Pulse Connect Secure Virtual Appliance on OpenStack Fabric Deployment Guide
Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

https://www.pulsesecure.net

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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.

**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

<table>
<thead>
<tr>
<th>Revision and Date</th>
<th>Added/Updated/Removed</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.1, May 2020</td>
<td>Updated the Limitations section</td>
<td></td>
</tr>
<tr>
<td>1.0, October 2019</td>
<td>None</td>
<td>Initial release</td>
</tr>
</tbody>
</table>
# Table of Contents

- **Revision History** .......................................................... 3
- **Overview** ........................................................................ 5
  - About This Guide .......................................................... 5
  - Assumptions .................................................................... 5
  - Prerequisites and System Requirements ............................ 5
- **Deploying PCS on OpenStack Using Horizon Dashboard** .......................................................... 5
- **Deploying PCS on OpenStack Using Heat** .......................................................... 14
- **PCS Provisioning Parameters** ........................................... 15
- **Limitations** ................................................................. 17
- **Appendix A: Setting Up Prerequisites** .................................. 18
  - Creating Required Flavors of PSA-V .................................. 18
  - Uploading Required Image to OpenStack .......................... 19
  - Creating Snapshot Image ................................................ 20
  - Creating Internal, External and Management Networks on OpenStack .......................................................... 21
  - Creating Required Security Groups for Internal, External and Management Ports .......................................................... 22
    - Creating Rules .......................................................... 22
- **Appendix B: HEAT Template** ............................................. 27
  - parameters ................................................................. 27
  - resources .................................................................... 28
  - outputs .................................................................. 28
- **References** ................................................................. 29
- **Requesting Technical Support** ........................................... 29
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.
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
5. The Source window displays the details of the image used. Click Next.

**Figure 8: Source Selection**

<table>
<thead>
<tr>
<th>Source</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image</td>
<td>Yes</td>
</tr>
<tr>
<td>Volume Size (GB)</td>
<td>40</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Flavor</th>
<th>Allocated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>VCPUS</td>
</tr>
<tr>
<td>psa7k-flavor</td>
<td>8</td>
</tr>
</tbody>
</table>

| Available 5 |
| 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


Figure 5: Network Ports Selection
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](image)

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

![Figure 7: Key Pair](image)
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**

![Configuration Script](image)

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](image)
- The Interface tab shows the networks that are created.

- The Log tab shows the log details of the device that is created.
- The console tab provides the virtual console to view the device coming up.
13. Next, the Internal and External interfaces are configured by DHCP (Zero touch configuration).

**Figure 10: Internal and External Interfaces Configuration by DHCP**

```
Connected (unencrypted) to: QEMU (instance-00000000)

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.

```
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**

```
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>abf35a2c-85e5-4018-a164-fd0f4e2edbb0</td>
</tr>
<tr>
<td>stack_name</td>
<td>smc_pcs_with_config_url_stack</td>
</tr>
<tr>
<td>description</td>
<td>Launch a basic instance with 91r3 KVM image</td>
</tr>
<tr>
<td>creation_time</td>
<td>2019-10-24T06:14:44Z</td>
</tr>
<tr>
<td>updated_time</td>
<td>None</td>
</tr>
<tr>
<td>stack_status</td>
<td>CREATE_IN_PROGRESS</td>
</tr>
<tr>
<td>stack_status_reason</td>
<td>Stack CREATE started</td>
</tr>
</tbody>
</table>

[root@openstack-controller openstack]#
```

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

```xml
<Template xmlns:oe="http://mulee.org/" xmlns:s="http://mulee.org/">
  <Section id="Properties">
    <Properties>
      <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"/>
    </Properties>
  </Section>
</Template>
```

<table>
<thead>
<tr>
<th>#</th>
<th>Parameter Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>vaIPAddress</td>
<td>IP address</td>
<td>Internal interface IP</td>
</tr>
<tr>
<td>2</td>
<td>vaNetmask</td>
<td>IP address</td>
<td>Internal interface subnet mask</td>
</tr>
<tr>
<td>3</td>
<td>vaGateway</td>
<td>IP address</td>
<td>Internal interface IP gateway</td>
</tr>
<tr>
<td>4</td>
<td>vaDefaultVlan</td>
<td>integer</td>
<td>VLAN number to assign to this interface</td>
</tr>
<tr>
<td>5</td>
<td>vaExternalIPAddress</td>
<td>IP address</td>
<td>External interface IP</td>
</tr>
<tr>
<td>6</td>
<td>vaExternalNetmask</td>
<td>IP address</td>
<td>External interface subnet mask</td>
</tr>
<tr>
<td>7</td>
<td>vaExternalGateway</td>
<td>IP address</td>
<td>External interface IP gateway</td>
</tr>
<tr>
<td>8</td>
<td>vaExternalDefaultVlan</td>
<td>Integer</td>
<td>VLAN number to assign to this interface</td>
</tr>
<tr>
<td>#</td>
<td>Parameter Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----</td>
<td>------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9</td>
<td>vaManagementIPAddress</td>
<td>IP address</td>
<td>Management interface IP</td>
</tr>
<tr>
<td>10</td>
<td>vaManagementNetmask</td>
<td>IP address</td>
<td>Management interface subnet mask</td>
</tr>
<tr>
<td>11</td>
<td>vaManagementGateway</td>
<td>IP address</td>
<td>Management interface gateway IP</td>
</tr>
<tr>
<td>12</td>
<td>vaManagementDefaultVlan</td>
<td>Integer</td>
<td>VLAN number to assign to this interface</td>
</tr>
<tr>
<td>13</td>
<td>vaPrimaryDNS</td>
<td>IP address</td>
<td>Primary DNS IP</td>
</tr>
<tr>
<td>14</td>
<td>vaSecondaryDNS</td>
<td>IP address</td>
<td>Secondary DNS IP</td>
</tr>
<tr>
<td>15</td>
<td>vaWINSServer</td>
<td>IP address</td>
<td>Windows server IP</td>
</tr>
<tr>
<td>16</td>
<td>vaDNSDomain</td>
<td>string</td>
<td>Windows domain name</td>
</tr>
<tr>
<td>17</td>
<td>VaAdminUsername</td>
<td>string</td>
<td>Admin username</td>
</tr>
<tr>
<td>18</td>
<td>vaAdminPassword</td>
<td>string</td>
<td>Admin password</td>
</tr>
<tr>
<td>19</td>
<td>vaCommonName</td>
<td>string</td>
<td>Common name</td>
</tr>
<tr>
<td>20</td>
<td>vaOrganization</td>
<td>string</td>
<td>Organization name</td>
</tr>
<tr>
<td>21</td>
<td>vaRandomText</td>
<td>string</td>
<td>Random text to generate self-signed certificate</td>
</tr>
<tr>
<td>22</td>
<td>vaAcceptLicenseAgreement</td>
<td>character</td>
<td>&quot;y&quot; to accept the license agreement</td>
</tr>
<tr>
<td>23</td>
<td>vaEnableLicenseServer</td>
<td>character</td>
<td>&quot;y&quot; to enable it as VLS server. &quot;n&quot; to bring it up as a PCS node.</td>
</tr>
<tr>
<td>24</td>
<td>vaAdminEnableREST</td>
<td>character</td>
<td>&quot;y&quot; to enable REST for administrator user</td>
</tr>
<tr>
<td>25</td>
<td>vaAuthCodeLicense</td>
<td>string</td>
<td>Authentication code that needs to be obtained from Pulse Secure</td>
</tr>
<tr>
<td>26</td>
<td>vaConfigURL</td>
<td>String URL</td>
<td>Http based URL where XML based PCS configuration can be found.</td>
</tr>
<tr>
<td>27</td>
<td>vaConfigServerCACertPEM</td>
<td>string</td>
<td>PEM format of CA certificate.</td>
</tr>
<tr>
<td>28</td>
<td>vaConfigData</td>
<td>string</td>
<td>base64 encoded XML based PCS configuration.</td>
</tr>
<tr>
<td>29</td>
<td>vaInternalPortReconfigWithVAppProperties</td>
<td>integer</td>
<td>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.</td>
</tr>
<tr>
<td>30</td>
<td>vaManagementPortReconfigWithVAppProperties</td>
<td>integer</td>
<td>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.</td>
</tr>
<tr>
<td>31</td>
<td>vaExternalPortReconfigWithVAppProperties</td>
<td>integer</td>
<td>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.</td>
</tr>
</tbody>
</table>

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
- Uploading Required Image to OpenStack
- Creating Snapshot Image
- Creating Internal, External and Management Networks on OpenStack
- Creating Required Security Groups for Internal, External and Management Ports

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.

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

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**

![Create Snapshot button](image)

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

**Figure 15: Create Snapshot dialog box**

![Create Snapshot dialog box](image)
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

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.

**Figure 17: Create Security Group dialog box**

![Create Security Group dialog box](image)

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 page](image)
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

![Security Groups page – Manage Rules](image)

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

Figure 20: Add Rule button

![Add Rule button](image)
3. In the Add Rule window that appears, provide the required configuration details and **Add** the rule.

**Figure 21: Add Rule dialog box**
Follow the same procedure to add rules to External and Management ports.

**Figure 22**: Manage Security Group Rules page – Internal port

**Figure 23**: Manage Security Group Rules page – External port
Figure 24: Manage Security Group Rules page – Management port
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.

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

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

```yaml
image_name:
  type: string
  description: name of image to install
  default: 9lr3_3112_qcow2
  #default: 9lr3_3112_snapshot
```

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

```yaml
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.

```yaml
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.

```yaml
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.

```yaml
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.

```yaml
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.