TREND MICRO™

TippingPoint™ Virtual Threat Protection System (vTPS)

User Guide

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that the Security Management System collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Legal Notice

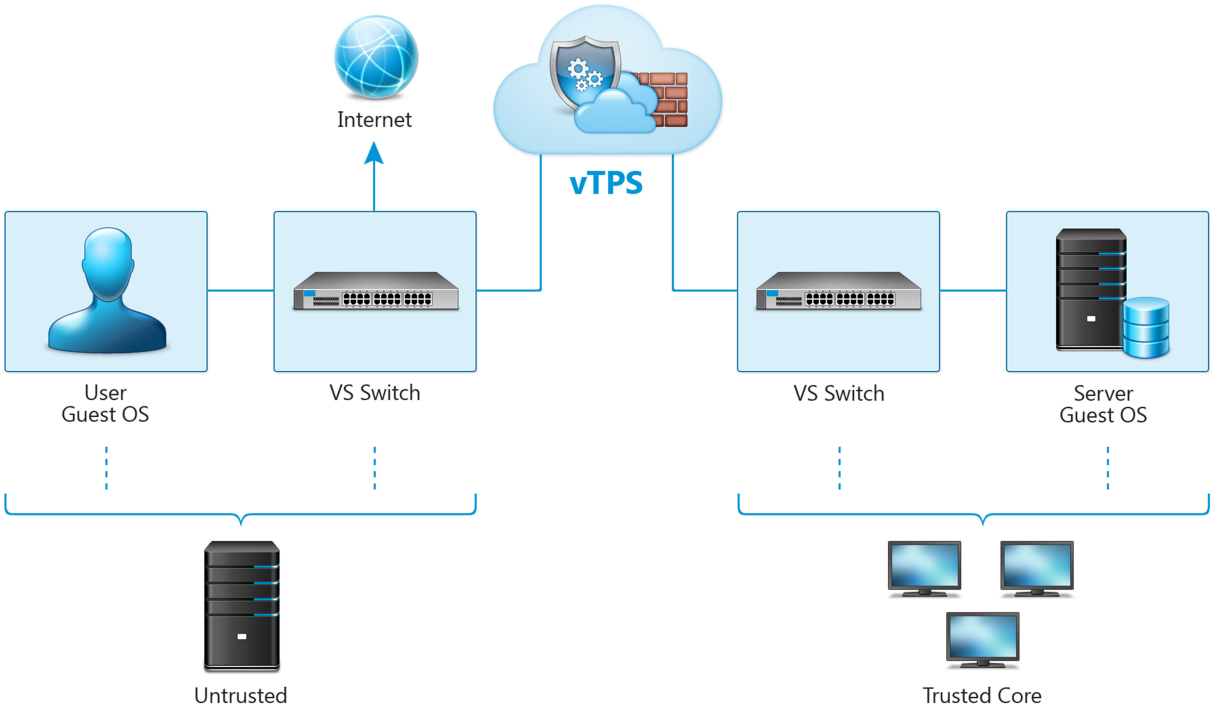
Publication: April 2020

Deployment overview

Use the configuration steps in these topics to deploy a TippingPoint Virtual Threat Protection System (vTPS) virtual appliance in either a VMware or kernel-based virtual machine (KVM) environment. The vTPS virtual appliance is a software appliance designed to give you the same level of functionality available in the TippingPoint Threat Protection System (TPS), but virtually rather than physically. Just as with a TPS device, the vTPS virtual appliance 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 virtual appliance. 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) or a virtual SMS (vSMS).

Learn more about 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.

Refer to the following illustration for an example of a basic hypothetical deployment. You must configure your vTPS virtual appliance between L2 broadcast domains (VLANs or switches).



After you deploy the vTPS virtual appliance, access the appliance by using the Local Security Manager (LSM) web interface or your SMS client. Learn more about these interfaces from the TPS product documentation.

vTPS functionality

The Virtual Threat Protection System (vTPS) virtual appliance is a software-based security appliance that can inspect traffic in a virtual network between Layer 2 broadcast domains. With few exceptions, the vTPS platform is designed to be functionally identical to a physical TPS device.

The vTPS virtual appliance has most of the same features as the TPS device, including:

- In-line, real-time threat protection for inbound IPv4 traffic that is SSL encrypted (Performance mode only)
- HTTP response processing to decode URL encodings and numeric character references
- DNS reputation remediation for enabling `NXDOMAIN (name does not exist)` responses to clients that make DNS requests for hosts that are blocked
- Layer 2 Fallback (Intrinsic High Availability)
- Enhanced SNMP support
- The ability to collect a client's true IP address.
- The ability to identify the HTTP URI and hostname information associated with an event.
- Flexibility to upgrade inspection throughput from 500 Mbps to 2 Gbps.

For successful TPS functionality in a virtual environment, the vTPS virtual appliance:

- Supports Layer 2 IPS deployments—The vTPS virtual appliance connects the virtual switches. Traffic between the virtual switches is bridged on these connections using promiscuous mode.
- Provides full protection of North-South traffic.
- Provides limited protection of East-West traffic (according to existing network policy constructs).

For optimal deployment of your vTPS virtual appliance, you should note the specific areas in which your virtual appliance functionality differs from a physical TPS device.

Note

Any unsupported features will not be displayed in the three vTPS interfaces—Local Security Manager (LSM), Command Line Interface (CLI), and Security Management System (SMS).

The following topics highlight the areas where a vTPS virtual appliance diverges functionally from a physical TPS device:

- *Deployment and licensing*
- *Specifications*
- *Unsupported features*
- *LSM user interface*
- *Commands*

Deployment and licensing

Because the vTPS virtual appliance is a virtual product, the out-of-box experience (OBE) for vTPS users is described in an email from Trend Micro TippingPoint. This email contains licensing and activation information and directs you to use the license manager on the Threat Management Center (TMC) to create and download vTPS certificate packages.

When setting up your vTPS virtual appliance, note the following:

- The vTPS virtual appliance initially starts up in vTPS Trial Mode. Trial Mode is primarily exploratory and comes with a limited number of security filters in the Digital Vaccine package. In this mode, an SMS can manage only one vTPS virtual appliance 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 Digital Vaccines.
- The vTPS virtual appliance remains in Trial Mode until you install a valid certificate for vTPS Standard Mode. *Learn more* on upgrading to vTPS Standard Mode,

- The vTPS virtual appliance does not support a hitless reboot or hitless upgrade. Traffic flow is interrupted until the boot sequence completes because, unlike on a TPS device, the network ports on a vTPS virtual appliance are virtual.

The following table highlights the ways in which getting set up on a TPS device and vTPS virtual appliance are different:

DEPLOYMENT	TPS DEVICE	vTPS VIRTUAL APPLIANCE
OBE	After you install the device in a rack, a setup wizard guides you through system checks, initializations, and configurations.	Obtain the license entitlement and certificate using the license manager on the TMC. Initial deployment defaults to a Trial Mode. You cannot perform any updates.
Digital Vaccine	Uses the V. 3.2.0.x Digital Vaccine package.	Uses a special Digital Vaccine package (4.0.0.*x*) that does not include Zero Day Initiative (ZDI) filters.

Specifications

Both the TPS device and the vTPS Standard virtual appliance share the following specifications.

DESCRIPTION	SPECIFICATION
Average IPS latency	Less than 100 microseconds
Security contexts	750,000

For the various licensed throughput options available for physical TPS devices and the vTPS, refer to the *SMS User Guide*.

The specifications of the physical TPS device and the vTPS Standard virtual appliance differ in the following areas.

DESCRIPTION	TPS DEVICE	vTPS VIRTUAL APPLIANCE
Concurrent sessions	440T: 7,500,000 2200T: 10,000,000 1100TX: 15,000,000 5500TX: 30,000,000 8200TX/8400TX: 120,000,000	1,000,000
New connections per second	440T: 70,000 2200T: 115,000 1100TX: 122,000 5500TX: 397,000 8200TX/8400TX: 650,000	VMware: Up to 120,000 KVM: Up to 60,000
Ethernet maximum transmission units (MTU)	9050	1500

Note

All virtual machines (VMs) on a shared host compete for resources. To achieve optimal performance numbers for the vTPS virtual appliance, ensure that the hypervisor provides adequate CPU and RAM for the VM. Performance numbers will vary depending on hypervisor configuration and hardware resources available.

The SSL performance of the physical TPS device and the vTPS Standard virtual appliance (must have Performance mode deployed) differ in the following areas.

Note

The TPS 440T and 1100TX devices do not support SSL inspection.

DESCRIPTION	TPS DEVICE	vTPS VIRTUAL APPLIANCE
Profiles	8096	756
Policies	8096	756
Policy IP Exceptions	1024	128
Servers	1024	128
Server IPs	8	8
Server Ports	8	8
Certificates	2200T: 256 5500TX: 256 8200TX/8400TX: 256	32

The following functionality is different in the vTPS Standard virtual appliance.

SPECIFICATION	TPS DEVICE	vTPS STANDARD VIRTUAL APPLIANCE
Port configuration	Eight data ports. You can configure physical characteristics of ports (such as speed and duplex). Ports are fixed.	Two virtual data ports. You cannot configure physical characteristics of ports (such as speed and duplex). You can remove and replace a port.
User disk	External 8 GB CFast (440T/2200T or SSD (1100TX) card. External 32 GB SSD (5500TX, 8200TX/8400TX)	No separate user disk. The vTPS Standard virtual appliance has a single-disk architecture with an 8-GB user disk partition.
Environmental requirements	For operating, storage, and environmental requirements, refer to the *Threat Protection System Hardware Specification and Installation Guide*.	Not applicable.
External HA interfaces	1 HA port 1 ZPHA port	No HA ports supported.

Unsupported features

You can configure all available features using the vTPS interfaces (LSM, CLI, SMS). Any unsupported features will not be displayed in these interfaces.

The following features supported in the physical TPS devices are not supported in the vTPS Standard virtual appliance:

- Physical characteristics of ports (such as speed and duplex). Ports are virtual instead of copper or fiber.
- Data security (encrypting the removable disk that stores logs)
- Link setting updates when you configure a port

- Transparent High Availability (TRHA) deployments
- Zero Power High Availability (ZPHA) deployments

> **Note**
>
> This means that the vTPS virtual appliance does not pass traffic at all during a software upgrade or during a reboot of the device.

- VLAN Translation
- Inspection bypass
- sFlow® sampling
- Jumbo frames
- Reputation Enforcement Options (SMS-managed vTPS virtual appliance deployed in Normal Mode only)
- East-West protocol (such as VXLAN)
- Direct-attach network interface controller (NIC)

LSM user interface

The following LSM options for a physical TPS device are not available on the vTPS virtual appliance. Any unsupported options are not displayed in the LSM.

Operation	Explanation
Monitor > Health > HA	The vTPS virtual appliance does not support high availability deployments.
Monitor > Health > Fan Speed	Environmental and operational constraints do not apply.
Monitor > Health > Temperature	Environmental and operational constraints do not apply.
Network > VLAN Translations	VLAN translations are not supported.
Network > Ports > Settings page.	When you use the **Edit** button, you can only enable or disable the port.
Network > sFlow	The hardware required to run this feature is not available on vTPS virtual appliances.
Policy > Inspection Bypass	The Broadcom switch chip required to run this feature is not available on vTPS virtual appliances.
System > Data Security	vTPS virtual appliances do not have an external storage card. Although users can provide a master key, the external storage card cannot be encrypted.
System > High Availability	Transparent High Availability (TRHA) and Zero Power High Availability (ZPHA) deployments cannot be configured on this page.

Commands

The following commands that a physical TPS device supports are not available for the vTPS virtual appliance:

- Data security
  - `log-storage`
- Health
  - `reports (reset|enable|disable) fan`
  - `reports (reset|enable|disable) temperature`
- Port settings
  - `interface <port_identifier> physical-media`
  - `interface mgmt physical-media`
- High availability – You can use the following high-availability commands, but *only* for Layer 2 Fallback settings:
  - `high-availability`
  - `high-availability force (normal | fallback)`
  - `show high-availability`
- sFlow sampling
  - `sflow`
  - `show sflow`
- Inspection bypass
  - `running-inspection-bypass` context commands
  - `show inspection-bypass`
- VLAN translation
  - `running-vlan-translations` context commands
  - `show vlan-translations`
- SSL inspection – You can use the `running-sslinsp` context commands, but *only* if you deploy in Performance mode.

Normal mode versus Performance mode

You can deploy your single-image vTPS virtual appliance in either Normal mode or Performance mode. Select which mode to deploy in according to the features they provide and the resources they require. You can switch between modes without redeploying. *Learn more* about switching between modes.

Download this deployment from the TMC (**Releases > Software > TPS > vTPS VM**):

- For VMware, download `signed_vTPS_5.1.0.xxxx.ova`
- For KVM, download `vTPS_kvm_5.1.0.xxxx.tar.gz`

Your vTPS automatically detects the resources available and deploys in the appropriate mode.

Normal mode – For scaled-down deployments to replace older Intrusion Prevention System (IPS) devices. Normal mode does not support SSL inspection and has the following specifications:

- Minimum of two vCPUs (500 Mbps inspection configuration) and a maximum of three vCPUs (1 Gbps inspection configuration, default)

- 8 GB memory
- 16 GB disk space
- Inspection capacity of 2 Gbps (upgrade license required)

Normal mode runs the engine in *N*-thread mode, where *N* is 1 or 2, depending on how many vCPUs you reserve for the vTPS operating system. One vCPU must always be reserved for the operating system. For example, three vCPUs allows for two engine threads.

Performance mode – For an increased capacity for vCPUs and threading. Deploy Performance mode to enable SSL inspection. This mode has the following specifications:

- Six vCPUs (default)
- 16 GB memory
- 16 GB disk space
- Inspection capacity of 2 Gbps (upgrade license required)

Performance mode runs its engine in multi-queue mode. One vCPU must always be reserved for the operating system.

Use the `show version` command to display which operational mode, Normal or Performance, your vTPS virtual appliance is running.

Configure the vTPS virtual appliance for SSL Inspection

You can change from Normal mode to Performance mode without redeploying to enable in-line, real-time threat protection for inbound IPv4 traffic that is SSL-encrypted.

To change the vTPS virtual appliance from Normal mode to Performance mode:

1. Shut down the vTPS virtual appliance. If the appliance is managed, you can also shut it down from the SMS client by right-clicking the device on the Devices page and selecting **Edit > Device Configuration**.
2. Using specific options associated with your hypervisor—such as virt-manager, VMmanager, vSphere, or Vcenter—configure the vTPS parameters to 6 vCPUs and 16 GB memory.
3. Turn on the vTPS virtual appliance. The SMS automatically recognizes the resource allocation and changes to Performance mode.
4. Configure SSL Inspection on the device. Learn more about configuring SSL inspection from the *TPS Local Security Manager User Guide* and the *SMS User Guide*.

To preserve system resources and operate without SSL inspection, you can use a similar procedure to return to Normal mode by reconfiguring the vTPS parameters to 3 vCPUs and 8 GB memory.

Install and configure the vTPS virtual appliance

Use the following topics to configure your vTPS virtual appliance:

- *General requirements*
- *Install and deploy a vTPS virtual appliance by using VMware ESXi*
- *Install and deploy a vTPS virtual appliance by using KVM*

Note

All virtual machines (VMs) on a shared host compete for resources. When a hypervisor becomes overloaded with too many VMs or with VMs that are resource-intensive, a system boot can potentially slow down to the point of failure. To prevent delays or timeout errors in the boot process, watch for deviations in system performance and reallocate the appropriate resources as necessary.

Learn more about configuring security policy for your virtual appliance from your SMS and LSM documentation.

General requirements

IPS performance can vary according to the hypervisor setting and use of resources on the host VM. To deploy a vTPS virtual appliance in any software environment, follow these specifications:

- **Memory (RAM)** – 8 GB (Normal mode), 16 GB (Performance mode)
- **Number of CPU cores:**
  - Normal mode – 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)
  - Performance mode – requires six cores
- **Disk space** – 16.2 GB

Note

Although the vTPS virtual appliance supports both thin and thick provisioning, use thick provisioning for optimum performance.

- **CPU** – Host CPU must support the SSSE3 instruction set. These CPU configurations were tested:
  - Intel Xeon CPU E5-2697v2
  - Intel Xeon CPU E5-2690
  - Intel Xeon CPU E5-2683v3
  - Intel Xeon CPU X5670
  - Intel Xeon CPU X5650

Note

For users with an SSL license who are deploying in Performance mode, use Intel Xeon CPUs based on Ivy Bridge or newer (for example, E5-2697v2 and E5-2683v3) for their support of hardware random number generation (RDRAND instruction). In order for the VM to incorporate the CPU features, additional hypervisor configuration might be necessary:

- For VMWare, adjust the EVC mode to `Ivy Bridge` or newer as necessary. Learn more about adjusting the EVC mode.
- For Red Hat, set the guest CPU to `host-passthrough`, `Haswell`, or newer. Learn more about Red Hat virtualization deployments.

Install and deploy a vTPS virtual appliance by using VMware ESXi

Use the information in these topics to configure the vTPS virtual appliance for startup by using the vCenter application:

- *VMware ESXi requirements*

VMware ESXi requirements

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

- **ESXi Hypervisor version**:
  - Version 5.5 (Patch 3116895)
  - Version 6.0 (Patch 5572656)

    Note

    When you deploy the vTPS virtual appliance on the vSphere Hypervisor (ESXi 6.0), always install the latest Update 3 (U3) to prevent IPv6 packet drops.

  - Versions 6.5 and 6.7

    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. The vTPS supports both vSwitches and distributed vSwitches (dvSwitches).
  - You must configure the two data vNICs in promiscuous mode for Layer 2 routing. To avoid ARP request flooding, configure the two data ports on separate networks. Ensure that you set any Forged Transmits and MAC Address Changes to ACCEPT so that network packets get forwarded.
  - Layer 3 virtual segments do not require promiscuous mode.

Configure the vTPS virtual appliance on VMware

To configure vTPS virtual appliance on VMware:

Procedure

1. Create three virtual switches on the ESXi host—one for the management port and two for the data ports, and ensure that you connect the three vNICs to the correct virtual switches.

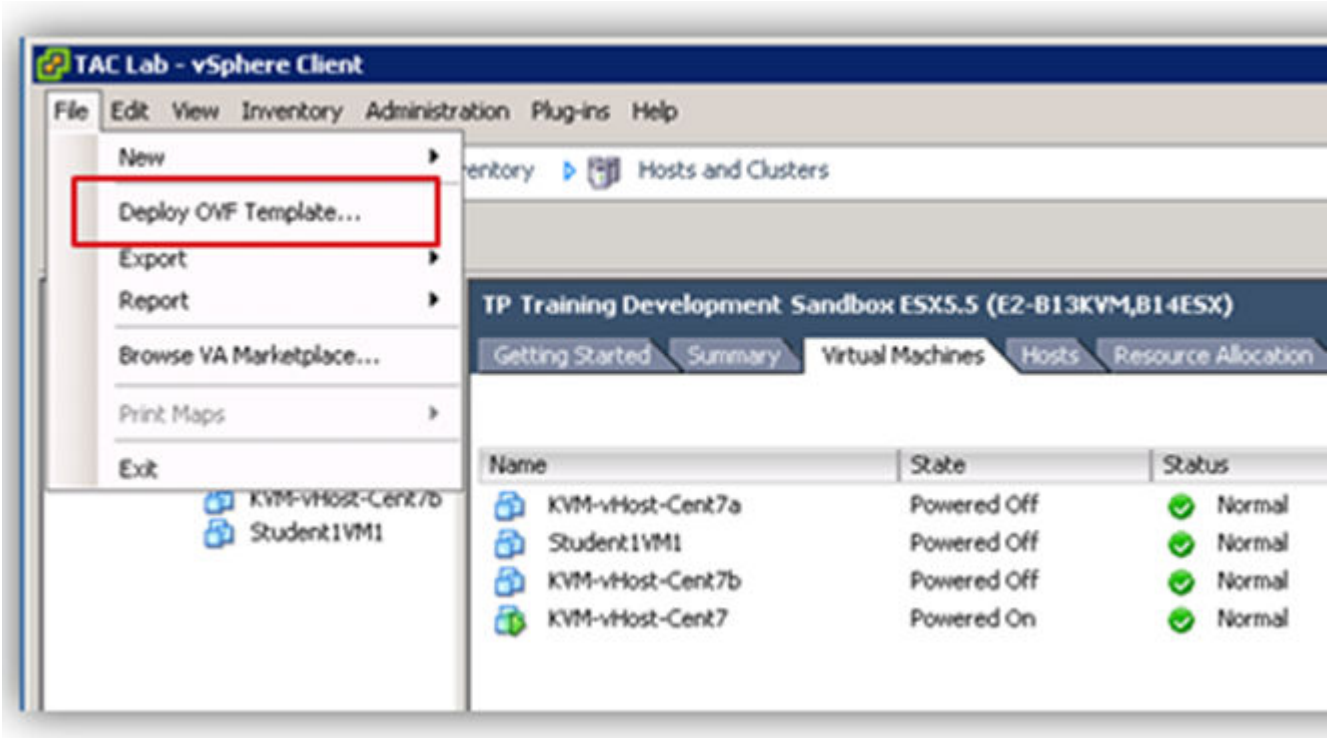
   Learn more about VMware.

Note

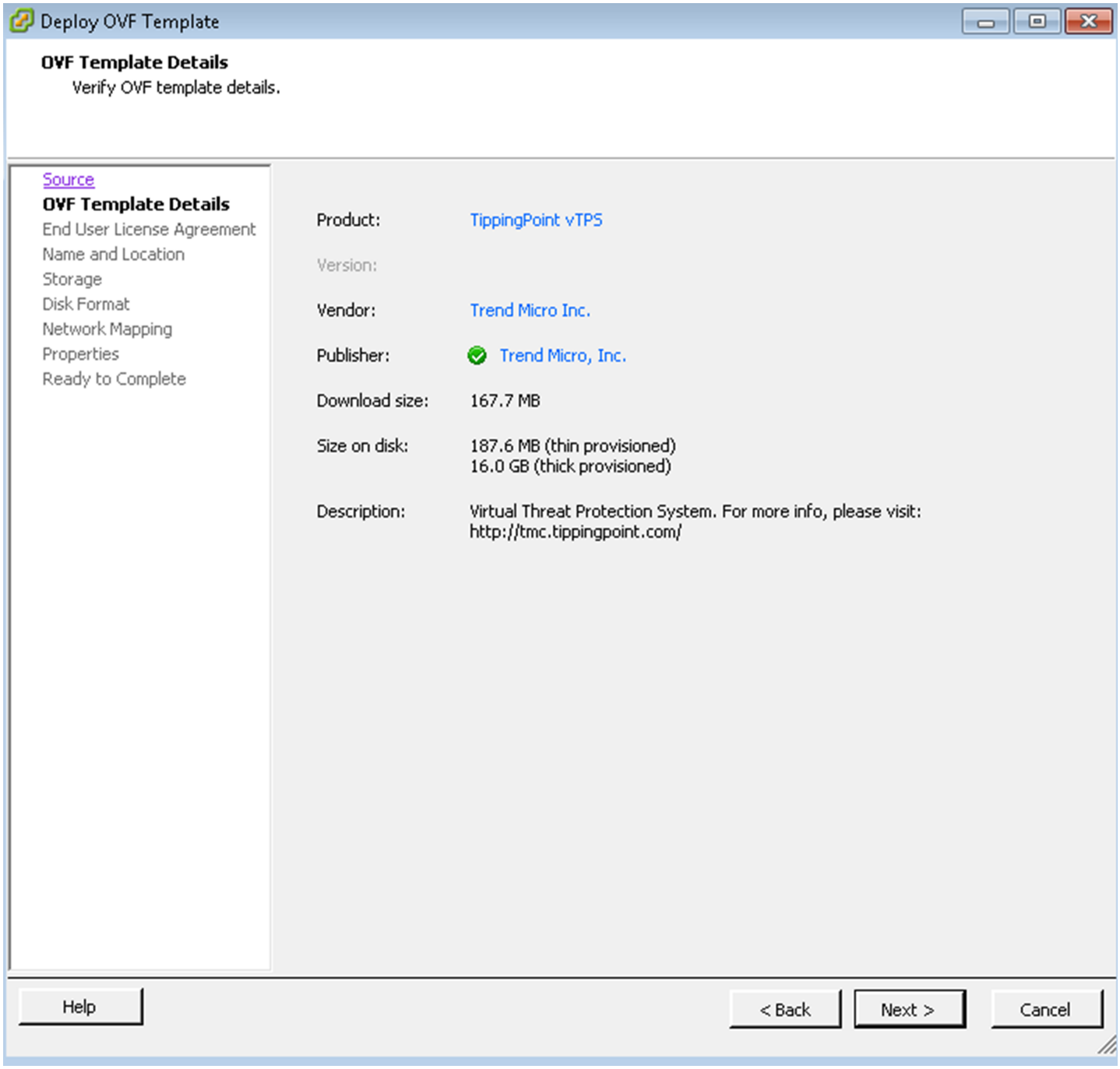
Consider the following when configuring your network ports.

- In order for the vTPS to function properly for Layer 2 routing, create the ports, map them to their correct interfaces, and enable them in promiscuous mode. (Promiscuous mode is not required for Layer 3 virtual segments.)
- By default, ESXi attempts to attach all the adapters to the virtual switch that was created first.
- Make sure that you set any Forged Transmits and MAC Address Changes to ACCEPT for network packets to get forwarded.
- If you deploy two vTPS devices using the same two networks, traffic loops through both devices.
- You must configure the VLAN ID field to `All(4095)` for data port virtual switches if you intend to use VLANs for data ports.
- If your configuration requires traffic to cross multiple VLANs before reaching the vTPS, make sure that your remove the VLAN tags from the ports to prevent the traffic from going through the same network on its way back.

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

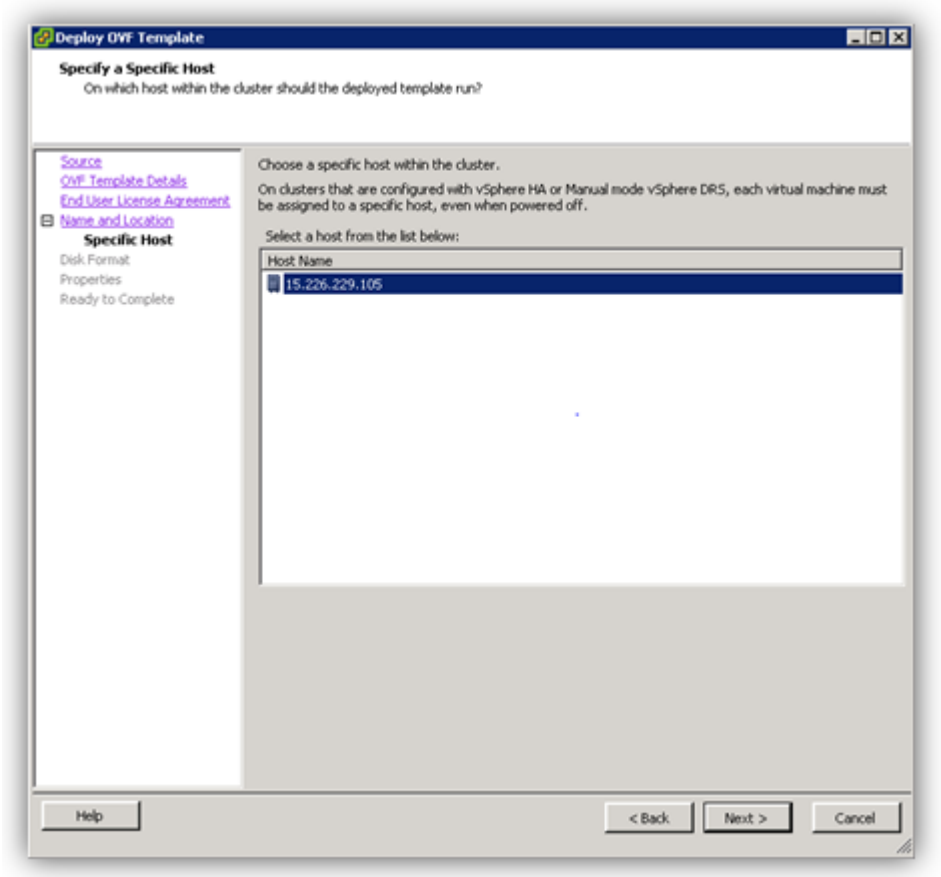


Ensure that the publisher information displayed on the OVF Template Details screen is correct before proceeding further. When you are satisfied you have opened the correct package, click **Next**.



4. 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**.



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, select the format in which to store the virtual disks and click **Next**.

> **Note**
>
> The vTPS virtual appliance supports both thin and thick provisioning. For optimum performance, use thick provisioning.

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

> **Note**
>
> Accepting the default values configures the management port and the data ports on the same network, which can flood the environment with ARP requests. To avoid this, ensure that you configure the two data ports on different networks.

The first interface you provide is your management port. Ensure that your management network can access this port. 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 virtual appliance by using the LSM, CLI, and SMS client.

10. If you use a vSphere client to deploy directly on a host, you can configure the vTPS parameters only after the vTPS boots using the out-of-box experience (OBE) interface on the console. If you use a vCenter server to deploy, the Properties screen prompts you 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, first install the vTPS virtual appliance with IPv4 by using the OBE interface on the console. Configure an IPv6 address after you boot the device.

- 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, *Learn more* about how to configure it

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

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

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

    The initial boot displays your deployment progress and any messages with the VGA console, even if you previously selected `serial` as the console. The interface prompts you to provide values for any deployment questions you previously skipped.

After the OBE boot completes:

- If you provided a certificate URL during the deployment, the vTPS virtual appliance automatically downloads the certificate and reboots to activate it.
- If you selected to use the serial console, the vTPS virtual appliance automatically reboots. The serial console displays all messages from this next boot.

> **Note**
>
> The vTPS virtual appliance does not support a hitless reboot or hitless upgrade. Traffic flow is interrupted until the boot sequence completes because, unlike on a TPS device, the network ports on a vTPS virtual appliance are virtual.

- If neither of the preceding bullets apply, a login prompt is displayed. You can now access the device using the console, SSH, LSM, or SMS client.

Start your vTPS virtual appliance

Follow these steps to complete the initial deployment:

Procedure

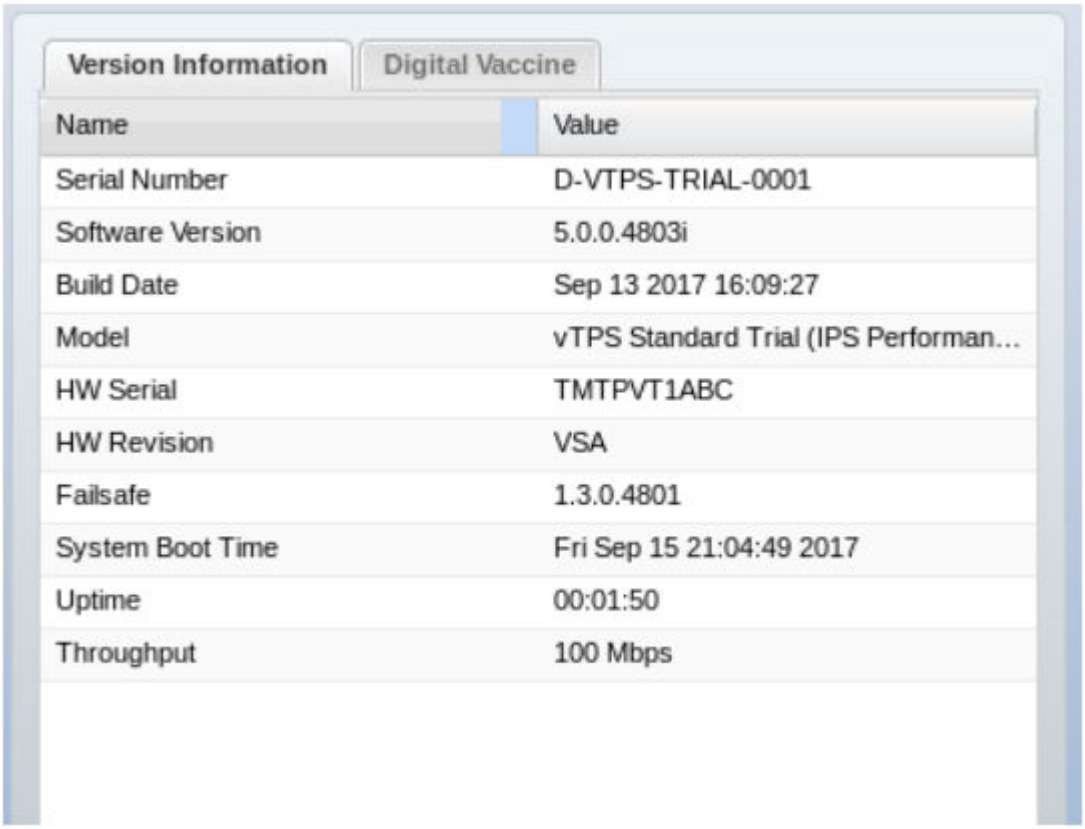
1. In vCenter, right-click your new VM and select **Power > Power on** from the menu.
2. If you did not use vCenter to provide network settings, you can access the vCenter VGA console for the vTPS virtual appliance to configure those settings.

What to do next

If you did not use vCenter to provide license key information in the preceding step, the vTPS virtual appliance boots in Trial Mode by default. The following graphic indicates from the CLI that you are in Trial Mode.

```
docvtps{}show version
              Serial: D-VTPS-TRIAL-0001
            Software: 5.0.0.4803i Build Date: "Sep 13 2017 16:09:27" Production [9ac20f021]
     Digital Vaccine: 4.0.0.1000
       Reputation DV: N/A
               Model: vTPS Standard Trial (IPS Normal)
          HW Serial: TMTPVT1ABC
        HW Revision: VSA
           Failsafe: 1.3.0.4801
         Throughput: 100 Mbps
   System Boot Time: Fri Sep 15 20:56:55 2017
             Uptime: 00:02:06
```

The following graphic indicates from the LSM that you are in Trial Mode.



Upgrade to Standard Mode

If you did not provide a certificate URL during deployment, upgrade to Standard Mode. *Learn More* about upgrading to Standard Mode.

If you did provide a certificate URL during deployment, activation of the certificate occurs automatically.

Install and deploy a vTPS virtual appliance by using KVM

Use the information in these topics to configure the vTPS virtual appliance for startup by using a kernel-based virtual machine (KVM):

- *KVM requirements*
- *Obtain software licensing and certificates*
- *Deploy a Normal mode vTPS virtual appliance on KVM*
- *Automating vTPS installation on KVM*
- *Upgrade to Standard Mode*

KVM requirements

A KVM deployment of the vTPS virtual appliance 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.

  Ensure that the bridges used for the data ports can forward all Layer 2 frames to the vTPS virtual appliance. To do this, use the **brctl** shell utility to configure the bridges to disable address learning by setting `setageing` to `0`:

```
# brctl setageing data-A 0
# brctl setageing data-B 0
```

  To prevent this setting from being overwritten by a reboot, add the `AGEING=0` parameter to the bridge's `/etc/sysconfig/network-scripts` configuration.

Note

Disabling address learning ensures that bridges properly forward all Layer 2 frames to the vTPS. Otherwise, especially in cases where a single data port sees both sides of the network connection (such as in an IDS mode), the bridge is prevented from sending the frames to the vTPS virtual appliance by the default address learning mode.

- **Console access** – Default and recommended console is a graphical UI, such as virt-manager, virt-viewer, vncviewer, or other VNC client. *Learn more* about configuring the serial console.

Note

The vTPS virtual appliance 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*.

Deploy a Normal mode vTPS virtual appliance on KVM

To install a vTPS virtual appliance on KVM in Normal mode:

Procedure

1. Copy the vTPS tar package to your system.
2. Extract the package with the `tar --sparse -zxvf vTPS_kvm_x.x.x_xxxxx.tar.gz` command.
3. Use the `chmod` command to change permissions so that the QEMU user can access the file:

```
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 virtual appliance 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, 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
```

This completes the vTPS Normal mode deployment.

Deploy a vTPS virtual appliance on KVM in Performance mode

To install a vTPS on KVM in Performance mode:

Procedure

1. Copy the vTPS tar package to your system.
2. Extract the package with the `tar --sparse -zxvf vTPS_performance_kvm_x.x.x_xxxxx.tar.gz` command.
3. Use the `chmod` command to change permissions so that the QEMU user can access the file:

   ```
   chmod a+rwx system_disk.raw
   ```

4. Use the `virt-install` command to deploy the vTPS package according to your RHEL version:

   To deploy a vTPS virtual appliance 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. For either configuration, specify `cores=6` and `driver_queues=6`.

```
virt-install \
--name=<name of your VM> --ram=<specify ram size{for 16GB specify 16384}>
--vcpus sockets=1,cores=6 \
--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=6 \
--network bridge=<data bridge 2>,model=virtio,driver_queues=6 \
--graphics vnc,port=59<xy>,listen=<ip_of_kvm_host> \
--virt-type=kvm --cpu qemu64,+ssse3,-svm \
--force --wait -1
```

Important:

You must specify the `--cpu` option as `qemu64` when running the `virt-install` command. If you specify another CPU, the `vtps-env.txt` file will be ignored. For users with an SSL license who are deploying in Performance mode, use Intel Xeon CPUs based on Ivy Bridge or newer (for example, E5-2697v2 and E5-2683v3) for their support of hardware random number generation (RDRAND instruction). In order for the VM to incorporate the CPU features, additional configuration might be necessary. *Learn more* about configuring CPU features for Performance mode.

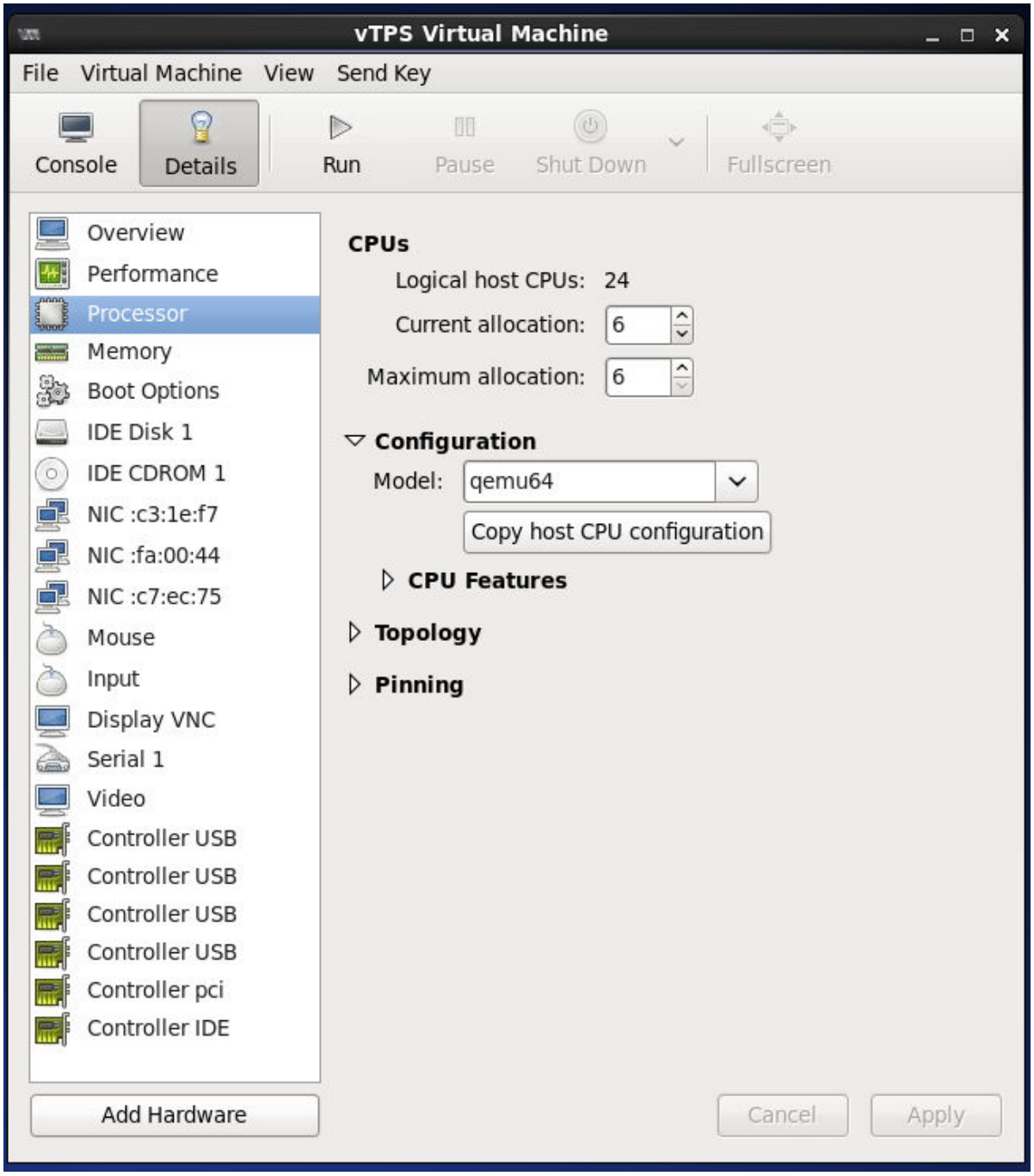
After running the preceding `virt-install` command, shut down the VM. Use `virt-manager` to adjust the CPU parameter to `host`, `Westmere`, `Haswell`, or newer:

a. Select **Processor** from the list of hardware.

b. Toggle the **Configuration** triangle and select the appropriate processor model.

c. Either pick a CPU type manually from the list or click **Copy Host CPU Configuration** for the best CPU to match with this host.

d. Click **Apply**.



You can also accomplish this task by using `virsh edit VM-NAME` to edit the VM XML file. Learn more about this option.

Note

The `--wait` option keeps your program running on the shell. After you have installed the vTPS Software License Key and the vTPS virtual appliance 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, 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`

This completes the vTPS Performance mode deployment.

Automating vTPS installation on KVM

Procedure

1. Use the `yum install genisoimage` command to install `genisoimage` on an RHEL system.
2. Copy the vTPS tar package to your system.
3. Use the `tar --sparse -zxvf vTPS_kvm_x.x.x_xxxxx.tar.gz` command to extract the package.
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/low/medium/high>
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.

   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. Use the `chmod` command to change permissions so that the QEMU user can access the file:

```
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 for Normal mode, specify `cores=2` and `driver_queues=1`. For 2 fast paths, specify `cores=3` and `driver_queues=2`. For Performance mode, always specify `cores=6` and `driver_queues=6`. The following example shows 2 fast paths for Normal Mode.

```
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 virtual appliance 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, 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
```

This completes the automated KVM vTPS deployment.

Upgrade to Standard Mode

If you did not provide a certificate URL during deployment, upgrade to Standard Mode. *Learn More* about upgrading to Standard Mode.

If you did provide a certificate URL during deployment, activation of the certificate occurs automatically.

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 both a GUI deployment and a CLI 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 procedures.

- *vTPS emulation requirements*
- *vTPS functional requirements*
- *Deploy the TippingPoint vTPS on OpenStack using the CLI*
- *Deploy the TippingPoint vTPS on OpenStack using the GUI*

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 (Normal image), 6 (Performance image)
3. RAM – 8 GB (Normal image), 16 GB (Performance image)
4. Disk image – 1 (system disk required, 16 GB total size)

5. Configuration drive – optional

Deploy the TippingPoint vTPS on OpenStack using the CLI

Before you begin

Create a Linux virtual environment and text file with the following authorization credentials:

```
export OS_USERNAME=**********
export OS_PASSWORD********
export OS_TENANT_ID=*******
export OS_AUTH_URL=https://<keystone-url>:5000/v3
```

Source this text file so that you credentials can be loaded as environment variables:

```
source <auth_file>
```

Procedure

1. Install the OpenStack client:

   ```
   sudo apt install python3-openstackclient
   ```

   Note

   A different command is required if you are not running Ubuntu.

2. Import the image:

   ```
   sudo tar --sparse -zxvf <file_name>
   openstack image create --private --disk-format raw --container-format bare
          --file <file_name>  <image_name>
   ```

3. Specify the metadata:

   ```
   openstack image set <image_name> --property hypervisor_type=kvm
   openstack image set <image_name> --property hw_disk_bus=ide
   openstack image set <image_name> --property hw_vif_model=virtio
   openstack image set <image_name> --property hw_vif_multiqueue_enabled=true
   ```

4. Install the Heat client:

   ```
   sudo apt install python3-heatclient
   ```

   Note

   A different command is required if you are not running Ubuntu.

5. (Optional) Set the parameters as defaults within the HEAT orchestration Template (HOT):

   ```
   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 8 GB 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.

   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.

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
      - Low
      - Medium
      - High

admin_password:
  type: string
  label: Admin Password
```

```
    description: Password for the admin user
    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_EULA_accept = true
            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]}
```

Note

To access the vTPS using a serial connection, add `com_tippingpoint_Console = serial` below the `com_tippingpoint_EULA_accept = true` setting.

6. Create the stack:

```
openstack stack create -t /file/path/<heat_template> <Stack_Name> \
--parameter vtps_image_id=<image_id>                               \
--parameter vtps_instance_type=<flavor_id>                         \
--parameter private_net_vtps_mgmt=<network_id>                     \
--parameter private_net_vtps_trust=<network_id>                    \
--parameter private_net_vtps_untrust=<network_id>                  \
--parameter admin_username=<admin_username>                        \
--parameter admin_password_security_level=<None,Low,Medium,High>  \
--parameter admin_password=<admin_password>                        \
--parameter admin_ssh_key=<admin_keypair>                          \
--parameter instance_license=<license_string>
```

To get the parameters, use the following commands:

```
image_id = openstack image list
flavor_id = openstack flavor list
network_id = openstack network list
```

Deploy the TippingPoint vTPS on OpenStack using the GUI

Before you begin

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:

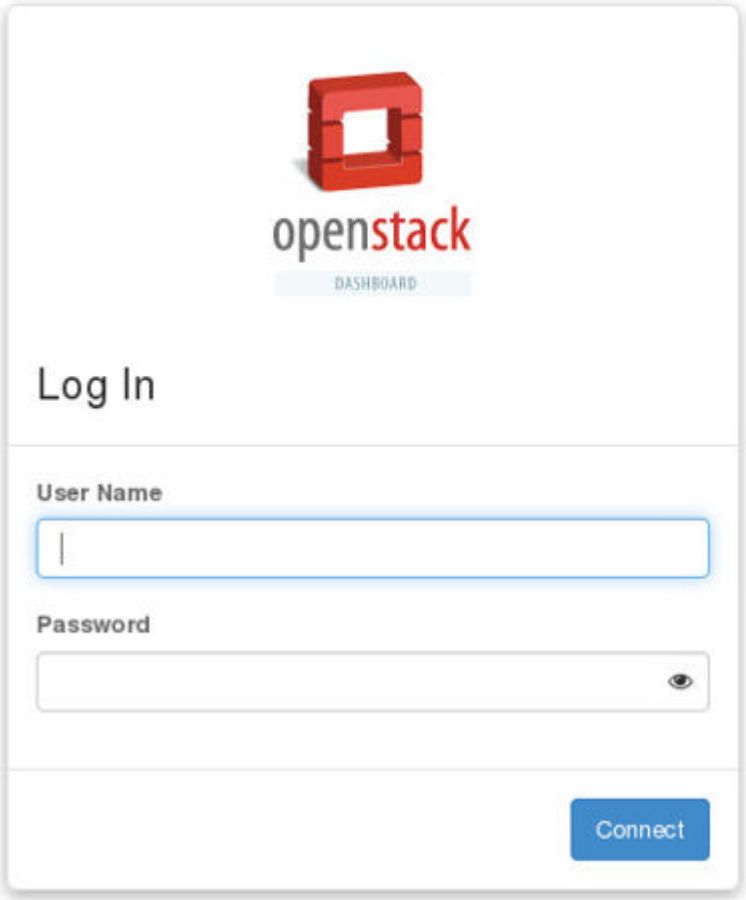
```
[libvirt]
virt_type = kvm
cpu_mode = passthrough
disk_prefix = hd
```

- 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).

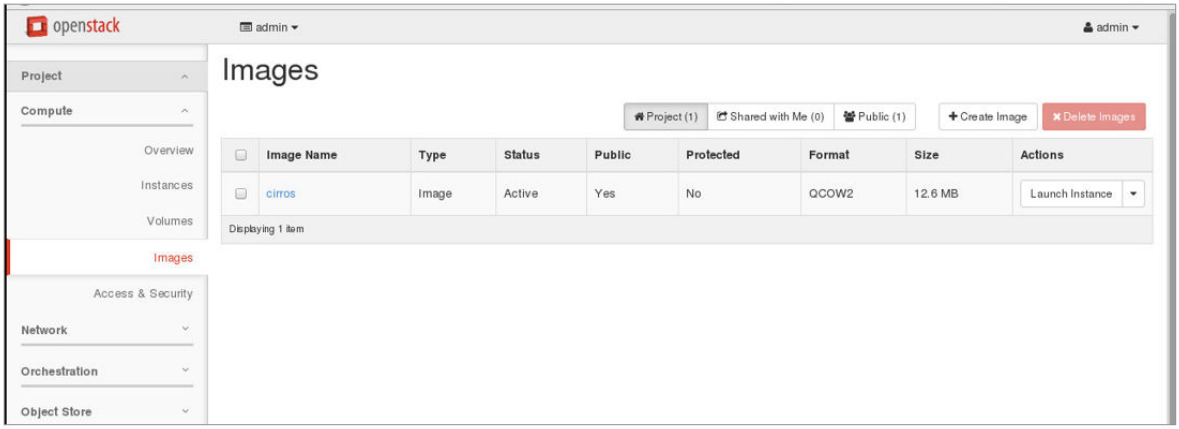
Procedure

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

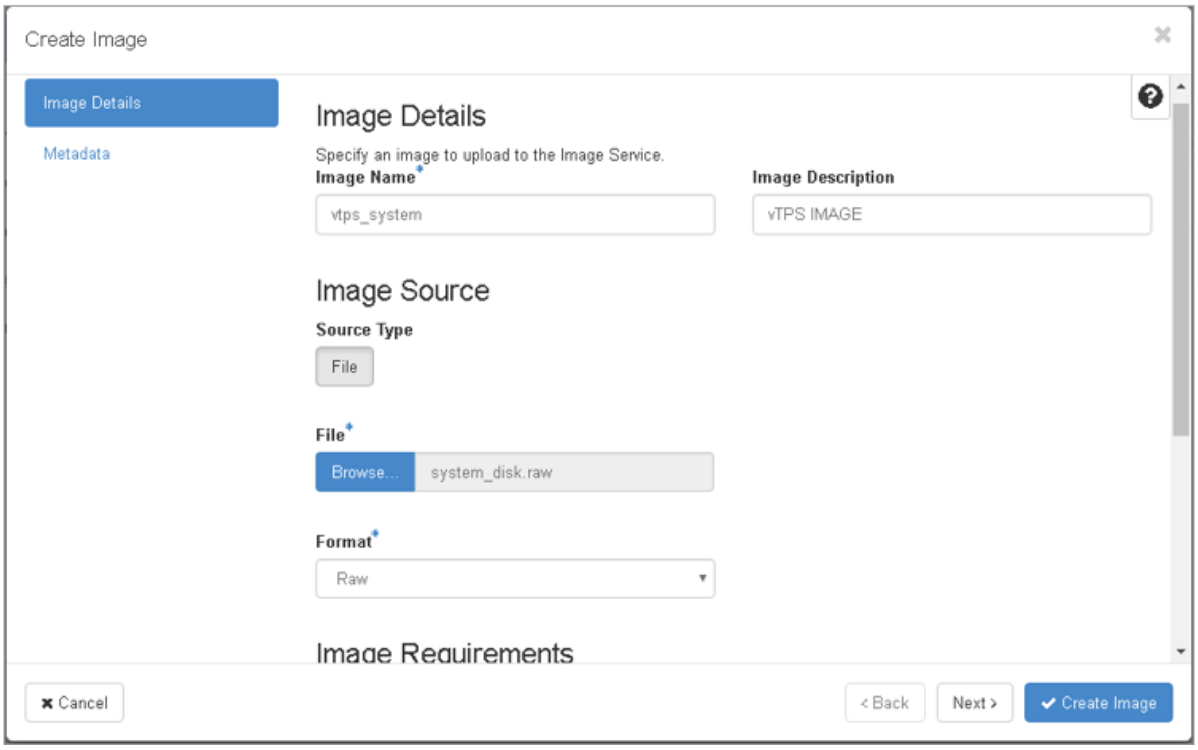


2. Add vTPS images to Horizon.

   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.



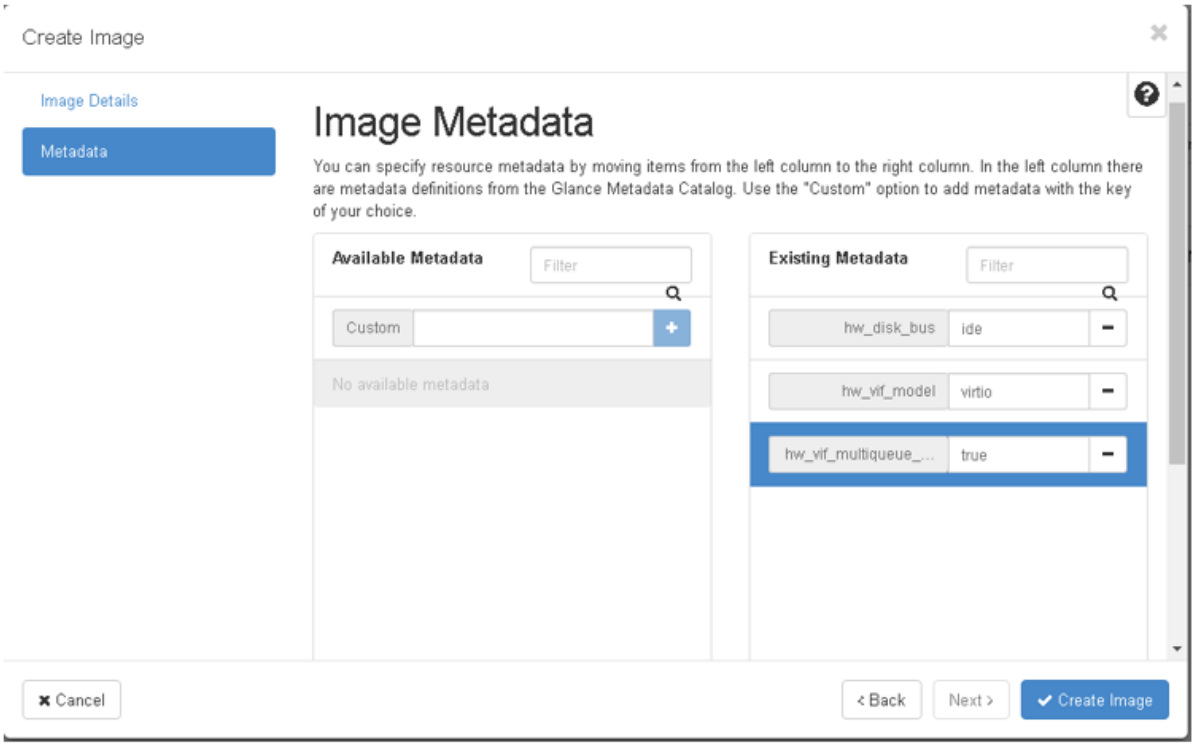
   b. In the Create Image screen, fill in the details for the system disk and select the vTPS system disk image.



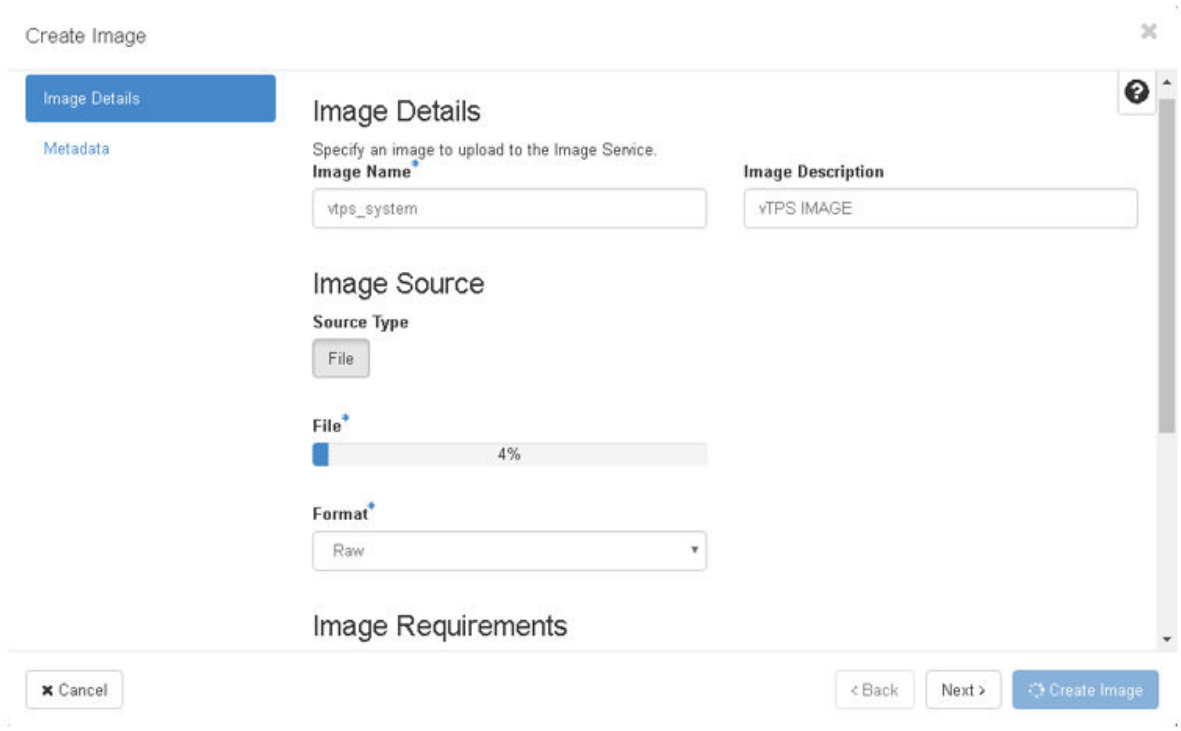
   c. Click the **Create Image** button.

   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_enabled` value (required for a 3-core image). Click **Create Image**.



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



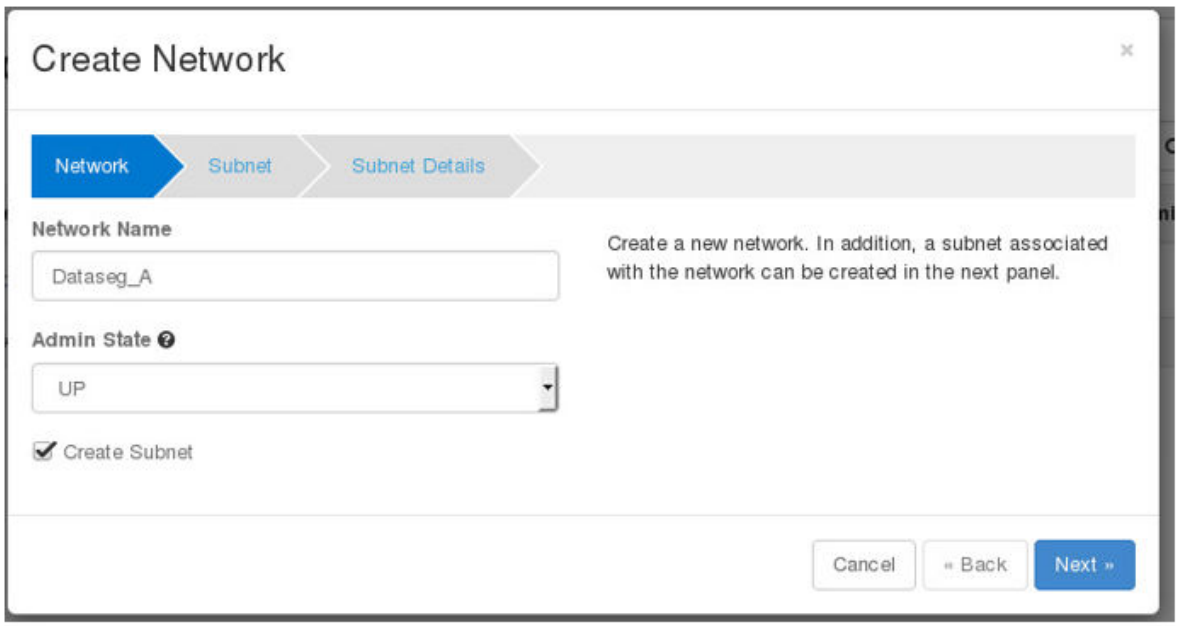
After the images are added, you can view them by selecting **Compute > Images**.

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

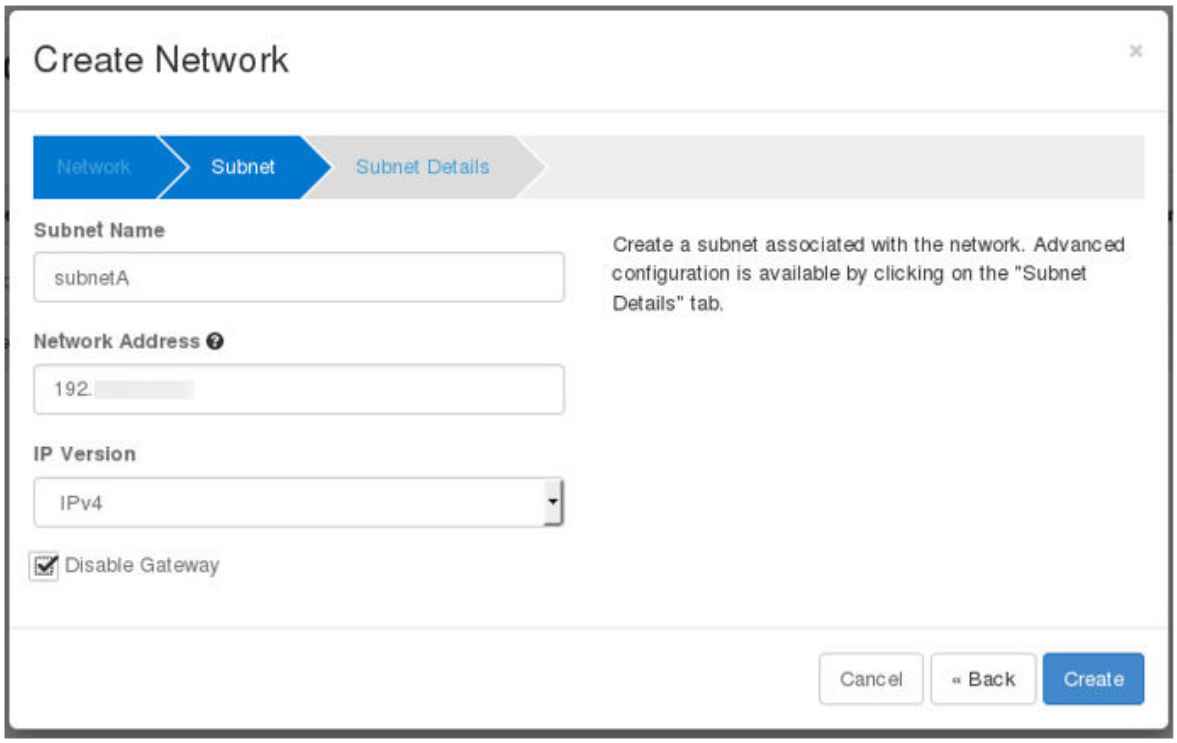
Note

The public subnet for the management network should already exist.

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



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

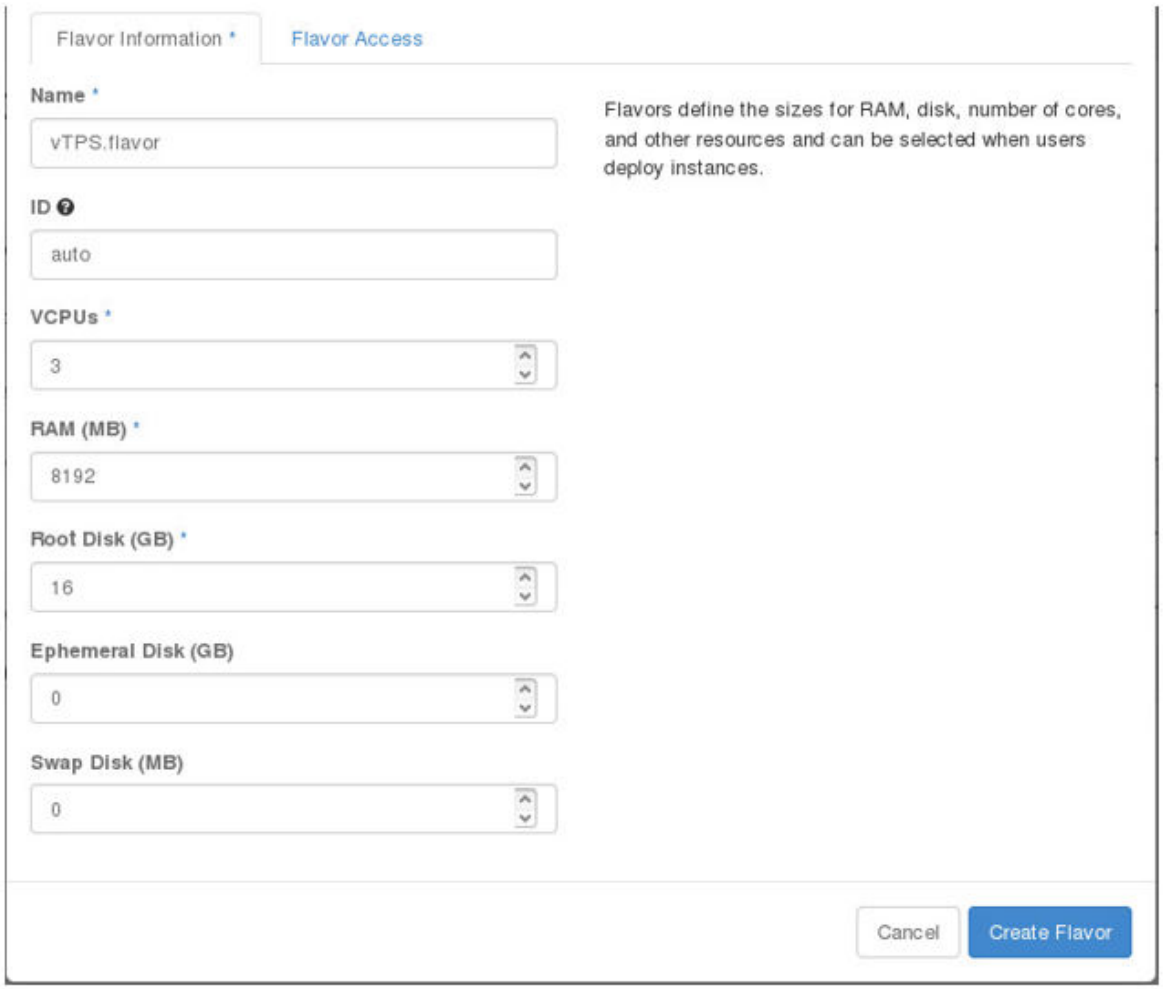


b. Repeat the preceding substeps accordingly to specify details for the second data port and subnet.

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

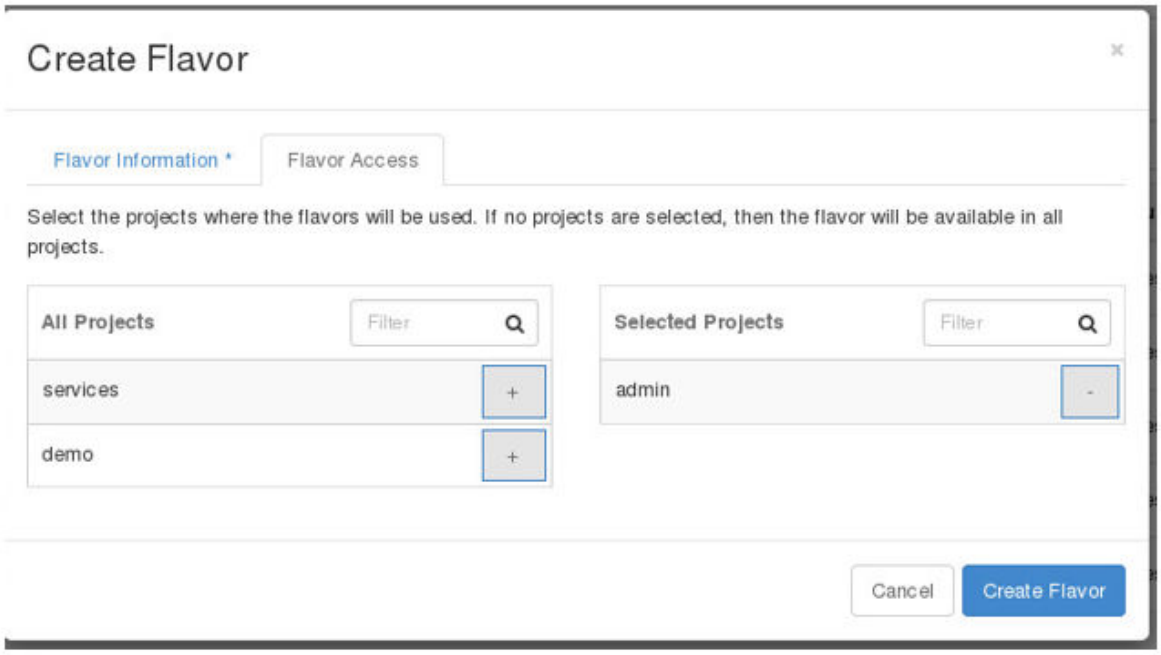
4. Select **Admin > System > Flavors** to create a vTPS flavor.

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



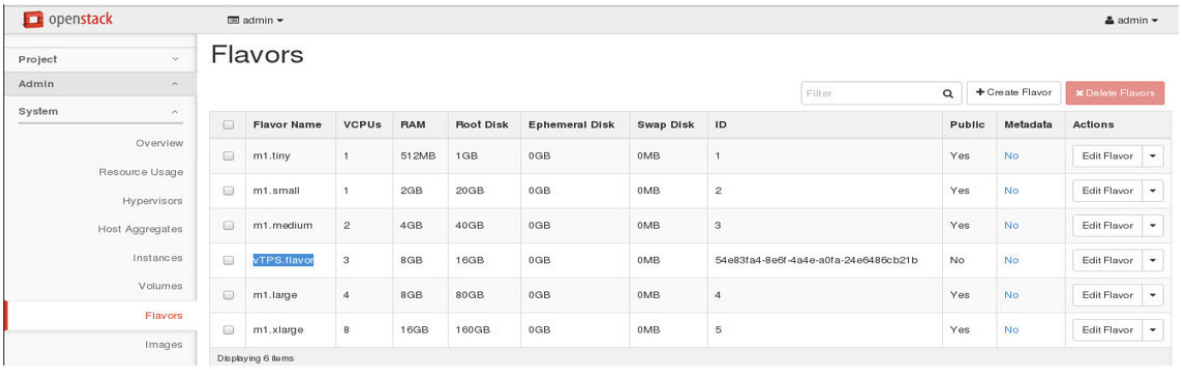
b. In the Flavor Access tab of the Create Flavor dialog, specify the access privileges for the flavor according to the needs of your project.

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

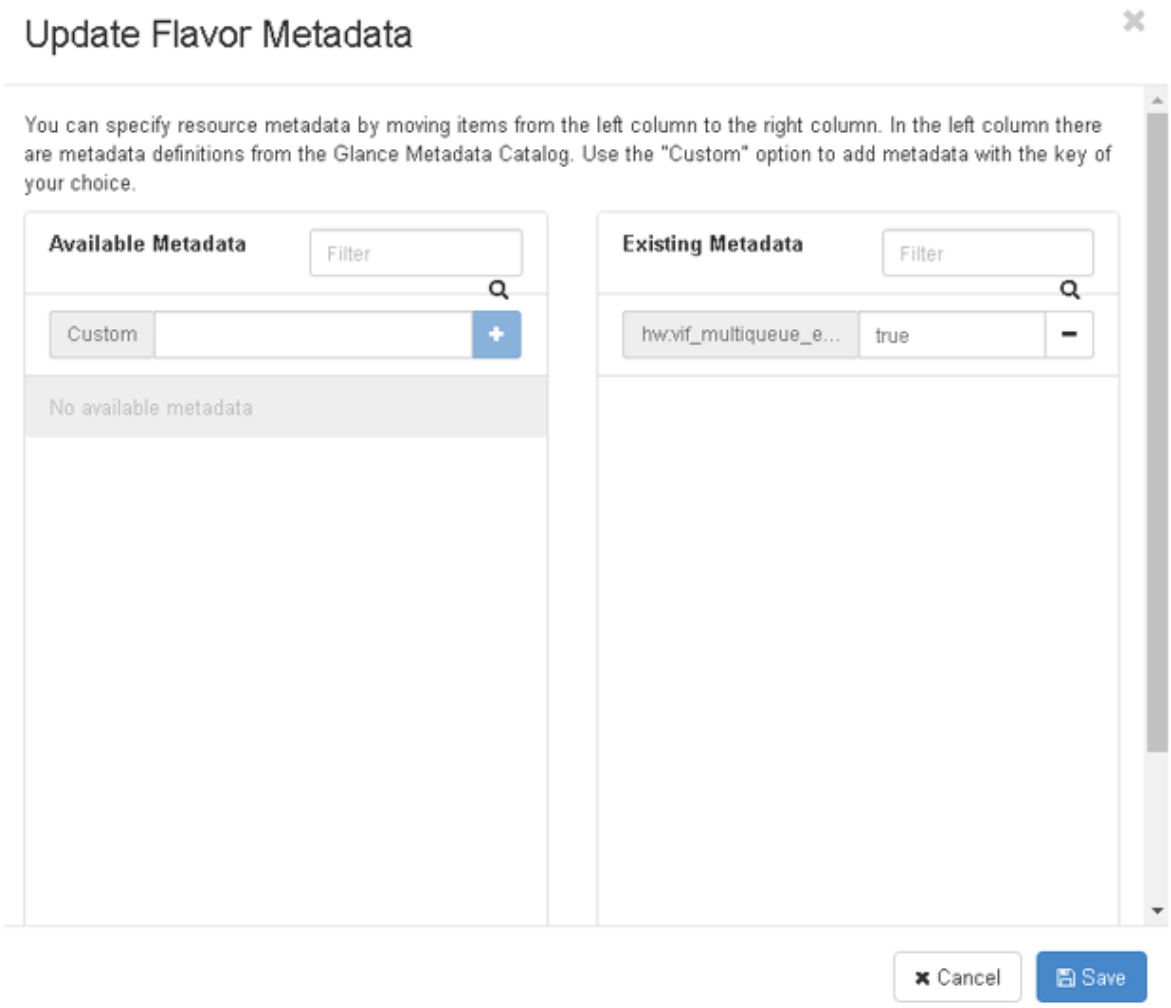


c. After you specify all details of the flavor, click **Create Flavor**.

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



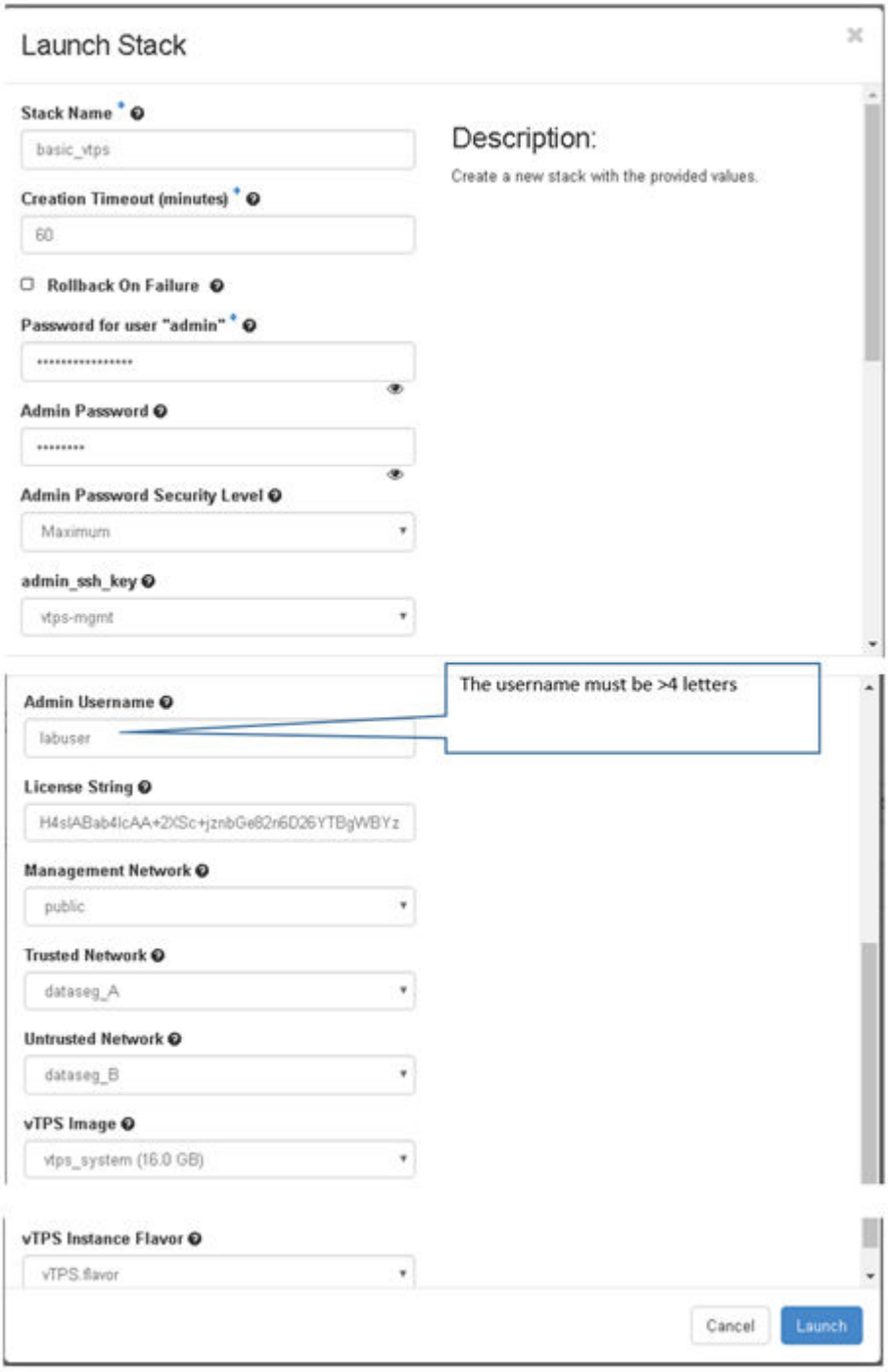
e. Click the down arrow next to **Edit Flavor** to set the `hw:vif_multiqueue_enabled` metadata as `True` for the flavor. This update is necessary for 3-core images.



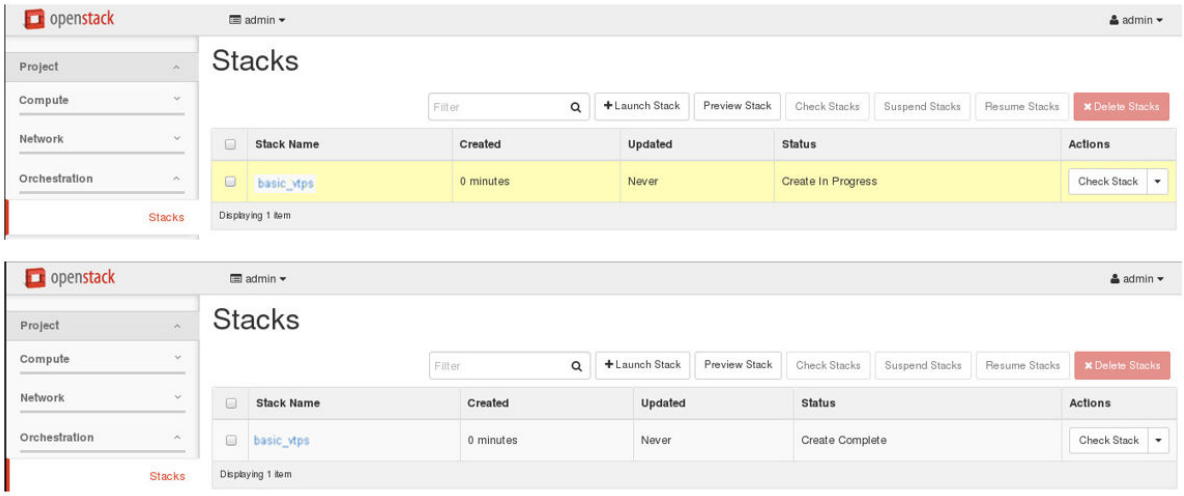
f. Click **Save**.

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**.

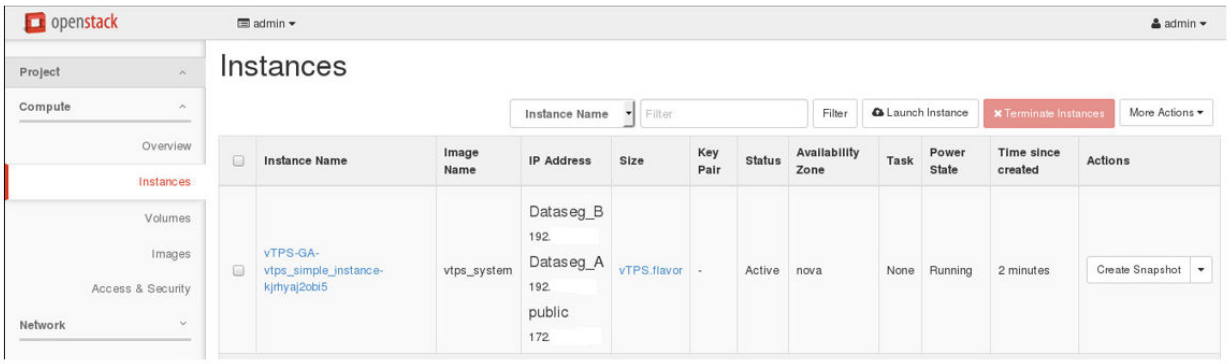
b. Specify the details for the stack, including appropriate values for the network, image, and flavor, and click **Launch**.



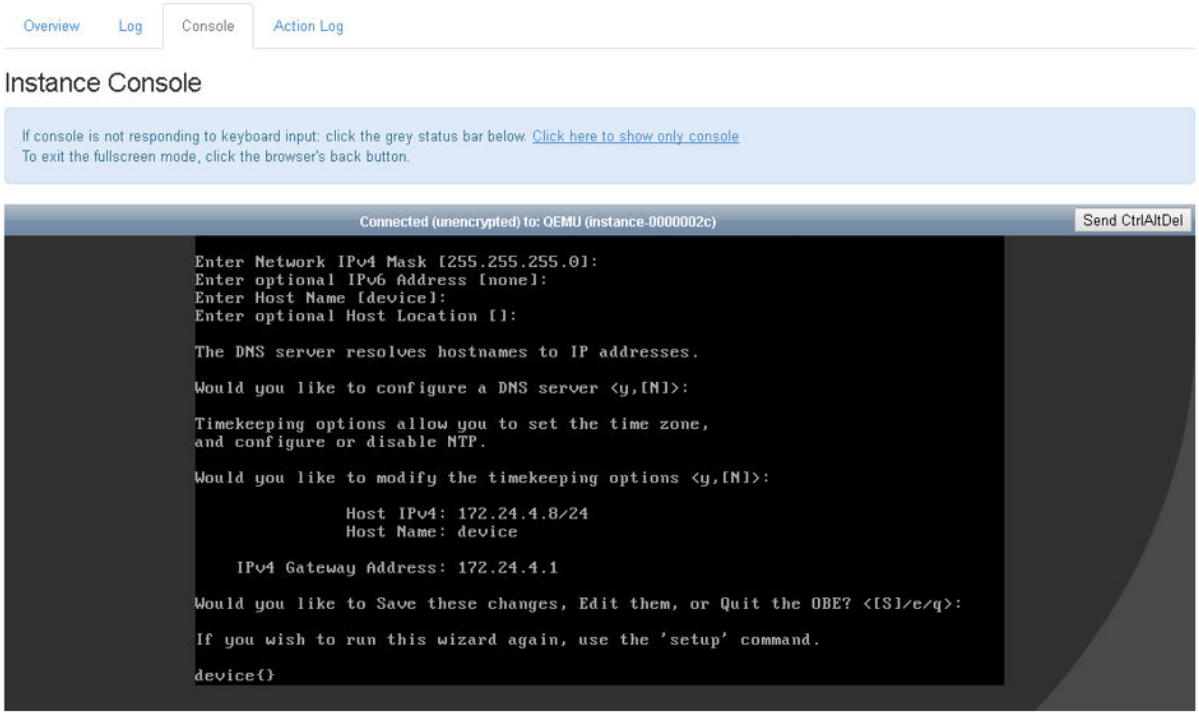
c. Confirm the creation status of the stack by selecting **Orchestration > Stacks**.



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



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



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.

Note

The vTPS virtual appliance does not support a hitless reboot or hitless upgrade. Traffic flow is interrupted until the boot sequence completes because, unlike on a TPS device, the network ports on a vTPS virtual appliance are virtual.

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 Normal image 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 8 GB 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.

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.

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
      - Low
      - Medium
      - High

admin_password:
  type: string
  label: Admin Password
  description: Password for the admin user
  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_EULA_accept = true
            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 virtual appliance from Trial Mode to vTPS Standard Mode, install the license entitlement package and the license certificate package. You can purchase a license through your regular sales channel.

The vTPS virtual appliance remains in Trial Mode until you install a valid certificate. The Trial Mode vTPS comes with limited feature capabilities. After you install a certificate, the vTPS virtual appliance deploys in Standard Mode, and the capabilities purchased with the license package are activated.

When the vTPS virtual appliance upgrades to Standard Mode, you can install your Digital Vaccine package.

Learn more about how to install the license entitlement package, create, download, and install the license certificate package, and install your Digital Vaccine package:

- *Install your license entitlement package*
- *Create and download vTPS virtual appliance license certificates*
  - *Install the vTPS license certificate using the LSM*
  - *Install the vTPS license certificate using the SMS client*
- *Install a Digital Vaccine package*

Install your license entitlement package

Note

If your vTPS virtual appliance is managed by an SMS, you can configure the SMS to automatically retrieve and distribute the most current license entitlement package. Learn more from the *SMS User Guide*.

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

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

Create and download vTPS virtual appliance license certificates

Use the following information to create a vTPS license certificate using the license manager. The license certificate package assigns a purchased inspection throughput license to a vTPS virtual appliance. After you create a vTPS license certificate, install the certificate on the vTPS virtual appliance.

To create a vTPS device license certificate

Procedure

1. Open the license manager.

   To access the license manager, navigate to **My Account** > **License Manager** on the TMC.

2. From the License Management page of the license manager, click **Create vTPS Licenses**.

3. (Optional) If you want to add SSL inspection to a vTPS device, but SSL is disabled, apply for SSL compliance.

   There are four states of SSL compliancy; Unknown, Pending, Compliant, and Non-Compliant. Before you enable SSL, the SSL compliancy state is set at Unknown.
   Complete the following steps to apply for SSL compliance:

   a. Next to **Your SSL is disabled**, click **Apply Now**.

   b. Fill out the Apply for SSL Compliance page.

   c. Click **Apply**.

      After you click **Apply**, the SSL compliance state changes to Pending. When the application process is completed, the state changes to either Compliant if SSL is approved or Non-Compliant if SSL is not approved.

      If you are SSL Compliant, SSL inspection is enabled on all of your vTPS virtual appliances.

4. Under **Action**, select the number of vTPS certificates that you want to create.

5. Click **Create**.

After the vTPS certificate is created, use the SMS client or LSM to install the certificate to a vTPS virtual appliance.

Important

If you do not use an SMS or if your SMS is not connected to the TMC, you must manually download and install the vTPS certificate package. After you download the vTPS certificate package, you can manually install the package from the SMS client or LSM.

To download the vTPS certificate package

Procedure

1. In the license manager, click **Download Cert**.

2. Select **vTPS Cert** from the drop down options.

   The vTPS Certificate Package page is displayed on the TMC.

3. Click **Download**.

4. Accept the EULA Agreement.

5. Save the vTPS certificate file to a local folder.

Install the vTPS license certificate using the LSM

Procedure

1. Download the vTPS license certificate package from the license manager.
2. Log in to the LSM on your vTPS virtual appliance.
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 vTPS license certificate package and click **Install**.
6. After the license certificate package is installed, click **OK** to reboot your device.

Note

The vTPS virtual appliance does not support a hitless reboot or hitless upgrade. Traffic flow is interrupted until the boot sequence completes because, unlike on a TPS device, the network ports on a vTPS virtual appliance are virtual.

The device starts up in Standard Mode.

Install the vTPS license certificate using the SMS client

Procedure

1. Ensure that the vTPS virtual appliance is managed by the SMS.
2. In the SMS client, navigate to the Devices workspace.
3. Right-click on the appropriate vTPS virtual appliance in **All Devices**, and then click **Edit** > **Install Certificate...**, which opens the **vTPS License Installation Wizard**.
4. Select an available vTPS certificate from the drop-down list to install on your vTPS virtual appliance.

   The certificates are grouped by type (speed, capabilities, expiration date) and quantity. After you select a certificate, the certificate ID is displayed.
5. Select one of the following options:
   - **Download from TMC** — The SMS automatically downloads the selected certificate from the TMC. The SMS must be connected to the TMC to use this option.
   - **Import file** — Import a locally saved certificate file to the SMS. If you select this option, you must first manually create and download the appropriate certificate file from the license manager.
6. After you select either **Download from TMC** or **Import file**, click **Next**.
   - If you selected **Download from TMC**, and if the download of the certificate file succeeds, the **Certificate Validated** page is displayed. Proceed to step 9.

> **Note**
>
> If the automatic download from the TMC fails, the **Manual Certificate Import** page is displayed with an error message. Retry the automatic TMC download or click **Next** to import the certificate file manually.

- If you selected **Import file**, the **Import Certificate File** page is displayed. Proceed to step 7.

7. On the **Import Certificate File** page, click **Browse**.
8. Select the appropriate certificate file that you created and downloaded in the license manager, and then click **Import**.

> **Note**
>
> If you select the incorrect certificate file, the **Certificate Validation Failed** page is displayed. Click **Previous** to go back to the **Import Certificate File** page, and then upload a different certificate file.

When the import of the certificate file succeeds, the **Certificate Validated** page is displayed.

9. On the **Certificate Validated** page, click **Finish**.

The SMS installs the license certificate package on the vTPS virtual appliance. You can view the progress of the installation on the **Distribute to Device** dialog.

The vTPS virtual appliance automatically reboots after installation of the license certificate on the device succeeds. After the reboot, the new license certificate capabilities activate on the vTPS virtual appliance.

> **Note**
>
> The vTPS virtual appliance does not support a hitless reboot or hitless upgrade. Traffic flow is interrupted until the boot sequence completes because, unlike on a TPS device, the network ports on a vTPS virtual appliance are virtual.

Install a Digital Vaccine package

> **Note**
>
> If you use an SMS to manage your vTPS virtual appliance, you can configure the SMS to automatically retrieve and distribute the most current Digital Vaccine package each week. Learn more about how to configure this from the *SMS User Guide*.

While in Trial Mode, your vTPS virtual appliance has a base Digital Vaccine 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 Digital Vaccine package.

Learn more about installing your Digital Vaccine package from your LSM and SMS documentation.

Troubleshooting tips

Before contacting support, check to see if the following troubleshooting tips address your issues.

Difficulty logging in to the vTPS LSM

Resolution: Be sure to correctly map your network adapters so that you can access your vTPS virtual appliance 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: You must configure a vTPS virtual appliance in promiscuous (port-mirroring) mode for Layer 2 routing. If a vTPS virtual appliance 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 virtual appliance does not support VMware vMotion, you can emulate a vMotion configuration by connecting two or more different hosts with two or more vTPS virtual appliances that are actively connected to the distributed vSwitch. The vTPS virtual appliance that is connected to the active VM acts as an IPS, and the vTPS virtual appliance that is not connected to the VM acts as an IDS. If you connect your SMS to both vTPS instances, the SMS will also receive any blocks and alerts.

KVM deployment does not boot

Resolution: Ensure that you have all of the Ethernet ports configured. If you install your VM without the correct number of inspection ports, you must either delete the VM and reinstall it or perform a `debug factory-reset`. If you delete and reinstall the VM, you must be sure to also delete the `system_disk.raw` file. You can then re-extract the file from the KVM `tar.gz` image file.

KVM deployment does not pass traffic

Resolution: If a bridge learns that the source and destination MAC addresses are on the same external port, it stops sending packets to all the VMs. Disable address learning to enable promiscuous mode for Layer 2 routing so that your bridges can properly forward all packets to all the VMs. To disable address learning, set the ageing time to `0` for your bridges:

```
# brctl setageing <bridgeA> 0
# brctl setageing <bridgeB> 0
```

To prevent a reboot from overriding this setting, add the following line to the `ifcfg` file for the bridge:

```
AGEING=0
```

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. Learn more about resource pools.

Errors after Suspend and Resume operation

Resolution: Ignore HEALTH-ALERT errors generated after a Suspend and Resume operation.

Examining OpenStack HEAT template events

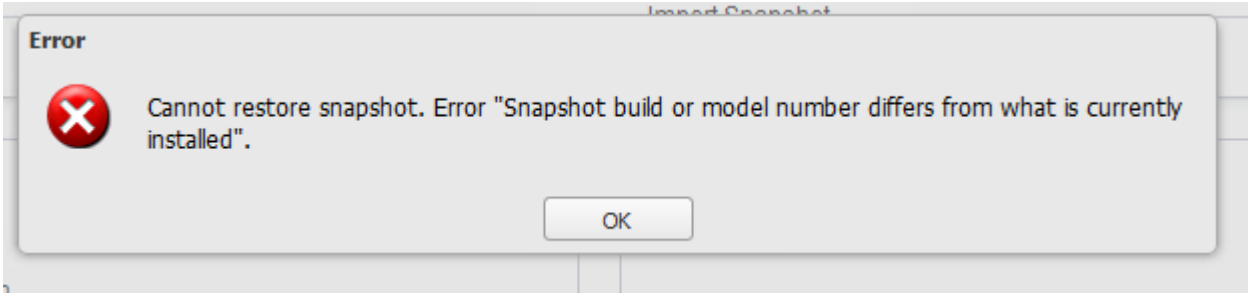
Resolution: Use the `heat event-list <name of stack>` command to see a list of events.

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 redeploy the vTPS virtual appliance.

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.



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 virtual appliance 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 that you properly configure three standard vSwitches or distributed vSwitches 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 virtual appliance performance as much as 20 percent in a KVM deployment.

Resolution: Make sure you enable port groups in promiscuous mode for Layer 2 routing. Ensure that you set any Forged Transmits and MAC Address Changes to ACCEPT so that network packets can get forwarded.

Resolution: Confirm that you have configured each vTPS device with its own data port group. Using the same vSwitches across multiple vTPS virtual appliances 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 virtual appliance. Before the console completes the change from VGA to Serial, the appliance reboots a second time automatically.

> **Note**
>
> The vTPS virtual appliance does not support a hitless reboot or hitless upgrade. Traffic flow is interrupted until the boot sequence completes because, unlike on a TPS device, the network ports on a vTPS virtual appliance are virtual.

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*. Specify the `com_tippingpoint_Console = serial` option in the `vtps-env.txt` file.

After you specify the serial console, enter the following to access the console from the KVM host:

```
virsh console <VM_NAME>
```

KVM also supports several alternative serial console modes, including TCP, UDP, and UNIX. For these options, use `virt-manager` to delete the existing serial device and add a different type. Learn more from the virtualization administrative guides for KVM or RedHat.