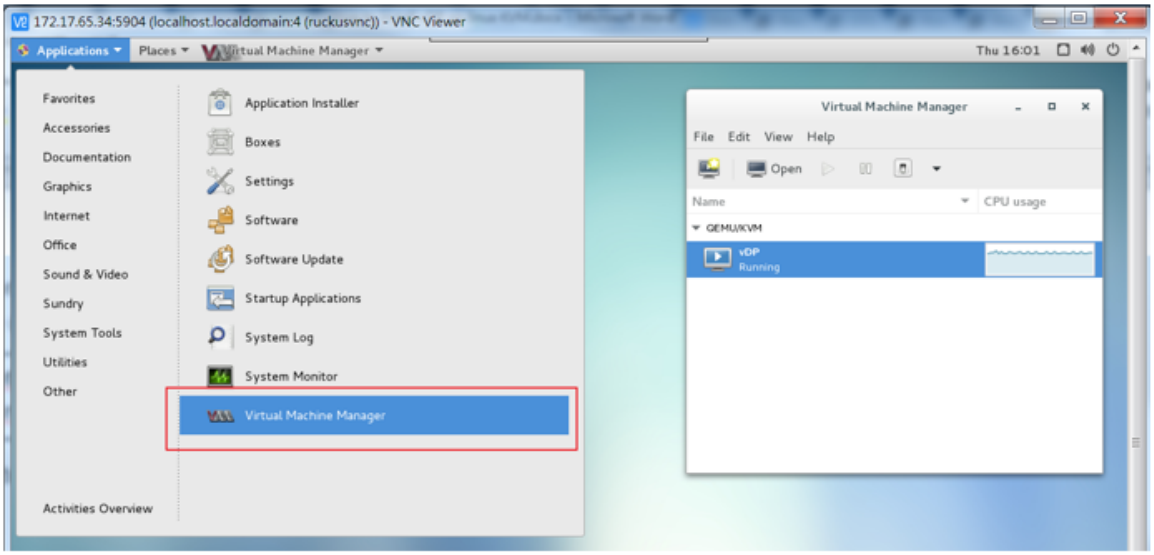
Deployment Procedure on the LINUX Server

The following are basic instructions for setting up vSZ on LINUX KVM.

LINUX CentOS 7 KVM Package is installed and working.

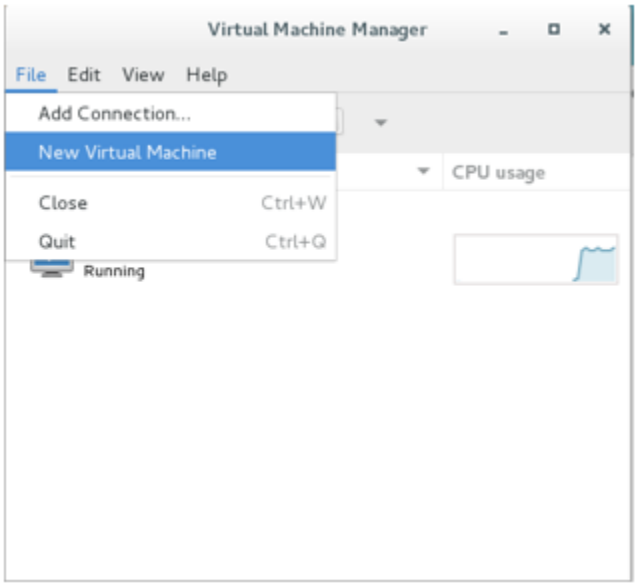
1. Download vSZ package (.qcow2 file) from Ruckus website.
2. From VNC Viewer, click **System Tools** and open the **Virtual Machine Manager** tool. The vSZ status must appear Running as shown in the following figure.

FIGURE 234 Virtual Machine Manager



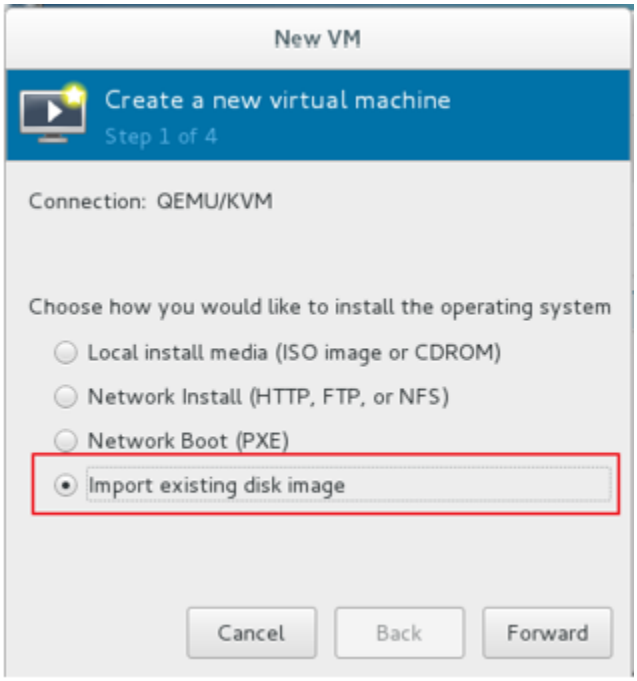
3. Create a new VM.
   a) Click **File** and select **New Virtual Machine** as shown in the following figure.

   FIGURE 235 Creating a Virtual Machine



   b) In the New VM dialog box, choose the disk format option as shown in the following figure.

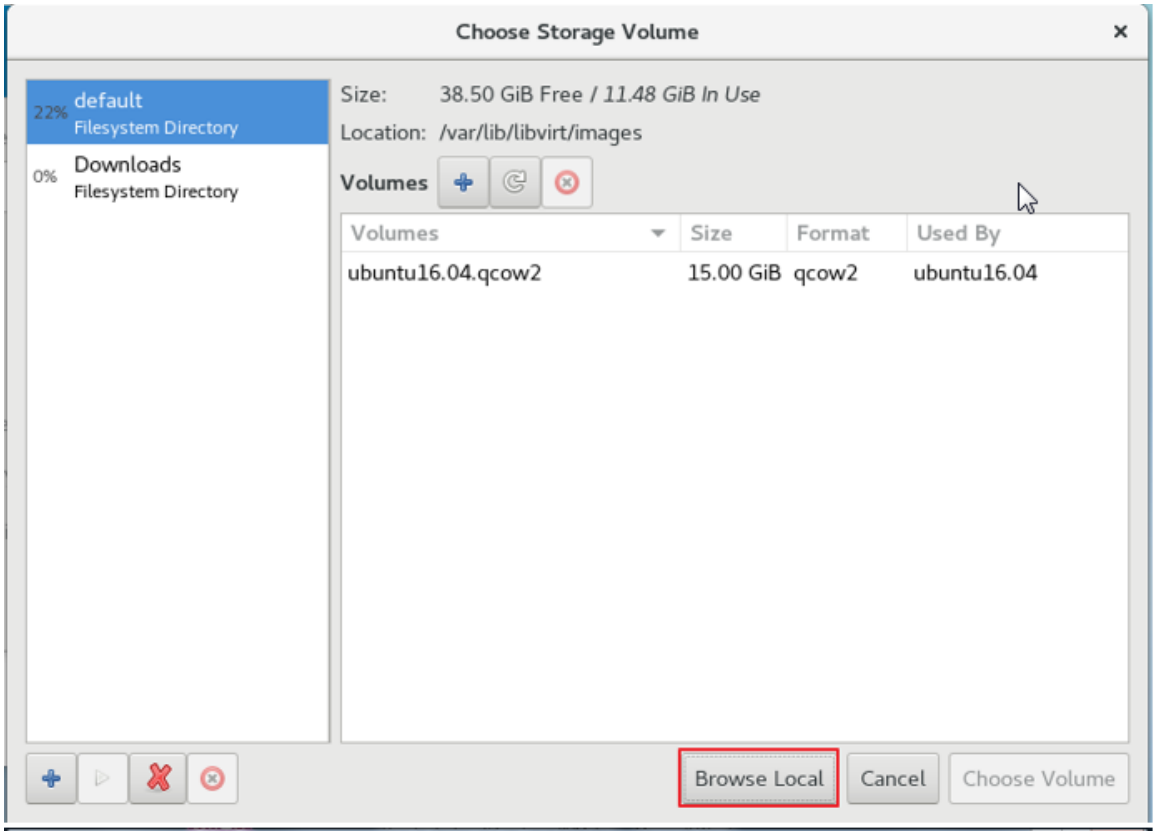
   FIGURE 236 Disk Format



c) Click **Forward**.

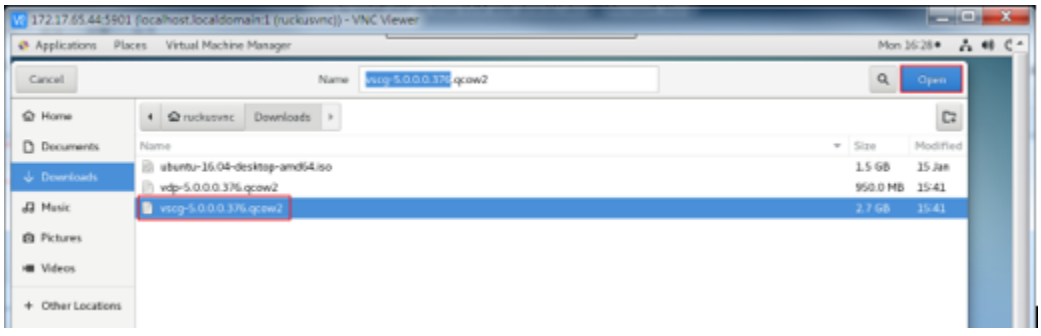
d) Choose destination storage path and storage volume. Click **Browse Local** as show in the following figure.

FIGURE 237 Storage Volume



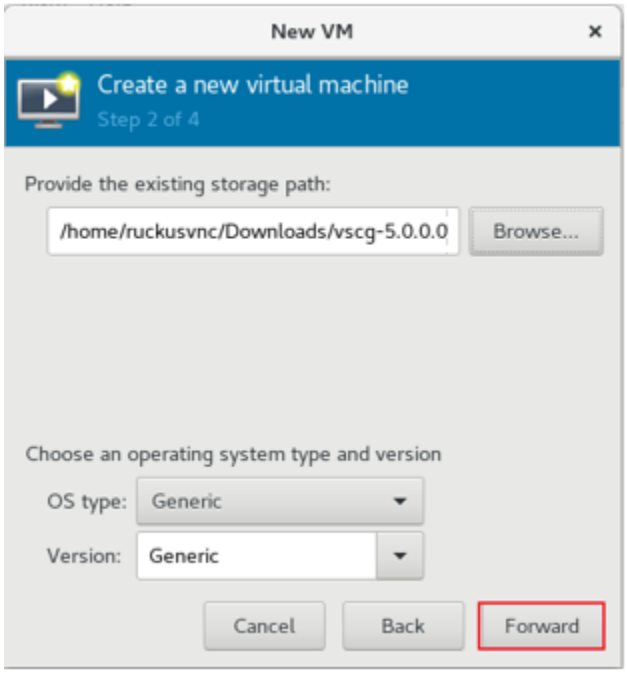
e) Select the vSZ file and click **Open** as shown in the following figure.

FIGURE 238 vSZ File



f) To select the storage path, click **Browse** as shown in the following figure.

FIGURE 239 Storage Path

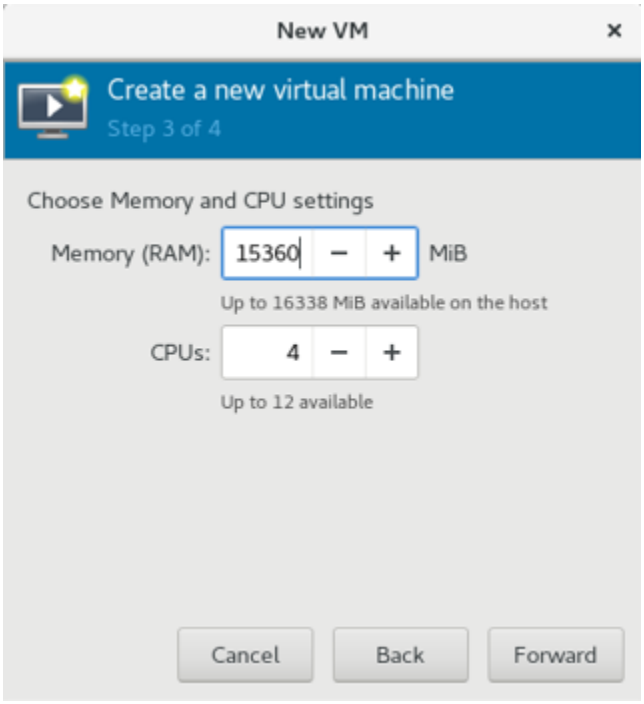


g) Click **Forward**.

h) Enter the **Memory (RAM)** and **CPUs** setting as shown in the following figure.

NOTE
Memory (RAM) must be 15GB and CPUs must be 4 cores.

FIGURE 240 Memory and CPU Settings

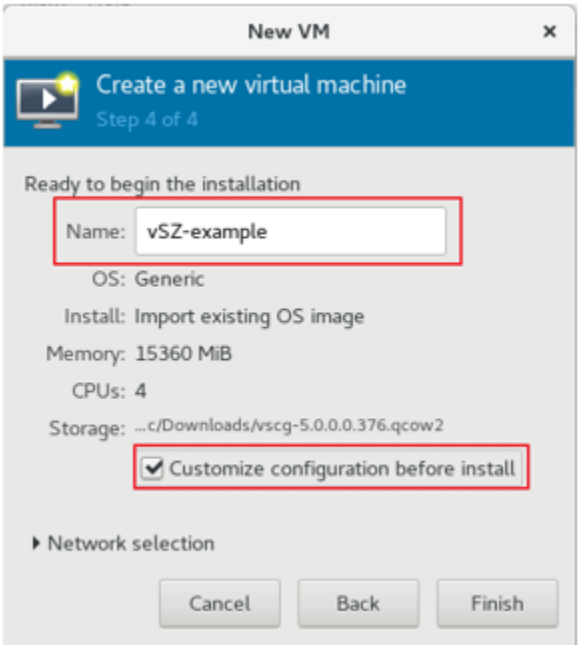


i) Click **Forward**.

j) To confirm the installation process, click **Finish** as shown in the following figure.

NOTE
The sequence for Network interfaces must first be Management and the Data.

FIGURE 241 Installation Confirmation



4. From the VNC Viewer, click **Add Hardware**, select the NIC and choose the **Device model** to update the Control, Cluster and Management interface associate as shown in the following figures.

   NOTE
   vSZ needs three interfaces; Control, Cluster, and Management.

   NOTE
   For Essential mode, you need not add two NICs.

FIGURE 242 Control Interface

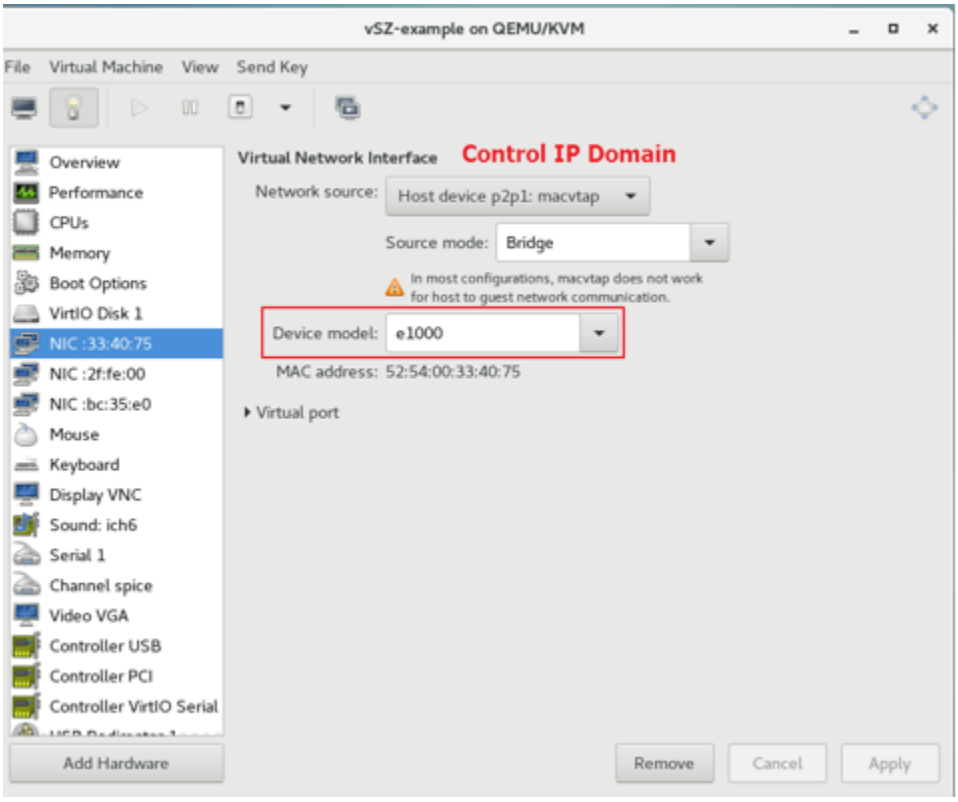


FIGURE 243 Cluster Interface

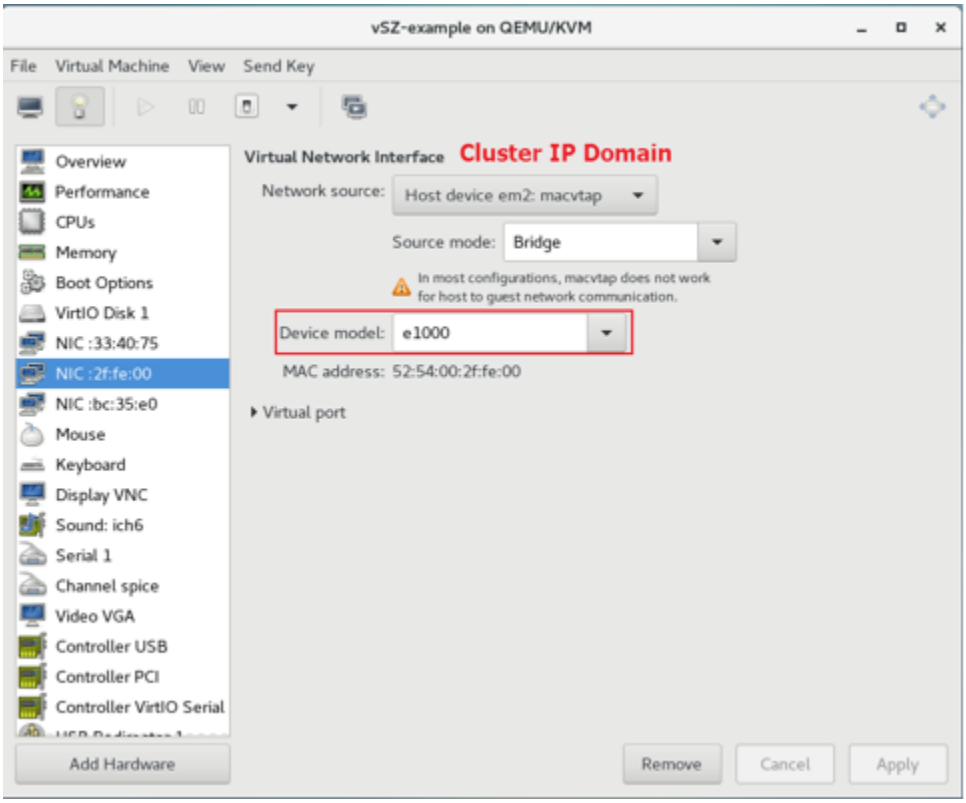
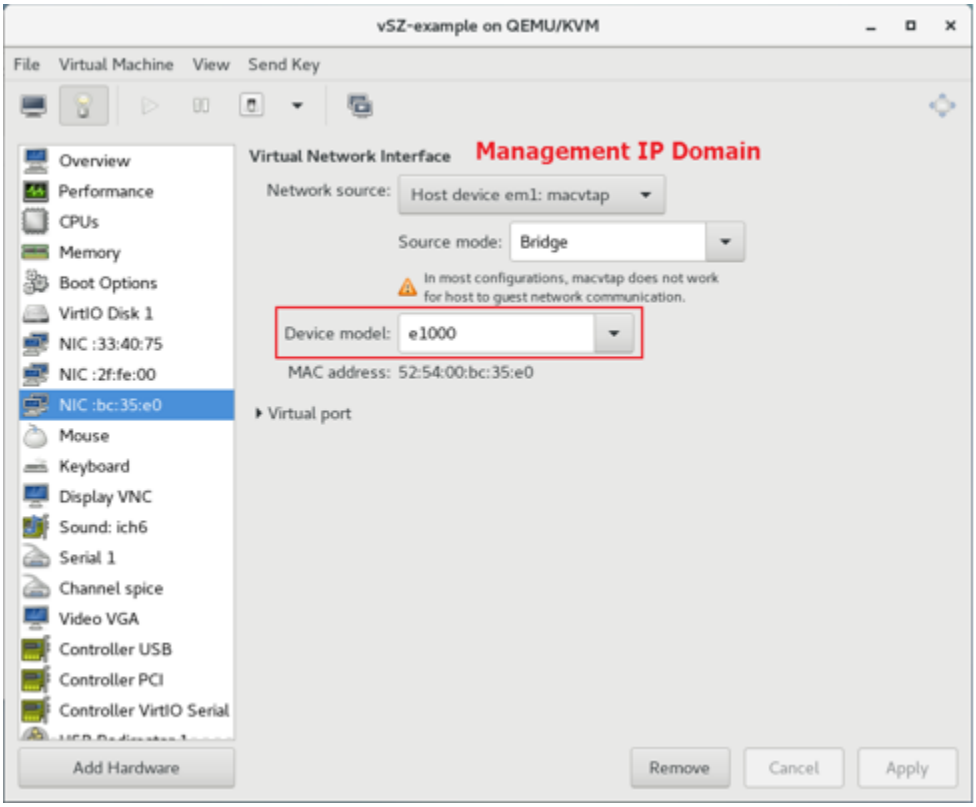
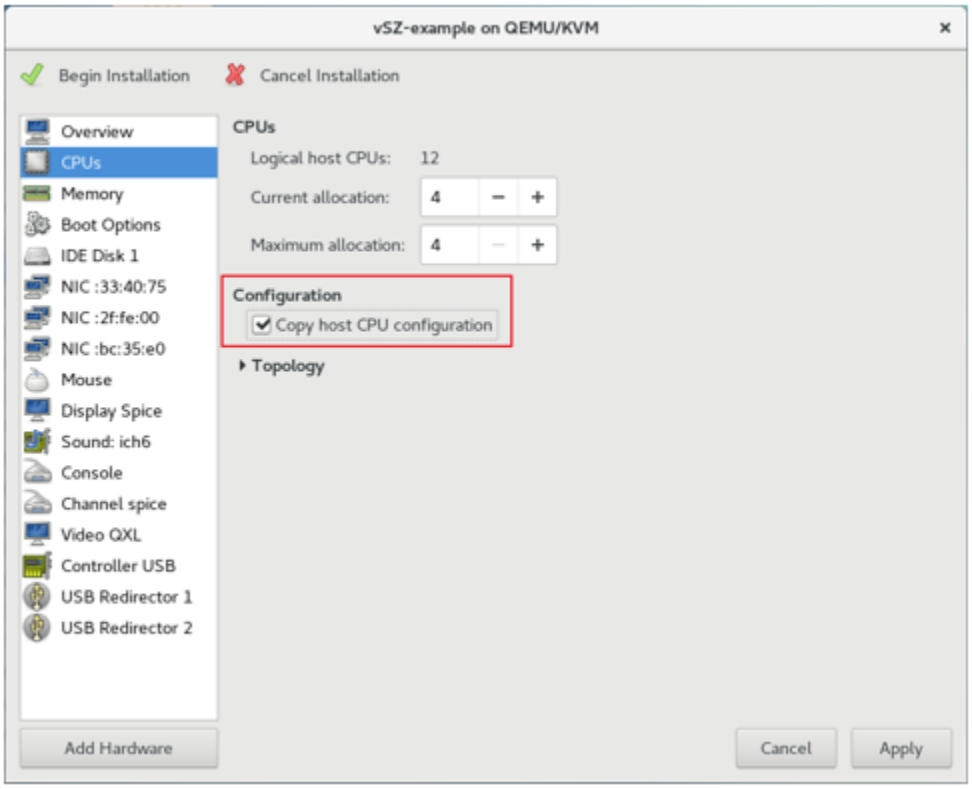


FIGURE 244 Management Interface



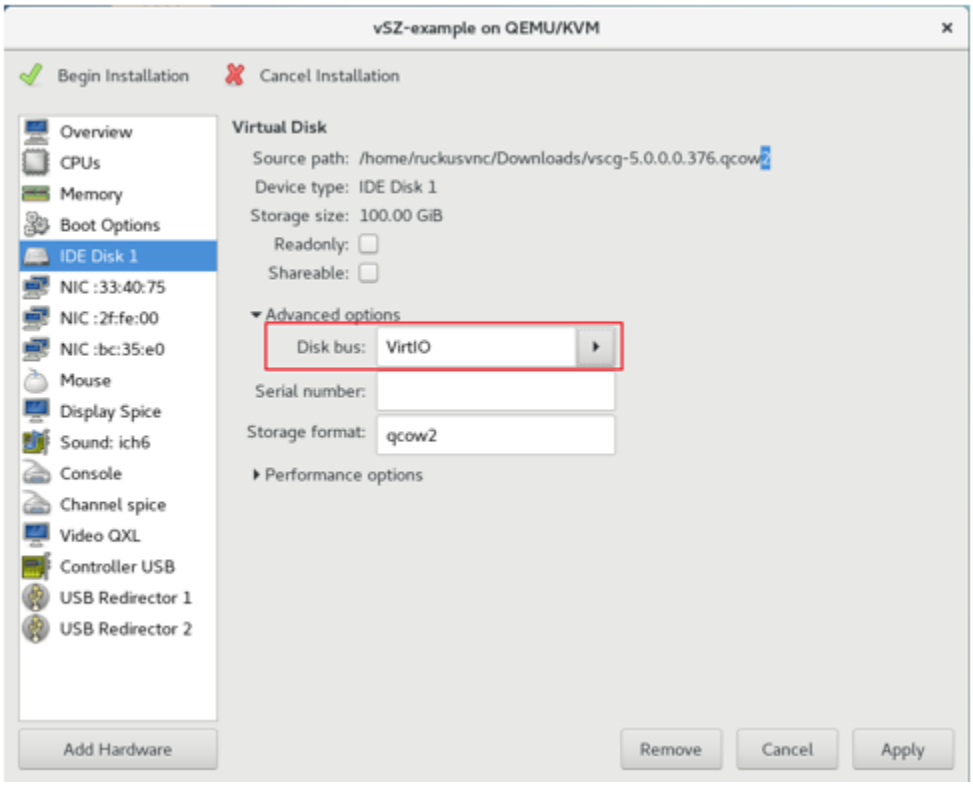
5. Define the CPU Configuration. Select the **Copy host CPU configuration** check box as shown in the following figure.

FIGURE 245 CPU Configuration



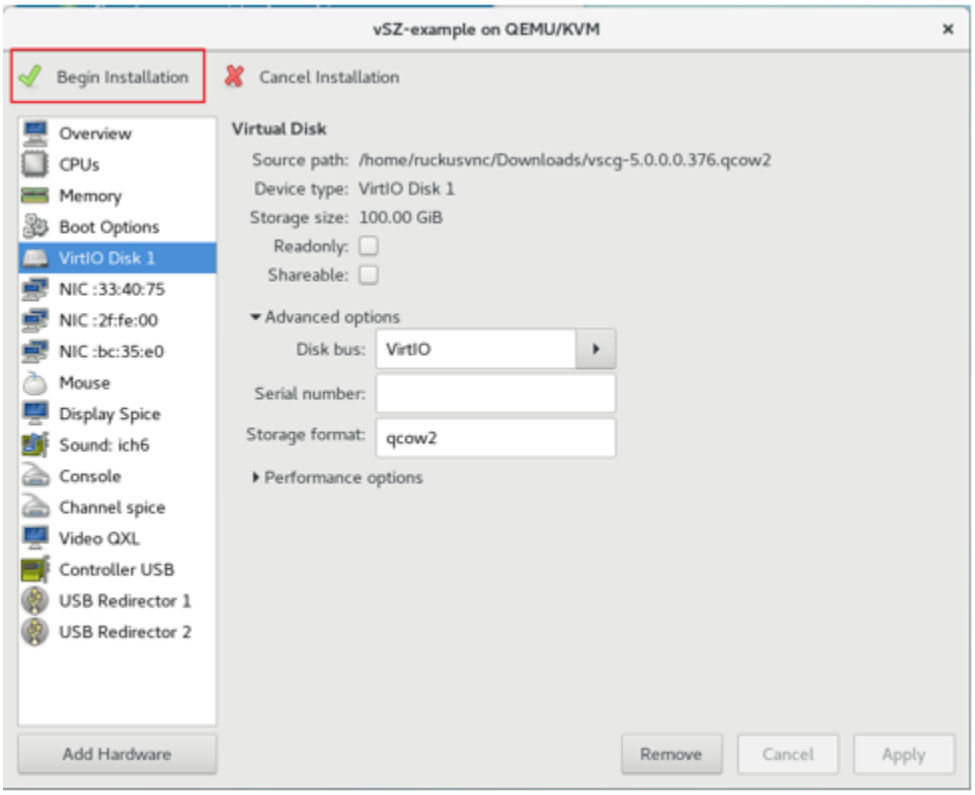
6. Define the IDE Disk Configuration. Choose the **Disk bus** option as shown in the following figure.

FIGURE 246 IDE Disk Configuration



7. Select **Begin Installation** as shown in the following figure.

FIGURE 247 Begin Installation

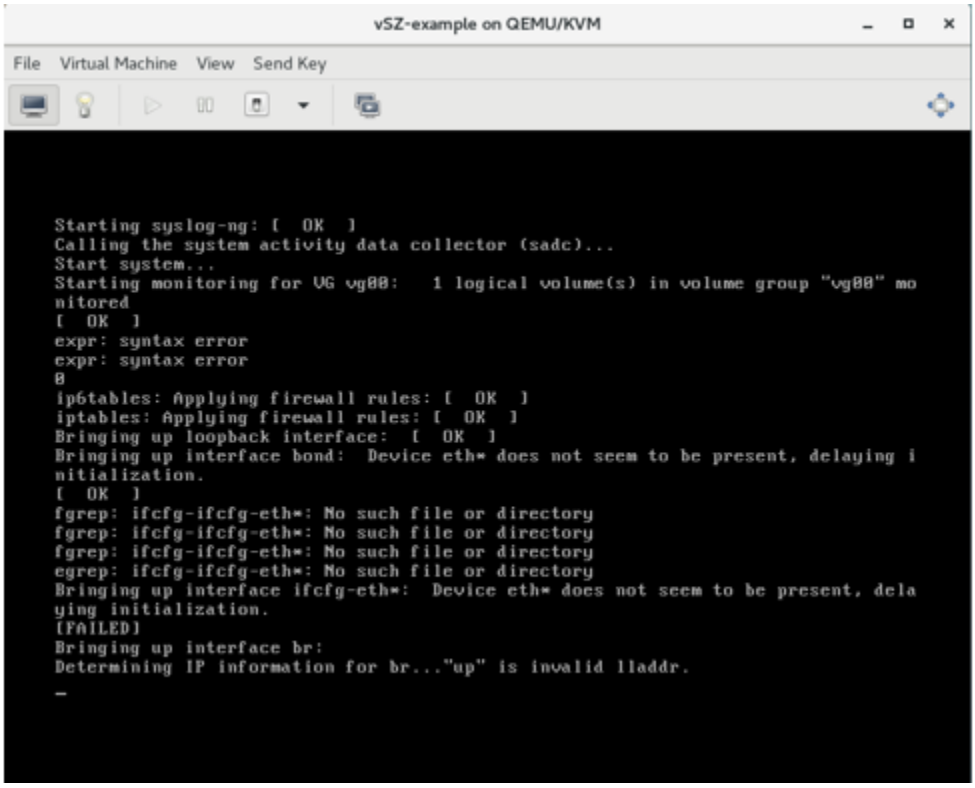


Connect to vSZ Using CLI on LINUX Server

Follow the below procedures to connect to vSZ.

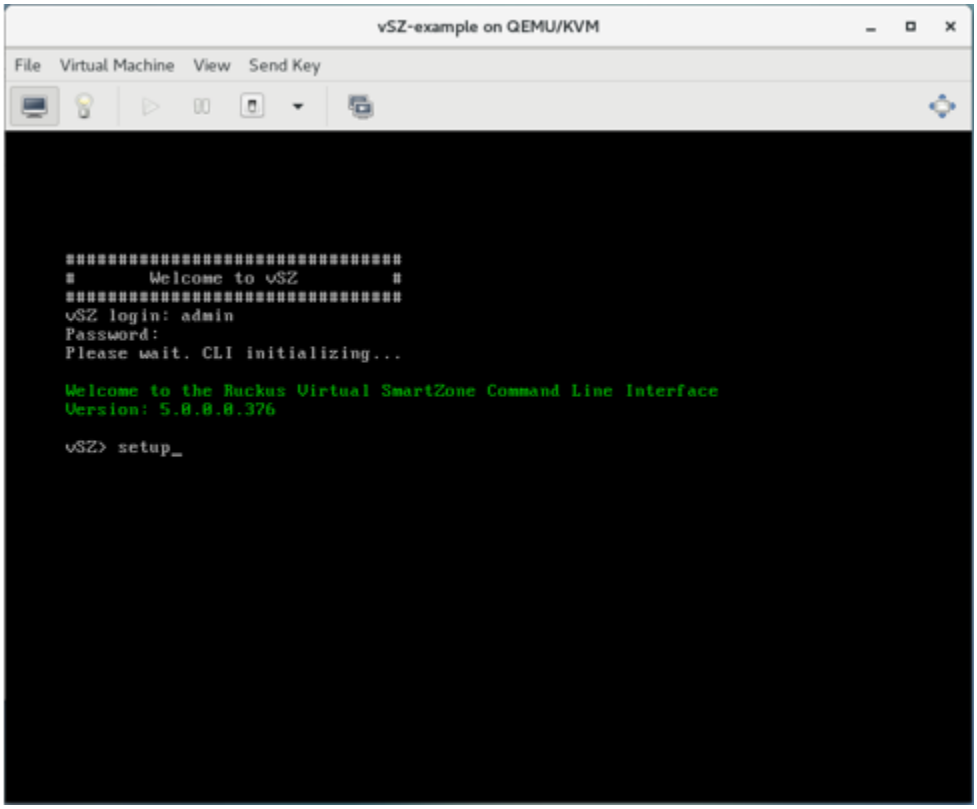
Open a CLI console window to run the deployed vSZ.

FIGURE 248 Run vSZ on the console



1. At the login prompt, login using **administrator** credentials of username and password. Run the **setup** command to initialize vSZ as shown in the figure below.

FIGURE 249 Login and Privileged mode

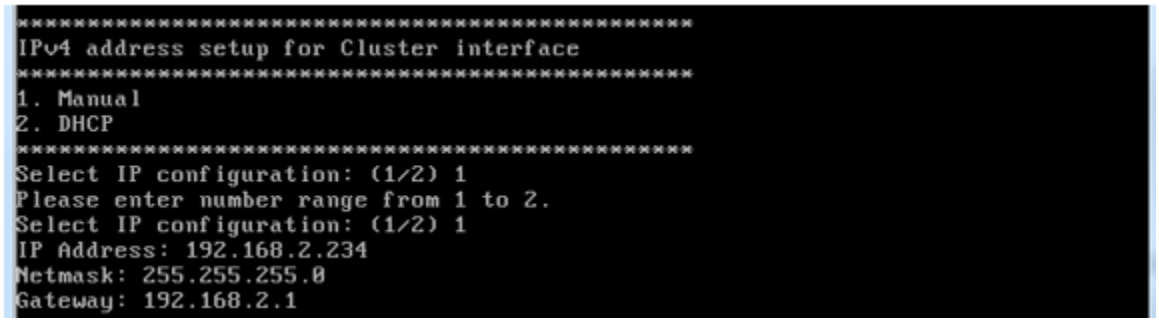


2. Enter **2** for High-Scale mode and press **Y** to continue.
3. Choose IP version **IPv4 only** or **IPv4 and IPv6**. For example, press **1** for **IPv4**.
4. Enter static IP address for control interface as shown in the figure below.

FIGURE 250 Static IP Address for Control Interface

5. Enter static IP address for cluster interface as shown in the figure below.

   FIGURE 251 Static IP Address for Cluster Interface



6. Enter static IP address for management interface as shown in the figure below.

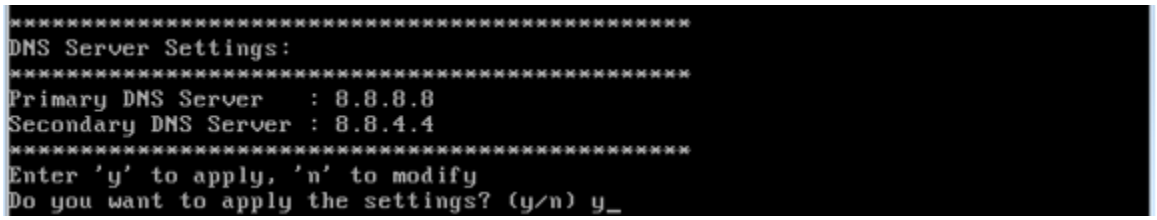
   FIGURE 252 Static IP Address for Management Interface

7. Select the default gateway interface. Enter **1** for control interface, **2** for cluster interface, and **3** for management interface as shown in the figure below.

   FIGURE 253 Default Gateway Interface

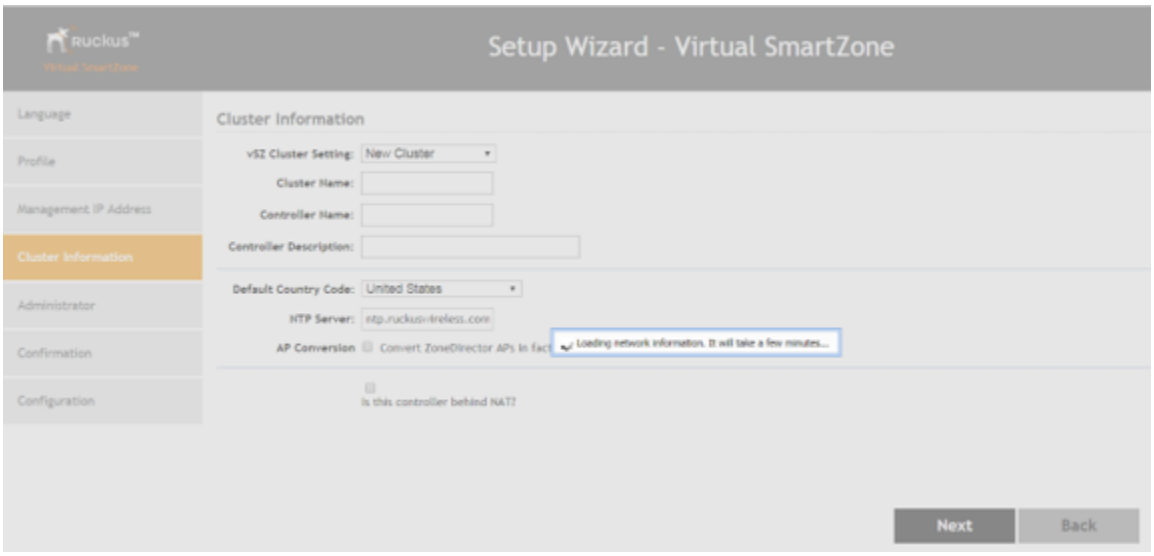
8. Enter the DNS server setting and press **Y** to apply all setting.

   FIGURE 254 DNS Server Settings



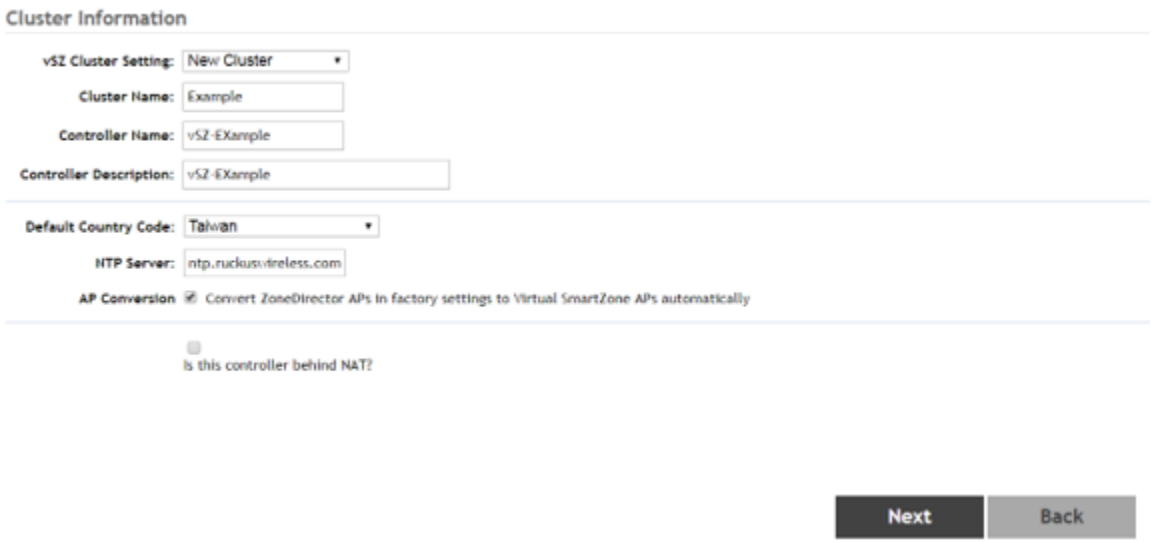
9. Access the web link http://172.17.65.234:8443 to continue other setting as shown in the figure below.

   FIGURE 255 vSZ Web UI



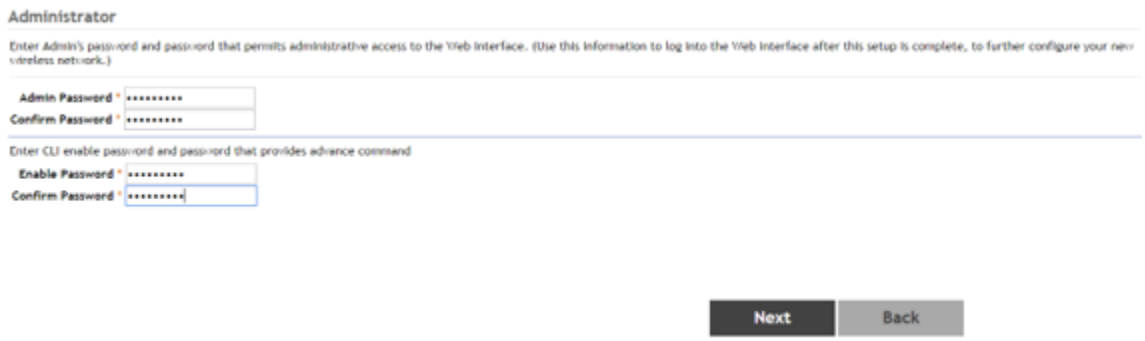
10. Enter your **Cluster Information** and click **Next** as shown in the following figure.

FIGURE 256 Cluster Information



11. Enter your vSZ Administrator password requirements and click **Next** as shown in the following figure.

FIGURE 257 vSZ Administrator Password

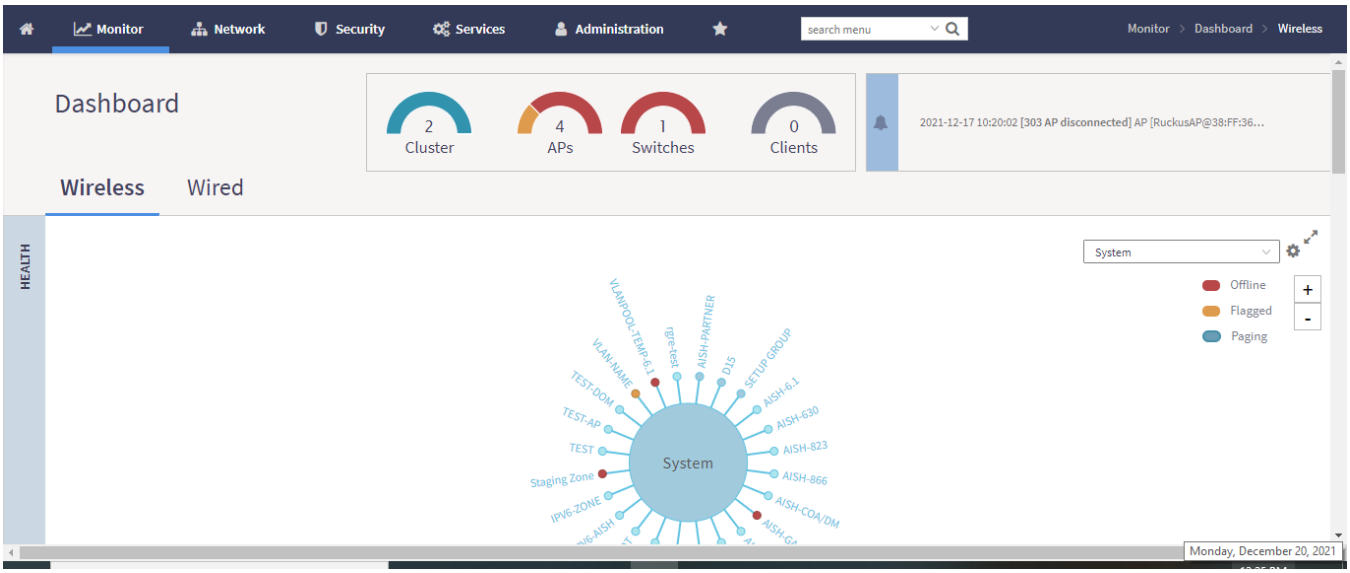


12. Click **Finish** and wait until vSZ is configured.
13. After vSZ is configured, reconnect to vSZ web as shown in the following figure.

FIGURE 258 vSZ Configuration

14. Enter **Username** and **Password** to access vSZ as shown in the following figure.

FIGURE 259 vSZ Homepage



Deploying vSZ on the OpenStack Platform

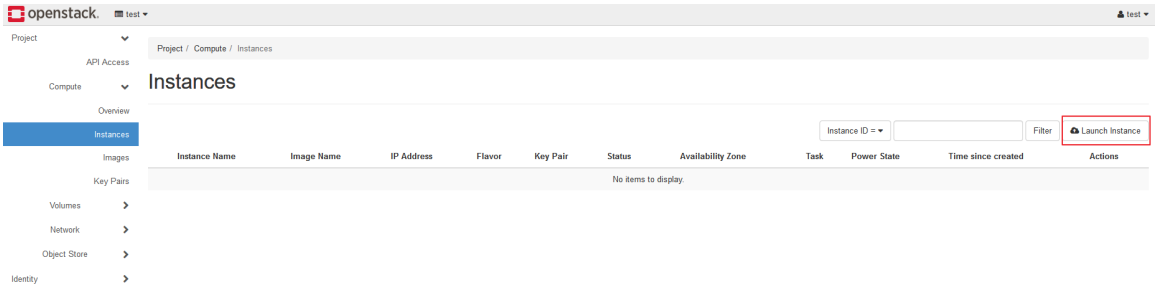
Deploying a Three-Interface vSZ Without a Built-in SNAT

Complete the following basic steps to deploy a three-interface vSZ on the OpenStack platform.

1. Log out of OpenStack as an administrator and log in to OpenStack with an existing user account.
2. Select **Project** > **Compute** > **Instances**.

   The **Instances** page is displayed.

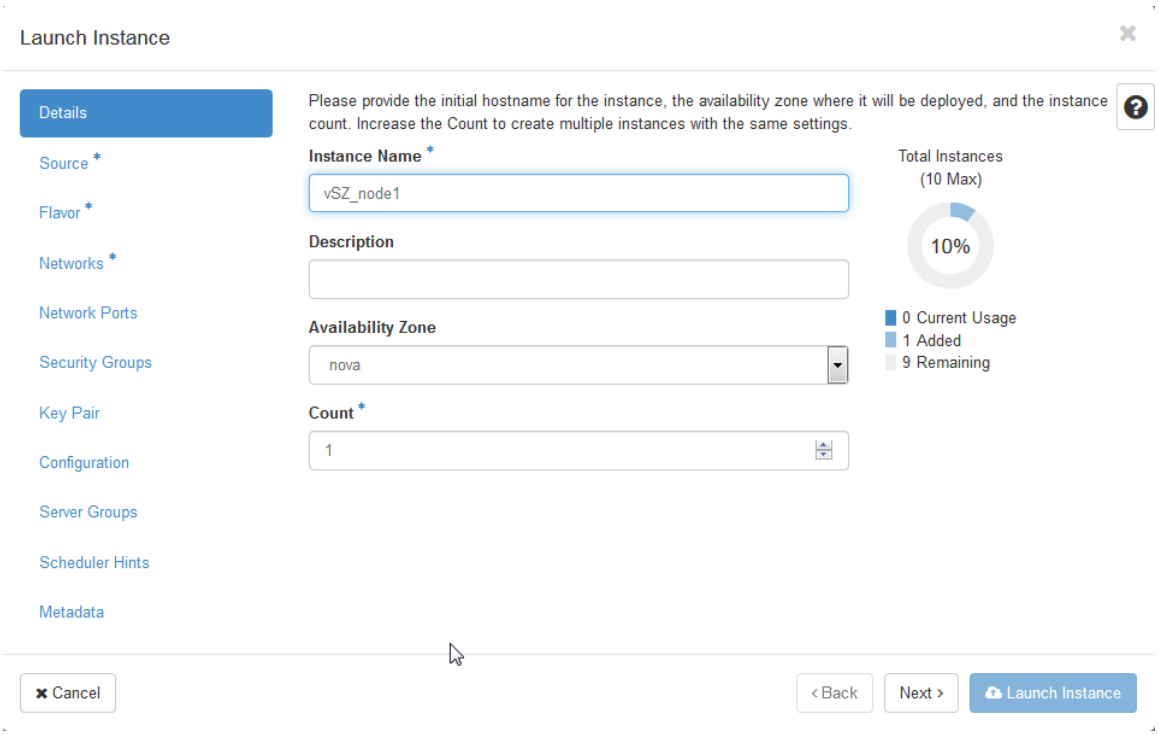
FIGURE 260 Viewing the Project Instances



3. Click **Launch Instance**.

   The **Launch Instance** page is displayed.

   FIGURE 261 Launching an Instance



4. Click **Details** to enter the **Instance Name** and click **Next**.
5. Click **Source** and perform the following steps:
   a. Move the required image from the **Available** to the **Allocated** list.

      NOTE
      The supported image format is **qcow2**.

   b. Under **Create New Volume**, select **No** and click **Next**.
6. Click **Flavor** to move the required resource plan from the **Available** to the **Allocated** list and click **Next**.

   NOTE
   You must use resources according to the requirements for the release being installed.

7. Click **Networks** to move the required network interface from **Available** to **Allocated** list and click **Next**.

   NOTE
   You must select the network interfaces in the following order:
   a. Control interface
   b. Cluster interface
   c. Management interface

8. Click **Network Ports** and then click **Next**.
9. Click **Security Groups** to move the required security rule from the **Available** to the **Allocated** list and click **Next**.
10. Click **Key Pair** to move the required key pair from the **Available** to the **Allocated** list and click **Next**.

    NOTE
    If only one key pair is available, then the system will automatically move the key pair to the **Allocated** list.

11. Click **Launch Instance**.

    NOTE
    When the new instance of vSZ is created, the Power State of the instance is shown as **Running**.

Deploying a One-Interface vSZ with a Built-in SNAT

Complete the following basic steps to deploy a one-interface vSZ with a built-in SNAT.

1. Create an internal network.
2. Create a router.
3. Allocate a floating IP address to a project.
4. Launch a vSZ instance.
5. Associate a floating IP address to a project.

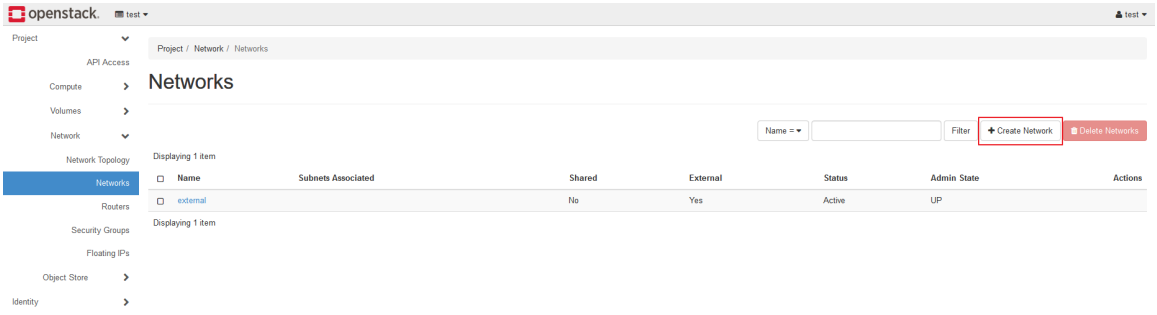
Creating an Internal Network

You must create an internal network to deploy vSZ instances.

1. Log out of OpenStack as an administrator and log in to OpenStack with an existing user account.
2. Select **Project** > **Network** > **Networks**.

   The **Networks** page is displayed.

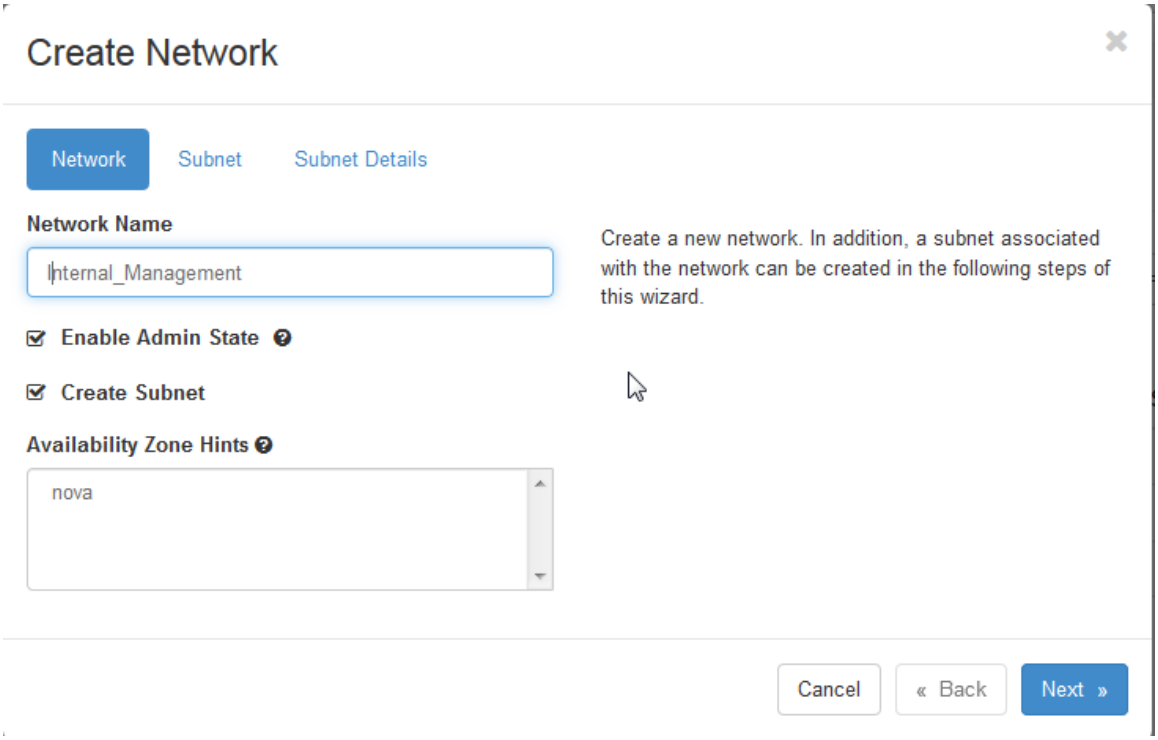
   FIGURE 262 Viewing the Internal Networks



3. Click **Create Network**.

   The **Create Network** page is displayed.

   FIGURE 263 Creating an Internal Network



4. Click **Network** to enter the network name and click **Next**.

   NOTE
   Enable Admin State and **Create Subnet** are enabled by default.

5. Click **Subnet** to enter the subnet name and network address, and click **Next**.

   NOTE
   IPv4 is the default value.

6. Click **Subnet Details** to enter DNS name servers.
7. Click **Create**.

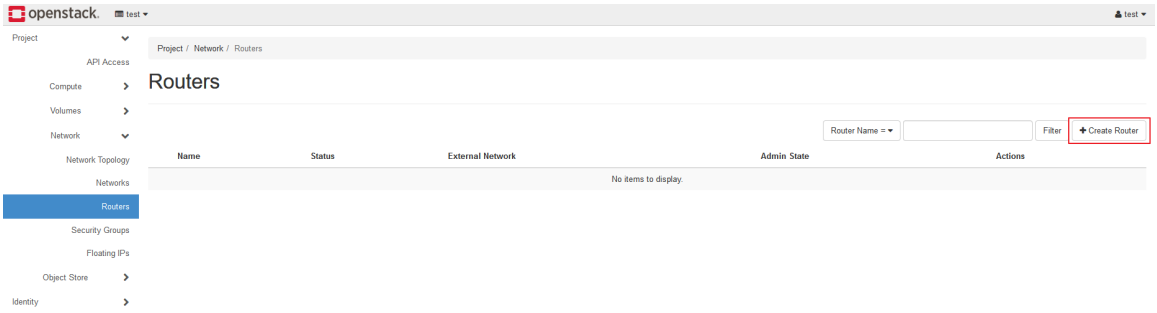
Creating a Router

Before creating a network interface, you must create a router.

1. Select **Project** > **Network** > **Routers**.

   The **Routers** page is displayed.

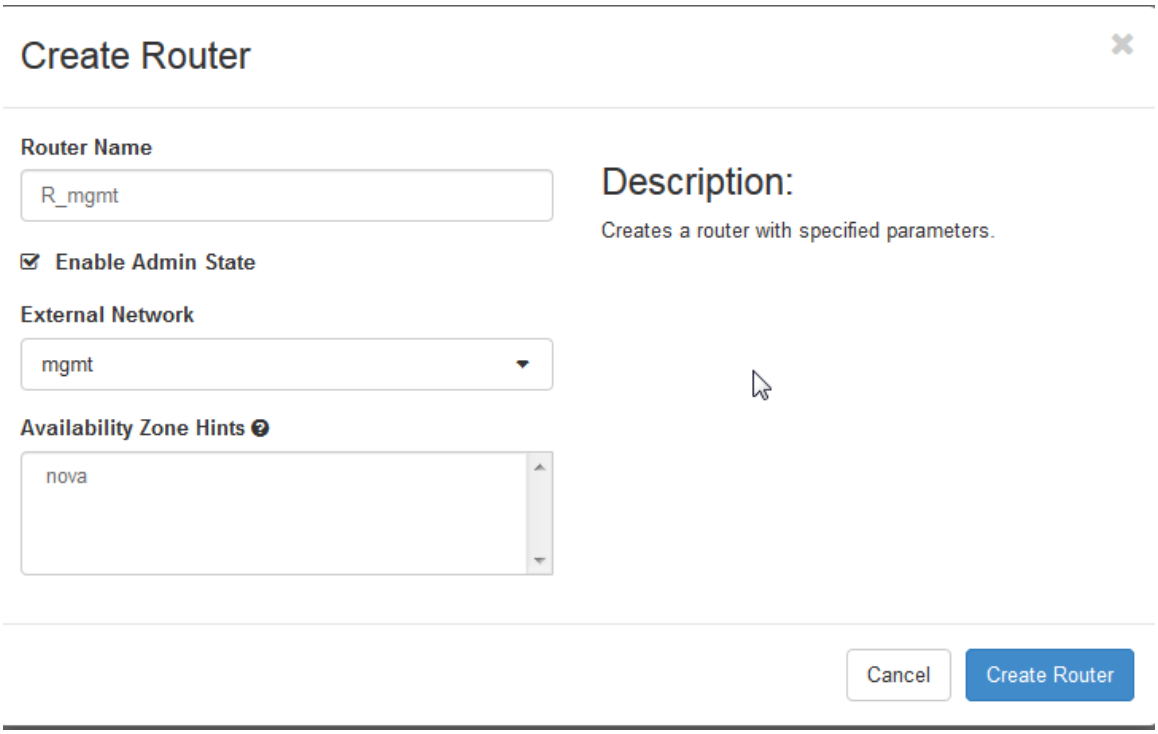
   FIGURE 264 Viewing the Routers



2. Click **Create Router**.

   The **Create Router** page is displayed.

   FIGURE 265 Creating a Router



3. In the **Router Name** field, enter the router name.

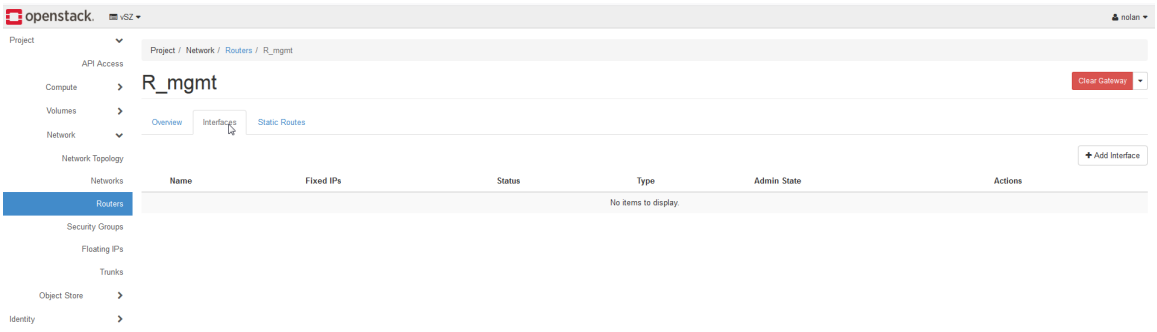
   NOTE
   Enable Admin State is enabled by default.

4. In the **External Network** list, select the network that must be the NAT interface.
5. Click **Create Router**.

   NOTE
   The **Routers** page reflects the router that was added.

6. Click the name of the router that was created.
7. Click **Interfaces**.

FIGURE 266 Viewing the Network Interfaces



8. Click **Add Interface**.

   The **Add Interface** page is displayed.

   FIGURE 267 Adding an Interface

9. In the **Subnet** list, select the subnet (internal interface).

   NOTE
   If an IP address is not specified, the gateway's IP address of the selected subnet is used. If the gateway's IP address is already in use, specify a different IP address that belongs to the selected subnet.

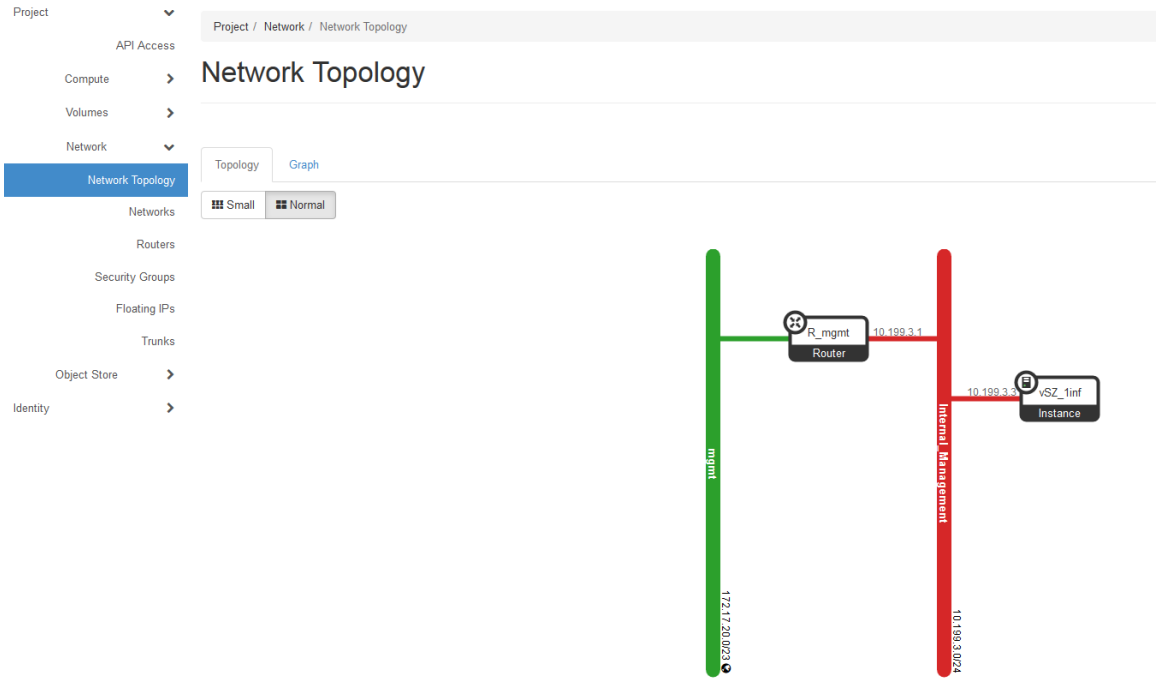
10. Click **Submit**.

Confirming the Router Creation

Complete the following steps to confirm the router is created correctly.

1. Select **Project** > **Network** > **Network Topology**.
2. Select **Normal** mode.

FIGURE 268 Checking the Network Topology



If the router is created successfully, it will be displayed as shown in the figure.

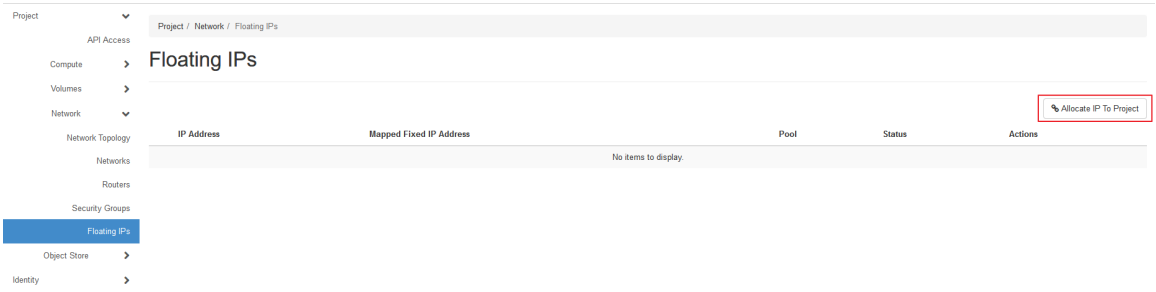
Allocating a Floating IP Address to a Project

You must allocate a floating IP address to a project from a pool of floating IP addresses.

1. Select **Project** > **Network** > **Floating IPs**.

   The **Floating IPs** page is displayed.

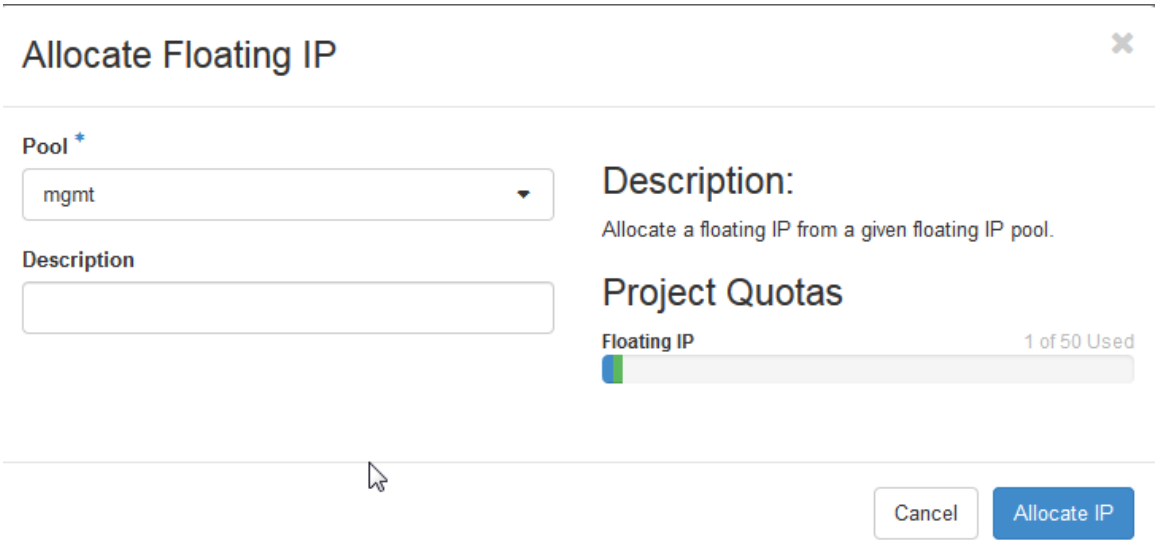
   FIGURE 269 Viewing the Floating IPs



2. Click **Allocate IP To Project**.

   The **Allocate Floating IP** page is displayed.

   FIGURE 270 Allocating a Floating IP Address



   NOTE
   After the allocation of a floating IP address to a project, the entry is reflected in the **Floating IPs** page.

3. Select a floating IP address (external interface) from the **Pool** list.
4. Click **Allocate IP**.

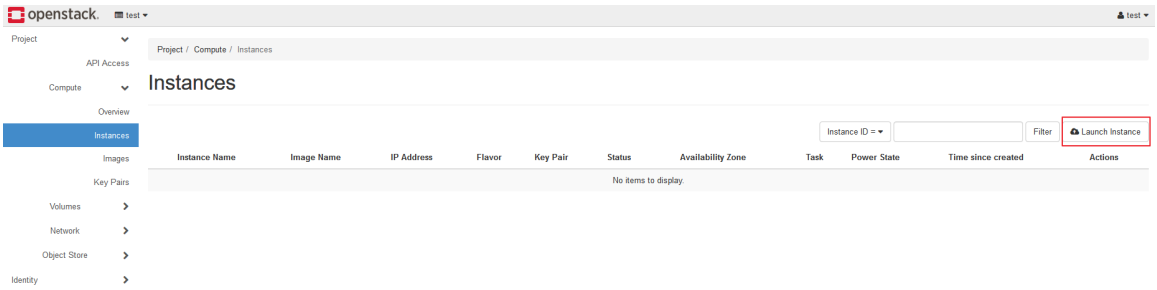
Launching a vSZ Instance

Complete the following basic steps to deploy a new instance of a one-interface vSZ on the OpenStack platform.

1. Select **Project** > **Compute** > **Instances**.

   The **Instances** page is displayed.

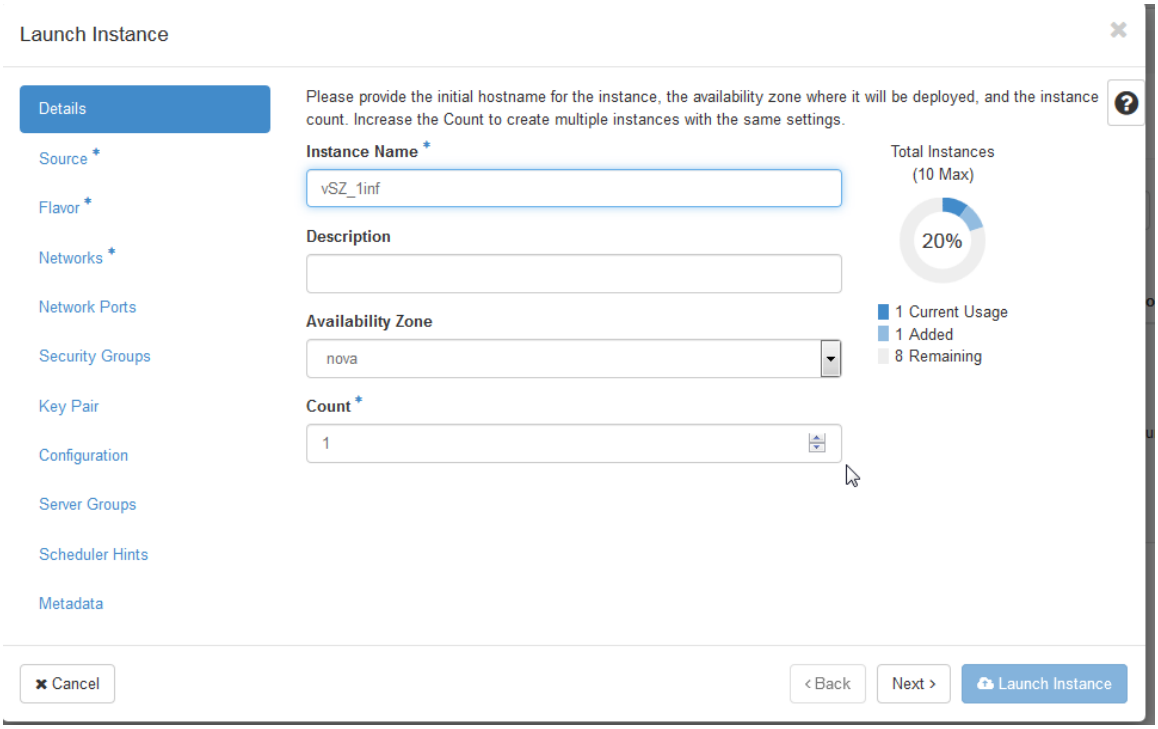
   FIGURE 271 Viewing the Project Instances



2. Click **Launch Instance**.

   The **Launch Instance** page is displayed.

   FIGURE 272 Launching an Instance



3. Click **Details** to enter the instance name and click **Next**.
4. Click **Source** and perform the following steps:
   a) Move the required image from the **Available** to the **Allocated** list.

      NOTE
      The supported image format is qcow2.

   b) Under **Create New Volume**, Select **No** and click **Next**.
5. Click **Flavor** to move the required resource plan from the **Available** to the **Allocated** list and click **Next**.

   NOTE
   You must use resources according to the requirements for the release being installed.

6. Click **Networks** to move the required network interface from the **Available** to the **Allocated** list and click **Next**.
7. Click **Network Ports** and then click **Next**.
8. Click **Security Groups** to move the required security rule from the **Available** to the **Allocated** list and click **Next**.

9. Click **Key Pair** to move the required key pair from the **Available** to the **Allocated** list.

   NOTE
   If only one key pair is available, then the system will automatically move the key pair to the **Allocated** list. Remove the default security rule from the **Allocated** list.

10. Click **Launch Instance**.

    NOTE
    When the new instance of vSZ is created, the power state of the instance is shown as **Running**.

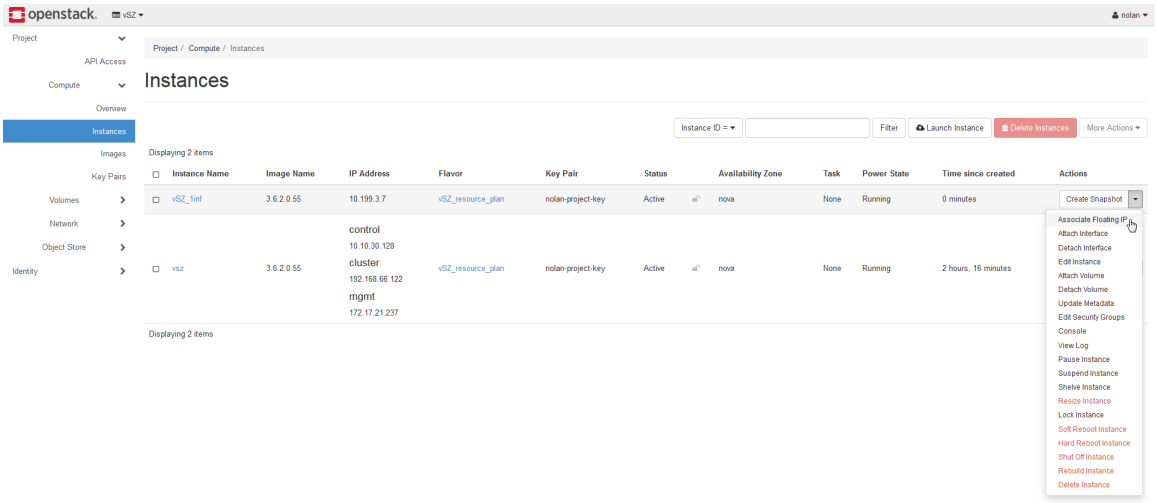
Associating a Floating IP Address to a Project

To direct network traffic to the OpenStack instances, you must associate a floating IP address to a project.

1. Select **Project** > **Compute** > **Instances**.

   The **Instances** page is displayed.

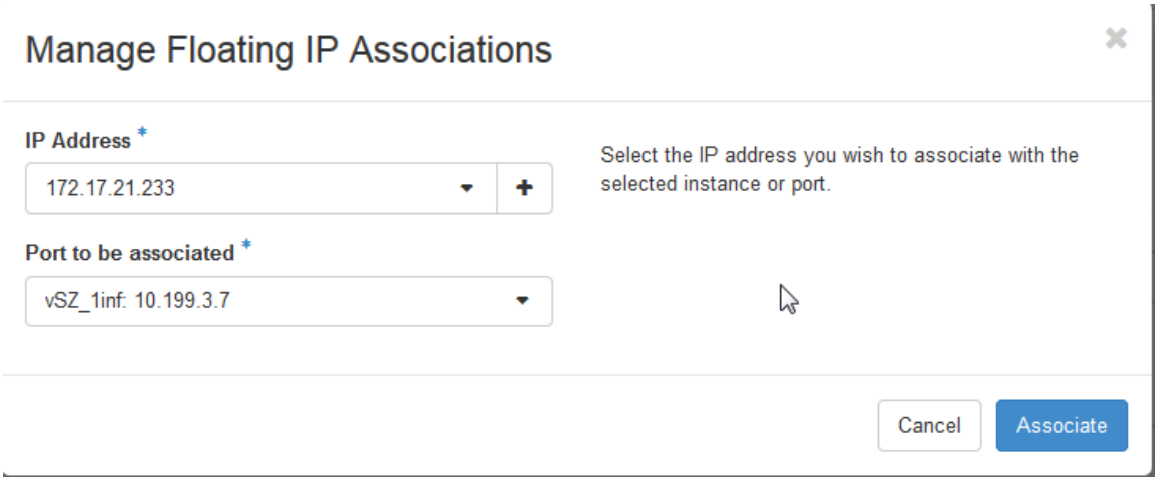
   FIGURE 273 Viewing the Project Instances



2. Click **Associate Floating IP** from the **Action** list.

   The **Manage Floating IP Associations** page is displayed.

   FIGURE 274 Managing a Floating IP Association



3. Select an IP address from the **IP Address** list or click **+** to allocate a floating IP address. Refer to Allocating a Floating IP Address to a Project on page 263 for more information.

   NOTE
   The **Port to be associated** is automatically selected by OpenStack in a one-interface vSZ.

4. Click **Associate**.

Setting Up a vSZ Cluster on OpenStack

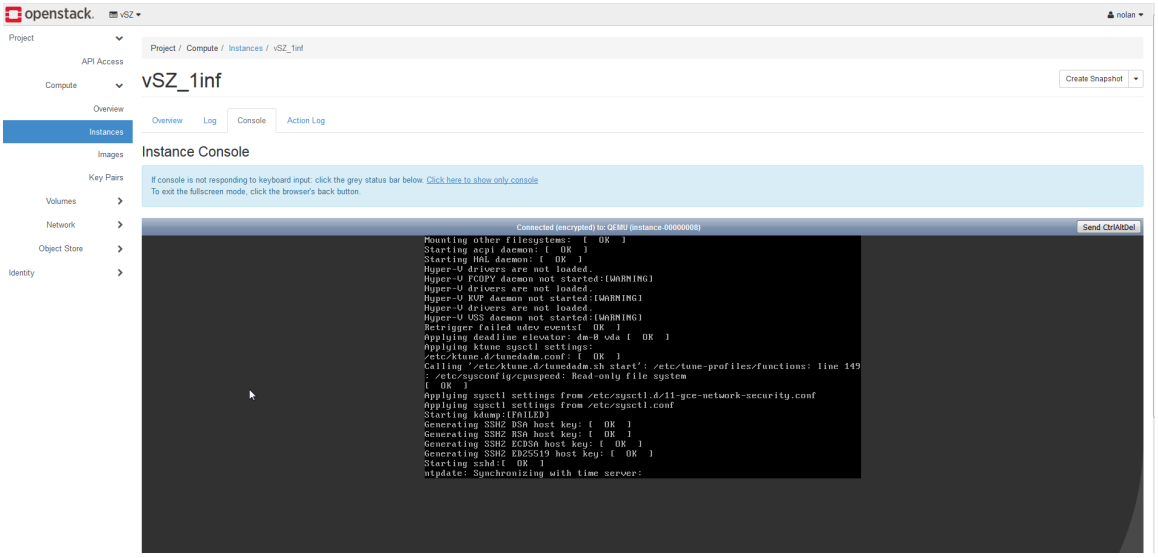
Complete the following steps to set up a vSZ cluster on the OpenStack platform.

1. Select **Project** > **Compute** > **Instances**.
2. Click the instance name of the vSZ.

3. Click **Console** to view the vSZ login prompt.

   NOTE
   The Linux PC uses a private key to connect to the vSZ console.

FIGURE 275 Viewing the vSZ Login Console



4. Complete the vSZ setup flow steps. Refer to Using the Setup Wizard to Install vSZ on page 201.

   NOTE
   You must configure the vSZ interface IP address as **DHCP** to avoid network issues.

Upgrading the Controller for Microsoft Azure, AWS, and GCE Platforms

Upgrading the Controller for Microsoft Azure, AWS, and GCE Platforms

Ruckus Networks may periodically release controller software updates that contain new features, enhancements, and fixes for known issues.

These software updates may be made available on the Ruckus Networkssupport website or released through authorized channels.

CAUTION

Although the software upgrade process has been designed to preserve all controller settings, Ruckus Networks strongly recommends that you back up the controller cluster before performing an upgrade. Having a cluster backup will ensure that you can easily restore the controller system if the upgrade process fails for any reason.

CAUTION

Ruckus Networks strongly recommends that you ensure that all interface cables are intact during the upgrade procedure.

CAUTION

Ruckus Networks strongly recommends that you ensure that the power supply is not disrupted during the upgrade procedure.

NOTE

If you are managing a vSZ, you can also perform system configuration backup, restore, and upgrade from the controller command line interface.

Upgrading the Controller Software

This section outlines the procedure to upgrade the controller software for Microsoft Azure, Amazon Web Services, Google Computing Engine platforms.

Follow these steps to upgrade the controller software.

CAUTION

Ruckus Networks strongly recommends backing up the controller cluster before performing the upgrade. If the upgrade process fails for any reason, you can use the latest backup file to restore the controller cluster.

NOTE

Before starting this procedure, you should have already obtained a valid controller software upgrade file from Ruckus Networks Support or an authorized reseller.

vSZ supports APs starting version 3.4. You must first upgrade the vSZ. Only a new vSZ can handle an old vDP. During the vSZ upgrade, all tunnels will stay up except the main tunnel which moves to the vSZ.

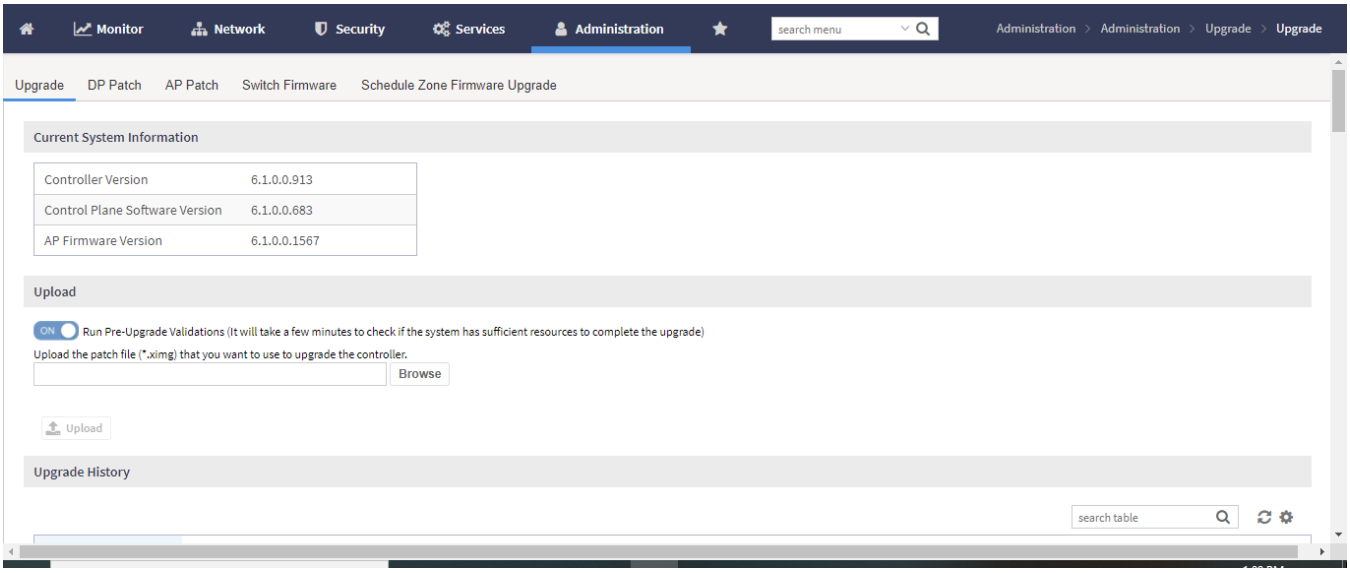
Upgrade to 5.0 does not support data migration (statistics, events, administrator logs). Existing system and network configuration is preserved. For further clarification, Contact Ruckus support.

To Upgrade:

1. Copy the software upgrade file that you received from Ruckus Networks to the computer where you are accessing the controller web interface or to any location on the network that is accessible from the web interface.
2. Go to **Administration** > **Administration** > **Upgrade** > **Upgrade**.
3. In the **Upload** section, select the **Run Pre-Upgrade Validations** box to verify if the data migration was successful. This option allows you to verify data migration errors before performing the upgrade. If data migration was unsuccessful, the following error is displayed: `Exception occurred during the validation of data migration. Please apply the system configuration backup and contact system administrator.`

   Typically, the file name of the software upgrade file is `scg-installer_{version}.ximg.`
4. Click the **Browse** button, and then browse to the location of the software upgrade file. 1q

   FIGURE 276 Click **Browse** in the Upload section to upload the software upgrade file



5. Select the software upgrade file, and then click **Open**.
6. Click **Upload** to upload the software upgrade file. The controller uploads the file to its database, and then performs file verification. After the file is verified, the **Upgrade Pending Patch Information** section is populated with information about the upgrade file.

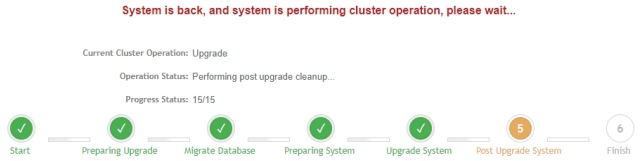
7. Start the upgrade process by clicking one of the following buttons:
   - **Upgrade**: Click this button to start the upgrade process without backing up the current controller cluster or its system configuration.
   - **Backup & Upgrade**: Click this button to back up the controller cluster and system configuration before performing the upgrade.

     CAUTION
     Ruckus Networks strongly recommends using Backup & Upgrade when performing the upgrade. If the upgrade process fails for any reason, you can use the latest backup file to restore the controller cluster.

   A confirmation message appears.
8. Click **Yes**.

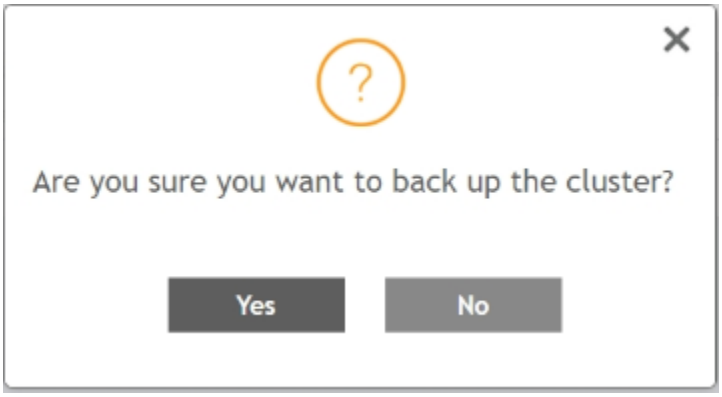
   The controller starts the process that you selected. The screens that appear next will depend on the process that you selected to upgrade immediately or to back up and then upgrade the controller.

FIGURE 277 The **System Upgrade** page displays the status of the upgrade process



When the upgrade (or backup-and-upgrade) process is complete, the controller logs you off the web interface automatically. Wait for a few minutes until the web interface log on page appears.

FIGURE 278 The controller web interface may display the following message as it completes the upgrade process



When the controller logon page appears again, you have completed upgrading the controller.

Continue to the Verifying the Upgrade task to check if the upgrade was completed successfully.

Verifying the Upgrade

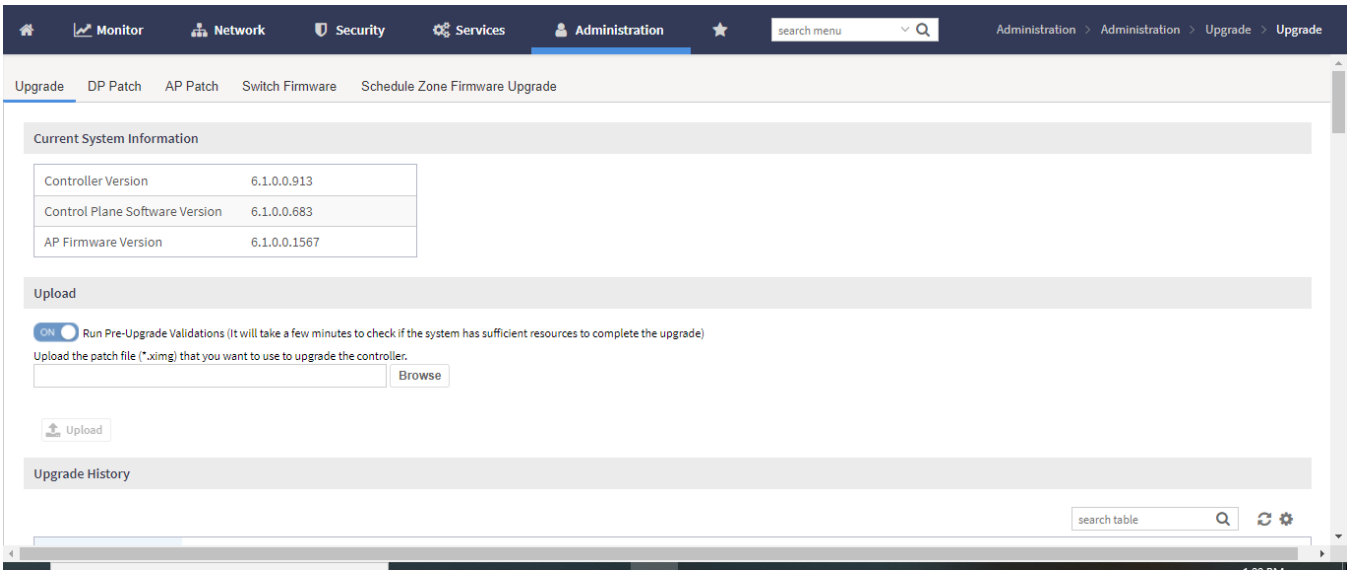
Follow these steps to verify that the controller upgrade was completed successfully.

1. Log on to the controller web interface.
2. Go to **Administration** > **Administration** > **Upgrade** > **Upgrade**.
3. In the **Current System Information** section, check the value for Controller Version.

   If the firmware version is newer than the firmware version that controller was using before you started the upgrade process, then the upgrade process was completed successfully.

   NOTE
   APs periodically send scheduled configuration requests to the controller, including the firmware version. Therefore, when an AP joins a zone for the first time, the firmware version is verified by the controller. If the firmware version is different from that which is configured for the zone, the controller responds with a request to upgrade it, after which the AP initiates a request to upgrade the firmware using HTTP.

FIGURE 279 Check the value for Controller Version



Rolling Back to a Previous Software Version

There are two scenarios in which you may want to roll back the controller software to a previous version:

1. You encounter issues during the software upgrade process and the controller cannot be upgraded successfully. In this scenario, you can only perform the software rollback from the **CLI** using the restore local command. If you have a two-node controller cluster, run the restore local command on each of the nodes to restore them to the previous software before attempting to upgrade them again.

2. You prefer a previous software version to the newer version to which you have upgraded successfully. For example, you feel that the controller does not operate normally after you upgraded to the newer version and you want to restore the previous software version, which was more stable. In this scenario, you can perform the software rollback either from the web interface or the **CLI**. If you have a two-node controller cluster, you must have cluster backup on both of the nodes.

To ensure that you will be able to roll back to a previous version, Ruckus Networks strongly recommends the following before attempting to upgrade the controller software:

- Always back up the controller before attempting a software upgrade. If you are managing a multi-node cluster, back up the entire cluster, and then verify that the backup process completes successfully. See Creating a Cluster Backup on page 273 for more information.
- If you have an FTP server, back up the entire cluster and upload the backup files from all the nodes in a cluster to a remote FTP server.

Backing Up and Restoring Clusters

Back up the controller cluster periodically to ensure that you can restore the control plane, data plane, and AP firmware versions as well as the system configuration in the cluster if is a system failure occurs.

This section covers the following topics:

> **NOTE**
> You can also perform these procedures from the vSZ command line interface. Note, however, that you will need to execute the commands on each node.

Creating a Cluster Backup

Follow these steps to back up an entire controller cluster.

1. Take note of the current system time.

   To view the current system time, go to **Administration** > **System** > **Time**.
2. Go to **Administration** > **Administration** > **Backup & Restore** > **Cluster**.
3. Click **Back Up Entire Cluster**.

   The following confirmation message appears: `Are you sure you want to back up the cluster?`
4. Click **Yes**.

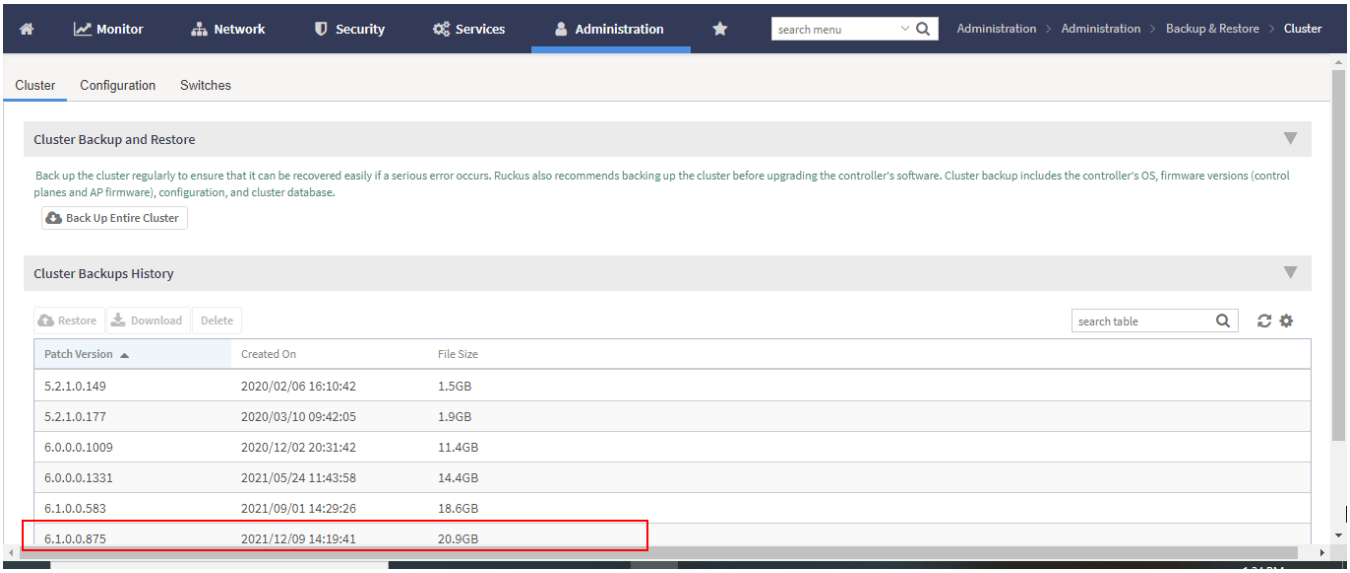
   The following message appears: `The cluster is in maintenance mode. Please wait a few minutes.`

When the cluster backup process is complete, a new entry appears in the **Cluster Backups History** section with a Created On value that is approximate to the time when you started the cluster backup process.

> **NOTE**
> If you have an FTP server, back up the entire cluster and upload the backup files from all the nodes in a cluster to a remote FTP server.

You have completed backing up the controller cluster.

FIGURE 280 A new entry appears in the Cluster Backups section



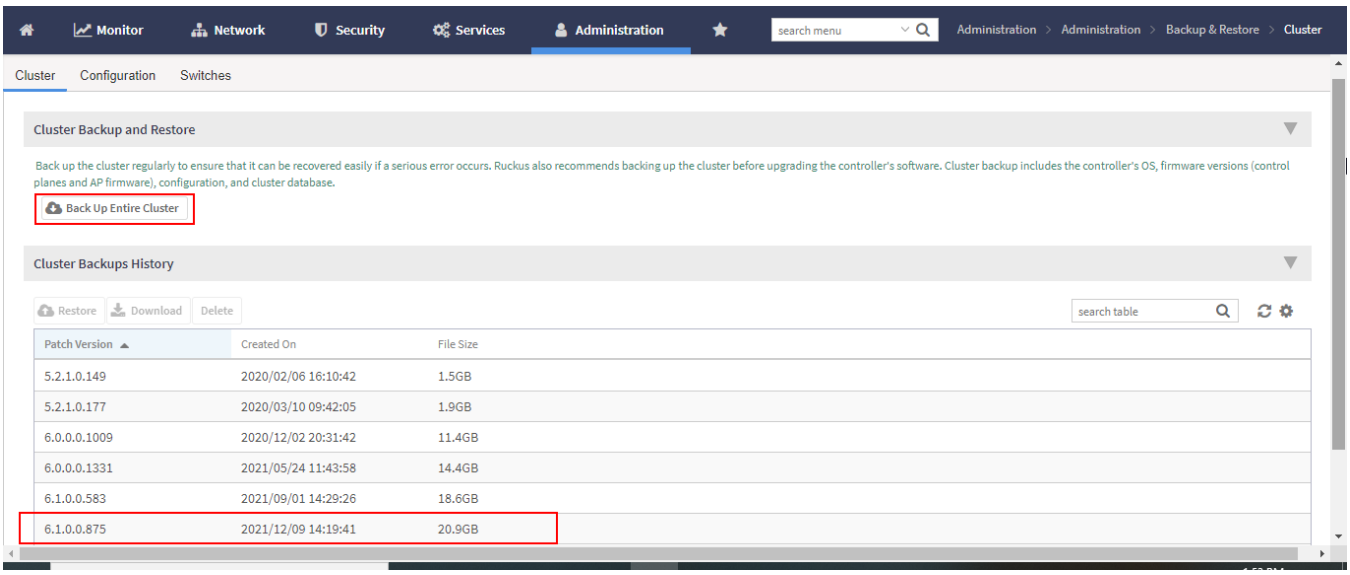
Restoring a Cluster Backup

When restoring a cluster backup, remember that you must perform the restore procedure on the exact same node which you generated the cluster backup.

Follow these steps to restore a cluster backup

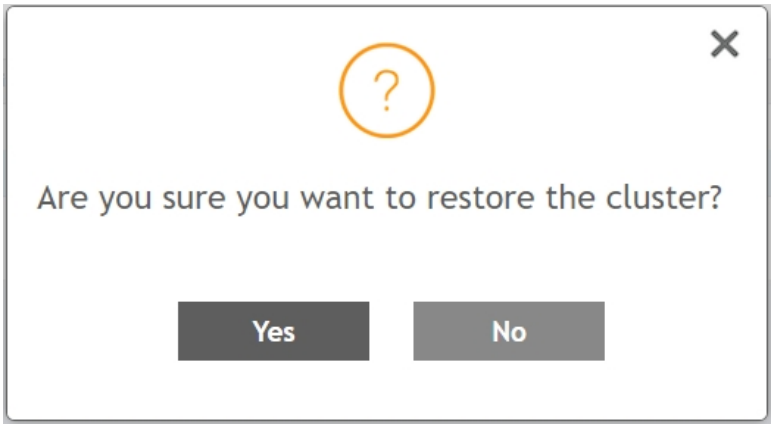
1. Go to **Administration** > **Administration** > **Backup & Restore** > **Cluster**.
2. In the **Cluster Backups History** section, locate the cluster backup that you want to restore.
3. Select the backup file that you want to restore, and then click **Backup Entire Cluster**.

FIGURE 281 Select the backup file, and then click Backup Entire Cluster



4. The following confirmation message appears: `Are you sure you want to restore the cluster?`. Click **Yes**.

   FIGURE 282 Confirm Backup

   The page refreshes, and then the following message appears: `System is restoring! Please wait...`

   NOTE
   The cluster restore process may take several minutes to complete.
   When the restore process is complete, the controller logs you off the web interface automatically.
   Do not refresh the controller web interface while the restore process is in progress. Wait for the restore process to complete successfully.

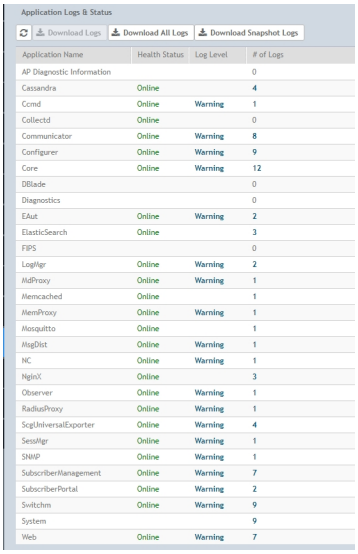
5. Log back on to the controller web interface.

   NOTE
   If the web interface displays the message `Cluster is out of service. Please try again in a few minutes.` appears after you log on to the controller web interface, wait for about three minutes. The dashboard will appear shortly. The message appears because the controller is still initializing its processes.

6. Go to **Administration** > **Administration** > **Upgrade** > **Upgrade**, and then check the **Current System Information** section and verify that all nodes in the cluster have been restored to the previous version and are all in service.
7. Go to **Monitor** > **Troubleshooting & Diagnostics** > **Application Logs** .
8. Check the **Health Status** column and verify that all of the controller processes are online.

You have completed restoring the cluster backup. After the upgrade is complete, go to the **Application Logs** page and verify that all of the controller processes are online.

FIGURE 283 On the Application Logs page, verify that all controller processes are online



Restoring a Cluster Backup Using the CLI

Follow these steps to restore a cluster backup using the CLI.

1. Enter the vSZ CLI.
2. Enter the following command and enter the password to log into the CLI.

```
VSCG35> en
Password:
```

3. Enter the following command to restore a cluster backup:

```
VSCG35> restore
```

   All the cluster backups are listed in an order of the cluster backup created date.

4. Specify the number mentioned against the cluster backup that you wish to restore.

You have restored the cluster backup.

FIGURE 284 Cluster Backup Restore Using CLI

```
##############################
#       Welcome to vSZ       #
##############################
admin@13.94.61.64's password:
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.1.1.0.571

C-26> en
Password: ********

C-26# restore
   No.   Created on                  Patch Version               File Size
   ----- --------------------------- --------------------------- ---------------------------
   1     2019-04-23 02:50:47 GMT     5.1.1.0.551                 2.4GB
   2     2019-04-23 03:47:41 GMT     5.1.1.0.571                 1.4GB

Please choose a backup to restore or 'No' to cancel: 2
This action will reboot the system. Do you want to restore "the entire" cluster system (or input 'no' to cancel)? [yes/no] yes
```

Deleting a Cluster Backup

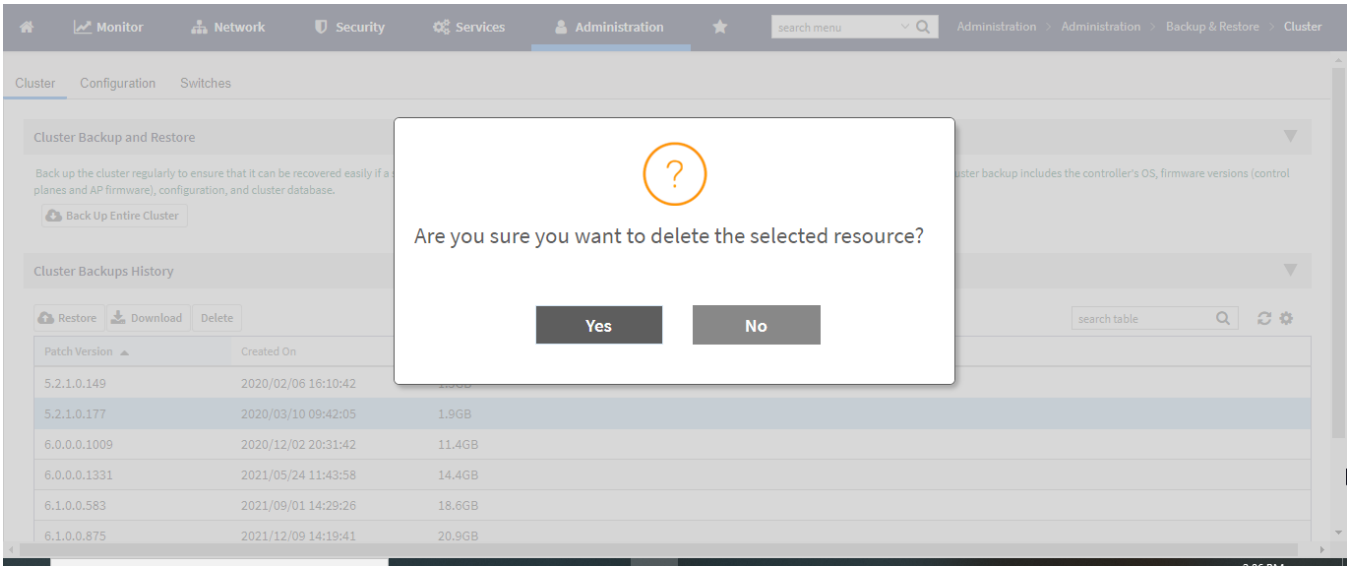
Follow these steps to delete a cluster backup.

1. Go to **Administration** > **Administration** > **Backup & Restore** > **Cluster**.
2. In the **Cluster Backups History** section of the **Cluster** tab, locate the cluster backup that you want to delete, and then click it.

   The cluster backup becomes highlighted, which indicates that you have selected it.
3. Click Delete.

   A confirmation message appears.

   FIGURE 285 After you click the Delete button, a confirmation message appears



4. Click **Yes**.

   The page refreshes, and then the cluster backup that you deleted disappears from the **Cluster Backups History** section.

You have completed deleting a cluster backup.

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com