TREND MICRO™

4.2.0

TippingPoint™ Virtual Threat Protection System (vTPS)

Deployment Guide

Virtual security appliance for threat prevention and network enforcement services in a cloud environment.

Virtual Threat Protection System Deployment Guide

Version 4.2.0

March 2017

Legal and notice information

Legal and notice information

TippingPoint Virtual Threat Protection System Deployment Guide

Contents

About this guide

The Virtual Threat Protection System (vTPS) is a software appliance designed to provide the same level of functionality available from the TippingPoint Threat Protection System (TPS), but virtually rather than physically.

This version of the vTPS supports the majority of features that are included with the corresponding version of physical TPS devices. This guide describes the configuration differences and other special considerations for deploying a TPS in a virtual environment.

This section covers the following topics:

Target audience

This guide is intended for security network administrators and specialists who are responsible for monitoring, managing, and improving system security. The audience for this material is expected to be familiar with the TippingPoint security systems and associated devices.

Users should be familiar with the following concepts:

- Basic networking
- Network security
- Routing

Related documentation

A complete set of documentation for this product is available online at the Threat Management Center (TMC): *https://tmc.tippingpoint.com*. The product document set generally includes conceptual and deployment information, installation and user guides, CLI command references, safety and compliance information, and release notes.

Conventions

This information uses the following conventions.

Typefaces

TippingPoint uses the following typographic conventions for structuring information.

Convention	Element
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes. Example: Click **OK** to accept.
Italics font	Text emphasis, important terms, variables, and publication titles
`Monospace font`	• File and directory names • System output • Code • Text typed at the command-line
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of file and directory names, system output, code, and text typed at the command line

Messages

Messages are special text that is emphasized by font, format, and icons.

Warning! Alerts you to potential danger of bodily harm or other potential harmful consequences.

Caution: Provides information to help minimize risk, for example, when a failure to follow directions could result in damage to equipment or loss of data.

Note: Provides additional information to explain a concept or complete a task.

Important: Provides significant information or specific instructions.

Tip: Provides helpful hints and shortcuts, such as suggestions about how to perform a task more easily or more efficiently.

Product support

Get support for your product by using any of the following options:

Email support

tippingpoint.support@trendmicro.com

Phone support

North America: +1 866 681 8324

International: See *https://tmc.tippingpoint.com*

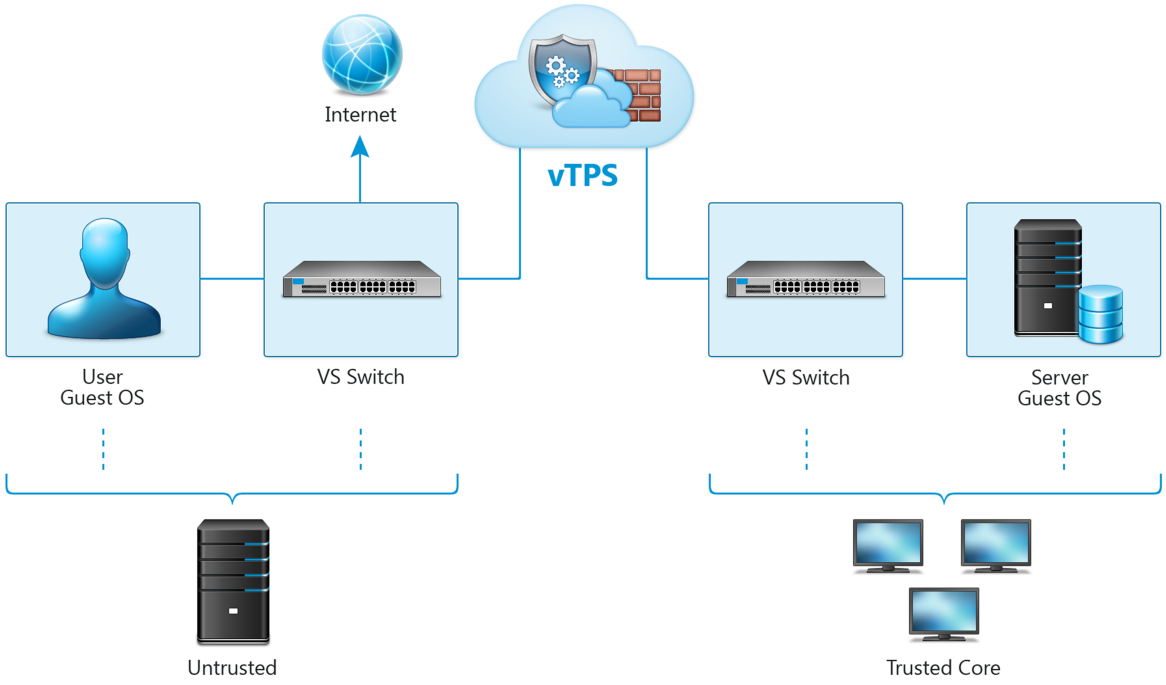
Deployment overview

This guide provides configuration steps to deploy a TippingPoint Virtual Threat Protection System (vTPS) in either a VMware or kernel-based virtual machine (KVM) environment. The vTPS is a software appliance designed to give you the same level of functionality available in the TippingPoint TPS, but virtually rather than physically. Just as with a TPS device, the vTPS protects your network with the Threat Suppression Engine (TSE) by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings you maintain on the vTPS. You can share the same policies across virtual and physical deployments, and you can centralize the management of your deployments with a Security Management System (SMS).

The few differences between vTPS and TPS functionality—for example, command line interface (CLI) operations that control hardware LEDs, and other functions specific to a physical device—are listed and described in the *vTPS Functional Differences Addendum*.

The following illustration shows an example of a basic hypothetical deployment. This version of the vTPS must be configured between L2 broadcast domains (VLANs or switches).

Figure 1. Basic vTPS deployment



After you deploy the vTPS, you can access the appliance by using the Local Security Manager (LSM) web interface or your SMS. For more information, see the TPS product documentation on the TMC (*https://tmc.tippingpoint.com*).

Obtain the vTPS Software License Key

After your product purchase order is received, TippingPoint supplies information on how to receive your Software License Key.

The vTPS Software License Key is provided as a text file.

Note: You can deploy your vTPS device in Trial Mode before you receive your Software License Key. Trial Mode is primarily exploratory and comes with a limited number of security filters in the Digital Vaccine (DV) package. In this mode, an SMS can manage only one vTPS at a time. Because Trial Mode has a fixed serial number and entitlement, you cannot use Trial Mode to perform TippingPoint Operating System (TOS) upgrades or distribute DVs.

After you receive the license key, save the key to a storage location that is accessible from your virtual environment. You will use the Software License Key to upgrade your vTPS from Trial Mode to Standard Mode. See *Upgrade from vTPS Trial to vTPS Standard* on page 35.

Install and configure the vTPS

This topic provides steps to configure your vTPS. This release supports the following configuration options:

For more information on configuring security policy for your virtual appliance, refer to your SMS and LSM documentation on the TMC (*https://tmc.tippingpoint.com*).

General requirements

To deploy a vTPS in any software environment, the following system specifications are required:

- **Memory (RAM)**—8 GB
- **Number of cores**—vTPS supports configurations of either two cores (meets general performance requirements) or three cores (for enhanced performance; upgrading to three cores after installation requires a shutdown, configuration change, and reboot)
- **Disk space**—16.2 GB

  Note: Both thin and thick provisioning are supported, but for optimum performance, use thick provisioning.

- **CPU**—Host CPU must support the SSSE3 instruction set. Tested CPU configurations:
  - Intel Xeon CPU E5-2697v2
  - Intel Xeon CPU E5-2690
  - Intel Xeon CPU E5-2683v3
  - Intel Xeon CPU X5670
  - Intel Xeon CPU X5650

Install and deploy vTPS by using VMware ESXi

This topic provides steps to configure the vTPS for startup by using the vCenter application. The information includes:

VMware ESXi requirements

The vTPS supports the following system and software environment for a VMware ESXi deployment:

- **Hypervisor version**: ESXi version 5.5 (Update-1) or 6.0

  Note: Install all updates on your hypervisor hosts before deploying virtual devices in your ESXi environment.

- **Networking requirements**:
  - Three vNICs — one for management and two for data. Both vSwitches and distributed vSwitches (dvSwitches) are supported.
  - The two data vNICs must be configured in promiscuous mode. Ensure that any Forged Transmits and MAC Address Changes are set to ACCEPT in order for network packets to get forwarded.

Configure the vTPS on VMware

To configure vTPS on VMware:

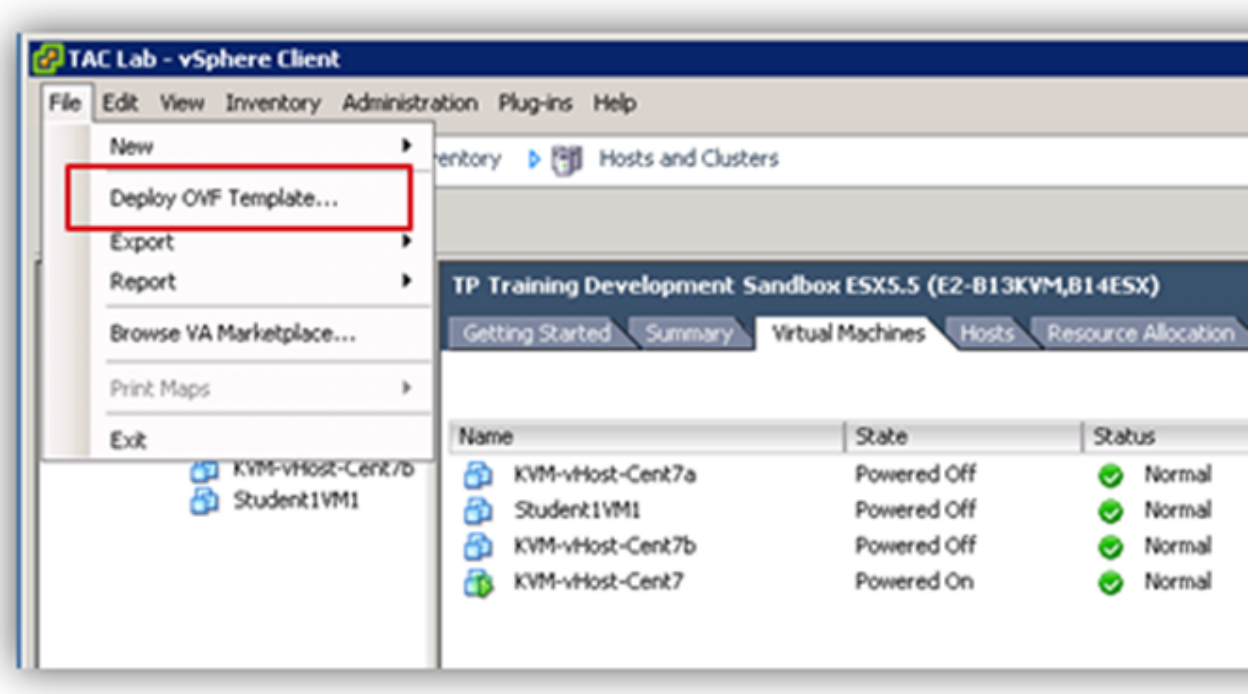
1. Create three vNICs on the ESXi host—one for the management port and two for the data ports.

   See the VMware content at the *VMware vSphere Documentation Center*.

   Note: In order for the vTPS to function properly, be sure you create the ports, map them to their correct interfaces, and enable them in promiscuous mode. By default, ESXi attempts to attach all the adapters to the virtual switch that was created first. Ensure that any Forged Transmits and MAC Address Changes are set to ACCEPT for network packets to get forwarded. You must configure the VLAN ID field to All(4095) for data port virtual switches if you intend to use VLANs for data ports.

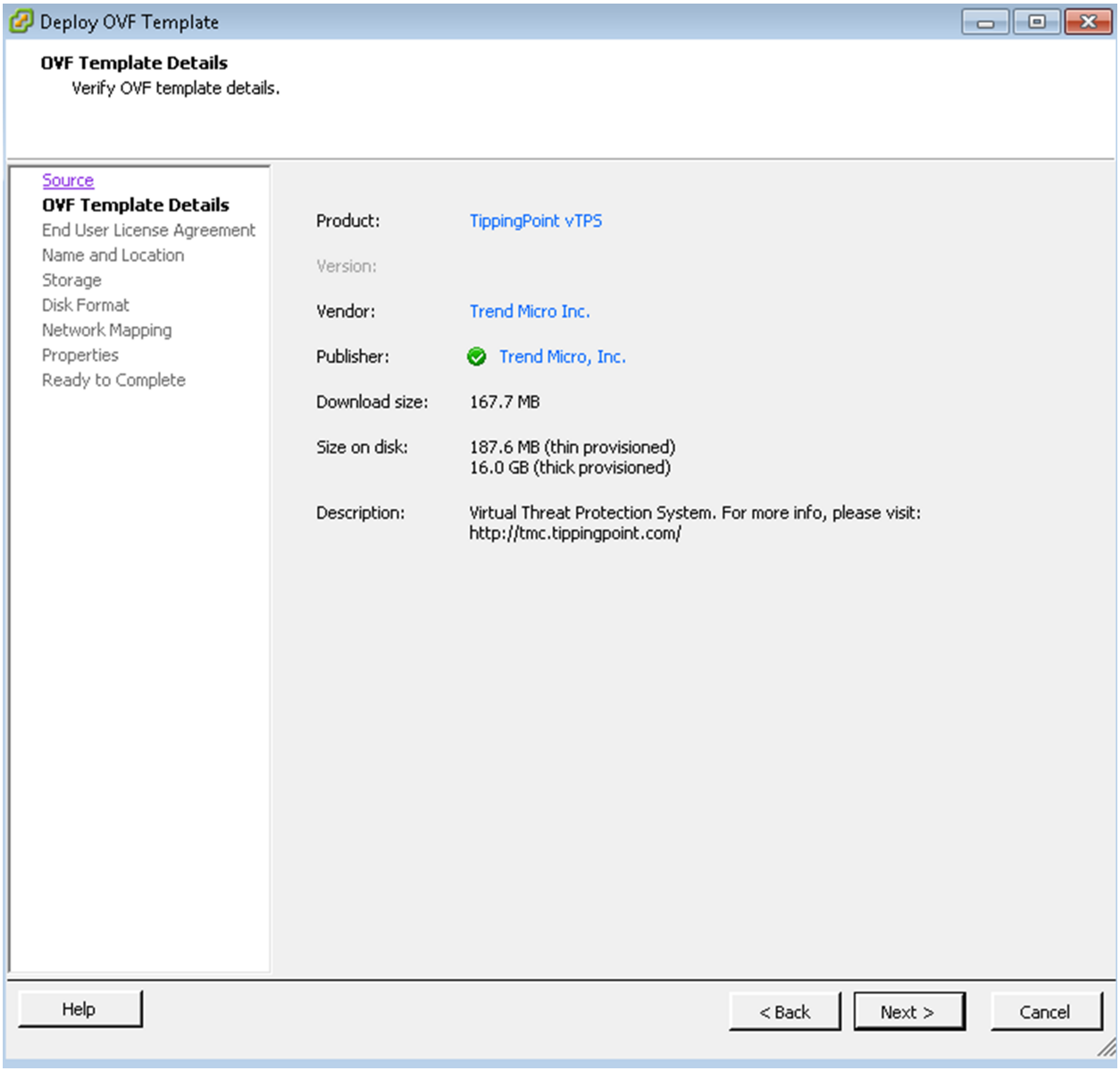
2. Copy the vTPS OVA package to your system.
3. From vSphere, open the package and launch the **Deploy OVF Template** wizard.

Figure 2. Deploy OVF Template wizard



The initial OVF Template Details screen of the wizard displays information that includes the product name, version, vendor, and publisher. Ensure that the publisher information is correct before proceeding further. When you are satisfied you have opened the correct package, click **Next**.

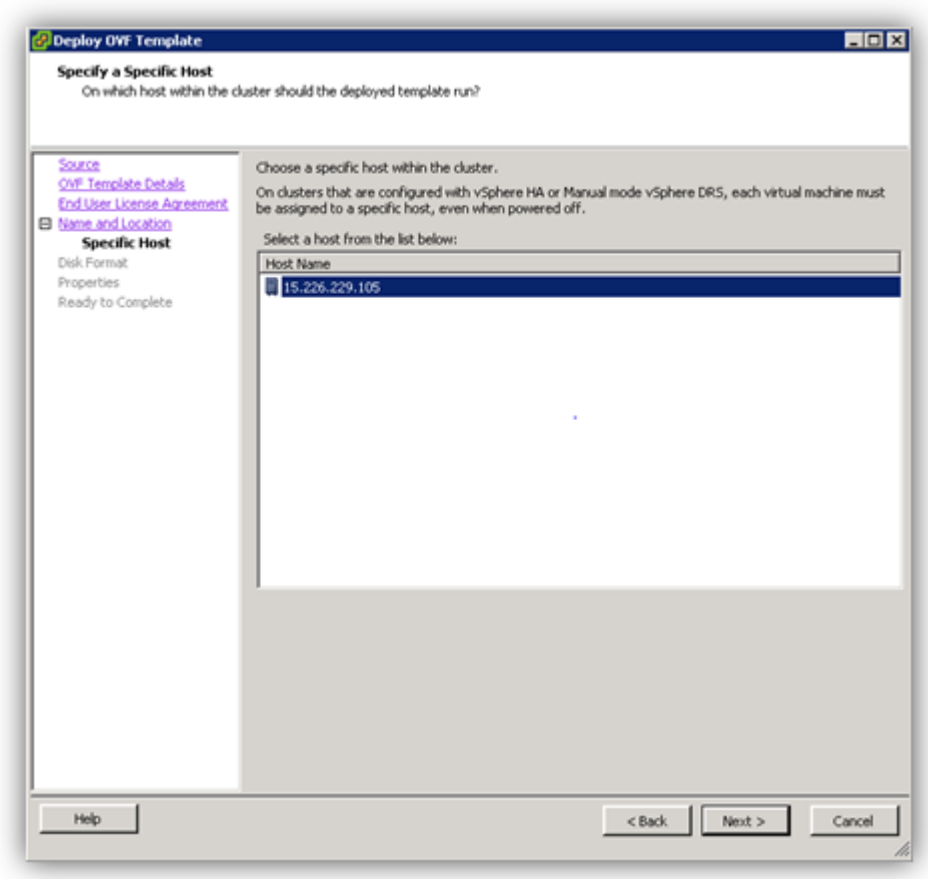
Figure 3. Deploy OVF Template wizard Details screen



4. Click **Accept** to accept the End User License Agreement (EULA), and then click **Next**.
5. On the Name and Location screen, you can rename and choose a specific install location for the VM instance, or you can accept the default name and location.

   Click **Next**.
6. Select the host that you want on the Host / Cluster screen, and then click **Next**.

Figure 4. Assign a host



7. Select a storage location if you are prompted. Consider also assigning a dedicated resource group for a vTPS instance.
8. On the Disk Format screen, you can select the format in which to store the virtual disks. Select your preference and click **Next** to continue.

   Note: Both thin and thick provisioning is supported. For optimum performance, use thick provisioning.

9. On the Network Mapping screen, configure the three network options.

   The first interface you provide is your management port. Ensure that this is accessible on your management network. Then select networks for the two data ports according to your virtual switch/port configuration. Click **Next**.

   Important: Ensure that you correctly map your network adapters so that you can access your vTPS device by using the LSM, CLI, and SMS.

10. If you are using a vSphere client to deploy directly on a host, you can configure the vTPS parameters only after the vTPS is booted using the out-of-box experience (OBE) interface on the console. If you are using a vCenter server to deploy, you are prompted by the Properties screen to configure the parameter values:

- IP address
- Netmask value
- Default Gateway
- IPv6 Address (optional)
- IPv6 Prefix Length (optional)
- IPv6 Default Gateway (optional)
- Hostname (required)
- Host location (optional)
- IP address of DNS servers (optional)—You can add up to two addresses

  Note: The VMware deployment screen supports setting up only an IPv4 IP address. If you want to set up an IPv6 address, you must first install the vTPS with IPv4 by using the OBE interface on the console. Configure an IPv6 address after the device is booted.

- DNS Domain Name (optional)
- Security Level
- Username—The SuperUser user name
- Password for the SuperUser
- Console—Default and recommended value is `vga`; if you specify `serial` as the console, refer to *Configuring a serial console* on page 39 to configure it

  Note: The vTPS supports only one console type. After you initially select the console type, you would have to redeploy the vTPS to change the console type.

- SSH Public Key for the superuser account (this field is optional)
- Certificate URL (optional)—Your vTPS attempts to get the file from the URL and install the device certificate to convert the vTPS from Trial Mode to Standard Mode; you can complete this task another time, if needed, by using the SMS or LSM

When you have entered values for all the properties, click **Next**.

Note: Any properties that you do not assign a value to remain unassigned. You must supply values to all the preceding properties before powering on. Refer to your VMware technical documentation for appropriate values.

11. Verify that all the properties have been correctly set for your deployment in the Ready to Complete screen.
12. Click **Finish**.

Your deployment progress is displayed.

Start your vTPS

Follow these steps to complete the initial deployment:

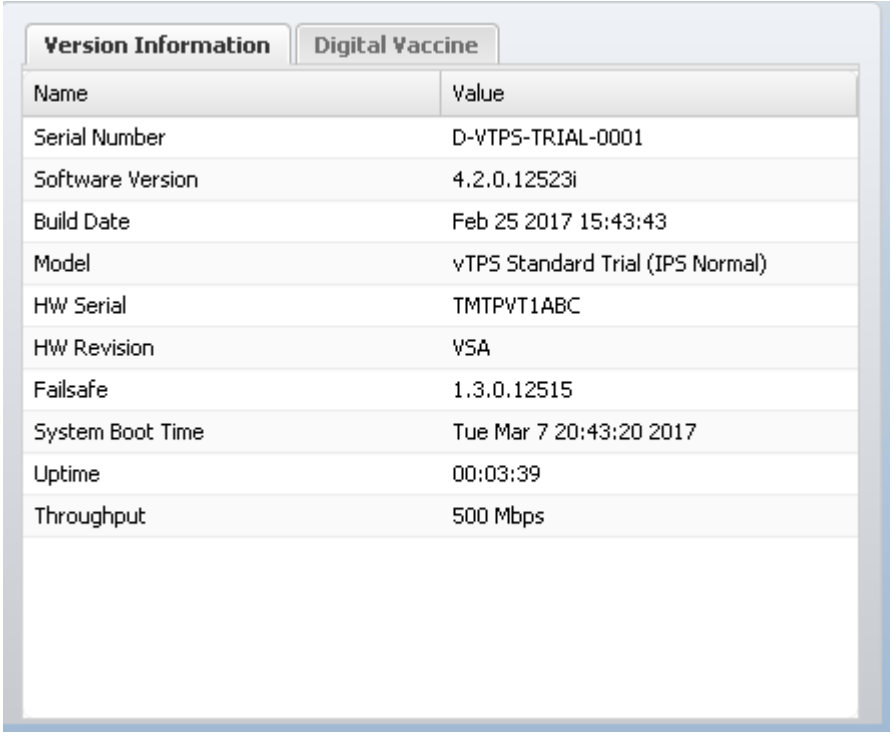
1. In vCenter, right-click your new VM and select **Power > Power on** from the menu.
2. If you did not use vCenter to provide network settings, you can access the vCenter VGA console for the vTPS to configure those settings.

If you did not use vCenter to provide license key information in the preceding step, the vTPS boots in Trial Mode by default. *Figure 5* on page 12 indicates from the CLI that you are in Trial Mode. *Figure 6* on page 13 indicates from the LSM that you are in Trial Mode.

Figure 5. Trial Mode – CLI

```
dev12523{}sho ver
              Serial: D-VTPS-TRIAL-0001
            Software: 4.2.0.12523i Build Date: "Feb 25 2017 15:43:43" Production
     Digital Vaccine: 4.0.0.1000
       Reputation DV: N/A
               Model: vTPS Standard Trial (IPS Normal)
          HW Serial: TMTPVT1ABC
        HW Revision: VSA
           Failsafe: 1.3.0.12515
         Throughput: 500 Mbps
    System Boot Time: Tue Mar  7 20:43:20 2017
              Uptime: 00:02:40
```

Figure 6. Trial Mode – LSM



Upgrade to Standard Mode

After you deploy your vTPS device, upgrade to Standard Mode. For information, see *Upgrade from vTPS Trial to vTPS Standard* on page 35.

Install and deploy vTPS by using KVM

This topic provides steps to configure the vTPS for startup by using a kernel-based virtual machine (KVM). The information includes:

KVM requirements

A KVM deployment of the vTPS that uses the following specifications has been verified:

- **Software environments**—Ensure you have the following minimum requirements:

  Note: vTPS installation has been verified with RHEL version 7.1 KVM hosts. A three-core configuration requires the following minimum software package versions:

  - libvirt version 1.1.0
  - Quick Emulator (QEMU) version 1.5.3
  - virt-install version 1.1.0

- **Networking requirements**—Three bridge interfaces — one for management and two for data.
- **Console access**— Default and recommended console is a graphical UI, such as virt-manager, virt-viewer, vncviewer, or other VNC client. To configure the serial console, refer to *Configuring a serial console* on page 39.

  Note: The vTPS supports only one console type. After you initially select the console type, you cannot change it later.

Obtain software licensing and certificates

For information, see *Upgrade from vTPS Trial to vTPS Standard* on page 35.

Deploy the vTPS on KVM

To install vTPS on KVM:

1. Copy the vTPS tar package to your system.
2. Extract the package with the `tar --sparse -zxvf VCloudSecure_kvm_4.2.0_12523.tar.gz` command.
3. Change permissions for the QEMU user to allow access to the file with the `chmod` command: `chmod a +rwx system_disk.raw`
4. Use the `virt-install` command to deploy the vTPS package according to your RHEL version:
   - To deploy vTPS on RHEL version 7. 1 in the libvirt 1.1.0 environment, use the virt-install command as follows.

     Note: RHEL 7.1 deployment supports two options: 1 fast path or 2 fast paths. To configure one fast path, specify cores=2 and `driver_queues=1`. For 2 fast paths, specify cores=3 and `driver_queues=2`.

     ```
     virt-install \
     --name=<name of your VM> --ram=<specify ram size{for 8GB specify 8192}>
     --vcpus sockets=1,cores=3 \
     --boot hd --disk path=<path of your system_disk.raw file>
     --network bridge=<management bridge>,model=e1000 \
     --network bridge=<data bridge 1>,model=virtio,driver_queues=2 \
     ```

```
--network bridge=<data bridge 2>,model=virtio,driver_queues=2 \
--graphics vnc,port=59<xy>,listen=<ip_of_kvm_host> \
--virt-type=kvm --cpu qemu64,+ssse3,-svm \
--force --wait -1
```

Note: The `--wait` option keeps your program running on the shell. After you have installed the vTPS Software License Key and the vTPS is running, you can type Control-C to return to the prompt.

The preceding commands create a vTPS VM with the name <name of your VM>. To manage or access the VM, you can use the `virsh` CLI.

To access the open console of the VM, use `vncviwer` or `virt-viewer` after setting the DISPLAY environment variable as follows:

`vncviewer <ip_of_kvm_host>:59<xy>` (the <port value> you supplied for the `graphics` field of the `virt-install` command)

or

```
virt-viewer --connect qemu+ssh://root@ip_of_kvm_host/system
$VM_NAME
```

The vTPS deployment is complete.

Automating vTPS installation on KVM

1. Install `genisoimage` with the `yum install genisoimage` command on an RHEL system.
2. Copy the vTPS tar package to your system.
3. Extract the package with the `tar --sparse -zxvf VCloudSecure_kvm_4.2.0_12523.tar.gz` command.
4. To configure the vTPS parameters from the KVM command line, create a text file named `vtps-env.txt` **(Note: the file *must* be named this)** with this format:

```
com_tippingpoint_IP = <Management IP address of vTPS>
com_tippingpoint_Netmask = <Subnet Mask>
com_tippingpoint_Gateway = <IP Address of Gateway>
com_tippingpoint_Username = <username>
com_tippingpoint_Password = <Password>
com_tippingpoint_DNS = <IP Address of DNS>
com_tippingpoint_DNS2 = <IP Address of DNS2> (optional)
com_tippingpoint_Security_Level = <none/maximum/basic>
com_tippingpoint_VSSH_Public_Key = SSH KEY (optional)
com_tippingpoint_Cert_URL = <Device Certificate URL> (optional)
com_tippingpoint_Console = serial  (optional; for serial consoles only)
```

For example, your file might look like the following sample:

```
com_tippingpoint_IP = 10.11.12.134
com_tippingpoint_Netmask = 255.255.255.0
```

```
com_tippingpoint_Gateway = 10.11.12.1
com_tippingpoint_Username = superuser
com_tippingpoint_Password = password
com_tippingpoint_DNS = 15.16.17.18
com_tippingpoint_DNS2 = 0.0.0.0
com_tippingpoint_Security_Level = None
com_tippingpoint_VSSH_Public_Key = SSH KEY
com_tippingpoint_Cert_URL = http://15.16.17.18/certificate.txt
```

5. From the KVM command line, generate an ISO image of the `vtps-env.txt` file with the `genisoimage -r -o vtps_test_metadata.iso vtps-env.txt` command. Executing this command generates the following output:

```
root@vtps-kvm06:/# genisoimage -r -o vtps_test_metadata.iso vtps-env.txt
I: -input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 252
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 0
176 extents written (0 MB)
root@vtps-kvm06:/#
```

Note: The exact output varies depending on the input to the `vtps-env.txt` file.

6. Change permissions for the QEMU user to allow access to the file with the `chmod` command: `chmod a +rwx system_disk.raw`

```
chmod a+rwx vtps_test_metadata.iso
```

7. Set the following environment variables to the displayed values:
   - `VM_NAME=$VM_NAME`
   - `RAM_SIZE=8192 #8388608 #8GB : 1GB = 1048576`
   - `SYSTEM_DISK_PATH=<location of the image files>/system_disk.raw`
   - `CDROM_IMAGE=<location of the iso file>/vtps_test_metadata.iso`
8. Use the `virt-install` command to deploy the vTPS package according to your RHEL version:
   - If you are using RHEL version 7.1, attach the generated ISO image (as if it were a CD-ROM) and the bootloader, and deploy the vTPS package in the libvirt 1.1.0 environment with the `virt-install` command.

     Note: RHEL 7.1 deployment supports two options: 1 fast path or 2 fast paths. To configure one fast path, specify cores=2 and `driver_queues=1`. For 2 fast paths, specify cores=3 and `driver_queues=2`.

```
virt-install \
--name=$VM_NAME --ram=$RAM_SIZE --vcpus sockets=1,cores=3 \
```

```
--boot hd --disk path=$SYSTEM_DISK_PATH
--cdrom=$CDROM_IMAGE \
--network bridge=<management bridge>,model=e1000 \
--network bridge=<data bridge 1>,model=virtio,driver_queues=2 \
--network bridge=<data bridge 2>,model=virtio,driver_queues=2 \
--graphics vnc,port=59<xy>,listen=<ip_of_kvm_host> \
--virt-type=kvm --cpu qemu64,+ssse3,-svm \
--force --wait -1
```

Note: The `--wait` option keeps your program running on the shell. After you have installed the vTPS Software License Key and the vTPS is running, you can type Control-C to return to the prompt.

The preceding commands create a vTPS VM with the name <name of your VM>. To manage or access the VM, you can use the `virsh` CLI.

To access the open console of the VM, use `vncviwer` or `virt-viewer` after setting the DISPLAY environment variable as follows:

`vncviewer <ip_of_kvm_host>:59<xy>` (the <port value> you supplied for the `graphics` field of the `virt-install` command)

or

```
virt-viewer --connect qemu+ssh://root@ip_of_kvm_host/system
$VM_NAME
```

The vTPS deployment is complete.

Upgrade to Standard Mode

After you deploy your vTPS device, upgrade to Standard Mode. For information, see *Upgrade from vTPS Trial to vTPS Standard* on page 35.

Install and deploy by using OpenStack HEAT template for vTPS

A HEAT template can be used to describe the vTPS infrastructure.

Note: The instructions in this section describe a GUI deployment of a TippingPoint vTPS that uses the OpenStack Liberty release. If you use a different release or customization of OpenStack components, you might see small variations in the procedure.

vTPS emulation requirements

The OpenStack HEAT template requires the following emulation configuration:

1. Processor emulator – ssse3 eabled
2. Disk driver – ide

3. Support for virtio on all three interfaces (management port and two data ports)

vTPS functional requirements

The OpenStack HEAT template requires the following functional configuration:

1. Hypervisor – kvm
2. Virtual processors – 2 or 3
3. RAM – 8GB
4. Disk image – 1 (system disk required, 16GB total size)
5. Configuration drive – optional

Deploy the TippingPoint vTPS on OpenStack

To prepare for deployment:

- Ensure the Qemu processor type has the ssse3 flag enabled. To enable the flag in compute mode, edit the `nova.conf` file.
- Add the following lines to the [libvirt] section of the `/etc/nova/nova.conf` or `/etc/nova/nova-compute.conf` file:

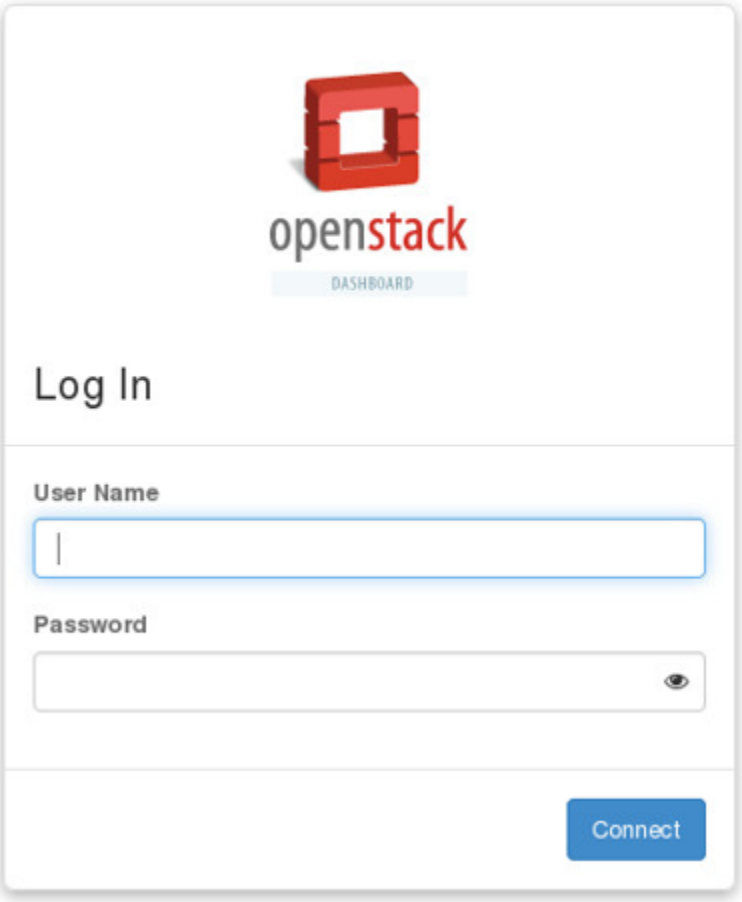
```
[libvirt]
virt_type = kvm
cpu_mode = passthrough
disk_prefix = hd
```

- After saving your modifications, restart any of the following available nova services that run on your server:
  - openstack-nova-api
  - openstack-nova-cert
  - openstack-nova-consoleauth
  - openstack-nova-scheduler
  - openstack-nova-conductor
  - openstack-nova-novncproxy

Enter the context of your task here (optional).

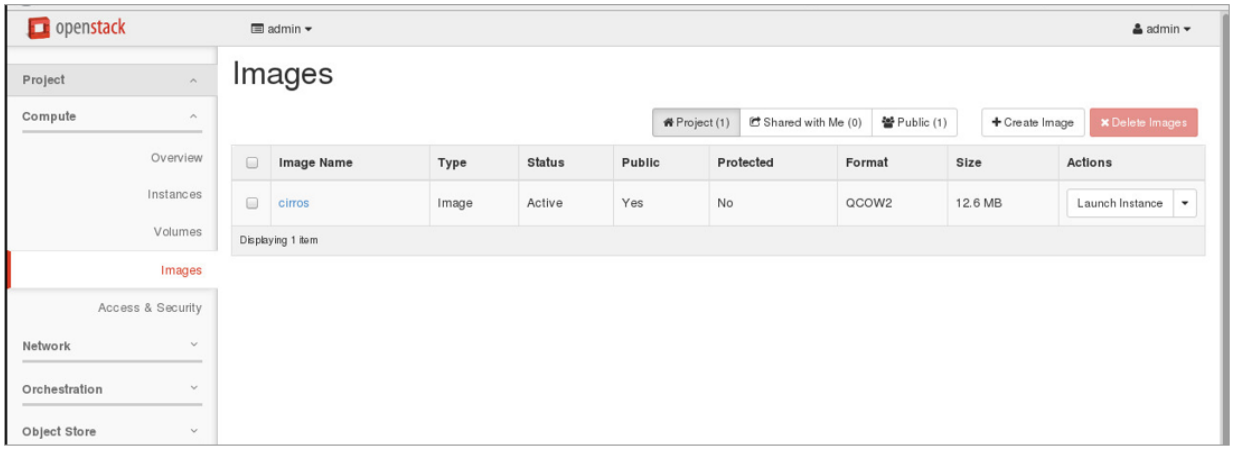
1. Log in to the OpenStack GUI (Horizon).

Figure 7. OpenStack Log In screen



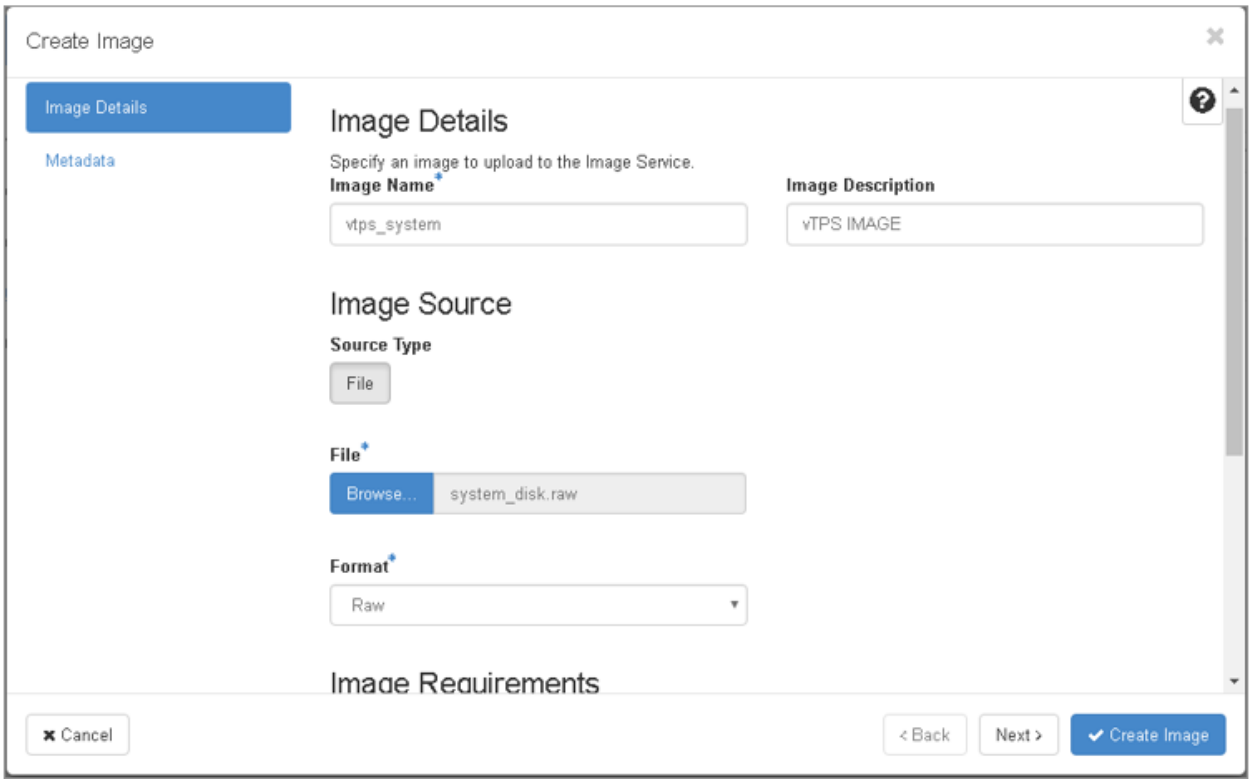
2. Add vTPS images to Horizon.
   a. To place raw system and user vTPS images in an accessible location, upload them by selecting **Compute > Images** and then clicking the **Create Image** button.

      Figure 8. Compute images screen



b. In the Create Image screen, fill in the details for the system disk and select the vTPS system disk image.

Figure 9. Create Image details screen



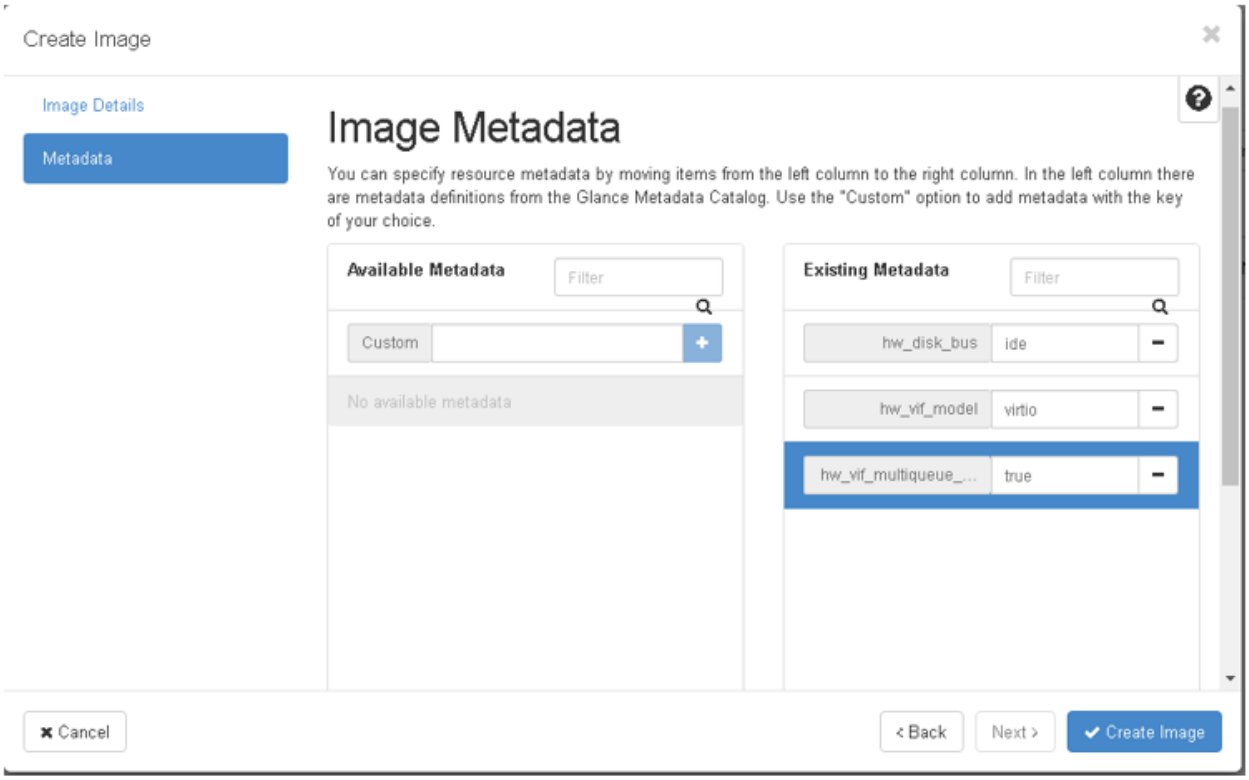
c. Click the **Create Image** button.

d. Click **Metadata** to update the image metadata.

To update the Existing Metadata for the system disk, type `hw_disk_bus` in the **Custom** field of the Available Metadata column and then click on the **+** button to add the value to the Existing

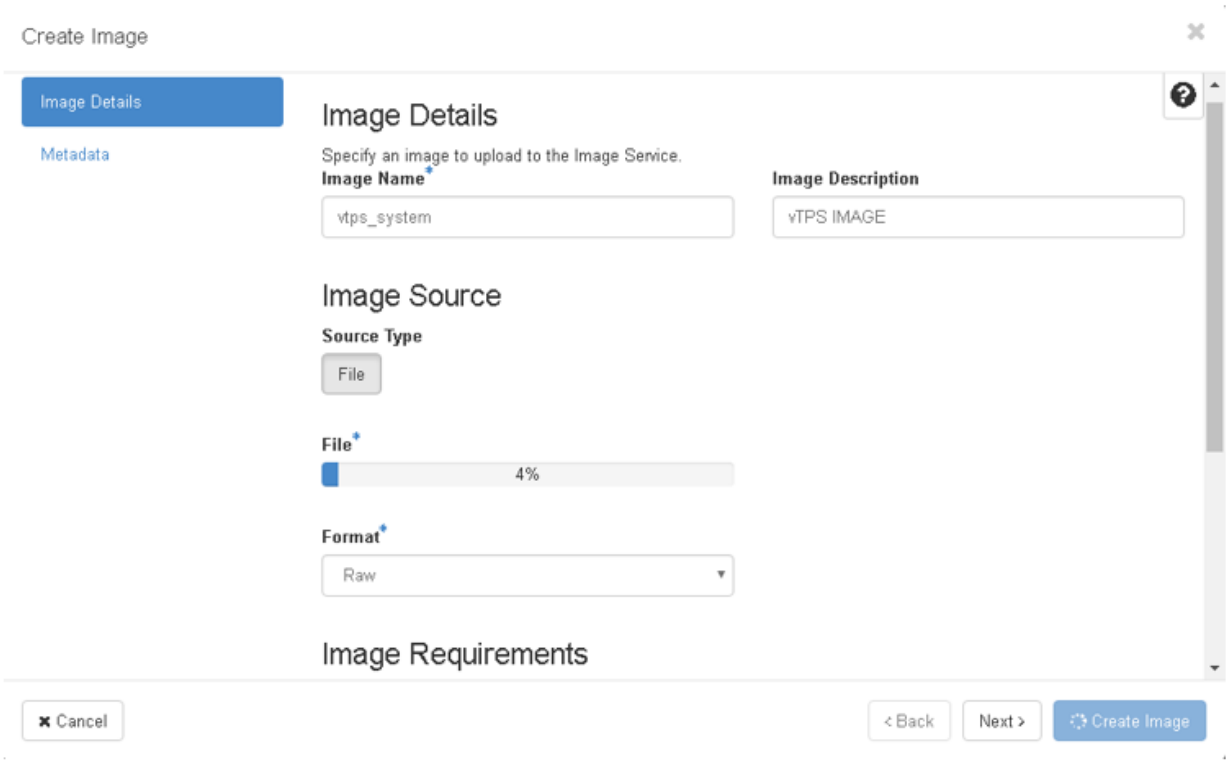
Metadata column. Repeat this step to add virtio as the `hw_vif_model` value and `true` for the `hw_vif_multiqueue` value (required for a 3-core image). Click **Create Image**.

Figure 10. Image Metadata screen



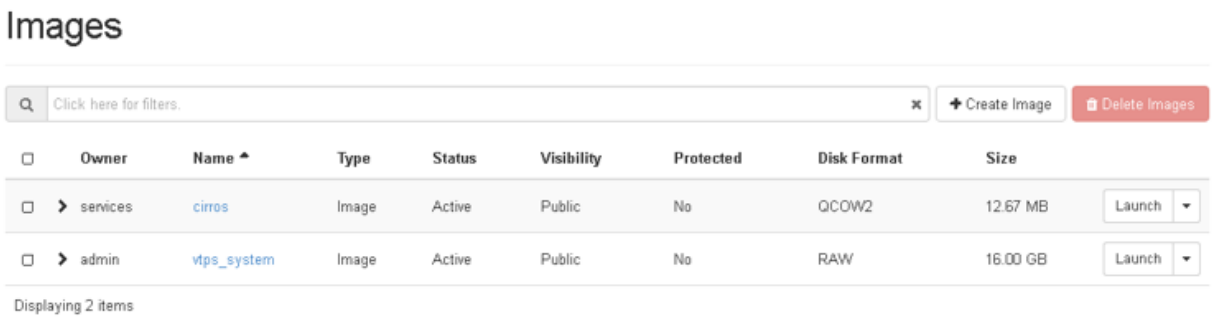
e. As the image uploads, you can monitor the status.

Figure 11. Image uploading status



After the images are added, you can view them by selecting **Compute > Images**.

Figure 12. Compute Images screen showing uploaded images



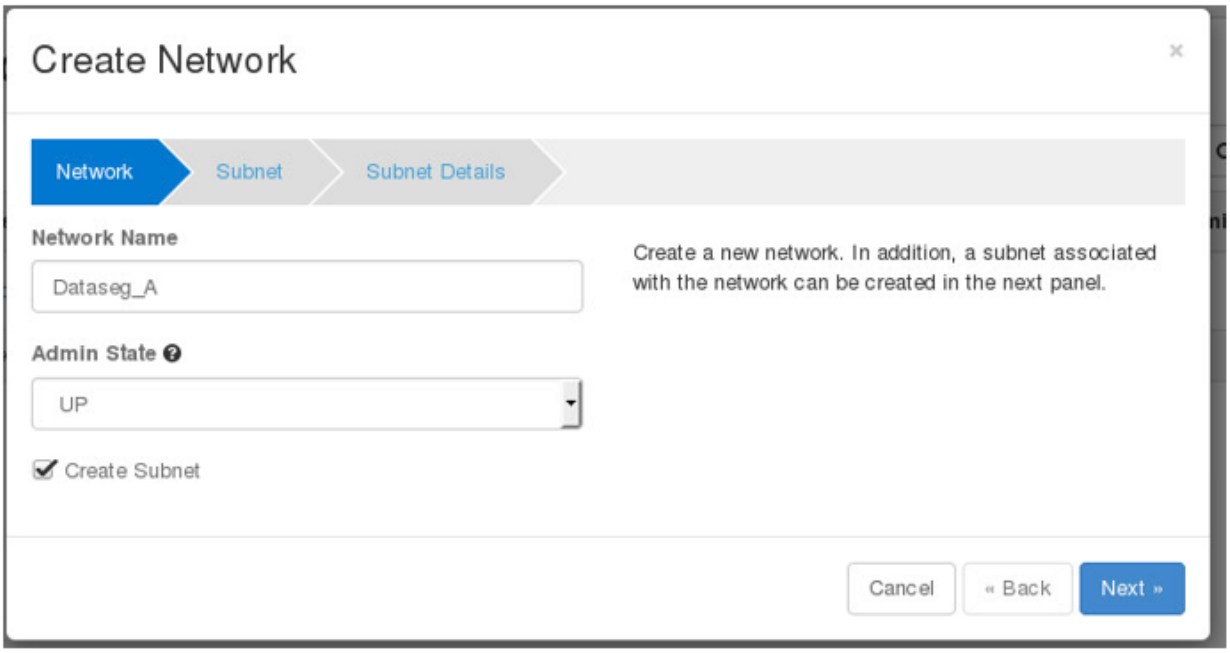
3. Select **Network > Networks** and click **Create Network** to create two data networks for data traffic.

Note: The public subnet for the management network should already exist.

Figure 13. Networks screen

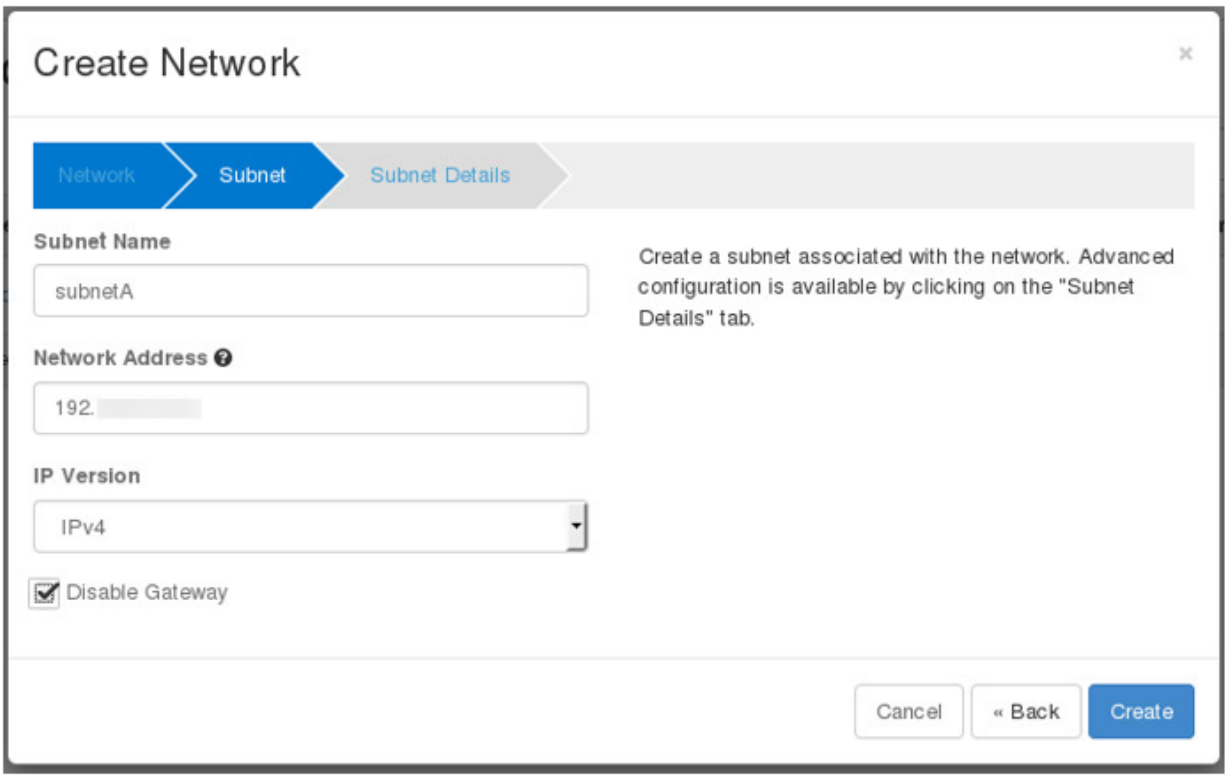
a. In the Create Network dialog, provide the details for the first network data port and click **Next**.

Figure 14. Create Network screen



Provide details of the first network data port's subnet and click **Create**.

Figure 15. Create Network Subnet screen



b. Repeat the preceding substeps accordingly to specify details for the second data port and subnet.

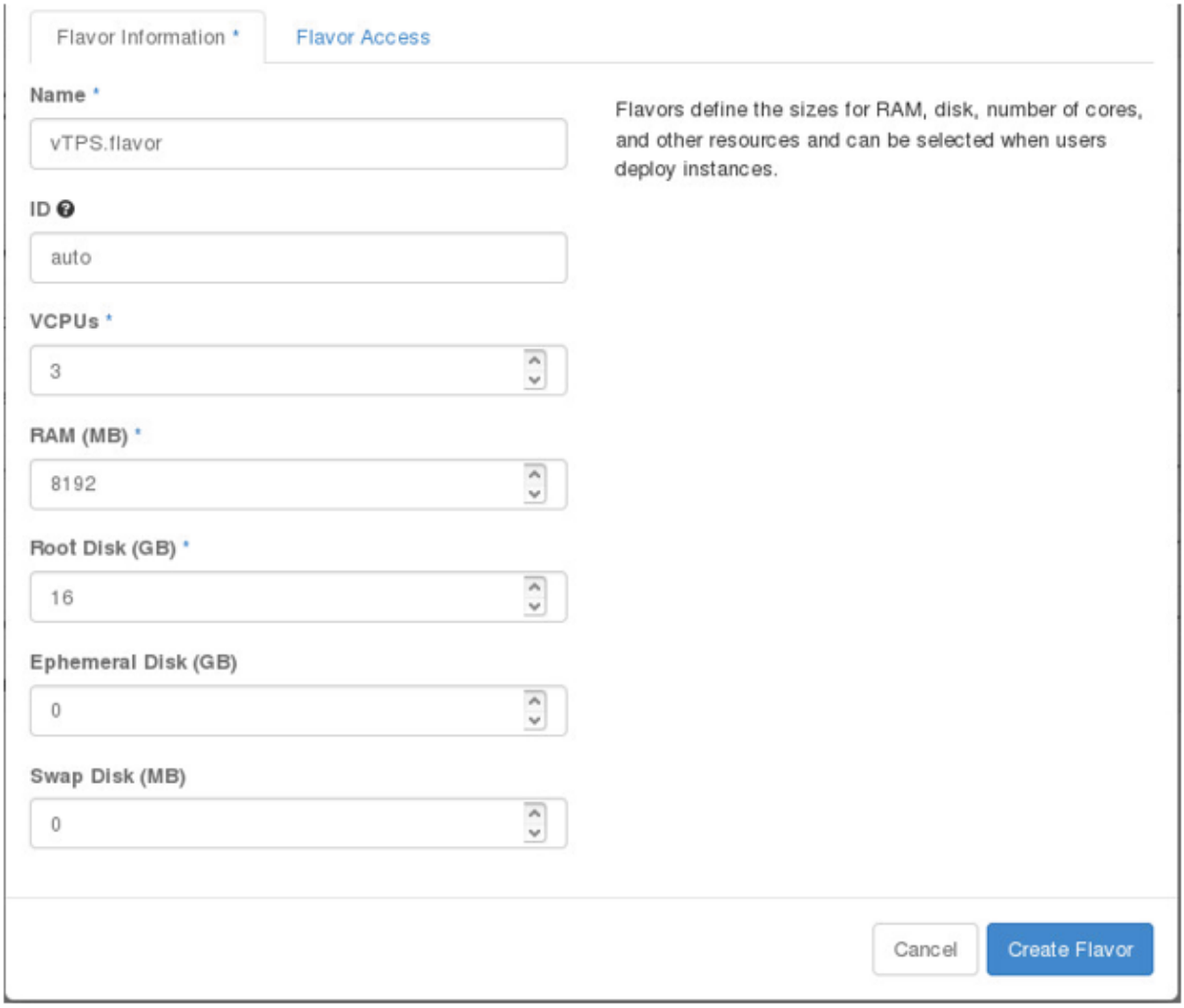
c. You can view the created networks by clicking **Network > Networks**.

Figure 16. Networks screen

4. Select **Admin > System > Flavors** to create a vTPS flavor.

a. In the Flavor Information tab of the Create Flavor dialog, specify the details for the flavor.

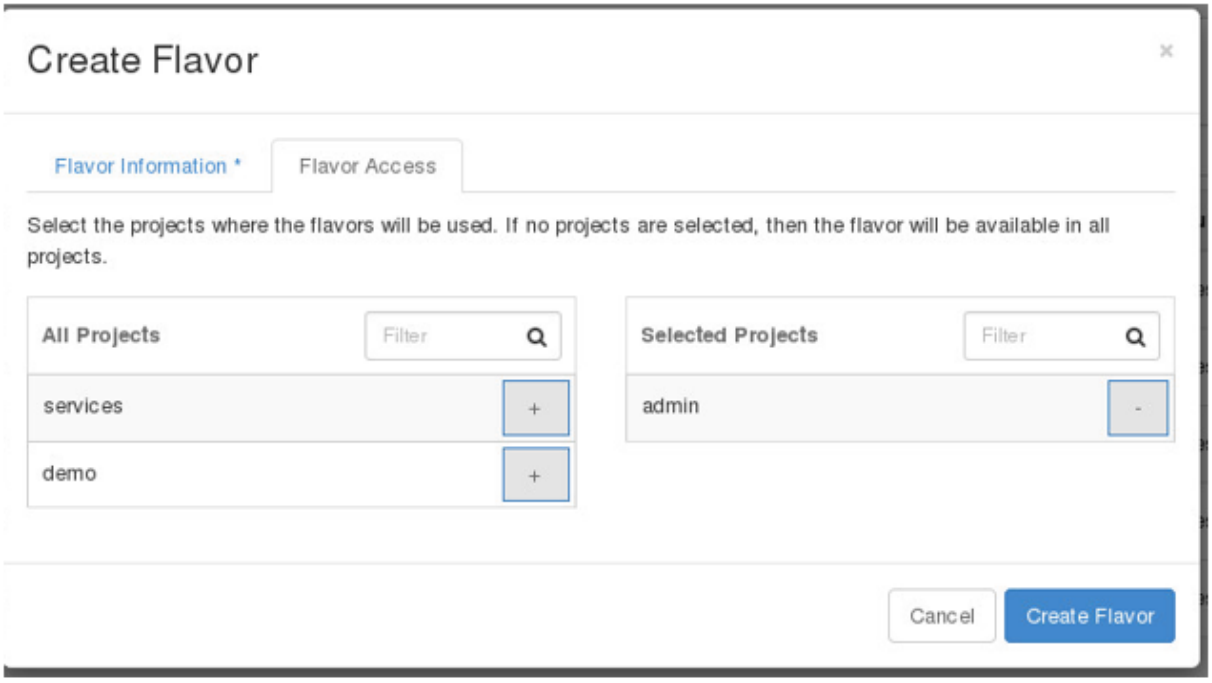
Figure 17. Flavor Information screen



b. In the Flavor Access tab of the Create Flavor dialog, specify the access privileges for the flavor according to the needs of your project.

   For example, the following configuration provides the admin project access to the flavor.

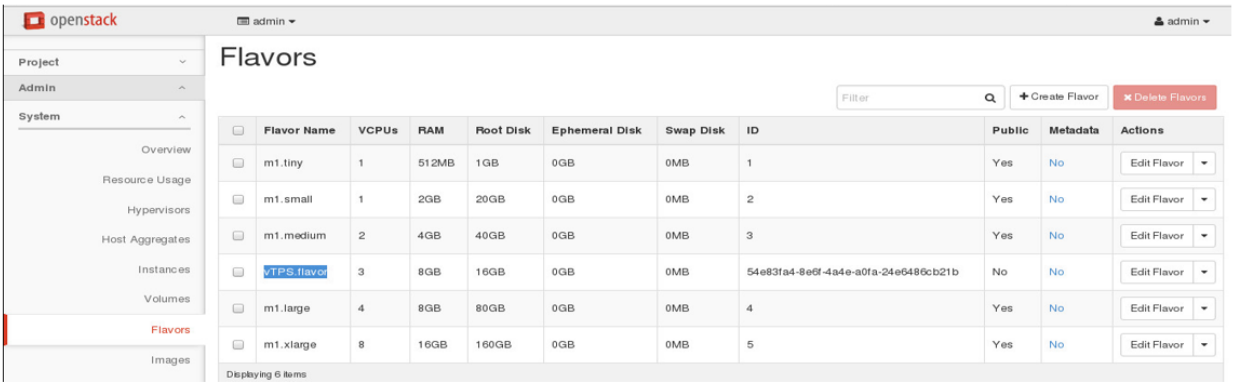
   Figure 18. Flavor configuration example



c. After you specify all details of the flavor, click **Create Flavor**.

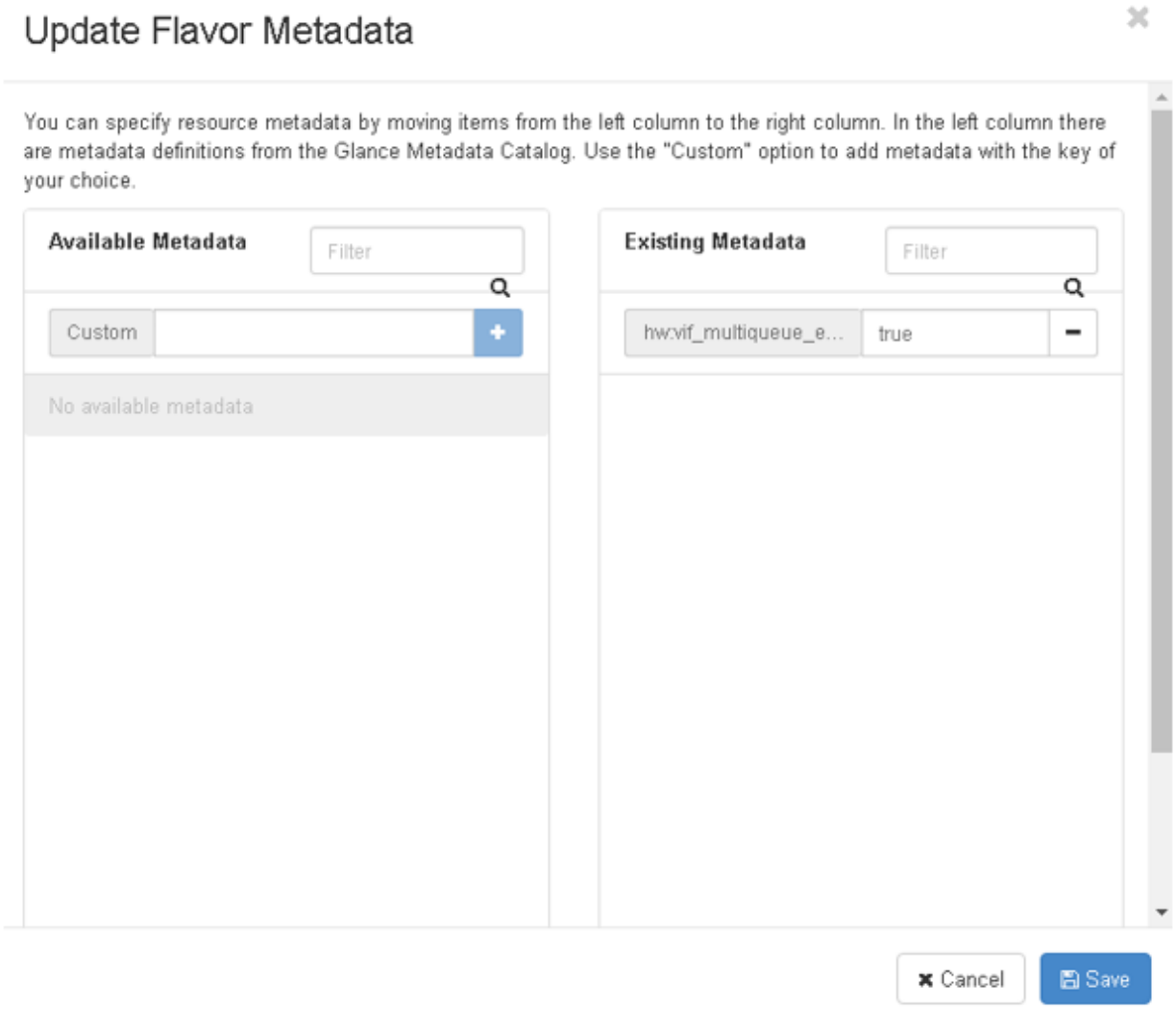
d. You can view the flavor by clicking **System > Flavors**.

Figure 19. Flavors screen



e. Click the down arrow next to **Edit Flavor** to set the `hw:vif_multiqueue_enabled` metadata as `True` for the flavor. This update is necessary for 3-core images.

Figure 20. Update Flavor Metadata screen



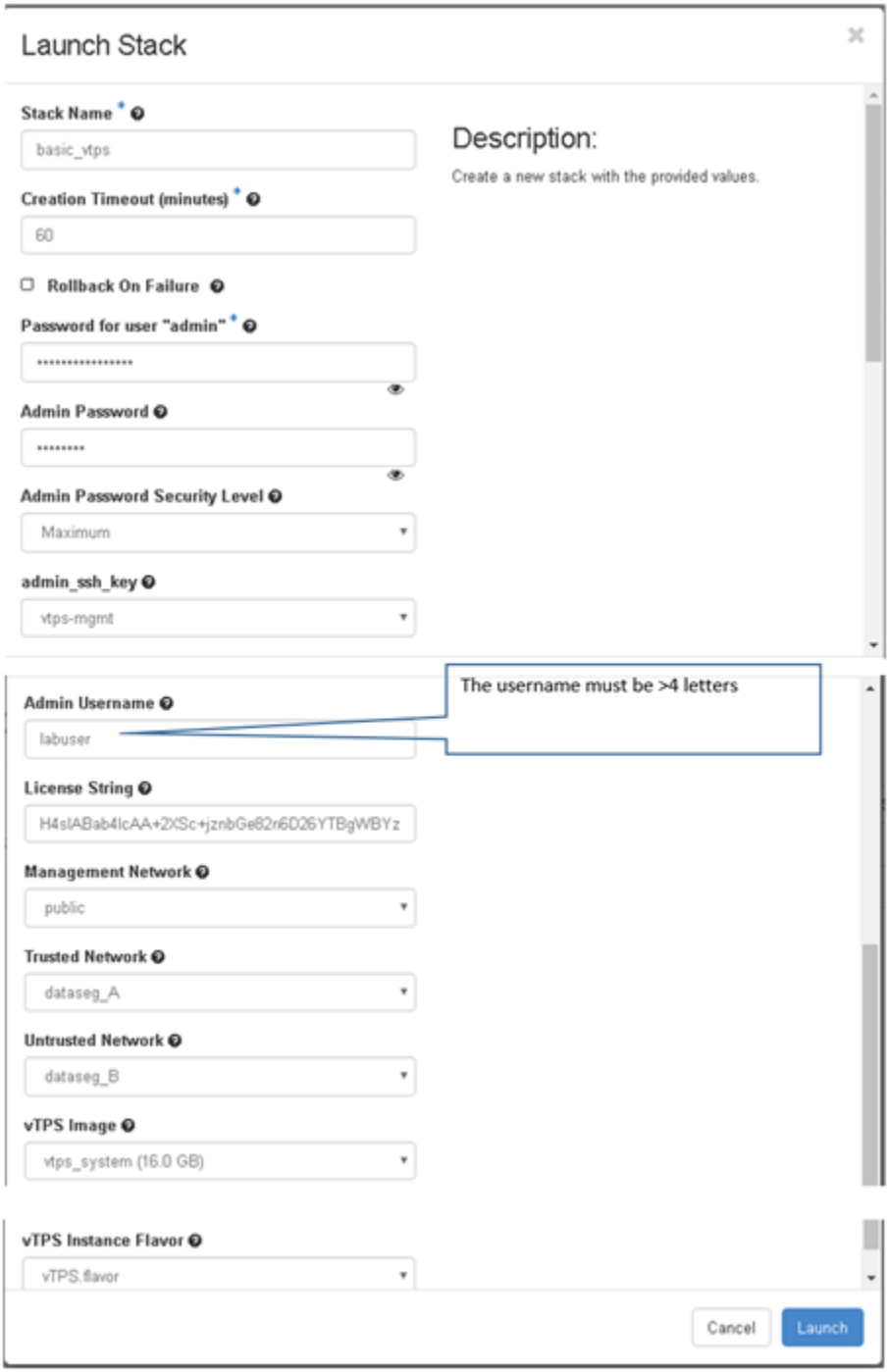
f. Click **Save**.

5. Before creating the stack, ensure your vTPS yml template file is in an accessible location on your system.
6. Select **Orchestration > Stacks** and click **Launch Stack** to launch the vTPS stack.
   a. In the Select Template dialog, specify the yml template file and click **Next**.

Figure 21. Select Template screen for your stack

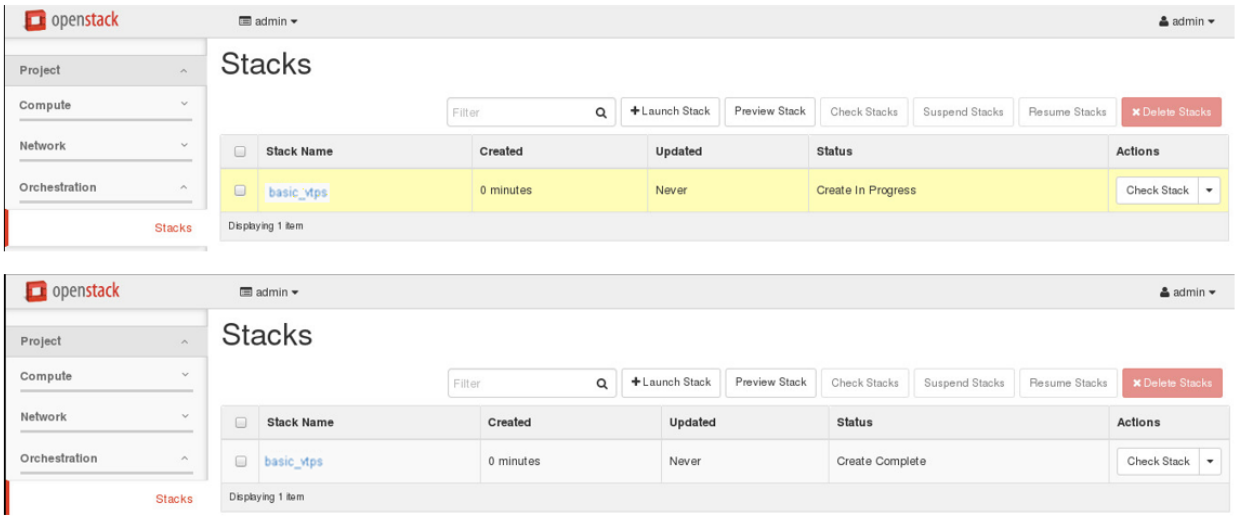
b. Specify the details for the stack, including appropriate values for the network, image, and flavor, and click **Launch**.

Figure 22. Launch stack screen



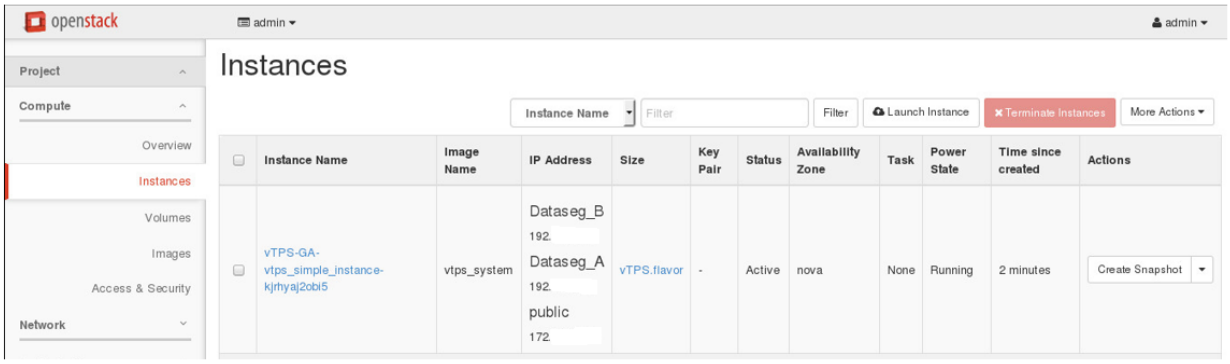
c. Confirm the creation status of the stack by selecting **Orchestration > Stacks**.

Figure 23. Stacks screen



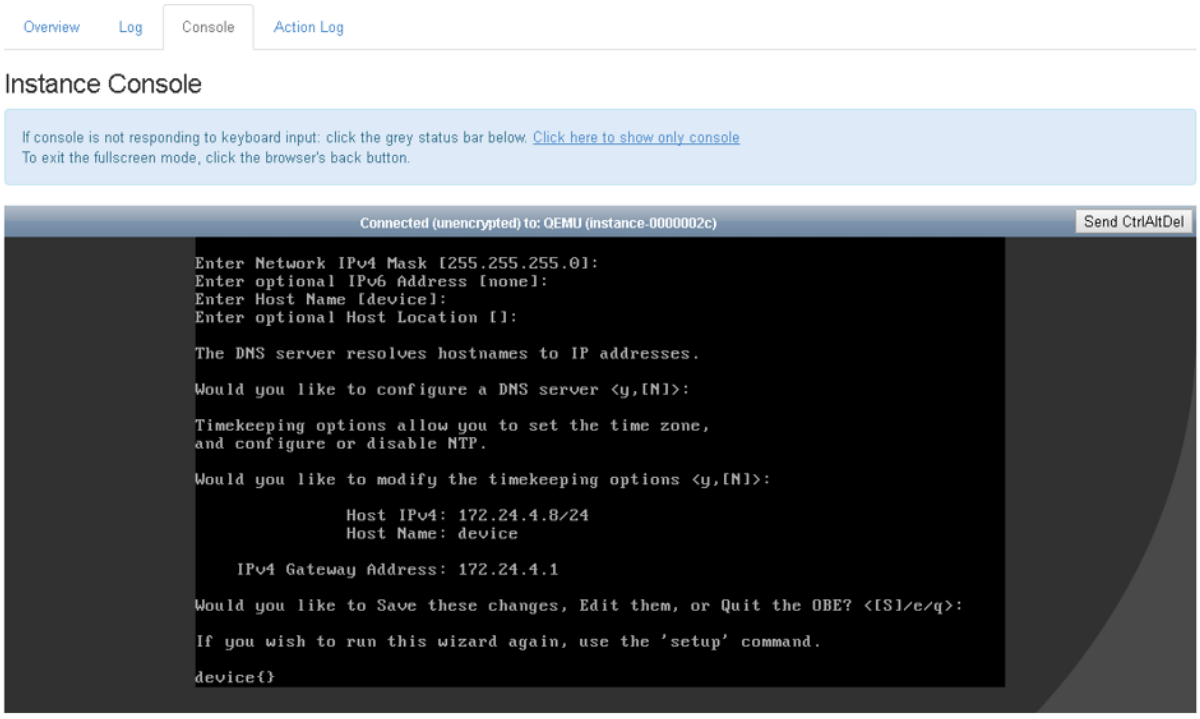
7. Select **Compute > Instances** and select the vTPS instance so you can connect to it.

Figure 24. Instances screen



8. Click on the Console tab to access the vTPS console and begin the OBE configuration.

Figure 25. Instance Console screen



Based on how you configured your yml file, the OBE wizard runs automatically, including a reboot to retrieve the OBE parameters and another reboot to install the device certificate.

Template sample

To access a sample HEAT template file, untar the vTPS Tar package and open the `basic_port_vtps.yaml` template file. The following template shows values for a sample environment only. In an actual deployment, values will vary according to each environment.

```
heat_template_version: 2015-10-15
description: Simple vtps instance with 1 mgmt port and 2 data ports. It will use
4/3 VCPU and 8GB memory. The template will require the user to use the fixed IP
address for the management port. The flavor should be based on the compute host
capability. Refer to the deployment guide.
parameters:
  vtps_image_id:
    type: string
    label: vTPS Image
    description: Image to be used for vTPS instance
    constraints:
      - custom_constraint: glance.image
        description: Select the Glance image
  vtps_instance_type:
```

```
    type: string
    label: vTPS Instance Flavor
    description: Type of instance (flavor) to be used for vTPS
    constraints:
      - custom_constraint: nova.flavor
        description: Select the Nova flavor
  private_net_vtps_mgmt:
    type: string
    label: Management Network
    description: ID of network into which vTPS is deployed
    constraints:
      - custom_constraint: neutron.network
        description: Select the Management network
  private_net_vtps_untrust:
    type: string
    label: Untrusted Network
    description: ID of network into which vtps data port 1A is deployed
    constraints:
      - custom_constraint: neutron.network
        description: Select the untrusted network
  private_net_vtps_trust:
    type: string
    label: Trusted Network
    description: ID of network into which vtps data port 1B is deployed
    constraints:
      - custom_constraint: neutron.network
        description: Select the trusted network
  admin_username:
    type: string
    label: Admin Username
    description: default admin user name.
    default:
  admin_password_security_level:
    type: string
    label: Admin Password Security Level
    description: the security level for the password for the admin user
    default: None
    constraints:
      - allowed_values:
        - None
        - Basic
        - Maximum
  admin_password:
    type: string
    label: Admin Password
    description: Password for the admin user
    default:
    hidden: true
  admin_ssh_key:
```

```
      type: string
      description: SSH key pair for admin account
      constraints:
       - custom_constraint: nova.keypair
      description: Must name a public key (pair) known to Nova
  instance_license:
    type: string
    label: License String
    description: vTPS instance license certificate
    default:
resources:
  vtps_mgmt_port:
    type: OS::Neutron::Port
    properties:
      network: { get_param: private_net_vtps_mgmt }
  vtps_data_port_A:
    type: OS::Neutron::Port
    properties:
      network: { get_param: private_net_vtps_untrust }
  vtps_data_port_B:
    type: OS::Neutron::Port
    properties:
      network: { get_param: private_net_vtps_trust }
  vtps_instance:
    type: OS::Nova::Server
    depends_on: [ vtps_mgmt_port, vtps_data_port_A, vtps_data_port_B ]
    properties:
      key_name: { get_param: admin_ssh_key }
      image: { get_param: vtps_image_id }
      flavor: { get_param: vtps_instance_type }
      networks:
        - port: { get_resource: vtps_mgmt_port  }
        - port: { get_resource: vtps_data_port_A  }
        - port: { get_resource: vtps_data_port_B  }
      config_drive: "true"
      user_data_format: RAW
      user_data:
        str_replace:
          template: |
            com_tippingpoint_IP = __instance_mgmt_IP__
            com_tippingpoint_Gateway = __instance_Gateway__
            com_tippingpoint_Security_Level = __admin_level__
            com_tippingpoint_Username = __admin_username__
            com_tippingpoint_Password = __admin_password__
            com_tippingpoint_VSSH_Public_Key = __admin_ssh_key__
            com_tippingpoint_Cert_License = __instance_license__
          params:
            __instance_mgmt_IP__:
                 list_join:
```

```
                      - ''
                      - - {get_attr: [vtps_mgmt_port, fixed_ips, 0, ip_address]}
                        - '/'
                        - {str_split: ['/', {get_attr: [vtps_mgmt_port,
                                        subnets, 0, cidr]}, 1]}
            __instance_Gateway__: { get_attr: [vtps_mgmt_port, subnets, 0,
                                               gateway_ip] }
            __admin_level__: { get_param: admin_password_security_level }
            __admin_username__: { get_param: admin_username }
            __admin_password__: { get_param: admin_password }
            __admin_ssh_key__: { get_param: admin_ssh_key }
            __instance_license__: { get_param: instance_license }
outputs:
  vtps_instance_name:
    description: Name of the instance
    value: { get_attr: [vtps_instance, name] }
  vtps_instance_id:
    description: ID of the instance
    value: { get_resource: vtps_instance }
  mgmt_ip:
    description: IP with CIDR for the vtps mgmt network.
    value:
        list_join:
          - ''
          - - {get_attr: [vtps_mgmt_port, fixed_ips, 0, ip_address]}
            - '/'
            - {str_split: ['/', {get_attr: [vtps_mgmt_port, subnets, 0, cidr]}, 1]}
```

Upgrade from vTPS Trial to vTPS Standard

To upgrade your vTPS from Trial Mode to vTPS Standard Mode, you must have first obtained your Software License Key from the TMC. See *Obtain the vTPS Software License Key* on page 5.

After you install the key, you must also install your license package and DV package.

The following information describes how to install the Software License Key, install your license package, and install your DV package:

Software License Key installation by using LSM

You can convert your vTPS device to Standard Mode by installing your Software License Key from the LSM.

1. Send TippingPoint a request for the Software License Key. See *Obtain the vTPS Software License Key* on page 5.
2. Log in to the LSM on your vTPS device.
3. Select **System > System, DV, License**.
4. On the System Software, Digital Vaccine, Certificate and Licenses page, click **Install Certificate**.
5. In the dialog screen that is displayed, browse to the location where you saved the license key file that TippingPoint sent you and click **Install**.
6. After the Software License Key is installed, click **OK** to reboot your device.

The device starts up in Standard Mode.

Software License Key installation by using the SMS

You can convert your vTPS device to Standard Mode by installing your Software License Key from the SMS.

1. Log in to your SMS client with an account that has the capability to add devices in SMS.

   For more information, refer to the *TippingPoint Security Management System (SMS) User Guide*.
2. Add the vTPS device, which will be in Trial Mode (**Devices > All Devices > New Device**).
3. Right-click on the device and select **Edit > Install Certificate**.

4. Browse to and select the vTPS certificate license file, and then click **OK**.

   The distribution process displays on the Distribution Progress panel. When the process is complete, the vTPS reboots, at which point the new certificate is loaded on the device and the vTPS starts up in Standard Mode. The device status changes from Trial Mode to Standard Mode in the SMS client.

Install your license package

Note: If your vTPS is being managed by an SMS, you can configure the SMS to automatically retrieve and distribute the most current license package.

You can retrieve your license package from the TMC (**My Account > TippingPoint License Package**).

For information on installing your license package, refer to your LSM and SMS documentation.

Install a Digital Vaccine package

Note: If your vTPS is being managed by an SMS, you can configure the SMS to automatically retrieve and distribute the most current DV package each week.

While in Trial Mode, your vTPS has a base DV installed with a limited number of security filters that cannot be changed. After you upgrade your device to Standard Mode, you can then install a full DV package.

For information on installing your DV package, refer to your LSM and SMS documentation.

Troubleshooting tips

Before contacting support, check to see if your issues are addressed in the following troubleshooting tips.

Difficulty logging in to the vTPS LSM

Resolution: Be sure to correctly map your network adapters so that you can access your vTPS device by using the LSM and CLI: **vTPS > Getting Started > Edit Virtual Machine settings > Hardware > Network Adapter**.

Configuring a distributed switch environment in promiscuous mode

Resolution: A vTPS must be configured in promiscuous (port-mirroring) mode. If a vTPS is connected to a distributed switch, ensure that any Forged Transmits and MAC Address Changes are set to ACCEPT so that network packets can be forwarded to each host in the port group.

Resolution: Although the vTPS does not support VMware vMotion, you can emulate a vMotion configuration by connecting two or more different hosts with two or more vTPS devices that are actively connected to the distributed vSwitch. The vTPS that is connected to the active VM acts as an IPS, and the vTPS that is not connected to the VM acts as an IDS. If you connect your SMS to both vTPS instances, any blocks and alerts will also be received by the SMS.

CPU usage always displays as 100% in hypervisor

Resolution: To see the actual CPU usage, enter the `show health cpu` command for the device.

Resolution: To manage the CPU usage, create a resource pool in the vSphere Web Client. For more information, refer to *Manage Resource Pools*.

Errors after Suspend and Resume operation

Resolution: HEALTH-ALERT errors generated after a Suspend and Resume operation can be ignored.

Examining OpenStack HEAT template events

Resolution: Use the `heat event-list <name of stack>` command to see a list of events.

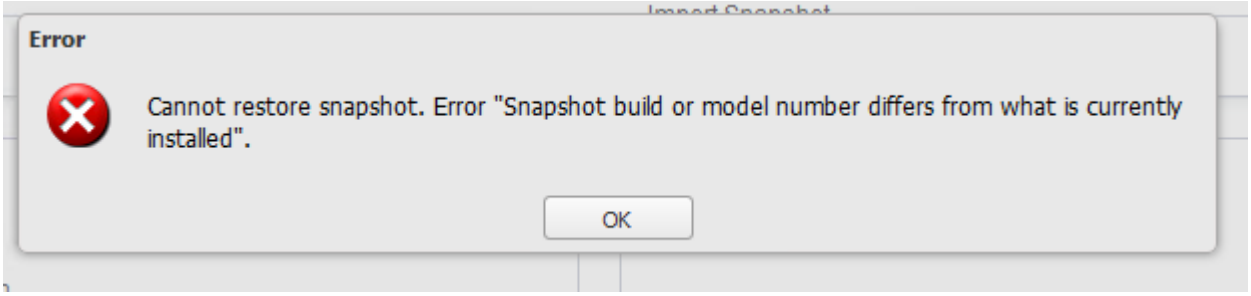
Resetting OBE parameters after a factory reset

Resolution: A factory reset does not reset the initial deployment parameter values—including IP address, username, and password. To change these values, you must deploy a new vTPS.

Snapshot cannot be restored

Resolution: Only vTPS to vTPS snapshots are supported. Restoring snapshots from other TippingPoint devices is not supported. Attempts will fail with the following error.

Figure 26. Snapshot error



Time synchronization issues in KVM environment

Resolution: If after an extended Suspend and Resume operation the device time does not sync with the server time, shut down and restart the system.

Verifying OpenStack HEAT template properties

Resolution: Use the virsh utility to dump the template xml file and examine your property settings, including the cpu count, the disk adapter type, and the network adapters:

```
localuser@vTPS-Helion1:~/heat_templates$ virsh
Welcome to virsh, the virtualization interactive terminal.
Type:  'help' for help with commands
       'quit' to quit
virsh #
virsh # list --all
 Id    Name                           State
----------------------------------------------------
 3     instance-00000002              running
virsh # dumpxml instance-00000002
  <cpu mode='custom' match='exact'>
    <model fallback='allow'>Conroe</model>
    <topology sockets='3' cores='1' threads='1'/>
  </cpu>
    <emulator>/usr/bin/kvm-spice</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2' cache='none'/>
      <source file=
'/opt/stack/data/nova/instances/56a5d809-5df5-435d-a665-24885891fff6/disk'/>
      <target dev='hda' bus='ide'/>
      <alias name='ide0-0-0'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
    <interface type='bridge'>
      <mac address='fa:16:3e:c0:b9:8a'/>
      <source bridge='qbr4edb826d-6d'/>
      <target dev='tap4edb826d-6d'/>
```

```
    <model type='virtio'/>
    <alias name='net0'/>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
  </interface>
  <interface type='bridge'>
    <mac address='fa:16:3e:d8:1e:be'/>
    <source bridge='qbr37a85eb2-d0'/>
    <target dev='tap37a85eb2-d0'/>
    <model type='virtio'/>
    <alias name='net1'/>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
  </interface>
  <interface type='bridge'>
    <mac address='fa:16:3e:7a:1f:90'/>
    <source bridge='qbre8d767e5-f9'/>
    <target dev='tape8d767e5-f9'/>
    <model type='virtio'/>
    <alias name='net2'/>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
  </interface>
```

vTPS device experiencing data port performance problems

Example: `ID HEALTHCHECKD Device is still experiencing performance problems (loss=<xx>%, threshold=<x>%). 0 alerts not logged.`

Resolution: Make sure three standard vSwitches or distributed vSwitches are properly configured on the ESXi or vCenter with multiple port groups for data and vTPS management traffic.

Resolution: Avoid large iptable entries. Larger iptable entries can reduce vTPS performance as much as 20 percent in a KVM deployment.

Resolution: Make sure port groups are enabled in promiscuous mode. Ensure that any Forged Transmits and MAC Address Changes are set to ACCEPT in order for network packets to get forwarded.

Resolution: Confirm each vTPS is configured with its own data port group. Using the same vSwitches across multiple vTPS devices can cause performance issues.

Configuring a serial console

ESXi Resolution: If you specified a serial console for your VM, add a serial port by editing the properties of the VM:

1. Right-click your new VM and click **Add**.
2. Select **Serial port** and click then **Next**.
3. Select **Connect via Network** and click then **Next**.
4. Select **Server** and provide a port for the Port URI (for example, `telnet://:1239`).
5. Click **Next**, and then click **Finish**.

6. Reboot the vTPS device. Before the console completes the change from VGA to Serial, the device reboots a second time automatically.
7. Enter the following command from a Linux shell to access the serial console:

   ```
   telnet <esxi host> <port number>
   ```

   For example:

   ```
   telnet esxi01 1239
   ```

KVM Resolution: Follow the procedure in *Automating vTPS installation on KVM* on page 15. Specify the `com_tippingpoint_Console = serial` option in the `vtps-env.txt` file.

To access the serial console from the KVM host, enter:

```
virsh console <VM_NAME>
```

TREND MICRO INCORPORATED
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com
Item Code: APEM47350/160315