Pulse Connect Secure Virtual Appliance on OpenStack Fabric

Deployment Guide

Document Revision	1.0.1
Published Date	May 2020

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

https://www.pulsesecure.net

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Pulse Secure or components thereof might be covered by one or more of the following patents that are owned by or licensed to Pulse Secure: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Pulse Connect Secure Virtual Appliance on OpenStack Fabric - Deployment Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at https://www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Revision History

Revision and Date	Added/Updated/Removed	Remarks
1.0.1, May 2020	Updated the Limitations section	
1.0, October 2019	None	Initial release

Table of Contents

Overview

About This Guide

This guide helps in deploying the Pulse Connect Secure Virtual Appliance (PCS VA) on OpenStack. From 9.1R3 release onwards, Pulse Connect Secure (PCS) KVM image is can be deployed on OpenStack.

Assumptions

The basic understanding of deployment models of PCS on a data center and basic experience in using OpenStack is needed for the better understanding of this guide.

Prerequisites and System Requirements

The OpenStack Fabric has various components such as Controller, Compute, Identity, Image, Networking etc. that are separately installed. For details about these services, refer to OpenStack Install Guide.
To deploy the PCS VA on OpenStack, you need the following:

- Access to the OpenStack Dashboard
- An OpenStack account with deployment rights
- PCS KVM Image
- (Optional) PCS licenses
- (Optional) PCS configuration in xml format, required only for zero touch deployment
- Desired flavors of PSA-V (PSA3000-V, PSA5000-V, PSA7000-V). For details refer to Appendix A.
- Desired PCS KVM image on OpenStack (for details refer to Appendix A)
- Internal, External and Management networks on OpenStack (for details refer to Appendix A)
- Security Groups for Internal, External and Management Ports (for details refer to Appendix A)

Below are the steps to be followed for each deployment of Pulse Connect Secure:

- Deploying PCS on OpenStack Using Horizon Dashboard
- Deploying PCS on OpenStack Using Heat

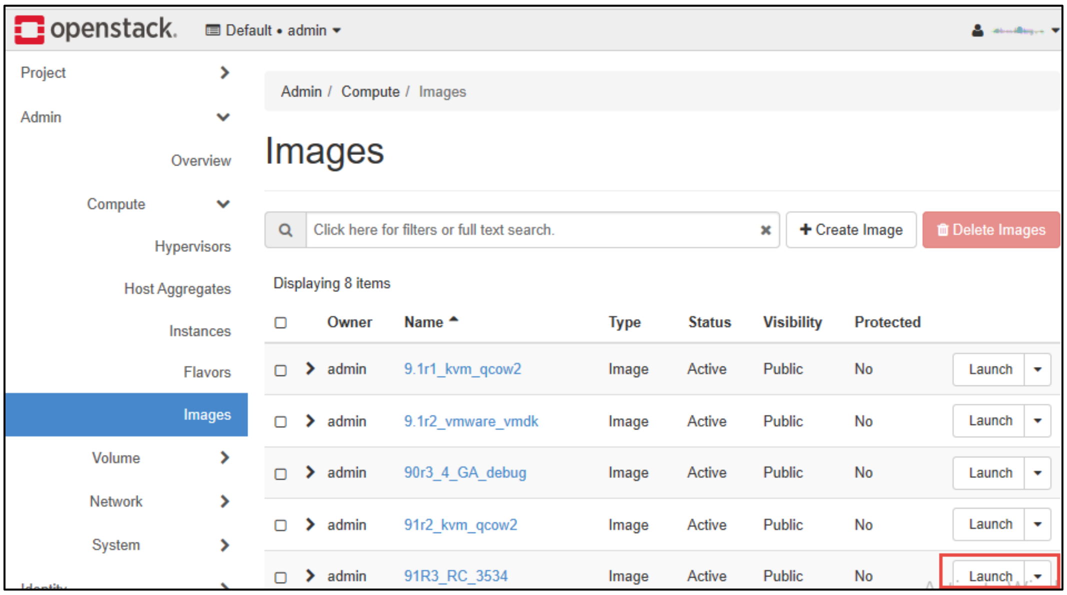
Deploying PCS on OpenStack Using Horizon Dashboard

Before proceeding with the PCS deployment, ensure that the necessary prerequisites are set up. For details, refer to Appendix A.

To deploy PCS on OpenStack, do the following:

1. Log in to the OpenStack.
2. In the OpenStack dashboard displayed, select **Project > Compute > Images**.
3. From the list of images displayed, click on **Launch** corresponding to the PCS KVM image you want to launch.

Figure 1: PCS VA Images



Admin / Compute / Images

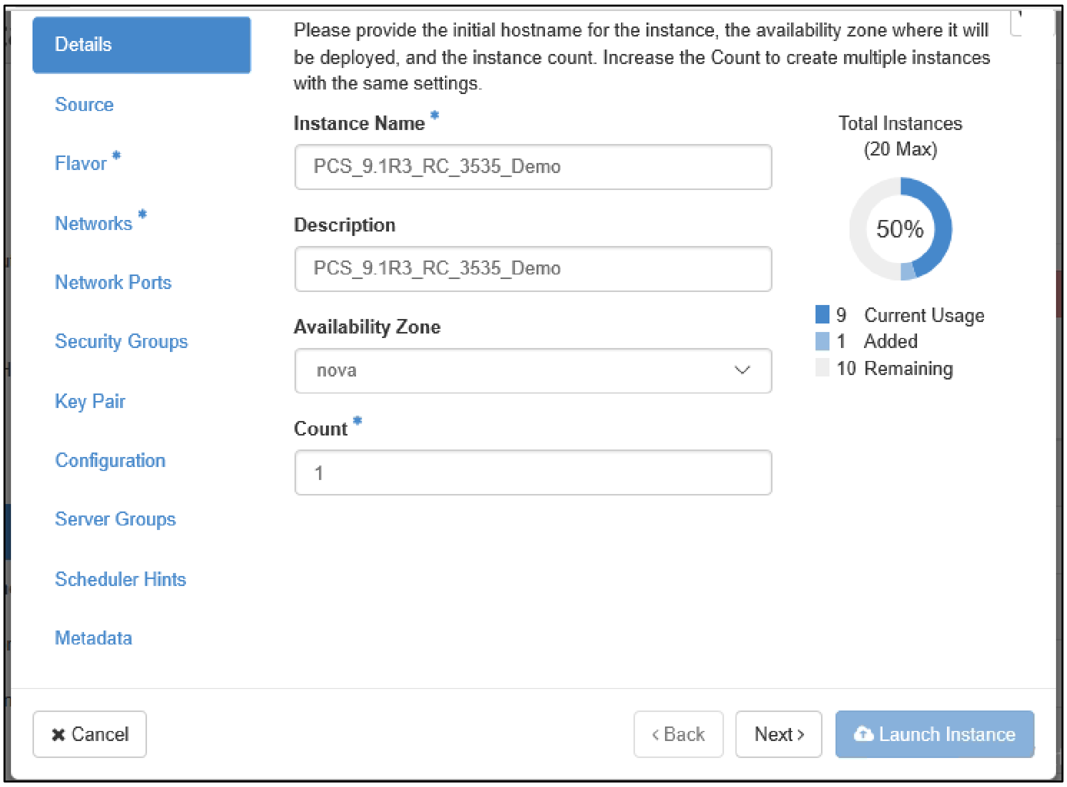
Images

Displaying 8 items

□	Owner	Name	Type	Status	Visibility	Protected
□	admin	9.1r1_kvm_qcow2	Image	Active	Public	No
□	admin	9.1r2_vmware_vmdk	Image	Active	Public	No
□	admin	90r3_4_GA_debug	Image	Active	Public	No
□	admin	91r2_kvm_qcow2	Image	Active	Public	No
□	admin	91R3_RC_3534	Image	Active	Public	No

4. In the Launch Instance Details window, fill the following and then click **Next**.
   - Instance Name: Specify host name of the PCS Virtual instance
   - Description: Enter a brief description on this instance
   - Availability Zone: Select the zone where the instance is deployed
   - Count: Number of VM instances

Figure 2: Device Details



Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Instance Name *: PCS_9.1R3_RC_3535_Demo

Description: PCS_9.1R3_RC_3535_Demo

Availability Zone: nova

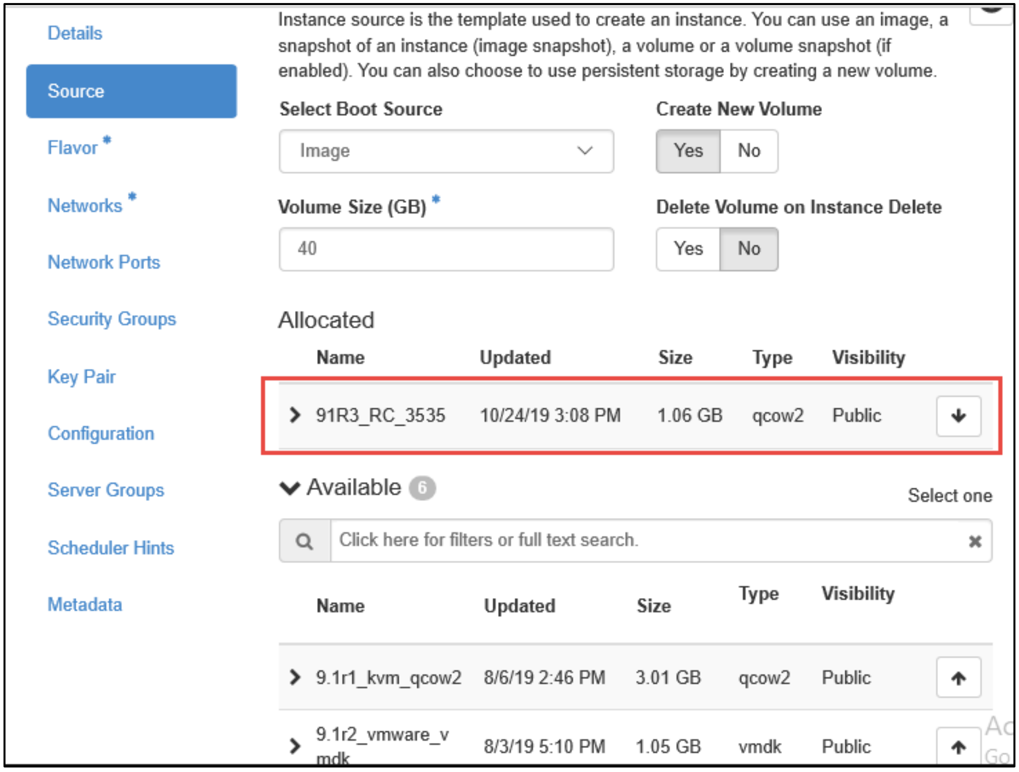
Count *: 1

Total Instances (20 Max)

🟦	9	Current Usage
🟦	1	Added
⬜	10	Remaining

5. The Source window displays the details of the image used. Click **Next**.

Figure 8: Source Selection



Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume.

Select Boot Source: Image

Create New Volume: Yes No

Volume Size (GB) *: 40

Delete Volume on Instance Delete: Yes No

Allocated

Name	Updated	Size	Type	Visibility
91R3_RC_3535	10/24/19 3:08 PM	1.06 GB	qcow2	Public

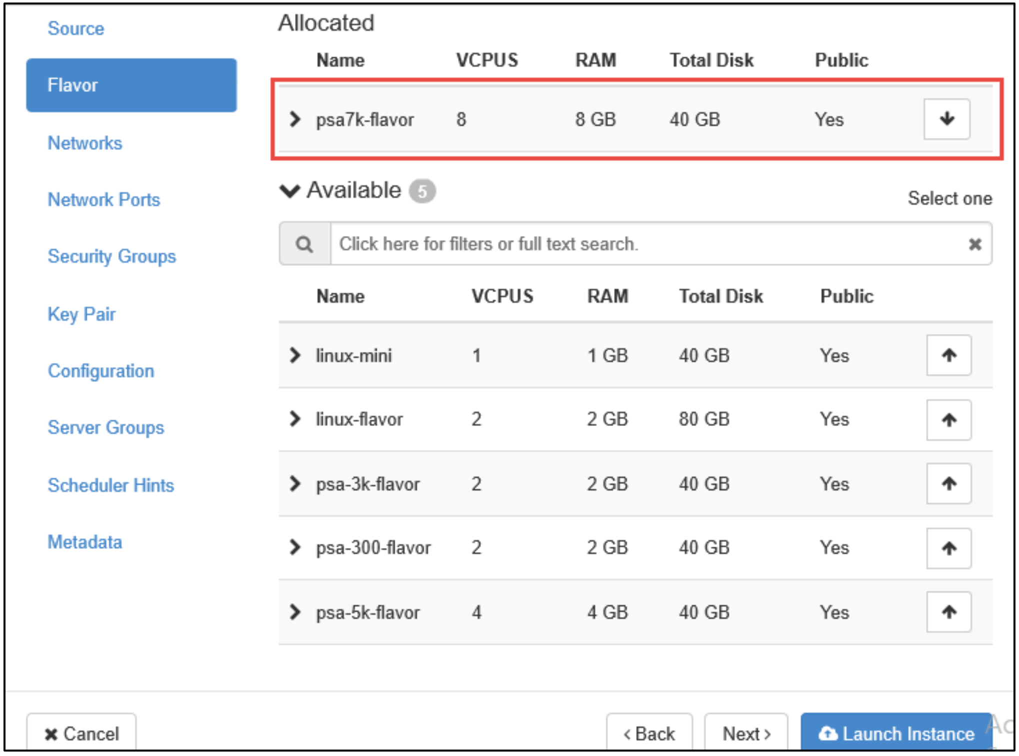
Available 6 — Select one

Click here for filters or full text search.

Name	Updated	Size	Type	Visibility
9.1r1_kvm_qcow2	8/6/19 2:46 PM	3.01 GB	qcow2	Public
9.1r2_vmware_vmdk	8/3/19 5:10 PM	1.05 GB	vmdk	Public

6. In the Flavor window, select required flavors of PSA-V (PSA3000-V, PSA5000-V, PSA7000-V) from the list based on the memory and storage capacity of the instance. Click **Next**.

Figure 3: Flavor Selection



Allocated

Name	VCPUS	RAM	Total Disk	Public
psa7k-flavor	8	8 GB	40 GB	Yes

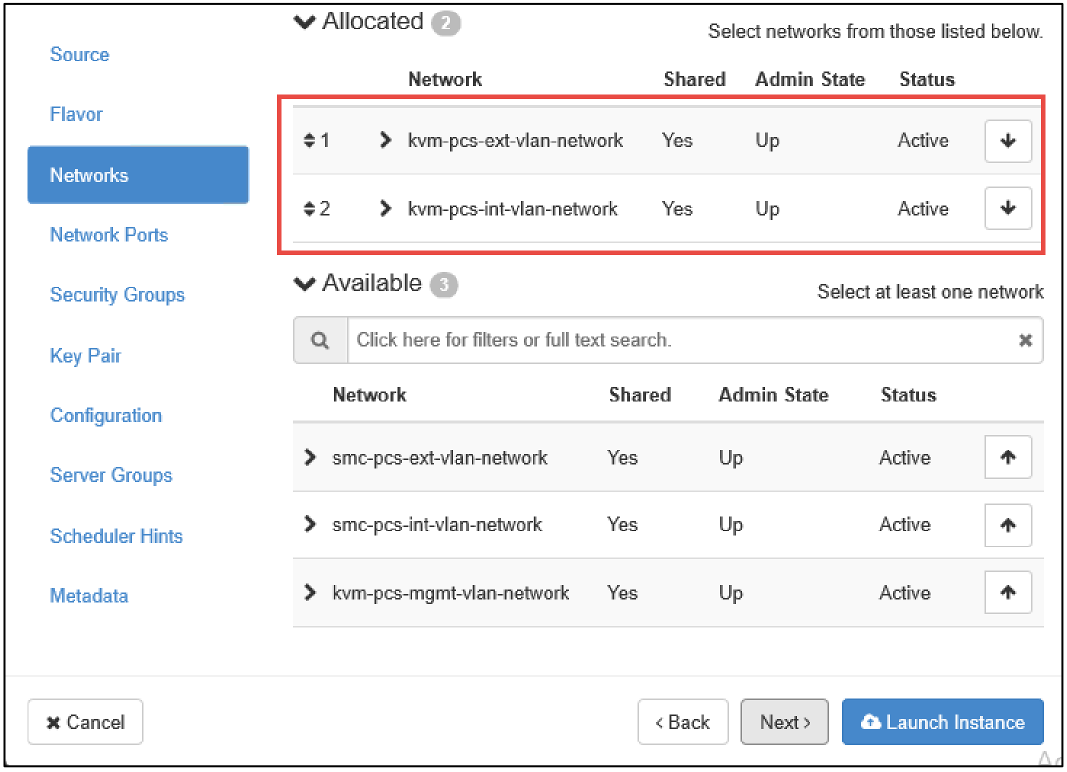
Available 5 — Select one

Click here for filters or full text search.

Name	VCPUS	RAM	Total Disk	Public
linux-mini	1	1 GB	40 GB	Yes
linux-flavor	2	2 GB	80 GB	Yes
psa-3k-flavor	2	2 GB	40 GB	Yes
psa-300-flavor	2	2 GB	40 GB	Yes
psa-5k-flavor	4	4 GB	40 GB	Yes

7. In the Networks window, select networks from the list that specifies internal, external and management subnets. PCS supports VM with 2-NICs model and 3-NICs model for deployment. Click **Next**.

Figure 4: Network Selection



Select networks from those listed below.

	Network	Shared	Admin State	Status
1	kvm-pcs-ext-vlan-network	Yes	Up	Active
2	kvm-pcs-int-vlan-network	Yes	Up	Active

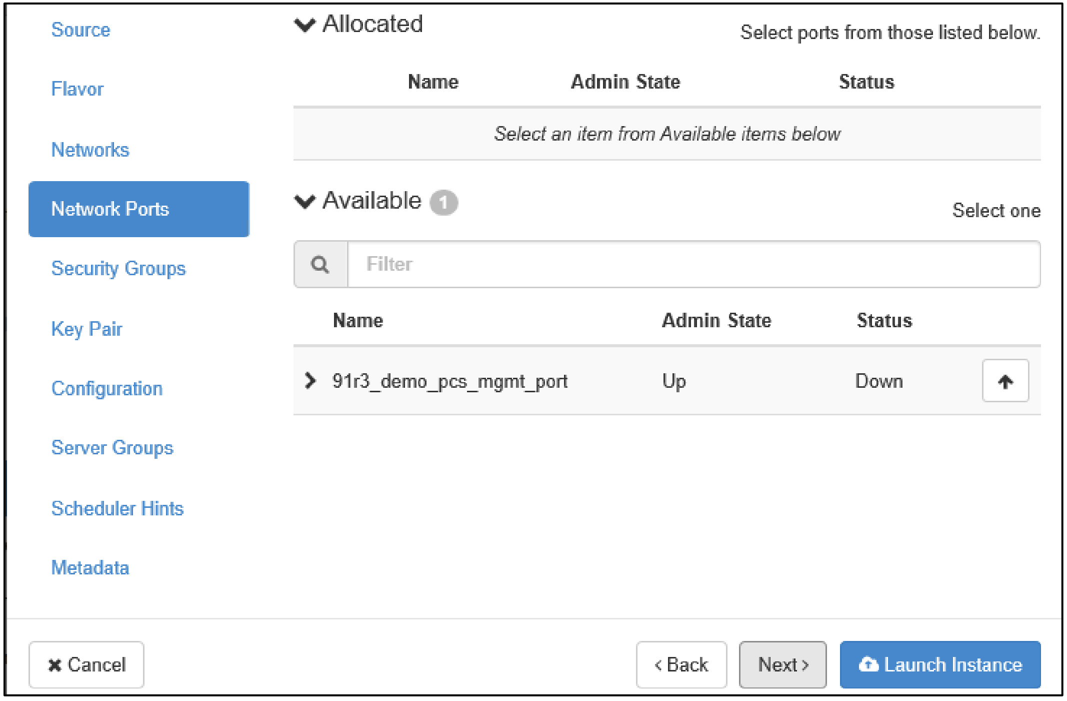
Select at least one network

Click here for filters or full text search.

Network	Shared	Admin State	Status
smc-pcs-ext-vlan-network	Yes	Up	Active
smc-pcs-int-vlan-network	Yes	Up	Active
kvm-pcs-mgmt-vlan-network	Yes	Up	Active

8. (Optional) Network Ports window. Click **Next**.

Figure 5: Network Ports Selection



Select ports from those listed below.

Name	Admin State	Status

Select an item from Available items below

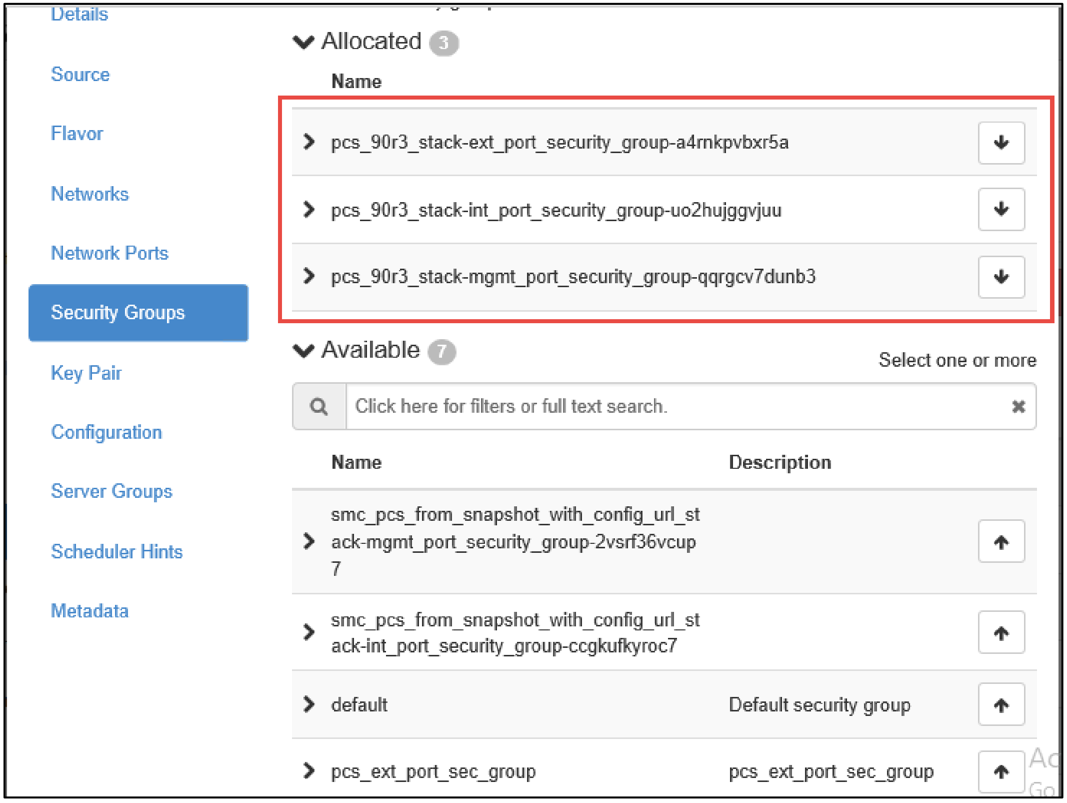
Select one

Filter

Name	Admin State	Status
91r3_demo_pcs_mgmt_port	Up	Down

9. In the Security Groups window, select the required network security groups from the list for internal, external and management ports. Click **Next**.

Figure 6: Security Groups Selection



Allocated 3

Name
pcs_90r3_stack-ext_port_security_group-a4rnkpvbxr5a
pcs_90r3_stack-int_port_security_group-uo2hujggvjuu
pcs_90r3_stack-mgmt_port_security_group-qqrgcv7dunb3

Available 7

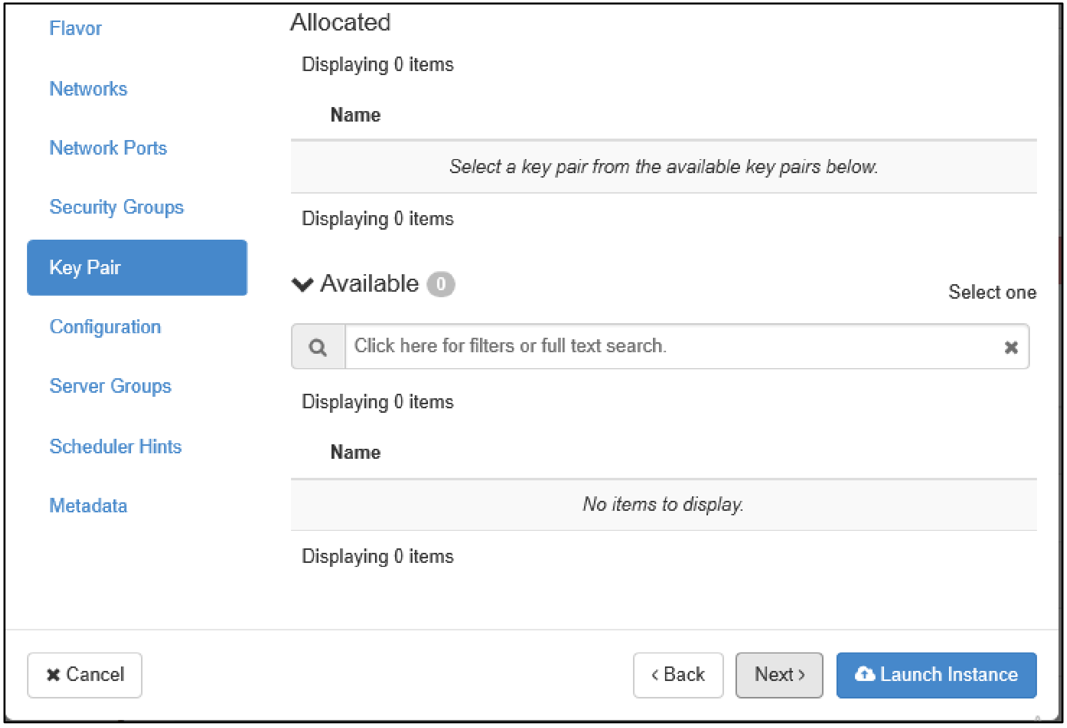
Select one or more

Click here for filters or full text search.

Name	Description
smc_pcs_from_snapshot_with_config_url_stack-mgmt_port_security_group-2vsrf36vcup7	
smc_pcs_from_snapshot_with_config_url_stack-int_port_security_group-ccgkufkyroc7	
default	Default security group
pcs_ext_port_sec_group	pcs_ext_port_sec_group

10. Key Pair is not used. Click **Next**.

Figure 7: Key Pair



Allocated

Displaying 0 items

Name
Select a key pair from the available key pairs below.

Displaying 0 items

Available 0

Select one

Click here for filters or full text search.

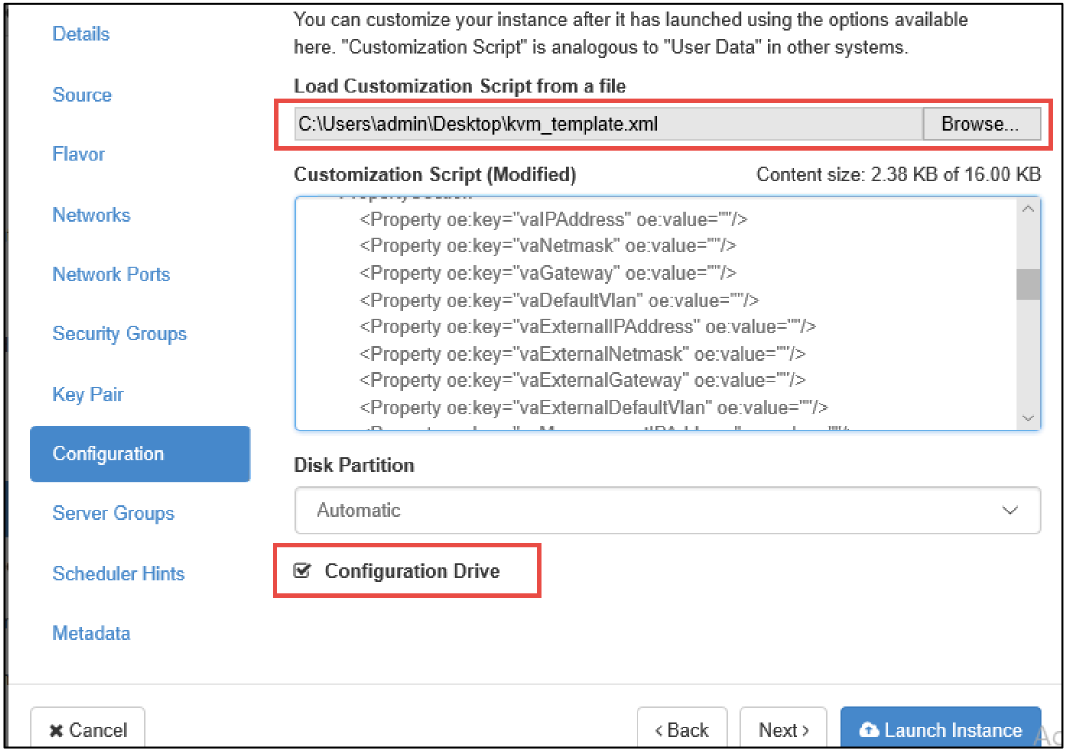
Displaying 0 items

Name
No items to display.

Displaying 0 items

11. In the Configuration window:
    a. Click **Choose file** and import the file that contains the provisioning parameters in XML format.
    b. Select the **Configuration Drive** check box. Only when the Configuration Drive flag is selected, the template file is available for PSA-V instance.
    c. Click **Launch Instance**.

Figure 8: Configuration Script



You can customize your instance after it has launched using the options available here. "Customization Script" is analogous to "User Data" in other systems.

Load Customization Script from a file

C:\Users\admin\Desktop\kvm_template.xml [Browse...]

Customization Script (Modified) Content size: 2.38 KB of 16.00 KB

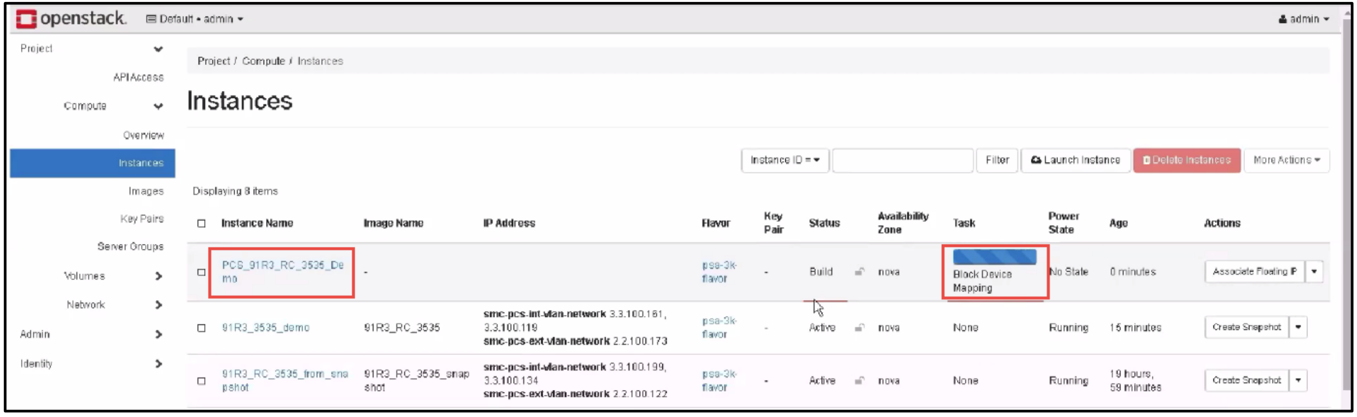
```
    <Property oe:key="vaIPAddress" oe:value=""/>
    <Property oe:key="vaNetmask" oe:value=""/>
    <Property oe:key="vaGateway" oe:value=""/>
    <Property oe:key="vaDefaultVlan" oe:value=""/>
    <Property oe:key="vaExternalIPAddress" oe:value=""/>
    <Property oe:key="vaExternalNetmask" oe:value=""/>
    <Property oe:key="vaExternalGateway" oe:value=""/>
    <Property oe:key="vaExternalDefaultVlan" oe:value=""/>
```

Disk Partition: Automatic

☑ Configuration Drive

12. The Instances window lists all the PCS VA instances. The blue bar in the Task column shows the status of creation of the instance. This will take a few minutes.
    - Open the created PCS VA instance by clicking on the Instance Name link.

Figure 9: Instances

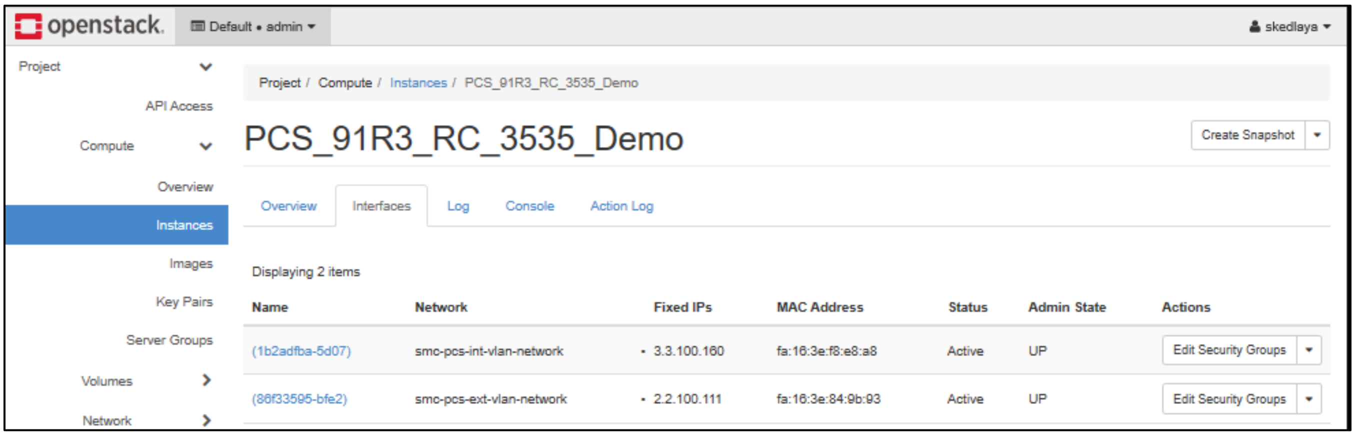


Instances

Displaying 8 items

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
PCS_91R3_RC_3535_Demo	-		psa-3k-flavor	-	Build	nova	Block Device Mapping	No State	0 minutes	Associate Floating IP
91R3_3535_demo	91R3_RC_3535	smc-pcs-int-vlan-network 3.3.100.161, 3.3.100.119 smc-pcs-ext-vlan-network 2.2.100.173	psa-3k-flavor	-	Active	nova	None	Running	15 minutes	Create Snapshot
91R3_RC_3535_from_snapshot	91R3_RC_3535_snapshot	smc-pcs-int-vlan-network 3.3.100.199, 3.3.100.134 smc-pcs-ext-vlan-network 2.2.100.122	psa-3k-flavor	-	Active	nova	None	Running	19 hours, 59 minutes	Create Snapshot

- The Interface tab shows the networks that are created.

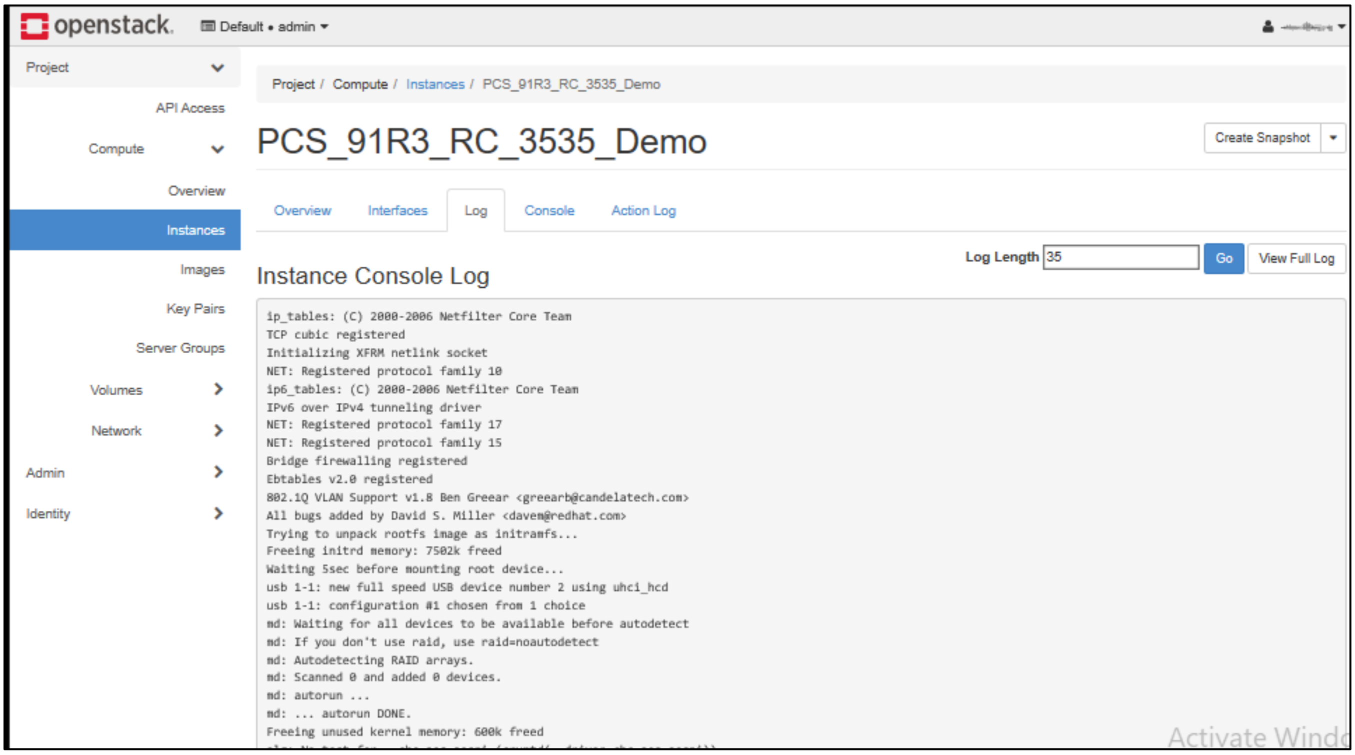


PCS_91R3_RC_3535_Demo

Displaying 2 items

Name	Network	Fixed IPs	MAC Address	Status	Admin State	Actions
(1b2adfba-5d07)	smc-pcs-int-vlan-network	• 3.3.100.160	fa:16:3e:f8:e8:a8	Active	UP	Edit Security Groups
(86f33595-bfe2)	smc-pcs-ext-vlan-network	• 2.2.100.111	fa:16:3e:84:9b:93	Active	UP	Edit Security Groups

- The Log tab shows the log details of the device that is created.



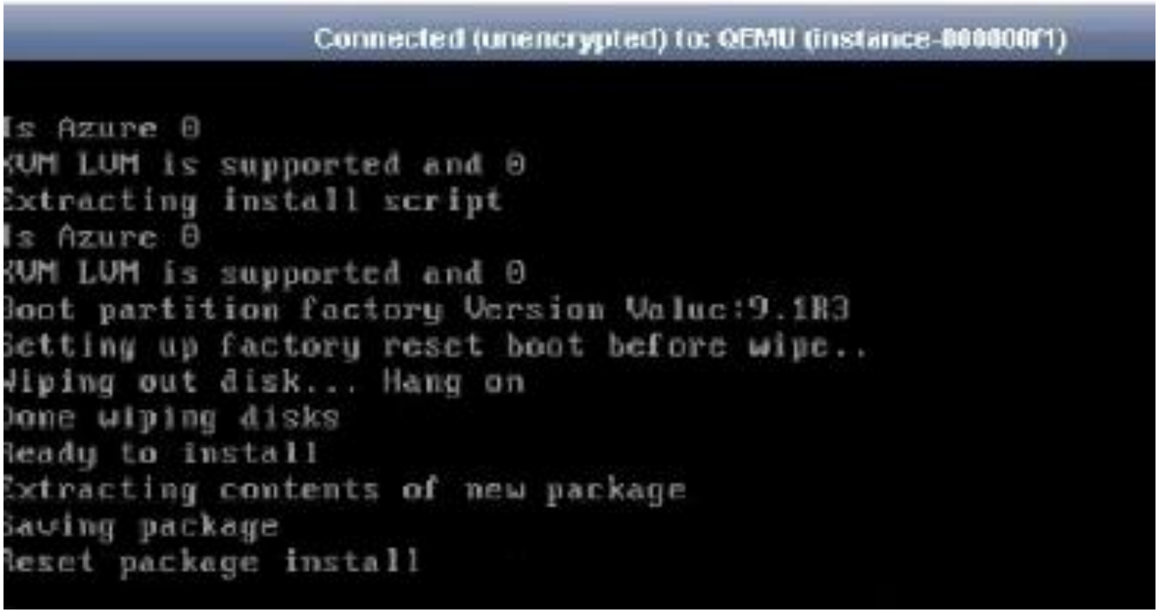
PCS_91R3_RC_3535_Demo

Instance Console Log

Log Length 35

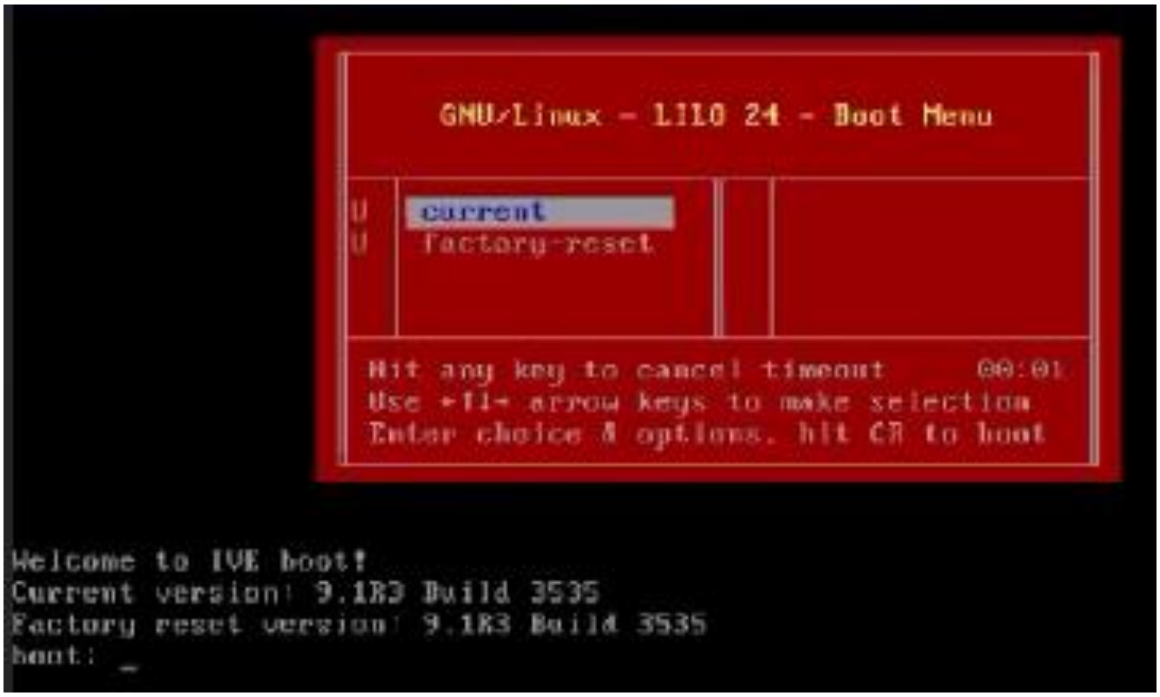
```
ip_tables: (C) 2000-2006 Netfilter Core Team
TCP cubic registered
Initializing XFRM netlink socket
NET: Registered protocol family 10
ip6_tables: (C) 2000-2006 Netfilter Core Team
IPv6 over IPv4 tunneling driver
NET: Registered protocol family 17
NET: Registered protocol family 15
Bridge firewalling registered
Ebtables v2.0 registered
802.1Q VLAN Support v1.8 Ben Greear <greearb@candelatech.com>
All bugs added by David S. Miller <davem@redhat.com>
Trying to unpack rootfs image as initramfs...
Freeing initrd memory: 7502k freed
Waiting 5sec before mounting root device...
usb 1-1: new full speed USB device number 2 using uhci_hcd
usb 1-1: configuration #1 chosen from 1 choice
md: Waiting for all devices to be available before autodetect
md: If you don't use raid, use raid=noautodetect
md: Autodetecting RAID arrays.
md: Scanned 0 and added 0 devices.
md: autorun ...
md: ... autorun DONE.
Freeing unused kernel memory: 600k freed
```

- The console tab provides the virtual console to view the device coming up.



Connected (unencrypted) to: QEMU (instance-000000f1)

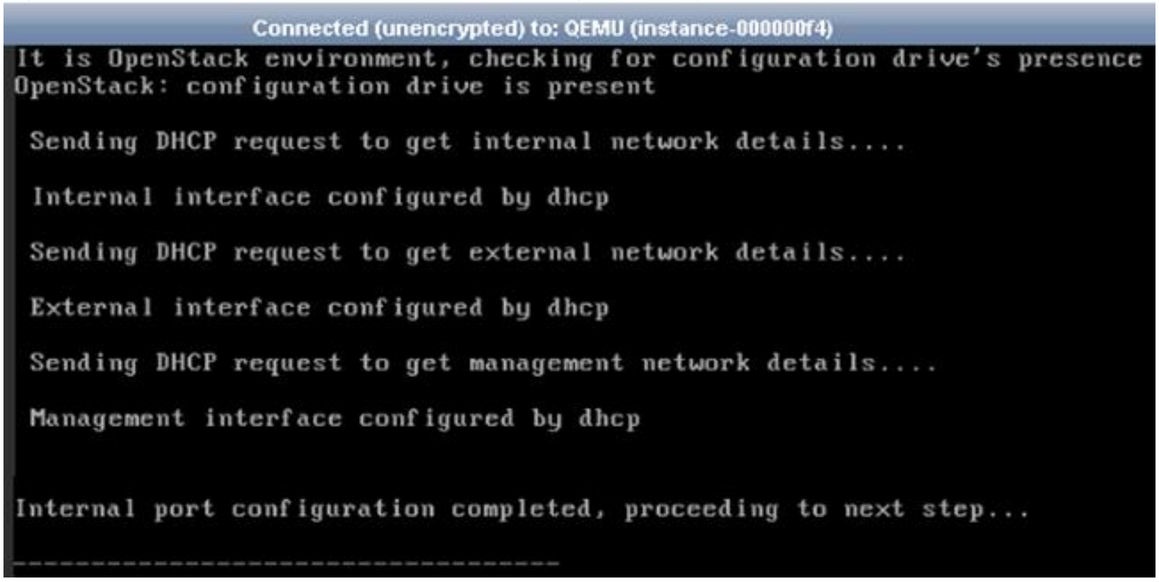
```
Is Azure 0
KVM LVM is supported and 0
Extracting install script
Is Azure 0
KVM LVM is supported and 0
Boot partition factory Version Value:9.1R3
Setting up factory reset boot before wipe..
Wiping out disk... Hang on
Done wiping disks
Ready to install
Extracting contents of new package
Saving package
Reset package install
```



```
GNU/Linux - LILO 24 - Boot Menu

current
factory-reset

Hit any key to cancel timeout      00:01
Use ↑↓ arrow keys to make selection
Enter choice & options, hit CR to boot

Welcome to IVE boot!
Current version: 9.1R3 Build 3535
Factory reset version: 9.1R3 Build 3535
boot: _
```

13. Next, the Internal and External interfaces are configured by DHCP (Zero touch configuration).

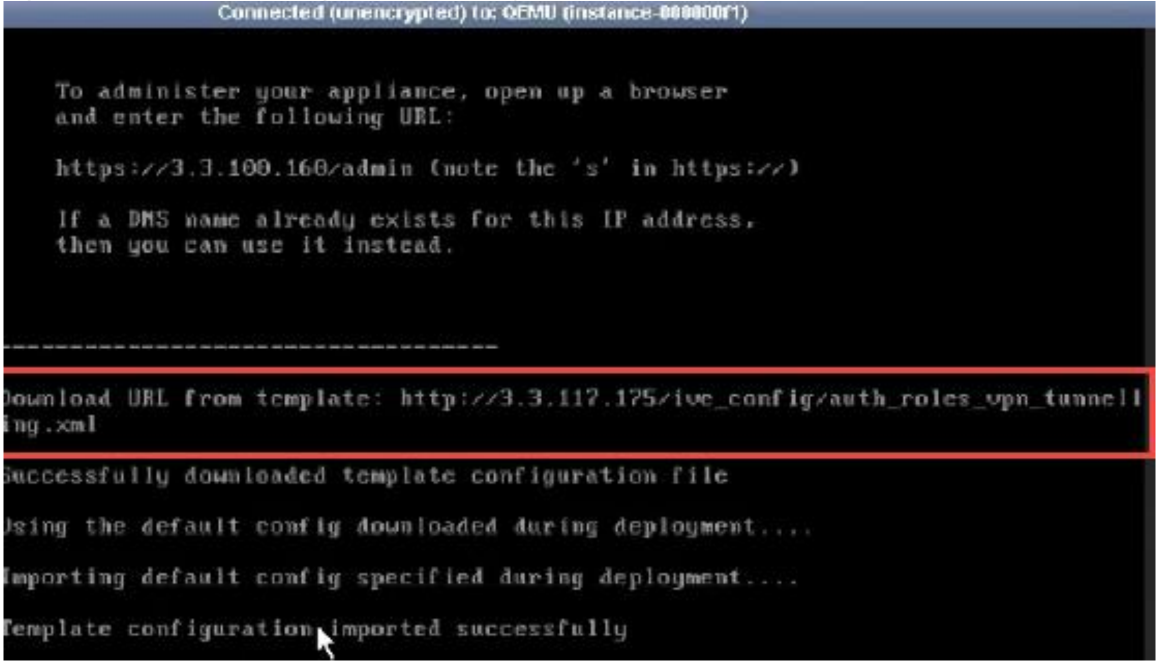
Figure 10: Internal and External Interfaces Configuration by DHCP



```
It is OpenStack environment, checking for configuration drive's presence
OpenStack: configuration drive is present

 Sending DHCP request to get internal network details....

 Internal interface configured by dhcp

 Sending DHCP request to get external network details....

 External interface configured by dhcp

 Sending DHCP request to get management network details....

 Management interface configured by dhcp


Internal port configuration completed, proceeding to next step...

-----------------------------------
```

14. The Config URL is downloaded for initial configuration.

Figure 11: Download Config URL from Template



```
    To administer your appliance, open up a browser
    and enter the following URL:

    https://3.3.100.160/admin (note the 's' in https://)

    If a DNS name already exists for this IP address,
    then you can use it instead.



-----------------------------------

Download URL from template: http://3.3.117.175/ive_config/auth_roles_vpn_tunnell
ing.xml

Successfully downloaded template configuration file

Using the default config downloaded during deployment....

Importing default config specified during deployment....

Template configuration imported successfully
```

This completes deploying PCS VA on OpenStack.

Deploying PCS on OpenStack Using Heat

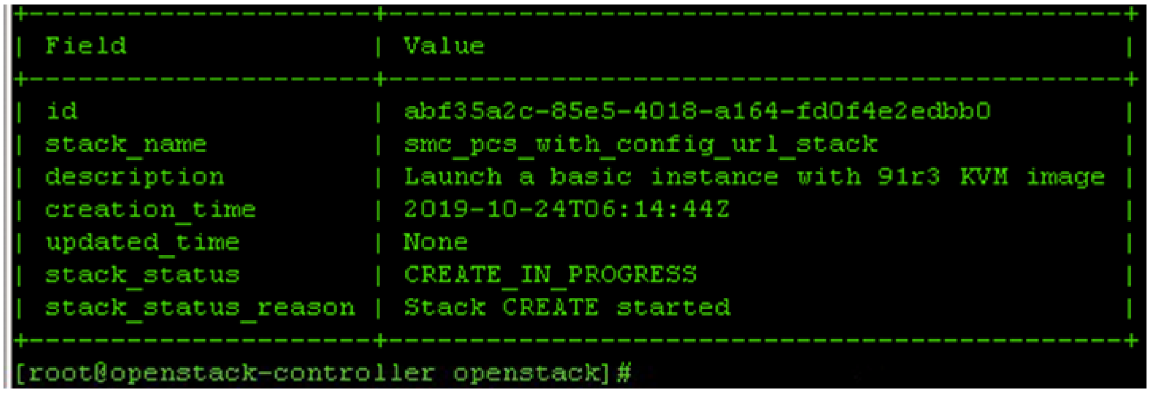
OpenStack provides Heat Orchestration template that can be used to automate the deployment of PSA-V.
Before proceeding with the deployment, ensure the image is uploaded to OpenStack. For details, see Appendix A.
Visit www.pulsesecure.net, download and unzip the package to extract the yml file. Ensure that parameters section in the template has correct default values:

- vm_name: Name of the PCS Virtual instance.
- image_name: Name of the PCS KVM image to install
- pcs_int_network: PCS Internal network to use for the instance.
- pcs_ext_network: PCS External network to use for the instance.
- pcs_mgmt_network: PCS Management network to use for the instance
- psa_v_flavor: PSA-V flavor to use for the instance.
- availability_zone: The Availability Zone to launch the instance.

To deploy PCS using OpenStack Heat, run the following command:

```
openstack stack create -t <.yml> <stack-name> --parameter <command line params>
```

Sample Output



```
+---------------------+---------------------------------------------+
| Field               | Value                                       |
+---------------------+---------------------------------------------+
| id                  | abf35a2c-85e5-4018-a164-fd0f4e2edbb0        |
| stack_name          | smc_pcs_with_config_url_stack               |
| description         | Launch a basic instance with 91r3 KVM image |
| creation_time       | 2019-10-24T06:14:44Z                        |
| updated_time        | None                                        |
| stack_status        | CREATE_IN_PROGRESS                          |
| stack_status_reason | Stack CREATE started                        |
+---------------------+---------------------------------------------+
[root@openstack-controller openstack]#
```

For command details refer to https://docs.openstack.org/heat/stein/getting_started/create_a_stack.html.

PCS Provisioning Parameters

Provisioning parameters are those parameters which are required during the deployment of a virtual appliance. PCS accepts the following parameters as provisioning parameters in the XML format.

```
<PropertySection>
    <Property oe:key="vaIPAddress" oe:value=""/>
    <Property oe:key="vaNetmask" oe:value=""/>
    <Property oe:key="vaGateway" oe:value=""/>
    <Property oe:key="vaDefaultVlan" oe:value=""/>
    <Property oe:key="vaExternalIPAddress" oe:value=""/>
    <Property oe:key="vaExternalNetmask" oe:value=""/>
    <Property oe:key="vaExternalGateway" oe:value=""/>
    <Property oe:key="vaExternalDefaultVlan" oe:value=""/>
    <Property oe:key="vaManagementIPAddress" oe:value=""/>
    <Property oe:key="vaManagementNetmask" oe:value=""/>
    <Property oe:key="vaManagementGateway" oe:value=""/>
    <Property oe:key="vaManagementDefaultVlan" oe:value=""/>
    <Property oe:key="vaPrimaryDNS" oe:value=""/>
    <Property oe:key="vaSecondaryDNS" oe:value=""/>
    <Property oe:key="vaWINSServer" oe:value=""/>
    <Property oe:key="vaDNSDomain" oe:value=""/>
    <Property oe:key="vaAdminUsername" oe:value=""/>
    <Property oe:key="vaAdminPassword" oe:value=""/>
    <Property oe:key="vaCommonName" oe:value=""/>
    <Property oe:key="vaOrganization" oe:value=""/>
    <Property oe:key="vaRandomText" oe:value=""/>
    <Property oe:key="vaAcceptLicenseAgreement" oe:value="n"/>
    <Property oe:key="vaEnableLicenseServer" oe:value=""/>
    <Property oe:key="vaAdminEnableREST" oe:value=""/>
    <Property oe:key="vaAuthCodeLicense" oe:value=""/>
    <Property oe:key="vaConfigURL" oe:value=""/>
    <Property oe:key="vaConfigServerCACertPEM" oe:value=""/>
    <Property oe:key="vaConfigData" oe:value=""/>
    <Property oe:key="vaInternalPortReconfigWithValueInVAppProperties" oe:value="0"/>
    <Property oe:key="vaManagementPortReconfigWithValueInVAppProperties" oe:value="0"/>
    <Property oe:key="vaExternalPortReconfigWithValueInVAppProperties" oe:value="0"/>
</PropertySection>
```

#	Parameter Name	Type	Description
1	vaIPAddress	IP address	Internal interface IP
2	vaNetmask	IP address	Internal interface subnet mask
3	vaGateway	IP address	Internal interface IP gateway
4	vaDefaultVlan	integer	VLAN number to assign to this interface
5	vaExternalIPAddress	IP address	External interface IP
6	vaExternalNetmask	IP address	External interface subnet mask
7	vaExternalGateway	IP address	External interface IP gateway
8	vaExternalDefaultVlan	Integer	VLAN number to assign to this interface.

#	Parameter Name	Type	Description
9	vaManagementIPAddress	IP address	Management interface IP
10	vaManagementNetmask	IP address	Management interface subnet mask
11	vaManagementGateway	IP address	Management interface IP gateway
12	vaManagementDefaultVlan	Integer	VLAN number to assign to this interface
13	vaPrimaryDNS	IP address	Primary DNS IP
14	vaSecondaryDNS	IP address	Secondary DNS IP
15	vaWINSServer	IP address	Windows server IP
16	vaDNSDomain	string	Windows domain name
17	VaAdminUsername	string	Admin username
18	vaAdminPassword	string	Admin password
19	vaCommonName	string	Common name
20	vaOrganization	string	Organization name
21	vaRandomText	string	Random text to generate self-signed certificate
22	vaAcceptLicenseAgreement	character	"y" to accept the license agreement
23	vaEnableLicenseServer	character	"y" to enable it as VLS server. "n" to bring it up as a PCS node.
24	vaAdminEnableREST	character	"y" to enable REST for administrator user
25	vaAuthCodeLicense	string	Authentication code that needs to be obtained from Pulse Secure.
26	vaConfigURL	String URL	Http based URL where XML based PCS configuration can be found.
27	vaConfigServerCACertPEM	string	PEM format of CA certificate.
28	vaConfigData	string	base64 encoded XML based PCS configuration.
29	vaInternalPortReconfigWithValueInVAppProperties	integer	The Internal port overwrite property. If set to 1, overwrite the virtual appliance's internal port settings with the ones specified during deployment. Set this value as 1.
30	vaManagementPortReconfigWithValueInVAppProperties	integer	The Management port overwrite property. If set to 1, overwrite the management port-related parameters in the PCS with the ones defined here. Set this value as 1.
31	vaExternalPortReconfigWithValueInVAppProperties	integer	The External port overwrite property. If set to 1, overwrite the external port-related parameters in PCS/PPS with the ones defined here. Set this value as 1.

From 9.1R3 release, PCS supports zero touch provisioning. This feature can detect and assign DHCP networking settings automatically at the PCS boot up. The following PCS parameters should be set to null in order to fetch the networking configuration automatically from the DHCP server.

- vaIPAddress
- vaNetmask
- vaGateway
- vaPrimaryDNS
- vaExternalIPAddress
- vaExternalNetmask
- vaExternalGateway
- vaSecondaryDNS
- vaManagementIPAddress
- vaManagementNetmask
- vaManagementGateway
- vaDNSDomain

NOTE: Leased IP from DHCP server should be valid for a long time as PCS does not request for DHCP renewals.

Limitations

The following list of PCS features are not supported in this release:

- Default VLAN tagging
- VLAN-based Source IP functionality
- Layer 3 Tunnel IP pool assignment via DHCP
  Workaround: Use Static IP pool
- Layer 2 functionality like ARP Cache and ND Cache
- For Pulse Client connection, disable Port Security on Internal port
- Virtual Ports
  Workaround: To make use of virtual ports, disable Port Security on Internal and External ports
- Multicast capabilities
- Bandwidth management
- AP Cluster
  Workaround: Disable Port Security on Internal and External ports

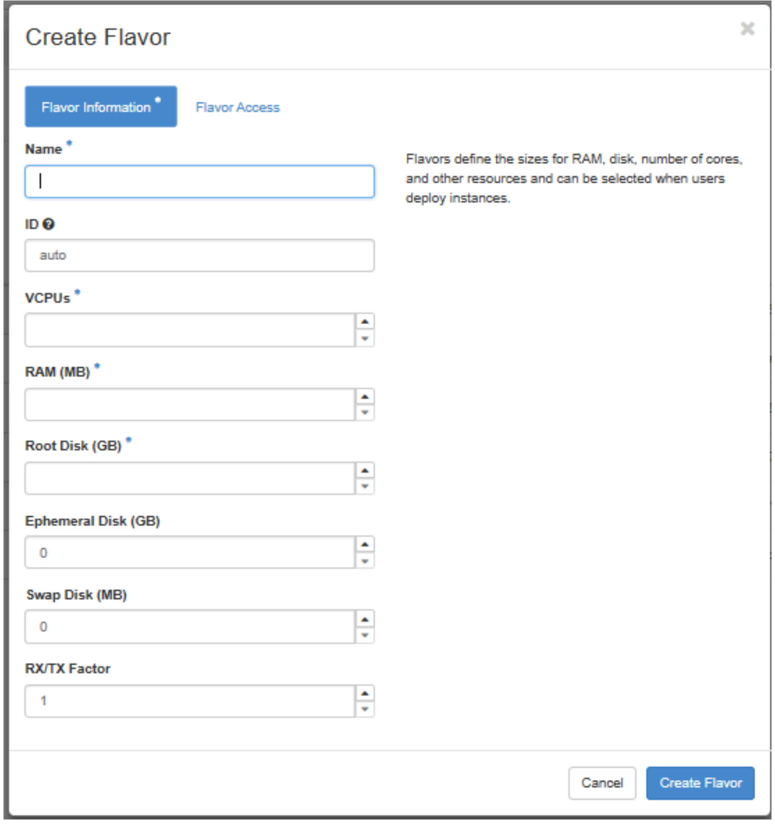
Appendix A: Setting Up Prerequisites

Creating Required Flavors of PSA-V

In OpenStack, a flavor is a hardware configuration of a server that defines vCPU, memory and storage capacity of computing instances.
To create flavor in OpenStack:

1. Log in to OpenStack.
2. In the OpenStack dashboard displayed, select **Admin** > **Compute** > **Flavors**. The Flavors page contains a list of existing flavors if already available.
3. Click on the **Create Flavor** button. The Create Flavor dialog box appears.
4. Enter a name in the **Name** box.
5. Enter the appropriate value in the **vCPUs** box.
6. Enter the appropriate value in the **RAM** box.
7. Enter the appropriate value in the **Root Disk** box.
8. Click **Create Flavor**.

Figure 12: Create Flavor



Create Flavor

Flavors define the sizes for RAM, disk, number of cores, and other resources and can be selected when users deploy instances.

Name *

ID: auto

VCPUs *

RAM (MB) *

Root Disk (GB) *

Ephemeral Disk (GB): 0

Swap Disk (MB): 0

RX/TX Factor: 1

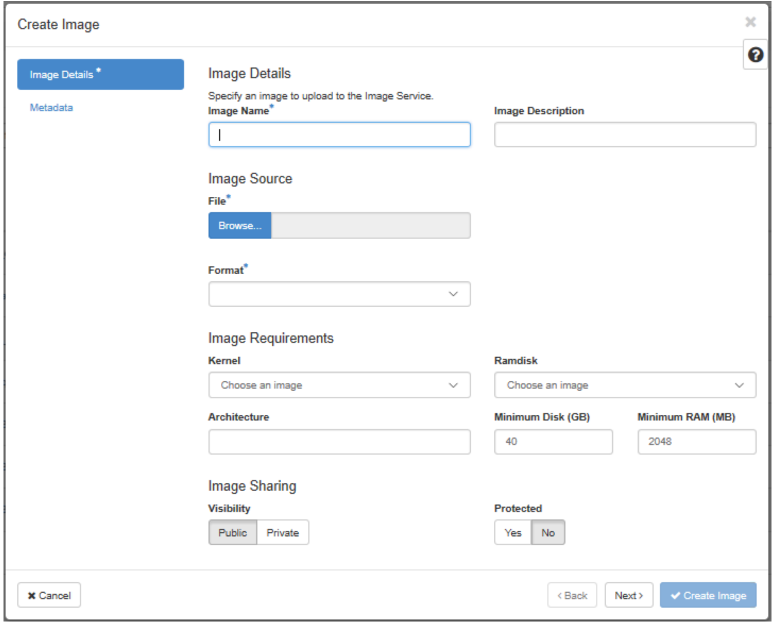
The flavor is created and is listed in the Flavors page.

Uploading Required Image to OpenStack

To upload PCS KVM image to OpenStack:

1. Log in to OpenStack.
2. In the OpenStack dashboard displayed, select **Project** > **Compute** > **Images**. The Images page contains a list of existing images if already available.
3. Click on the **Create Image** button.
4. Enter a name in the **Image Name** box.
5. Enter a suitable description in the **Image Description** box.
6. Click **Browse** and select the downloaded PCS KVM image file from your local drive.
7. Select **Format** from the drop-down list.
8. Enter **Minimum Disk** in GB required for the deployment.
9. Enter **Minimum RAM** in MB required for the deployment. Recommended is 2048 MB.
10. Click on the **Create Image** button.

Figure 13: Create Image



Specify an image to upload to the Image Service.

Minimum Disk (GB): 40

Minimum RAM (MB): 2048

Visibility: Public

Protected: No

The image is created and is listed in the Images page.

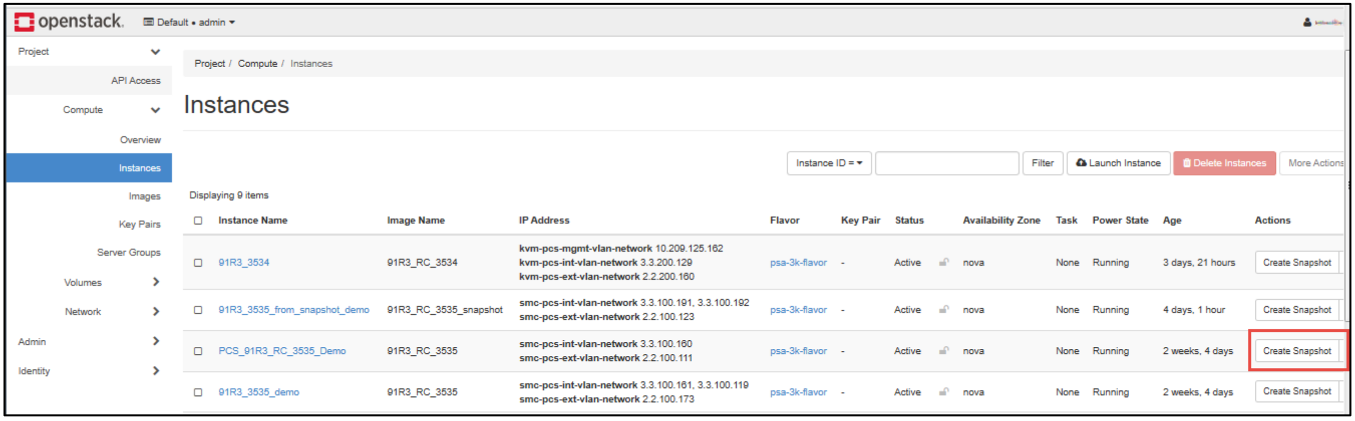
Creating Snapshot Image

A snapshot image is an image template or a logical copy of the image. It uses minimal storage space.

To create a snapshot image:

1. Log in to OpenStack.
2. In the OpenStack dashboard displayed, select **Project > Compute > Instances**. The Instances page contains a list of existing instances already available.
3. Click on the **Create Snapshot** button corresponding to the instance created.

Figure 14: Create Snapshot button



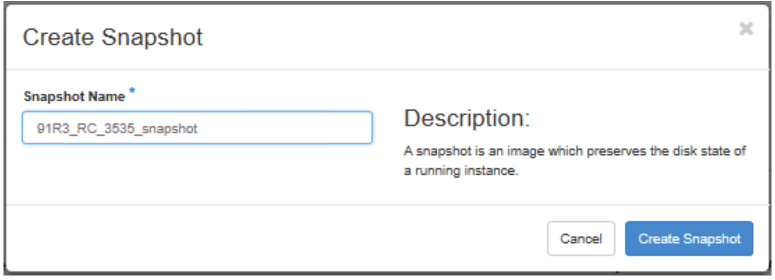
Instances

Displaying 9 items

☐	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
☐	91R3_3534	91R3_RC_3534	**kvm-pcs-mgmt-vlan-network** 10.209.125.162 **kvm-pcs-int-vlan-network** 3.3.200.129 **kvm-pcs-ext-vlan-network** 2.2.200.160	psa-3k-flavor	-	Active	nova	None	Running	3 days, 21 hours	Create Snapshot
☐	91R3_3535_from_snapshot_demo	91R3_RC_3535_snapshot	**smc-pcs-int-vlan-network** 3.3.100.191, 3.3.100.192 **smc-pcs-ext-vlan-network** 2.2.100.123	psa-3k-flavor	-	Active	nova	None	Running	4 days, 1 hour	Create Snapshot
☐	PCS_91R3_RC_3535_Demo	91R3_RC_3535	**smc-pcs-int-vlan-network** 3.3.100.160 **smc-pcs-ext-vlan-network** 2.2.100.111	psa-3k-flavor	-	Active	nova	None	Running	2 weeks, 4 days	Create Snapshot
☐	91R3_3535_demo	91R3_RC_3535	**smc-pcs-int-vlan-network** 3.3.100.161, 3.3.100.119 **smc-pcs-ext-vlan-network** 2.2.100.173	psa-3k-flavor	-	Active	nova	None	Running	2 weeks, 4 days	Create Snapshot

4. In the Create Snapshot dialog box, enter a name in the **Snapshot Name** box.

Figure 15: Create Snapshot dialog box



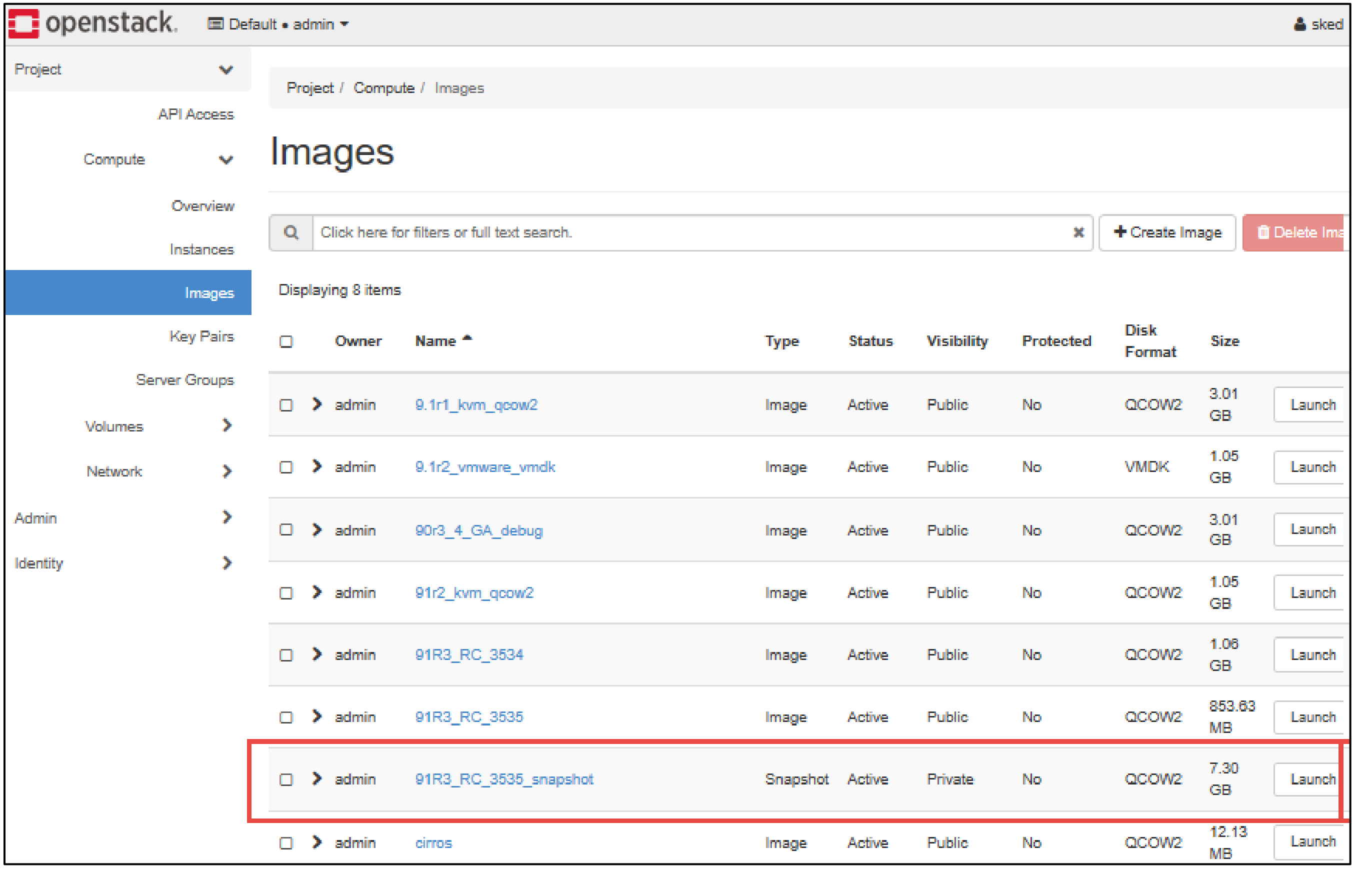
Snapshot Name *: 91R3_RC_3535_snapshot

Description:

A snapshot is an image which preserves the disk state of a running instance.

5. Select **Project > Compute> Images**. The snapshot image is listed in the Images page. The Type of the image indicates that it is a Snapshot. Image.

Figure 16: Snapshot Image



Images

Displaying 8 items

□	Owner	Name	Type	Status	Visibility	Protected	Disk Format	Size	
□	admin	9.1r1_kvm_qcow2	Image	Active	Public	No	QCOW2	3.01 GB	Launch
□	admin	9.1r2_vmware_vmdk	Image	Active	Public	No	VMDK	1.05 GB	Launch
□	admin	90r3_4_GA_debug	Image	Active	Public	No	QCOW2	3.01 GB	Launch
□	admin	91r2_kvm_qcow2	Image	Active	Public	No	QCOW2	1.05 GB	Launch
□	admin	91R3_RC_3534	Image	Active	Public	No	QCOW2	1.06 GB	Launch
□	admin	91R3_RC_3535	Image	Active	Public	No	QCOW2	853.63 MB	Launch
□	admin	91R3_RC_3535_snapshot	Snapshot	Active	Private	No	QCOW2	7.30 GB	Launch
□	admin	cirros	Image	Active	Public	No	QCOW2	12.13 MB	Launch

Creating Internal, External and Management Networks on OpenStack

To create Internal, External and Management networks in OpenStack:

1. Log in to OpenStack.
2. In the OpenStack dashboard displayed, select **Admin > Network > Networks**. The Networks page contains a list of existing networks if already available.
3. Click on the **Create Network** button.
4. In the Networks page, provide the required configuration details for Internal network and click **Create Network**.

   The Internal network is created and is listed in the Networks page.
5. Follow the same procedure to create External and Management networks.

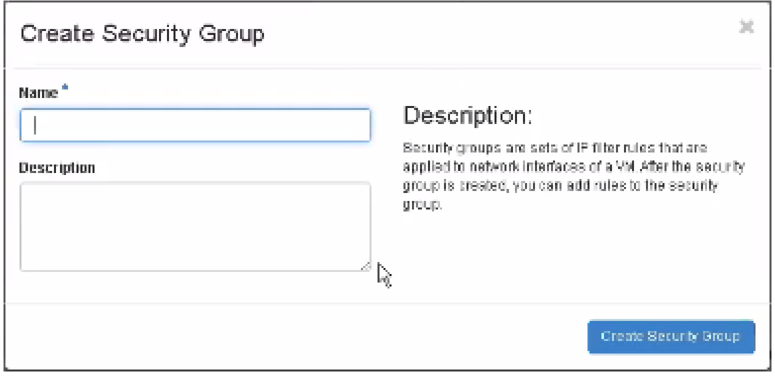
Creating Required Security Groups for Internal, External and Management Ports

The Security Groups is a type of firewall provided by OpenStack to assign to Internal, External and Management ports.

To create Security Groups in OpenStack:

1. Log in to OpenStack.
2. In the OpenStack dashboard displayed, select **Project > Network > Security Groups**. The Security Groups page contains a list of existing Security Groups if already available.
3. Click on the **Create Security Group** button. The Create Security Group dialog box appears.

Figure 17: Create Security Group dialog box



Description:

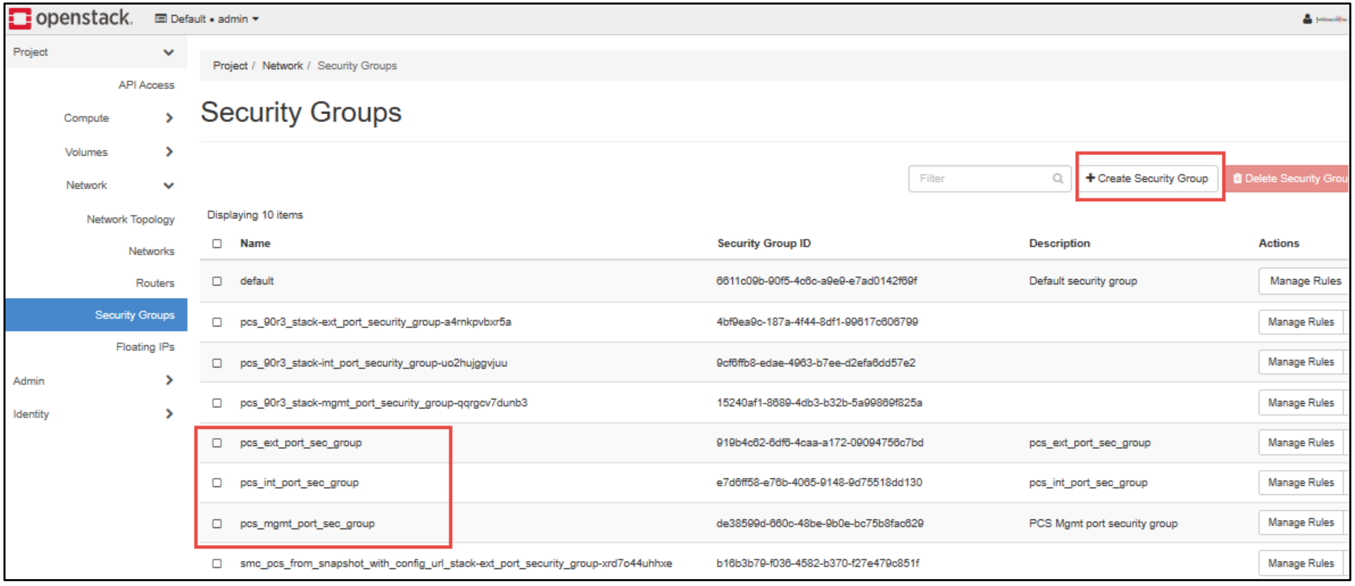
Security groups are sets of IP filter rules that are applied to network interfaces of a VM. After the security group is created, you can add rules to the security group.

4. Enter a name for the Security Group to assign to Internal port in the **Name** box.
5. Enter a suitable description in the **Description** box.
6. Click the **Create Security Group** button.

   The Security Group is created and is listed in the Security Groups page.
7. Follow the same procedure to create Security Groups to assign to External and Management ports.

   The Security Groups are created and are listed in the Security Groups page.

Figure 18: Security Groups page



Security Groups

Displaying 10 items

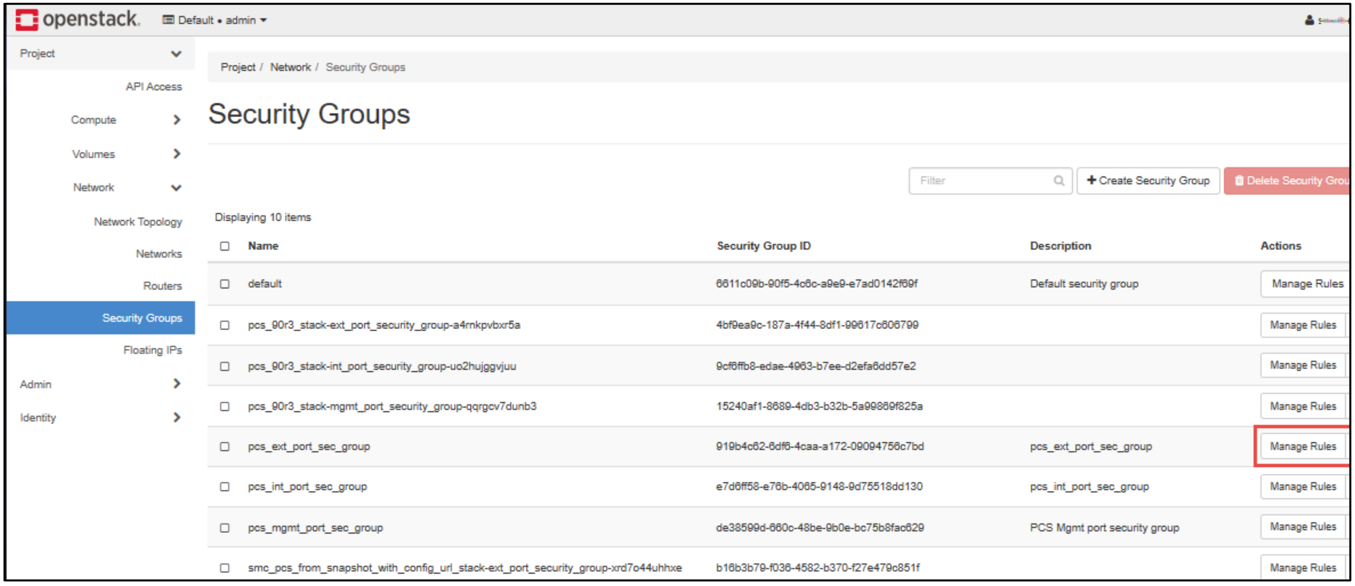
□	Name	Security Group ID	Description	Actions
□	default	6611c09b-90f5-4c6c-a9e9-e7ad0142f69f	Default security group	Manage Rules
□	pcs_90r3_stack-ext_port_security_group-a4rnkpvbxr5a	4bf9ea9c-187a-4f44-8df1-99617c606799		Manage Rules
□	pcs_90r3_stack-int_port_security_group-uo2hujggvjuu	9cf6ffb8-edae-4963-b7ee-d2efa6dd57e2		Manage Rules
□	pcs_90r3_stack-mgmt_port_security_group-qqrgcv7dunb3	15240af1-8689-4db3-b32b-5a99869f825a		Manage Rules
□	pcs_ext_port_sec_group	919b4c62-6df6-4caa-a172-09094756c7bd	pcs_ext_port_sec_group	Manage Rules
□	pcs_int_port_sec_group	e7d6ff58-e76b-4065-9148-9d75518dd130	pcs_int_port_sec_group	Manage Rules
□	pcs_mgmt_port_sec_group	de38599d-660c-48be-9b0e-bc75b8fac629	PCS Mgmt port security group	Manage Rules
□	smc_pcs_from_snapshot_with_config_url_stack-ext_port_security_group-xrd7o44uhhxe	b16b3b79-f036-4582-b370-f27e479c851f		Manage Rules

Creating Rules

Once the Security Groups are created, rules have to be set to the assigned Internal, External and Management ports for allowing/disallowing the traffic.
To create rules to a Security Group:

1. In the Security Groups page, click on **Manage Rules** associated with the required Security Group.

Figure 19: Security Groups page – Manage Rules



Project / Network / Security Groups

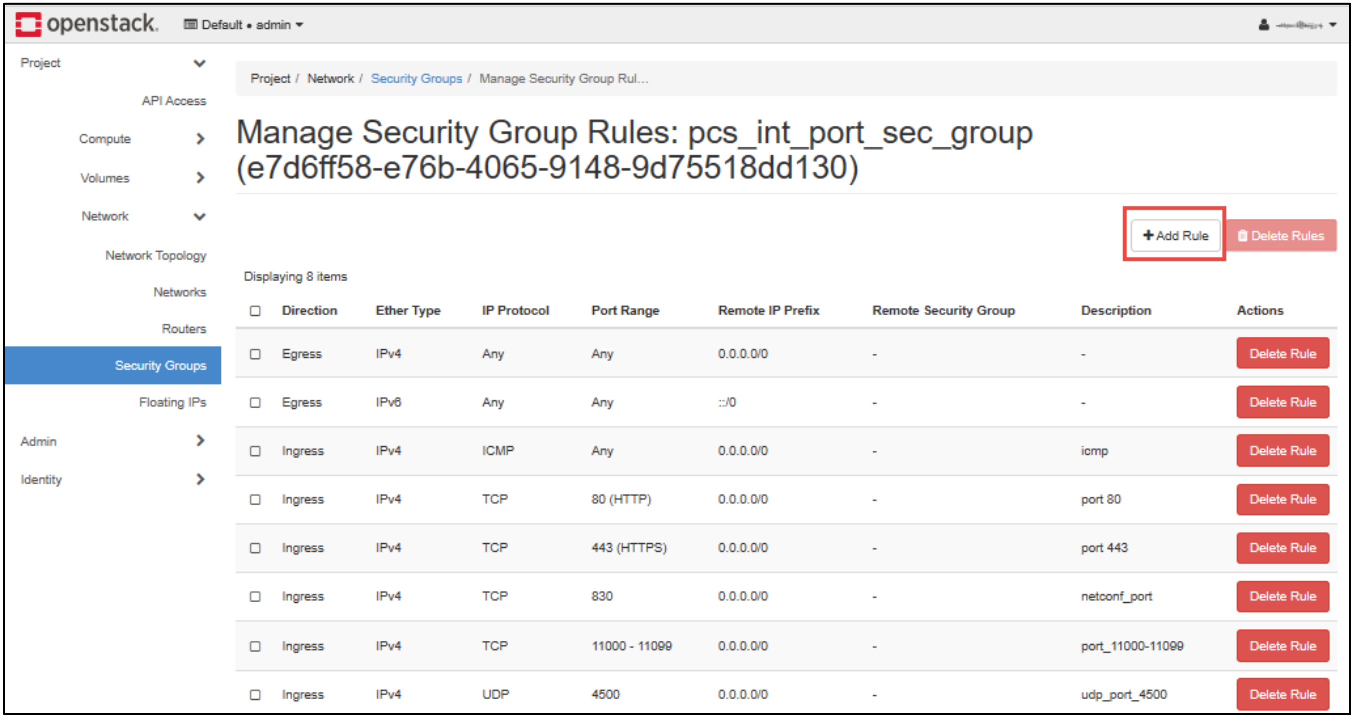
Security Groups

Displaying 10 items

☐	Name	Security Group ID	Description	Actions
☐	default	6611c09b-90f5-4c6c-a9e9-e7ad0142f69f	Default security group	Manage Rules
☐	pcs_90r3_stack-ext_port_security_group-a4rnkpvbxr5a	4bf9ea9c-187a-4f44-8df1-99617c606799		Manage Rules
☐	pcs_90r3_stack-int_port_security_group-uo2hujggvjuu	9cf6ffb8-edae-4963-b7ee-d2efa6dd57e2		Manage Rules
☐	pcs_90r3_stack-mgmt_port_security_group-qqrgcv7dunb3	15240af1-8689-4db3-b32b-5a99889f825a		Manage Rules
☐	pcs_ext_port_sec_group	919b4c62-6df6-4caa-a172-09094756c7bd	pcs_ext_port_sec_group	Manage Rules
☐	pcs_int_port_sec_group	e7d6ff58-e76b-4065-9148-9d75518dd130	pcs_int_port_sec_group	Manage Rules
☐	pcs_mgmt_port_sec_group	de38599d-660c-48be-9b0e-bc75b8fac629	PCS Mgmt port security group	Manage Rules
☐	smc_pcs_from_snapshot_with_config_url_stack-ext_port_security_group-xrd7o44uhhxe	b16b3b79-f036-4582-b370-f27e479c851f		Manage Rules

2. In the Manage Security Group Rules page that appears, click on the **Add Rule** button.

Figure 20: Add Rule button



Project / Network / Security Groups / Manage Security Group Rul...

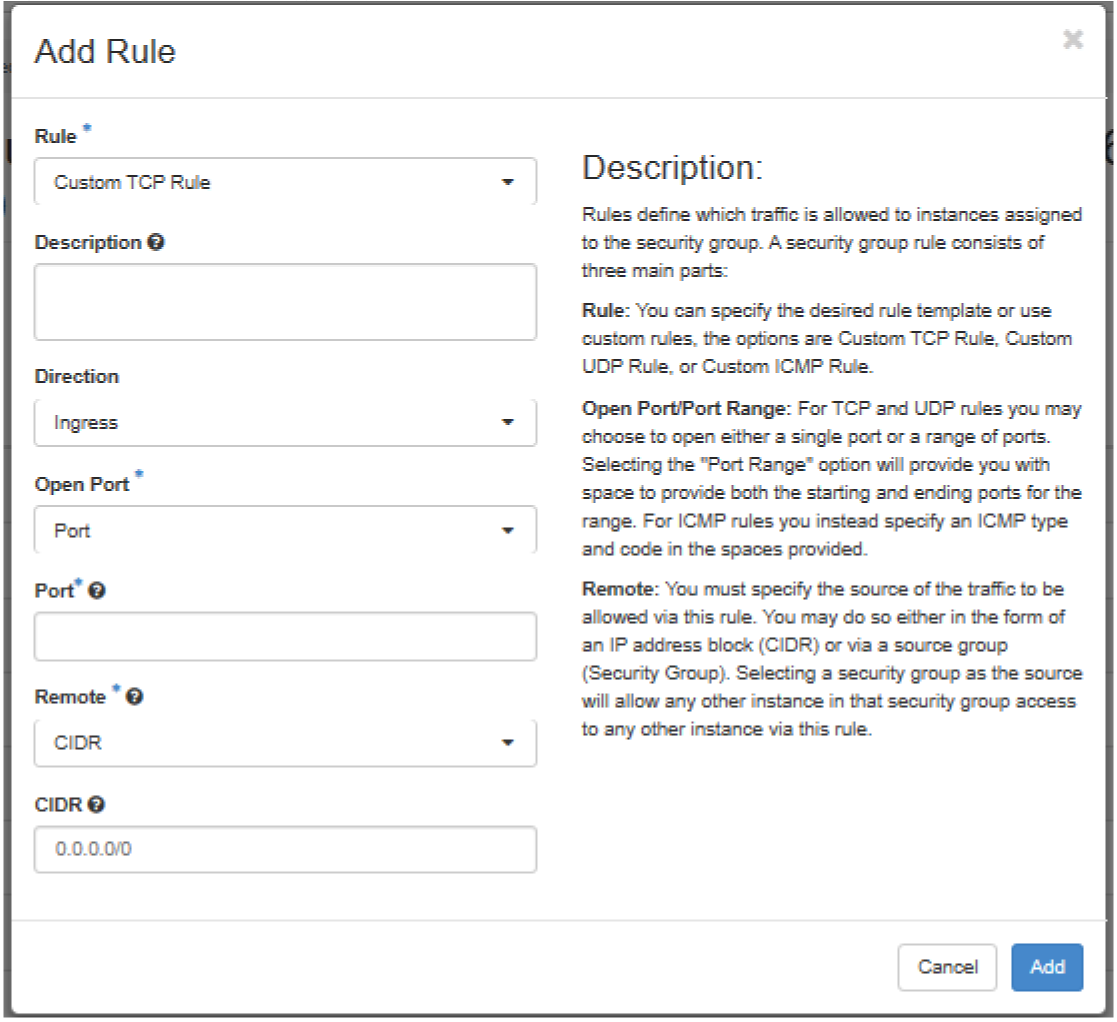
Manage Security Group Rules: pcs_int_port_sec_group (e7d6ff58-e76b-4065-9148-9d75518dd130)

Displaying 8 items

☐	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
☐	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
☐	Egress	IPv6	Any	Any	::/0	-	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	icmp	Delete Rule
☐	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0	-	port 80	Delete Rule
☐	Ingress	IPv4	TCP	443 (HTTPS)	0.0.0.0/0	-	port 443	Delete Rule
☐	Ingress	IPv4	TCP	830	0.0.0.0/0	-	netconf_port	Delete Rule
☐	Ingress	IPv4	TCP	11000 - 11099	0.0.0.0/0	-	port_11000-11099	Delete Rule
☐	Ingress	IPv4	UDP	4500	0.0.0.0/0	-	udp_port_4500	Delete Rule

3. In the Add Rule window that appears, provide the required configuration details and Add the rule.

Figure 21: Add Rule dialog box



Add Rule

Rule *

Custom TCP Rule

Description

Direction

Ingress

Open Port *

Port

Port *

Remote *

CIDR

CIDR

0.0.0.0/0

Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

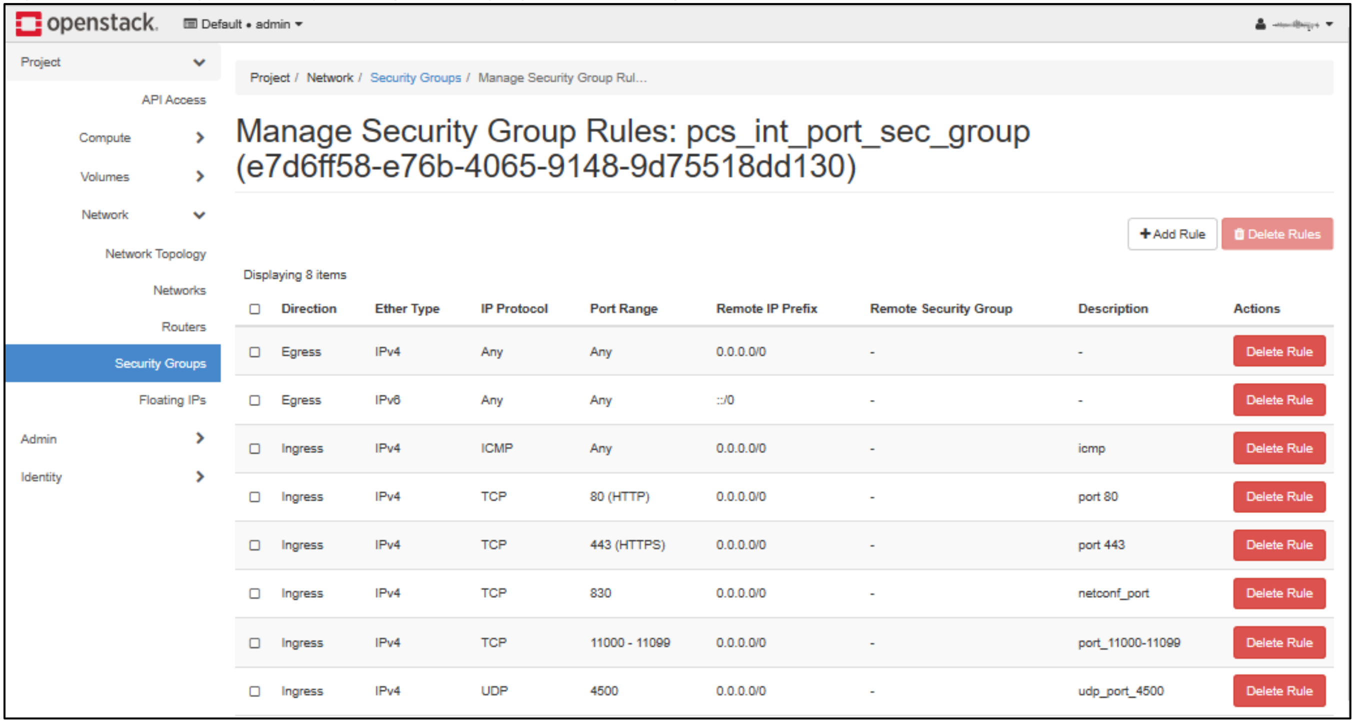
Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Follow the same procedure to add rules to External and Management ports.

Figure 22: Manage Security Group Rules page – Internal port



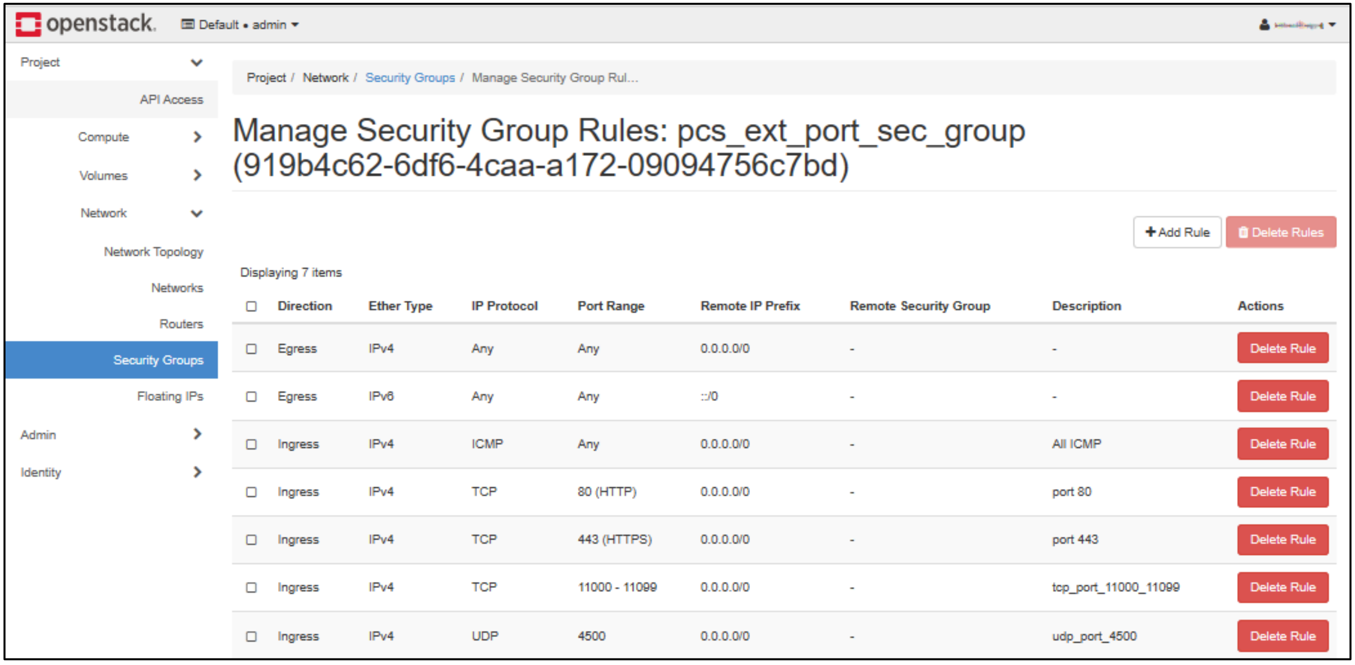
Project / Network / Security Groups / Manage Security Group Rul...

Manage Security Group Rules: pcs_int_port_sec_group (e7d6ff58-e76b-4065-9148-9d75518dd130)

Displaying 8 items

□	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
□	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
□	Egress	IPv6	Any	Any	::/0	-	-	Delete Rule
□	Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	icmp	Delete Rule
□	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0	-	port 80	Delete Rule
□	Ingress	IPv4	TCP	443 (HTTPS)	0.0.0.0/0	-	port 443	Delete Rule
□	Ingress	IPv4	TCP	830	0.0.0.0/0	-	netconf_port	Delete Rule
□	Ingress	IPv4	TCP	11000 - 11099	0.0.0.0/0	-	port_11000-11099	Delete Rule
□	Ingress	IPv4	UDP	4500	0.0.0.0/0	-	udp_port_4500	Delete Rule

Figure 23: Manage Security Group Rules page – External port



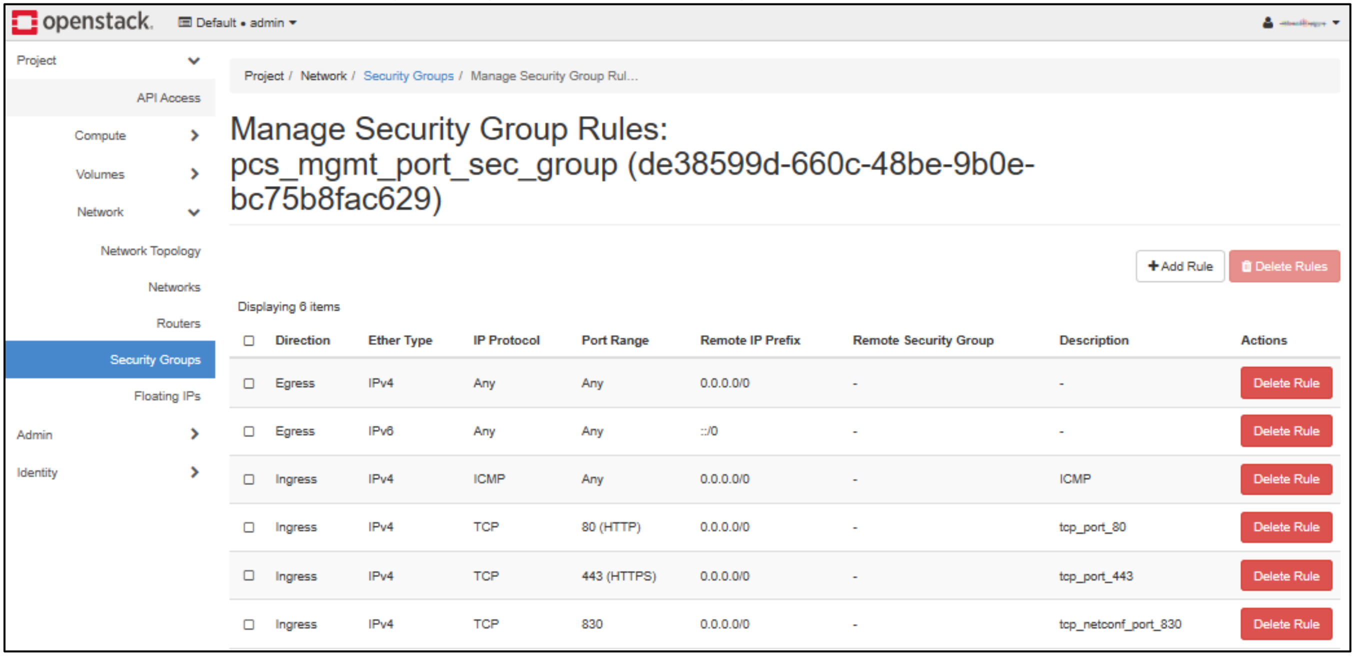
Project / Network / Security Groups / Manage Security Group Rul...

Manage Security Group Rules: pcs_ext_port_sec_group (919b4c62-6df6-4caa-a172-09094756c7bd)

Displaying 7 items

□	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
□	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
□	Egress	IPv6	Any	Any	::/0	-	-	Delete Rule
□	Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	All ICMP	Delete Rule
□	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0	-	port 80	Delete Rule
□	Ingress	IPv4	TCP	443 (HTTPS)	0.0.0.0/0	-	port 443	Delete Rule
□	Ingress	IPv4	TCP	11000 - 11099	0.0.0.0/0	-	tcp_port_11000_11099	Delete Rule
□	Ingress	IPv4	UDP	4500	0.0.0.0/0	-	udp_port_4500	Delete Rule

Figure 24: Manage Security Group Rules page – Management port



Manage Security Group Rules: pcs_mgmt_port_sec_group (de38599d-660c-48be-9b0e-bc75b8fac629)

Displaying 6 items

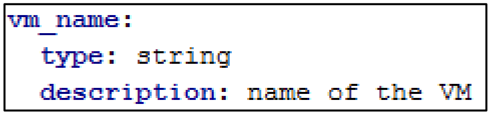
☐	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
☐	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	Delete Rule
☐	Egress	IPv6	Any	Any	::/0	-	-	Delete Rule
☐	Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	ICMP	Delete Rule
☐	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0	-	tcp_port_80	Delete Rule
☐	Ingress	IPv4	TCP	443 (HTTPS)	0.0.0.0/0	-	tcp_port_443	Delete Rule
☐	Ingress	IPv4	TCP	830	0.0.0.0/0	-	tcp_netconf_port_830	Delete Rule

Appendix B: HEAT Template

Pulse Secure provides sample HEAT template files to deploy PCS VA on OpenStack. Users can modify this to make it suitable for their need.

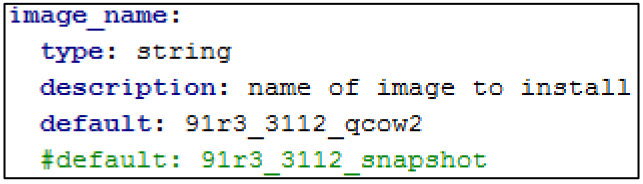
parameters

VM Name: This is the name given to PCS Virtual Appliance.



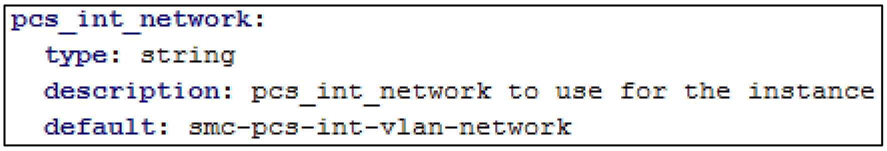
```
vm_name:
  type: string
  description: name of the VM
```

Image name: This is the name given to the PCS KVM image to install.



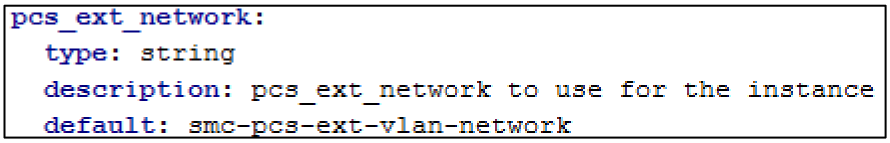
```
image_name:
  type: string
  description: name of image to install
  default: 91r3_3112_qcow2
  #default: 91r3_3112_snapshot
```

PCS Internal Network: This is PCS Internal network to use for the instance.



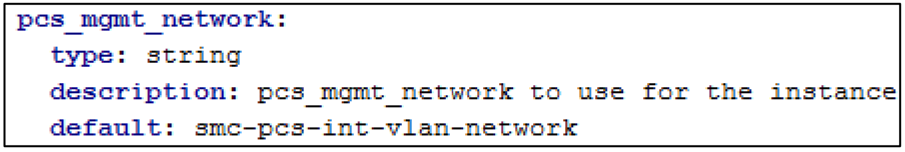
```
pcs_int_network:
  type: string
  description: pcs_int_network to use for the instance
  default: smc-pcs-int-vlan-network
```

PCS External Network: This is PCS External network to use for the instance.



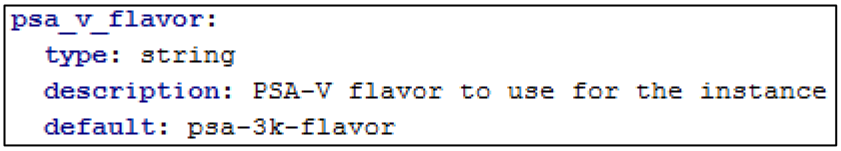
```
pcs_ext_network:
  type: string
  description: pcs_ext_network to use for the instance
  default: smc-pcs-ext-vlan-network
```

PCS Management Network: This is PCS Management network to use for the instance.



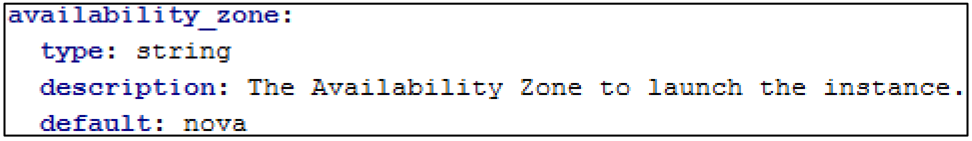
```
pcs_mgmt_network:
  type: string
  description: pcs_mgmt_network to use for the instance
  default: smc-pcs-int-vlan-network
```

PSA-V Flavor: This is the PSA-V flavor to use for the instance.



```
psa_v_flavor:
  type: string
  description: PSA-V flavor to use for the instance
  default: psa-3k-flavor
```

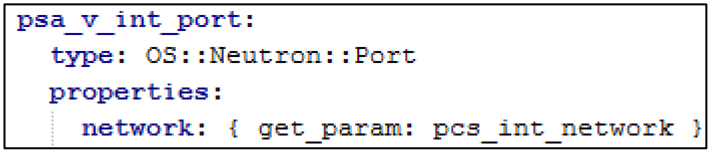
Availability Zone: This is the availability zone to launch the instance.



```
availability_zone:
  type: string
  description: The Availability Zone to launch the instance.
  default: nova
```

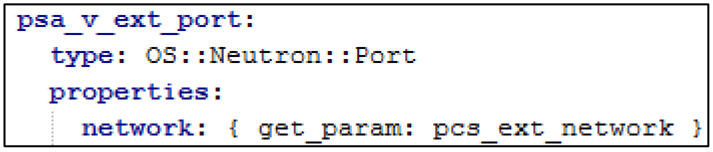
resources

PSA-V Internal Port: This block is responsible for creating network interface. The created network interface is applied to network interface card of PCS Internal interface.



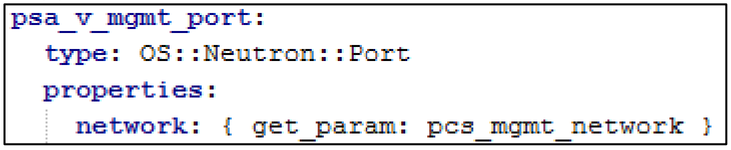
```
psa_v_int_port:
  type: OS::Neutron::Port
  properties:
    network: { get_param: pcs_int_network }
```

PSA-V External Port: This block is responsible for creating network interface. The created network interface is applied to network interface card of PCS External interface.



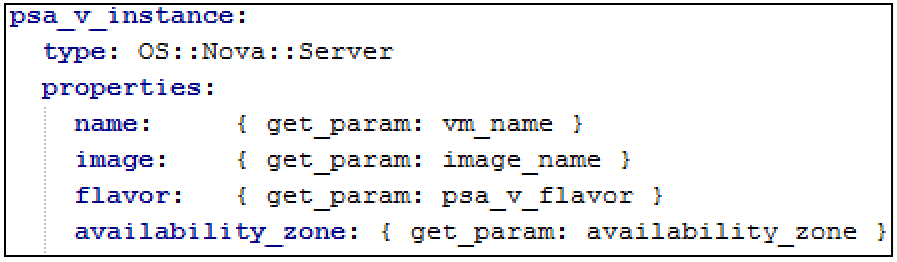
```
psa_v_ext_port:
  type: OS::Neutron::Port
  properties:
    network: { get_param: pcs_ext_network }
```

PSA-V Management Port: This block is responsible for creating network interface. The created network interface is applied to network interface card of PCS Management interface.



```
psa_v_mgmt_port:
  type: OS::Neutron::Port
  properties:
    network: { get_param: pcs_mgmt_network }
```

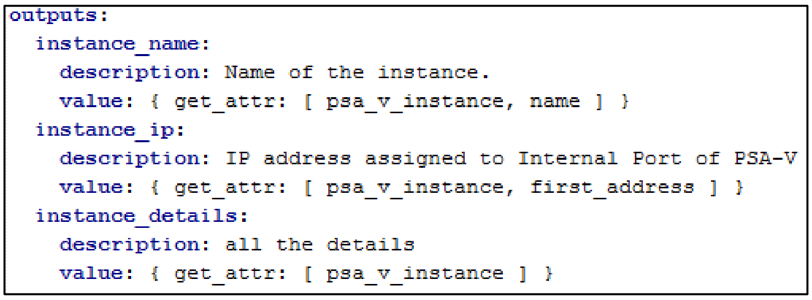
PSA-V Instance: This block is responsible for creating Virtual Machine name, PCS KVM image name, PSA-V flavor and Availability zone. It also gets Heat template file and sets Configuration Drive.



```
psa_v_instance:
  type: OS::Nova::Server
  properties:
    name:      { get_param: vm_name }
    image:     { get_param: image_name }
    flavor:    { get_param: psa_v_flavor }
    availability_zone: { get_param: availability_zone }
```

outputs

The outputs section defines the Instance name, Instance details and IP address assigned to Internal port of PSA-V that is displayed on successful deployment of PCS on OpenStack.



```
outputs:
  instance_name:
    description: Name of the instance.
    value: { get_attr: [ psa_v_instance, name ] }
  instance_ip:
    description: IP address assigned to Internal Port of PSA-V
    value: { get_attr: [ psa_v_instance, first_address ] }
  instance_details:
    description: all the details
    value: { get_attr: [ psa_v_instance ] }
```

References

OpenStack documentation: https://docs.openstack.org/install-guide/overview.html

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, then file a ticket with PSGSC.

- Product warranties—for product warranty information, visit https://www.pulsesecure.net.