Pulse Secure®

PCS/PPS

Virtual Appliance Deployment Guide

Published Date	**April 2019**
Document Revision	**3.0**

Pulse Secure, LLC

2700 Zanker Road, Suite 200
San Jose, CA 95134

https://www.pulsesecure.net/

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

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

PCS/PPS Virtual Appliance Deployment Guide

Printed in USA.

Revision History

Document Version	Revision Summary
3.0	Updated the "Hardware and Software Requirements" section Updated the "Supported Features on Virtual Appliances" section
2.1	Replaced SPE with PSA-V
2.0	Updated the "Deploying PSA-V Image Using Virt-Manager" section
1.0	Initial Release

Contents

About This Guide

Related Documentation and Release Notes

For a list of related Pulse Connect Secure documentation, see
https://www.pulsesecure.net/techpubs/pulse-connect-secure/pcs

If the information in the latest release notes differs from the information in the documentation, follow the *Pulse Connect Secure Release Notes*.

For a list of related Pulse Policy Secure documentation, see **https://www.pulsesecure.net/techpubs/pulse-policy-secure/pps**

If the information in the latest release notes differs from the information in the documentation, follow *the Pulse Policy Secure Release Notes*.

To obtain the most current version of all Pulse Secure technical documentation, see the product documentation page at **https://www.pulsesecure.net/techpubs/**

Document Conventions

Table 1 defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser Warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure, LLC has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: **https://www.pulsesecure.net/support**

- Search for known bugs: **https://www.pulsesecure.net/support**

- Find product documentation: **https://www.pulsesecure.net/techpubs/**

- Find solutions and answer questions using our Knowledge Base:
  https://www.pulsesecure.net/support

- Download the latest versions of software and review release notes:
  https://www.pulsesecure.net/support

- Search technical bulletins for relevant hardware and software notifications:
  https://www.pulsesecure.net/support

- Open a case online in the CSC Case Management tool: **https://www.pulsesecure.net/support**

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool:
https://www.pulsesecure.net/support

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at **https://www.pulsesecure.net/support**

- Call 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see
https://www.pulsesecure.net/support

7

PART 1 Virtual Appliances

- **CHAPTER 1 Virtual Appliances Overview**

- **CHAPTER 2 Deploying Virtual Appliances on VMware ESXi Through vCenter Using OVF Properties**

- **CHAPTER 3 Using NETCONF Perl Client to Configure the Virtual Appliance**

- **CHAPTER 4 Deploying Pulse Virtual Appliance on Kernel-Based Virtual Machine**

- **CHAPTER 5 Deploying Pulse Virtual Appliance on Hyper-V**

CHAPTER 1 Virtual Appliances Overview

Running Pulse Connect Secure or Pulse Policy Secure software in a VMware virtual machine as a virtual appliance provides service providers with robust scalability and isolation. The server software from VMware supports several virtual machines on a high-end multiprocessor platform. Deploying a dedicated virtual appliance for each customer guarantees complete isolation among systems.

- **Virtual Appliance Editions and Requirements**
- **Supported Features on Virtual Appliances**
- **Virtual Appliance Package Information**
- **PSA-V Virtual Appliance Utility Scripts**
- **Clustering Support for Virtual Appliances**
- **Cluster and License Support Combination**

Virtual Appliance Editions and Requirements

Two types of virtual appliances are available:

- Demonstration and Training Edition (DTE)
- PSA-V Edition

The DTE is targeted at demonstration, initial evaluation, and training purposes. DTE is not a supported product; Pulse Secure Support will not assist you with any questions or problems. If you are interested in the DTE, contact your Pulse Secure sales team or reseller.

PSA-V is targeted at service providers who are interested in provisioning a remote access solution for a large number of customers.

Hardware and Software Requirements

Table 2 and Table 3 list the virtual appliance systems qualified with this release.

Table 2: VMware Qualified System

VMware Tools Version	vCenter/ESXi Version	Qualified Pulse Connect Secure and Secure Access System Versions	Qualified Pulse Policy Secure and Access Control System Versions	Hardware Requirements
10.2.0	ESXi 6.7	9.0R3 and 9.0R4	9.0R3 and 9.0R4	ESXi 6.7 requires a host machine with: • At least two CPU cores • Requires the NX/XD bit to be enabled for the CPU in the BIOS. • Requires a minimum of 4 GB of physical RAM. It is recommended to provide at least 8 GB of RAM to run virtual machines in typical production environments. • Support for hardware virtualization (Intel VT-x or AMD RVI) must be enabled on x64 CPUs. Refer here for more details on VMware qualified system.
10.2.0	ESXi 6.5	9.0R3	9.0R3	
9.4.0	ESXi 6.5	9.0R1	9.0R1	
9.4.0	ESXi 6.5	8.3R3	5.4R3	

VMware Tools Version	vCenter/ESXi Version	Qualified Pulse Connect Secure and Secure Access System Versions	Qualified Pulse Policy Secure and Access Control System Versions	Hardware Requirements
9.4.0	ESXi 5.5, 5.5 U3 ESXi 6.0	8.2	5.3	
9.4.0.25793	4.1U3 5.5	8.1 8.0R5 7.4R10	5.1 5.0R5 4.4R10	

> (i) **Note:** VMware's HA feature is qualified; VMware's DRS & Fault Tolerance features are not qualified.

> (i) **Note:**
>
> PCS 9.0R3 supports OVF version 10 (pre-9.0R3 supported OVF version 7). It can be deployed only on ESXi 5.5 and later.

Table 3: KVM Qualified System

QEMU/KVM Version	Qualified Pulse Connect Secure and Secure Access System Versions	Qualified Pulse Policy Secure and Access Control System Versions	Hardware Requirements
QEMU emulator version 2.9.0	9.0R1	9.0R1	Linux Kernel 2.6.32(64-bit) and later
QEMU emulator version 2.9.0	8.3R3	5.4R3	Linux Kernel 2.6.32(64-bit) and later
QEMU emulator version 2.3.0	8.2	5.3	Linux Server Release 6.4 on an Intel Xeon CPU L5640 @ 2.27GHz NFS storage mounted in host 24GB memory in host
v1.4.0	8.1 8.0R5 7.4R10	5.1 5.0R5 4.4R10	

ⓘ   **Note:**

   PCS 9.0R3 supports "virtio" as a default disk driver.

Table 4: Hyper-V Qualified System

QEMU/KVM Version	Qualified Pulse Connect Secure and Secure Access System Versions	Qualified Pulse Policy Secure and Access Control System Versions	Hardware Requirements
Microsoft Hyper-V Server 2012R20	9.0R1	9.0R1	64-bit processor with second-level address translation (SLAT). VM Monitor Mode extensions Memory of at least 4 GB of RAM. Virtualization support turned on in the BIOS or UEFI. For more details refer here.
Microsoft Hyper-V Server 2012R20	8.3, 8.2R5	5.4, 5.3R5	64-bit processor with second-level address translation (SLAT). VM Monitor Mode extensions Memory of at least 4 GB of RAM. Virtualization support turned on in the BIOS or UEFI. For more details refer here.

Upgrading from a Previous Version

If you are upgrading the Pulse Connect Secure software on your PSA-V virtual appliance from a version earlier than 7.2 and if VMware high availability (HA) is configured with the VMware VM Monitoring feature, you must change the **das.minUptime** value in the HA configuration to 600 seconds. If you use the default value of 120 seconds, you will encounter problems during the post-installation processing.

Supported Features on Virtual Appliances

All features of Pulse Connect Secure and Pulse Policy Secure are available on virtual appliances with the exception of the following:

- Instant Virtual System (IVS)

An option is available for switching between a virtual terminal and a serial console. Switching between these options requires a restart of the virtual appliance.

Virtual appliances do not allow licenses to be installed directly on them. As such, virtual appliances can be only license clients. All virtual appliance licenses are subscription-based.

We recommend you use the same NTP server for the virtual appliance and the license server to keep the times synchronized. When synchronizing with an NTP server, the **Synchronize quest time with host** option in the VMware vSphere Client user interface must be enabled. On the virtual appliance, select **Edit Settings > Options > VMware Tools** to set this option.

Virtual appliances support the following SCSI controller types:

- BusLogic

- LSI Logic Parallel (default)

- LSI Logic SAS

vSphere users can select the SCSI controller type by opening their Virtual Machine Properties window, clicking the Hardware tab and then double-clicking the SCSI Controller entry.

Virtual Appliance Package Information

The PSA-V downloadable zip contains the following files:

- README-scripts.txt— Up-to-date information on the contents of the zip file and how to run the scripts.

- PSA-V-VMWARE-PCS-64003.5-VT-disk1.vmdk—A virtual disk file that contains the Pulse Connect Secure or Pulse Policy Secure software. The VT version assumes using a virtual terminal to set up the initial network configuration.

- PSA-V-VMWARE-PCS-64003.5-VT.ovf—An OVF specification that defines the virtual appliance and contains a reference to the disk image.

- create-va.pl—A script for deploying a virtual appliance connected to the VMware vCenter Server.

- va.conf—A sample configuration file for use with the create-va.pl script.

- perlclient/plugin/ive.pm—A side file for configuring virtual appliances through NETCONF.

- perlclient/plugin/ive_methods.pl—A side file for configuring virtual appliances through NETCONF.

- perlclient/examples/get_active_users.pl—A script used to get the current active users on the PSA-V virtual appliance. Cannot be used for configuring the PSA-V virtual appliance.

- perlclient/examples/get_active_users.xsl—A file used for formatting and displaying the output returned by get_active_users.pl.

- perlclient/examples/get_active_users.xml—A file used for formatting and displaying the output returned by get_active_users.pl.

- edit_config_ive.pl–-A Perl script for editing the PSA-V virtual appliance configuration.

The DTE downloadable zip contains the following files:

- README-DTE.txt—A quick start guide for the PSA-V virtual appliance.

- VA-DTE-*release-buildnumber*-VT-disk1.vmdk—A virtual disk file that contains the Pulse Connect Secure or Pulse Policy Secure software. The VT version assumes using a virtual terminal to set up the initial network configuration.

- VA-DTE-*release-buildnumber*-VT.ovf—An OVF specification that defines the virtual appliance and contains a reference to the disk image.

For Pulse Connect Secure, the virtual appliance is delivered in OVF and is preconfigured as follows:

- 40-GB virtual disk
- 2 virtual CPU
- 2-GB memory
- Three virtual network interfaces
- Roughly 400 MB in size

For Pulse Policy Secure, the virtual appliance is delivered in OVF and is preconfigured as follows:

- 40-GB virtual disk
- One virtual CPU
- 2-GB memory
- Three virtual network interfaces
- Roughly 400 MB in size

You can change this configuration by editing the OVF prior to importing it or by editing the virtual machine properties once it is created.

(i)   **Note:** When customizing the configuration, do not reduce the disk size.

Pulse Connect Secure version 7.3 and later and Pulse Policy Secure version 4.3 and later use VMware OVF version 7. This is the preferred version. Virtual appliances created with versions prior to Pulse Connect Secure version 7.3 and Pulse Policy Secure version 4.3 use VMware OVF version 4. To upgrade to VMware OVF version 7, you must run Pulse Connect Secure version 7.3 or later or Pulse Policy Secure version 4.3 or later.

The OVF specification defines three logical networks:

- Internal Network
- External Network
- Management Network

When importing the OVF file, these three networks must be mapped to the appropriate virtual networks on the ESXi server.

When the virtual appliance is powered on for the first time, it expands the software package and performs the installation. After creating a fully installed and configured PSA-V virtual appliance, clone it to a template and export that template. From the template, you can then instantiate additional PSA-V virtual appliances.

(i)   **Note:** Source Network names are not retained in the exported OVF template.

Once configured, you can use any of the following methods to manage the Pulse Connect Secure and Pulse Policy Secure portion of the virtual appliance:

- Pulse Secure's Device Management Interface (DMI)

ⓘ **Note:** The inbound DMI listens to port 830 on both the internal and management interfaces.

- Pulse Connect Secure or Pulse Policy Secure admin console
- Pulse Connect Secure or Pulse Policy Secure serial and virtual terminal console menus

The DMI is an XML-RPC-based protocol used to manage Pulse Secure appliance. This protocol allows administrators and third-party applications to configure and manage Pulse Secure appliance bypassing their native interfaces. Virtual appliances are compliant with DMI. By default, the inbound DMI is enabled in virtual appliances.

Related Documentation

- **DMI Solutions Guide**

PSA-V Virtual Appliance Utility Scripts

Several utility scripts are included with the PSA-V virtual appliance package. These scripts assist with:

- Deployment
- Initial setup of the PSA-V virtual appliance
- Configuring the PSA-V virtual appliance

You can configure your network with your own set of tools. However, be aware that using tools such as vApp lists options in a different order than what you would see during a typical Pulse Connect Secure or Pulse Policy Secure initial configuration session. As such, even though the scripts included in the PSA-V package are optional, we recommend you use them.

The scripts are divided into the following sets:

- Deploy the virtual appliance in the VMware vSphere environment on the ESXi hypervisor through vCenter using OVF properties.

  Use this script if you are using VMware vCenter Server and VMware ESXi for deploying the virtual appliance. This script can be used on both Virtualization Technology and serial editions of virtual appliances.

- Deploy the virtual appliance in the VMware vSphere environment using a serial port.

  If you are using VMware ESXi to run the virtual appliance, you can use these scripts for deployment. These scripts use the service console of ESXi and can be used only with the serial edition of virtual appliances.

- Use NETCONF Perl client to configure the virtual appliance.

  Plug-in and sample scripts for NETCONF Perl client can be used to configure the virtual appliance after it is deployed and powered on. The scripts use DMI for connecting to Pulse Connect Secure or Pulse Policy Secure on port 830.

- Deploy the virtual appliance on KVM.

  Use this script if you are using a kernel-based virtual machine (KVM) for deploying the virtual appliance.

Related Documentation

- **Overview of Deploying Virtual Appliances on VMware ESXi**
- **Using the PSA-V Sample Scripts**

Clustering Support for Virtual Appliances

From 9.0 onward, the clustering feature has been enabled on PSA-V in both the active-passive and active-active modes. Admins can now configure clustering settings similar to what is available on the hardware. VA-DTE already supports clustering and is limited to three users. PSA-V supports only two node cluster for both AP and A/A modes. The cluster works with both CONSEC and named user licenses. PSA-Vs will continue to dynamically lease licenses from a license server. The supported scale numbers on AP and A/A cluster will be available during GA time.

The supported platforms are:

- VMWare ESXi
- KVM
- Hyper-V
- Azure
- AWS

Cluster and License Support Combination

On Hypervisors the VA PCS cluster and VLS are supported. The table below provides the combination of cluster and license support

Sl. No	Hypervisors	Cluster AA	Cluster AP	VLS Standalone support	License server HA
1	VMware – ESXi	Yes	Yes	Yes	Yes
2	KVM	Yes	Yes	Yes	Yes
3	Hyper-V	Yes	Yes	Yes	Yes
4	Azure	Yes	NA*	Yes	NA*
5	AWS	Yes	NA*	Yes	NA*

* - this is due to limitations in AWS and Azure

ⓘ **Note:** Cluster needs to be formed with similar number of core nodes. Clusters which are formed with dissimilar number of cores/CPUs are not supported.

CHAPTER 2 Deploying Virtual Appliances on VMware ESXi Through vCenter Using OVF Properties

- **Overview of Deploying Virtual Appliances on VMware ESXi**

- **Using the Deployment Script to Define the Initial Configuration Parameters**

- **Verifying Your Deployment with vmware-cmd**

Overview of Deploying Virtual Appliances on VMware ESXi

VMware ESXi, like VMware ESXi, is a hypervisor that installs on top of a physical server and partitions it into multiple virtual machines. VMware ESXi does not contain the ESXi's service console and thus is a smaller footprint.

When first powering on the Pulse Connect Secure or Pulse Policy Secure, an administrator must wait for the serial console to appear and manually configure the initial settings. In the case of multiple virtual machines, this process becomes too tedious and time-consuming.

When deploying on a VMware ESXi, the dependencies on a serial console and service console are removed. Pulse Secure lets the administrator set up all initial configuration settings in one pass using a process based on the VMware Guest Customization feature.

With this approach:

1. You use a deployment script and OVF Tools to set up the initial configuration parameters.

2. ESXi passes these parameters into the VMware environment.

3. The virtual appliance retrieves the parameters from the VMware environment and configures the initial settings.

Related Documentation

- **Using the Deployment Script to Define the Initial Configuration Parameters**

- **Verifying Your Deployment with vmware-cmd**

Using the Deployment Script to Define the Initial Configuration Parameters

A **create-va.pl** script is included in your PSA-V package and is used to deploy a virtual appliance connected to the VMware vCenter Server. This script can be run on any system that has Perl and VMware OVF Tools installed.

Configuration parameters can be passed to the script through a configuration file, command-line options, or a combination of the two. Command-line parameters are passed to the scripts using the following format:

- - paramname paramvalue

Type two hyphens without a space between them for the "- -" string. The space shown here is for visual purposes only.

A sample configuration file (**va.conf**) is provided as an example.

Table 5 lists the parameters for **create-va.pl**. Type two hyphens without a space between them for the "- -" string. The space shown here is for visual purposes only.

Table 5: create-va.pl Parameters

vCenter-Related Parameters	
- -vCenterServer	Hostname or IP address of the vCenter Server.
- -vCenterUsername	Username for logging in to the VMware vCenter Server.
- -vCenterPassword	Password for logging in to the VMware vCenter Server. Special characters in the password must be escaped with a backslash (\). For example, **Pulsesecure123\$**
- -datacenterName	Data center under which the Cluster/ESXi Host is present or added.
- -clusterorHostName	Name of the VMware cluster where the virtual appliance is to be deployed. When deploying the virtual appliance in a cluster, this parameter must follow the format cluster-name/ESXi-server-name. For example, **ESXi_5_cluster/mydev.pulsesecure.net.** When deploying the virtual appliance in an ESXi server, this parameter must be following the format ESXI-server-name. For example, **mydev.pulsesecure.net.**
- -datastore	Name of the datastore where the virtual appliance is to be deployed.
- -vaname	Name of the virtual appliance to create.
Pulse Connect Secure and Policy Secure-Related Parameters	
- -vaIPAddress	IP address to assign to the internal port of the Pulse Connect Secure virtual appliance.
- -vaNetmask	Netmask to assign to the internal port of the virtual appliance.
- -vaGateway	Gateway to assign to the internal port of the virtual appliance.
- -vaAdminUsername	Username for the default administrator account for the virtual appliance.
- -vaAdminPassword	Password for the default administrator account for the virtual appliance.
- -vaPrimaryDNS	IP address for the primary DNS server.
- -vaSecondaryDNS	IP address for the secondary DNS server.
- -vaDNSDomain	Domain name for the virtual appliance.
- -vaWINSServer	Windows Internet Name Service (WINS) hostname or IP address.
- -vaCommonName	Common name for the default device certificate.
- -vaOrganization	Organization for the default device certificate.

- -vaRandomText	Random text to use during certificate creation. If spaces are included in the random text, make sure the entire value is enclosed within double-quotes. For example, Pulse Secure Your Net.
- -vaDefaultVlan	Specify Default VLAN ID for the internal interface. Default VLAN ID is an optional parameter. When this parameter is set, all the traffic on this interface subsequently will be tagged with the set VLAN ID and accept only incoming traffic with the same tag. Necessary changes are required on the connected switch port to handle bi-directional tagged traffic.

Virtual Appliance-Related Parameters	
- -ovffile	Path to the OVF file.
- -configFile	Name of configuration files containing parameters to pass to the create-va.pl script. Values specified on the command line override the ones specified in the configuration file.
– -ExternalNetwork	Virtual network in VMware vSwitch to map the external network of the virtual appliance.
- -InternalNetwork	Virtual network in VMware vSwitch to map the internal network of the virtual appliance.
- -ManagementNetwork	Virtual network in VMware vSwitch to map the management network of the virtual appliance.

Virtual Appliance Management Port-Related Parameters	
- -vaManagementIPAddress	Management network IP address.
- -vaManagementNetmask	Management network netmask address.
- -vaManagementGateway	Management network gateway address.
- -vaManagementDefaultVlan	Specify Default VLAN ID for the management interface. Default VLAN ID is an optional parameter. When this parameter is set, all the traffic on this interface subsequently will be tagged with the set VLAN ID and accept only incoming traffic with the same tag. Necessary changes are required on the connected switch port to handle bi-directional tagged traffic
- -vaManagementPortReconfigWithValueInVAppProperties	Management port overwrite property. If set to 1, overwrite the management port-related parameters in the Pulse Connect Secure with the ones defined here. See **Table 6** and **Table 9**.
- -vaInternalPortReconfigWithValueInVAppProperties	The internal por**t** overwrite property. If set to 1, overwrite the virtual appliance's internal port settings with the ones specified during deployment. See **Table 7** and **Table 10**.

Virtual Appliance External Interface Parameters	
- -vaExternalIPAddress	External network IP address.

- -vaExternalNetmask	External network netmask address.
- -vaExternalGateway	External network gateway address.
- -vaExternalDefaultVlan	Specify Default VLAN ID for the external interface. Default VLAN ID is an optional parameter. When this parameter is set, all the traffic on this interface subsequently will be tagged with the set VLAN ID and accept only incoming traffic with the same tag. Necessary changes are required on the connected switch port to handle bi-directional tagged traffic
- -vaExternalPortReconfigWithValueInVAppProperties	External port overwrite property. If set to 1, overwrite the external port-related parameters in Pulse Connect Secure or Pulse Policy Secure with the ones defined here. See **Table 8** and **Table 11**.
New Parameters	
- - vaAcceptLicenseAgreement	By default, this value is set to **y**. This specifies that admin has accepted the EULA.
- -vaEnableLicenseServer	Flag to specify if the Virtual Appliance has to come up as a Normal Virtual Appliance or a Virtual License Server. By default, this value is set to n. If set to **y**, then the Virtual Appliance would function as a Virtual License Server
- -enableRESTAPI	By default, this value is set to **n**. When set to **y**, enables REST access for the admin user created as part of initial config. (Default option is set to disabled)

(i) **Note:** The Pulse Connect Secure and Policy Secure-related parameters are used for the initial configuration of the virtual appliance. The script does not validate these parameters. If the values passed are not valid, the installation will stop at the location where a correct value needs to be provided. The administrator can connect to the virtual appliance using the VT or serial console to complete the initial setup.

Table 6 and **Table 7** define the behavior based on options passed while deploying the template.

Table 6: Management Port Behavior While Deploying a Template

Management Port Overwrite Value	Management Port Configuration Values	Pulse Connect Secure and Pulse Policy Secure Behavior
0	The management port IP address, netmask address and gateway address are valid values.	Because managementPortReconfigWithValueInVAppProperties is 0, the management port-related parameters are retained and are not overwritten with values in the passed configuration.
0	The management port IP address, netmask address and gateway address are not valid values.	Because managementPortReconfigWithValueInVAppProperties is 0, the management port-related parameters are retained and are not overwritten with values in the passed configuration.
1	The management port IP address, netmask address and gateway address are valid values.	You can configure the management port with the new values passed while deploying. The existing cache value is overwritten with new values.

Management Port Overwrite Value	Management Port Configuration Values	Pulse Connect Secure and Pulse Policy Secure Behavior
1	The management port IP address, netmask address and gateway address are not valid values.	During the boot process, the administrator is asked whether to configure the management port. Enter **N** to skip the management port configuration. Enter **Y** to specify valid values for the management port.

Table 7: Internal Port Behavior While Deploying a Template

Internal Port Overwrite Value	Internal Port Configuration	Pulse Connect Secure and Pulse Policy Secure Behavior
0	Valid or invalid configuration	Do nothing. The internal port should already be set in the Pulse Connect Secure or Policy Secure. If the internal port is not configured, prompt the administrator to enter the internal port configuration.
1	Valid configuration	Use the new values passed while deploying and configure the internal port.
1	Invalid configuration	During the boot process, the administrator is asked whether to configure the internal port. Enter **N** to skip the internal port configuration. Enter **Y** to specify valid values for the internal port.

Table 8: External Port Behavior While Deploying a Template

External Port Overwrite Value	Management Port Configuration Values	Pulse Connect Secure and Pulse Policy Secure Behavior
0	The external port IP address, netmask address and gateway address are valid values.	Because externalPortReconfigWithValueInVAppProperties is 0, the external port-related parameters are retained and are not overwritten with values in the passed configuration.
0	The external port IP address, netmask address and gateway address are not valid values.	Because externalPortReconfigWithValueInVAppProperties is 0, the external port-related parameters are retained and are not overwritten with values in the passed configuration.
1	The external port IP address, netmask address and gateway address are valid values.	You can configure the external port with the new values passed while deploying. The existing cache value is overwritten with new values.
1	The external port IP address, netmask address and gateway address are not valid values.	During the boot process, the administrator is asked whether to configure the external port. Enter **N** to skip the external port configuration. Enter **Y** to specify valid values for the management port.

When deploying a new virtual appliance, the Pulse Connect Secure or Pulse Policy Secure does not contain any configuration. The behavior in this case is shown in **Table 9** and **Table 10**.

Table 9: Management Port Behavior During a New Deployment

Management Port Overwrite Value	Management Port Configuration Values	Pulse Connect Secure and Pulse Policy Secure Behavior
0	The management port IP address, netmask address and gateway address are valid values.	Valid management configuration is available. Configure the Pulse Connect Secure or Pulse Policy Secure with these values.
0	The management port IP address, netmask address and gateway address are not valid values.	Invalid management configuration is present. Do not configure the management port properties.
1	The management port IP address, netmask address and gateway address are valid values.	Valid management configuration is available. Configure the Pulse Connect Secure or Pulse Policy Secure with these values. The existing cache value is overwritten with new values.
1	The management port IP address, netmask address and gateway address are not valid values.	During the boot process, the administrator is asked whether to configure the management port. Enter **N** to skip the management port configuration. Enter **Y** to specify valid values for the management port.

Table 10: Internal Port Behavior During a New Deployment

Internal Port Overwrite Value	Internal Port Configuration	Pulse Connect Secure and Pulse Policy Secure Behavior
0 or 1	Valid configuration	Configure the internal port based on the passed configuration values.
0 or 1	Invalid configuration	During the boot process, the administrator is asked whether to configure the internal port.

Table 11: External Port Behavior During a New Deployment

External Port Overwrite Value	External Port Configuration	Pulse Connect Secure and Pulse Policy Secure Behavior
0	The external port IP address, netmask address and gateway address are valid values.	Valid external configuration is available. Configure the Pulse Connect Secure or Pulse Policy Secure with these values.
0	The external port IP address, netmask address and gateway address are not valid values.	Invalid external configuration is present. Do not configure the management port properties.
1	The external port IP address, netmask address and gateway address are valid values.	Valid external configuration is available. Configure the Pulse Connect Secure or Pulse Policy Secure with these values. The existing cache value is overwritten with new values.
1	The external port IP address, netmask address and gateway address are not valid values.	During the boot process, the administrator is asked whether to configure the external port. Enter **N** to skip the external port configuration. Enter **Y** to specify valid values for the external port.

After running the create-va.pl script, you can use the VMware vSphere CLI **vmware-cmd** utility or the VMware vSphere Client to view the status. Once vSphere reports the system is ready, you can log in to the virtual appliance.

> (i) **Note:** The vSphere Client may display a "VMware Tools not installed on this virtual machine" message. You can ignore this message. You do not have to install VMware Tools.

Example Output

The following example passes the IP address of the internal port through the command line and uses the **va.conf** configuration file for the values of all other parameters.

```
perl create-va.pl --configFile /root/user1/ovf_dir//va_config_files/vlan_tagging.conf --ipAddress
3.3.125.3 --extipAddress 2.2.125.3 --mgmtipAddress 10.209.125.3 --vaName 9_0R3_PSA-V_125_3 --ovffile
/root/user1/ovf_dir//PSA-V-VMWARE-PCS-9.0R3-64003.5/PSA-V-VMWARE-PCS-64003.5-VT.ovf
```

Your output will look similar to the following:

```
The following values are used for creating and configuring the VA


        OVF File:                       /root/user1/ovf_dir//PSA-V-VMWARE-PCS-9.0R3-64003.5/PSA-V-
VMWARE-PCS-64003.5-VT.ovf

        VA Name:                        9_0R3_PSA-V_125_3


        vCenter Server:                 qavc.bnglab.psecure.net:443

        vCenter Username:               user1

        vCenter Password:               Psecure123\$


        Datacenter Name:                PBU-QA

        Cluster / Host Name:            PBU-QA-CLUSTER/pbuesx6.bnglab.psecure.net


        IP Address:                     3.3.125.3

        Netmask:                        255.0.0.0

        Gateway:                        3.0.0.1

        Default VLAN:                   3

        Management IP Address:                  10.209.125.3

        Management Netmask:                     255.255.240.0

        Management Gateway:                     10.209.127.254

        Management Default VLAN:                        -1

        External IP Address:            2.2.125.3

        External Netmask:               255.0.0.0

        External Gateway:               2.0.0.1

        External Default VLAN:          2

        Reconfigure Internal Port with value in VAapp properties:               0

        Reconfigure Management Port with value in VAapp properties:             0

        Reconfigure External Port with value in VAapp properties:               0

        Primary DNS:            1.1.1.1

        Secondary DNS:          3.3.115.226

        DNS Domains:            pcsqa.psecure.net

        WINS:                   2.2.2.2

        Admin Username:         admindb

        Admin Password:         dana123

        Enable REST API:                y

        Common Name:            pcs.psecure.net
```

```
        Organization:                 PulseSecure

        Ramdom Text:                  PulseSecure_your_Net

        Accept License Agreement:     y


        Enable Virtual License Server:  n


        ExternalNetwork Mapped to:      "VLAN_TAGGING"

        InternalNetwork Mapped to:      "VLAN_TAGGING"

        ManagementNetwork Mapped to:    "PBU-QA-MGMT"
```

```
Command = ovftool --skipManifestCheck --name=9_OR3_PSA-V_125_3 --
prop:vaIVEConfig="vaIPAddress=3.3.125.3;vaNetmask=255.0.0.0;vaGateway=3.0.0.1;vaDefaultVlan=3;vaMana
gementIPAddress=10.209.125.3

;vaManagementNetmask=255.255.240.0;vaManagementGateway=10.209.127.254;vaManagementDefaultVlan=-
1;vaInternalPortReconfigWithValueInVAppProperties=0;vaExternalIPAddress=2.2.125.3;vaExternalNetmask

=255.0.0.0;vaExternalGateway=2.0.0.1;vaExternalDefaultVlan=2;vaExternalPortReconfigWithValueInVAppPr
operties=0;vaManagementPortReconfigWithValueInVAppProperties=0;vaPrimaryDNS=1.1.1.1;vaSecondar

yDNS=3.3.115.226;vaDNSDomain=pcsqa.psecure.net;vaWINSServer=2.2.2.2;vaCommonName=pcs.psecure.net;vaO
rganization=PulseSecure;vaRandomText=PulseSecure_your_Net;vaAdminUsername=admindb;vaAdminPassw

ord=dana123;vaAcceptLicenseAgreement=y;vaEnableLicenseServer=n;vaAdminEnableREST=y " --
net:ExternalNetwork="VLAN_TAGGING" --net:InternalNetwork="VLAN_TAGGING" --
net:ManagementNetwork="PBU-QA-MGM

T" --datastore=HP_iSCSI_02 --powerOn /root/user1/ovf_dir//PSA-V-VMWARE-PCS-9.0R3-64003.5/PSA-V-
VMWARE-PCS-64003.5-VT.ovf.ovf vi://user1:Psecure123\$@qavc.bnglab.psecure.net:443/PBU-QA/host

/PBU-QA-CLUSTER/pbuesx6.bnglab.psecure.net


Deploying VA. /root/user1 , /root/user1/ovf_dir//PSA-V-VMWARE-PCS-9.0R3-64003.5/PSA-V-VMWARE-PCS-
64003.5-VT.ovf.ovf.......

Status: Task completed
```

Related Documentation

- **Overview of Deploying Virtual Appliances on VMware ESXi**
- **Verifying Your Deployment with vmware-cmd**

Verifying Your Deployment with vmware-cmd

Once deployed, the virtual appliance powers on and configures the initial settings for the Pulse Connect Secure or Pulse Policy Secure using the parameters passed by the **create-va.pl** script. The virtual appliance sets the status of the initial configuration in the **vaInitConfigStatus** guest environment variable. You can check the status of the virtual appliance setup with the VMware vSphere CLI **vmware-cmd** command. Use the following format:

vmware-cmd -H *vCenterName* -h *ESXi-name vm-cfg-path* getguestinfo guestinfo.vaInitConfigStatus

For example:

```
vmware-cmd -H 10.204.54.210 -h asgdevesx2.bngrd.pulsesecure.net \
-U Admin -P Passwd123 "/vmfs/volumes/ds1/SecureAccess/SecureAccess.vmx" \
getguestinfo guestinfo.vaInitConfigStatus
```

Your output should look similar to this:

```
getguestinfo(guestinfo.vaInitConfigStatus) = Status: Success Log: Configuring    VA settings from OVF; Initial
network configuration complete; The self-signed    digital certificate was successfully created; VA Initial
Configuration    completed successfully.
```

> **Note:** You can ignore the following message:
>
> ```
> vmsvc[280]: [warning] [powerops] Unable to send the status RPC
> ```
> This message appears when you are running Pulse Connect Secure release 8.0R5 and later with ESXi 4.1U3 or ESXi4.x and you power off and then power up the virtual appliance.

Related Documentation

- **Using the Deployment Script to Define the Initial Configuration Parameters**

CHAPTER 3 Using NETCONF Perl Client to Configure the Virtual Appliance

NETCONF API is an XML application that client applications can use to exchange information with Pulse Secure products. The purpose of the NETCONF Perl client is to connect and configure the device by establishing a DMI connection and sending specific remote procedure calls (RPCs). Both the general RPCs supported by Pulse Connect Secure and Pulse Policy Secure and the device-specific RPCs can be used. Some of the device-specific RPCs are used to retrieve runtime information and statistics.

The PSA-V package contains a NETCONF plug-in for the virtual appliance and sample Perl scripts. Using the supplied scripts as an example, you can write your own scripts for any DMI RPCs supported by the virtual appliance.

See the *DMI Solution Guide* located on the Pulse Secure Support website.

- **Installing the NETCONF Perl Client**
- **Using the PSA-V Sample Scripts**
- **Enabling the VMXNET3 Driver**

Installing the NETCONF Perl Client

This topic explains how to install the NETCONF Perl client. It includes the following sections:

- **Verifying the Installation and the Version of Perl**
- **Installation of NETCONF Perl Client**

Verifying the Installation and the Version of Perl

Perl must be installed on your system before you install the NETCONF Perl. The NETCONF Perl client requires Perl version 5.6.1 or later. To confirm whether Perl is installed on your system and to determine which version of Perl is currently running, issue the following commands:

$ which perl

$ perl –v

If the issued output indicates that Perl is not installed or that the version is earlier than the required version, you must download and install Perl version 5.6.1 or later in order to use the NETCONF Perl client. The Perl source packages are located at:

http://www.cpan.org/src/

After installing a suitable version of Perl, install the NETCONF Perl client application.

Installation of NETCONF Perl Client

ⓘ **Note:** Installation of Netconf Perl Client is tested on CentOS release 6.4 (Final) 64-bit.

---

1. Install libssh2 from https://www.libssh2.org/ [https://www.libssh2.org/download/libssh2-1.7.0.tar.gz] by executing the following commands:
   ```
   linux# ./configure --prefix=/usr/libssh2
   ```

```
(by default, libssh2 gets installed under /usr/localinclude and /usr/local/bin)

linux# make

linux# make install
```

2. Install Net::SSH2 (http://search.cpan.org/CPAN/authors/id/S/SA/SALVA/Net-SSH2-0.58.tar.gz)

```
linux# perl Makefile.PL lib=/usr/libssh2/lib inc=/usr/libssh2/include ldargs="-lz"

linux# make

linux# make install
```

3. Install CPAN

```
linux# yum install cpan
```

4. Install Netconf from CPAN:

```
linux# cpan Net::Netconf
```

5. Install Term::Readkey from CPAN:

```
linux# cpan Term::ReadKey
```

Related Documentation

- **Using the PSA-V Sample Scripts**

Using the PSA-V Sample Scripts

After you download and install the PSA-V and NETCONF packages, copy the following files to the linux machine where the NETCONF perl client is installed:

```
- get_active_users.pl
- edit_config_ive.pl
```

Using the get_active_users.pl Script

The following example uses admin1 for the username, passwd123 for the password and 10.20.30.40 for the IP address. When run, it connects to the virtual appliance, retrieves the list of active users, and prints it on the Standard Output.

```
perl get_active_users.pl -l admin1 -p passwd123 10.20.30.40
```

Using the edit_config_ive.pl Script

The **edit_config_ive.pl** script is used for editing the PSA-V virtual appliance configuration and has the following syntax:

perl edit_config_ive.pl *options request target*

where:

	One or more of the following:
options	-l login – Login name accepted by the target device. -p password - Password associated with the login name. -m access – The access method. The only supported value is ssh. -d level – Debug level. Values can be 1 (terse) through 6 (verbose).

request	Name of the file containing the configuration in XML format. An example of the contents of a configuration file is:
	
	<configuration>
	    <system>
	    <network>
	    <network-overview>
	    <settings>
	      <node>localhost2</node>
	      <hostname>pcs-hostname.mycompany.com</hostname>
	    </settings>
	    </network-overview>
	    </network>
	    </system>
	    </configuration>

target	Hostname of the target device.

Related Documentation

- **Installing the NETCONF Perl Client**

Enabling the VMXNET3 Driver

To enable the VMXNET3 driver in your virtual appliance, you must deploy from the 7.2 OVF package. Upgrading from earlier versions such as 7.0 or 7.1 will continue to use VMXNET instead of the VMXNET3 driver.

CHAPTER 4 Deploying Pulse Virtual Appliance on Kernel-Based Virtual Machine

- **About a Kernel-Based Virtual Machine**

- **Installing the KVM Modules**

- **Deploying PSA-V Image Using Virt-Manager**

About a Kernel-Based Virtual Machine

Kernel-based Virtual Machine (KVM) is a virtualization solution for Linux on x86 hardware containing Intel VT or AMD-V virtualization extensions. A wide variety of guest operating systems work with KVM, including Linux, Windows, OpenBSD and others. You can run a Pulse Secure virtual appliance as a guest operating system on any Linux machine with KVM hypervisor support.

ⓘ   **Note:** QEMU is an open source emulator that provides a monitor mode when using the KVM kernel module. This monitor mode can perform operations like powering on or off the virtual appliance. If you use this monitor mode to power on or off the virtual appliance, no logs are generated. Only administrators logged into the Pulse Connect Secure or Pulse Policy Secure console are informed of the pending shutdown.

Before proceeding, verify that your CPU supports virtualization by running one of the following commands:

egrep -c '(vmx|svm)' /proc/cpuinfo

cat /proc/cpuinfo | grep vmx

Your CPU supports virtualization if:

- The **egrep** command returns a non-zero value.

- The **cat** command returns a result that contains the string vmx.

You must also check that virtualization is enabled in your BIOS. After enabling this feature, you must turn your machine off and then on again for the change to take effect.

Once your machine reboots, check that everything is configured correctly by running the **kvm-ok** command. Your output should look similar to this:

/usr/bin/kvm-OK

INFO: Your CPU supports KVM extensions

INFO: /dev/kvm exists

KVM acceleration can be used.

Table 12: Number of cores to be allocated to each KVM model.

Platform	Cores Per VM
PSA3000-V	2

Platform	Cores Per VM
PSA5000-V	4
PSA7000-V	8

Limitations

For each KVM virtual appliance instance with 4 GB Memory and 4 CPU allocation, exceeding 5000 tunnels (Network Connect, Pulse Secure client ESP/SSL, or a combination of both) with 60 Mbps of bi-directional traffic may exhibit high CPU utilization and loss of throughput including disruption of the existing connections.

Related Documentation

- **Installing the KVM Modules**
- **Deploying PSA-V Image Using Virt-Manager**

Installing the KVM Modules

This topic describes how to install KVM modules. You can run these commands as root or by using sudo, if sudo is available on your system. The following examples are run as root.

Pulse Secure supports kernel modules version 2.6.18 and later.

To install KVM, run the following commands:

[root@localhost ~]# insmod lib/modules/KernelVersion/kermel/arch/x86/kvm/kvm.ko

[root@localhost ~]# insmod lib/modules/KernelVersion/kermel/arch/x86/kvm/kvm-intel.ko

These commands return no output unless an error has occurred. If an error occurs, details about that error are displayed.

Check that the KVM modules are installed by running the lsmod command. Your output should look similar to this.

[root@localhost ~]# lsmod | grep kvm

kvm_intel   50380 3

kvm   305081 1 kvm_intel

If the KVM modules are not installed, your output will look similar to this:

[root@localhost ~]# lsmod | grep kvm

[root@localhost ~]#

Refer to your KVM documentation if your KVM modules do not install properly.

For the virtual appliance to access the host system's network, set up a bridge interface. The following steps create a bridge interface, br0, and map it to the physical interface eth0 making your virtual appliances accessible from your local network. These instructions assume that your host system has only one network interface, eth0.

ⓘ　　**Note:** Depending on your installation, the bridge-util packages might be installed as part of another package. Check your installation and manually install the bridge-util packages if necessary before continuing.

---

1. Change directory to where the network scripts are located.

    [root@localhost /]# cd /etc/sysconfig/network-scripts/

2. Copy ifcfg-eth0 to ifcfg-br0 to create the bridge interface.

    cp ifcfg-eth0 ifcfg-br0

3. Edit the ifcfg-br0 file and change the DEVICE line to DEVICE="br0" and set TYPE="Bridge".

    [root@localhost network-scripts]# vim ifcfg-br0

    DEVICE="br0"   #Change

    BOOTPROTO="static"

    HWADDR="00:30:48:32:E0:4E"

    NM_CONTROLLED="yes"

    ONBOOT="yes"

    TYPE="Bridge"   #Change

    IPADDR="10.204.56.142"

    NETMASK="255.255.240.0"

    GATEWAY="10.204.63.254"

4. Edit the ifcfg-eth0 file and add BRIDGE="br0".

    [root@localhost network-scripts]# vim ifcfg-eth0

    DEVICE="eth0"

    HWADDR="00:30:48:32:E0:4E"

    NM_CONTROLLED="yes"

    ONBOOT="yes"

    TYPE="Ethernet"

    IPADDR="10.204.56.142"

    NETMASK="255.255.240.0"

    GATEWAY="10.204.63.254"

    BRIDGE="br0"   #Add

5. Apply the new network settings by running the following command.

    [root@localhost /]# /etc/rc.d/init.d/network restart

    Note that the eth0 device will no longer have an IP address; the br0 device has the IP after bridging is operational.

6. Display the current TCP/IP network configurations to confirm the bridge network is created.

[root@localhost /]# ifconfig

An example output is shown here:

```
br0      Link encap:Ethernet  HWaddr 00:30:48:32:E0:4E
         inet addr:10.204.56.142  Bcast:10.204.63.255  Mask:255.255.240.0
         inet6 addr: fdc6:3001:8e20:9ce9:230:48ff:fe32:e04e/64 Scope:Global
         inet6 addr: fe80::230:48ff:fe32:e04e/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:4406929 errors:0 dropped:0 overruns:0 frame:0
         TX packets:1080664 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:4082423409 (3.8 GiB)  TX bytes:158009811 (150.6 MiB)

eth0     Link encap:Ethernet  HWaddr 00:30:48:32:E0:4E
         inet6 addr: fe80::230:48ff:fe32:e04e/64 Scope:Link
         UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
         RX packets:8473303 errors:0 dropped:0 overruns:0 frame:0
         TX packets:2395178 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:8337051743 (7.7 GiB)  TX bytes:247546240 (236.0 MiB)
         Interrupt:18 Memory:d8000000-d8020000

lo       Link encap:Local Loopback
         inet addr:127.0.0.1  Mask:255.0.0.0
         inet6 addr: ::1/128 Scope:Host
         UP LOOPBACK RUNNING  MTU:16436  Metric:1
         RX packets:6617 errors:0 dropped:0 overruns:0 frame:0
         TX packets:6617 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:1594571 (1.5 MiB)  TX bytes:1594571 (1.5 MiB)

virbr0   Link encap:Ethernet  HWaddr 52:54:00:FE:C2:76
         inet addr:192.168.122.1  Bcast:192.168.122.255  Mask:255.255.255.0
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:746 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:0 (0.0 b)  TX bytes:39254 (38.3 KiB)
```
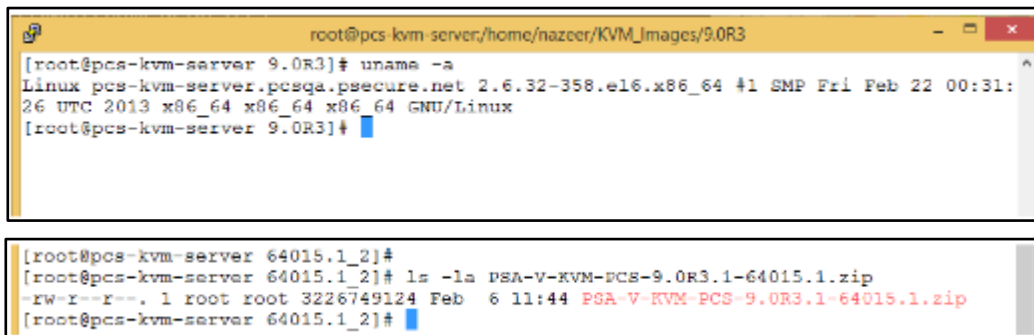
Related Documentation

- **About a Kernel-Based Virtual Machine**

- **Deploying PSA-V Image Using Virt-Manager**

Deploying PSA-V Image Using Virt-Manager

1. Copy **PSA-V -KVM-PCS-<Version No.>.zip** image on KVM Server

2. Unzip the file using the command "unzip PSA-V -KVM-PCS-<Version No.>.zip". This will extract PSA-V -KVM-PCS-<Version No.>-VT-kvm.img.gz along with other files

3. Gunzip the file "PSA-V -KVM-PCS-<Version No.>-VT-kvm.img.gz" using the command "gunzip PSA-V -KVM-PCS-<Version No.>-VT-kvm.img.gz" to get "PSA-V -KVM-PCS-<Version No.>-VT-kvm.img".

4. Use **qemu-img** command as follows: "qemu-img amend -f qcow2 -o compat=0.10 PSA-V -KVM-PCS-<Version No.>-VT-kvm.img".
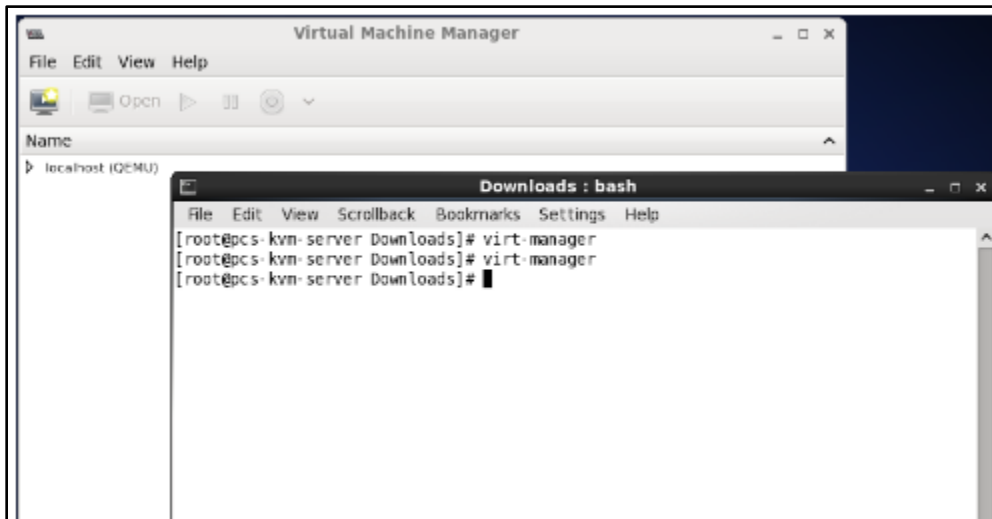
5. Execute **virt-manager** command on KVM server to launch virt-manager.

6. Select **localhost** and click on **New** to deploy KVM PSA-V virtual machine.
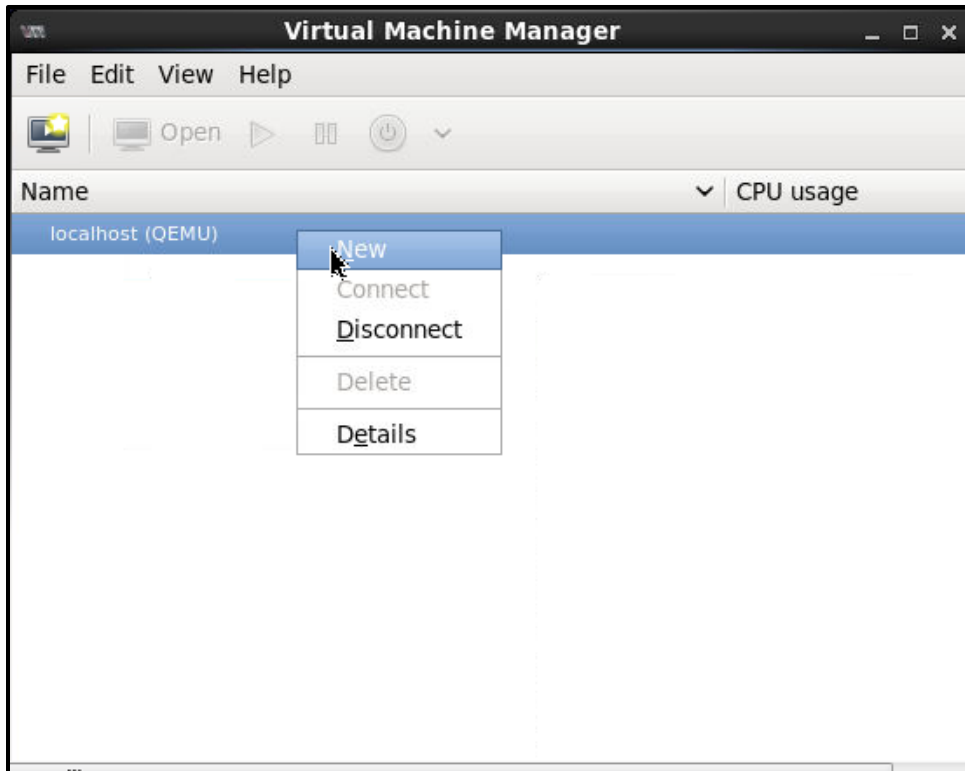
7. Provide name of PSA-V virtual machine and select **Import existing Disk Image** option.
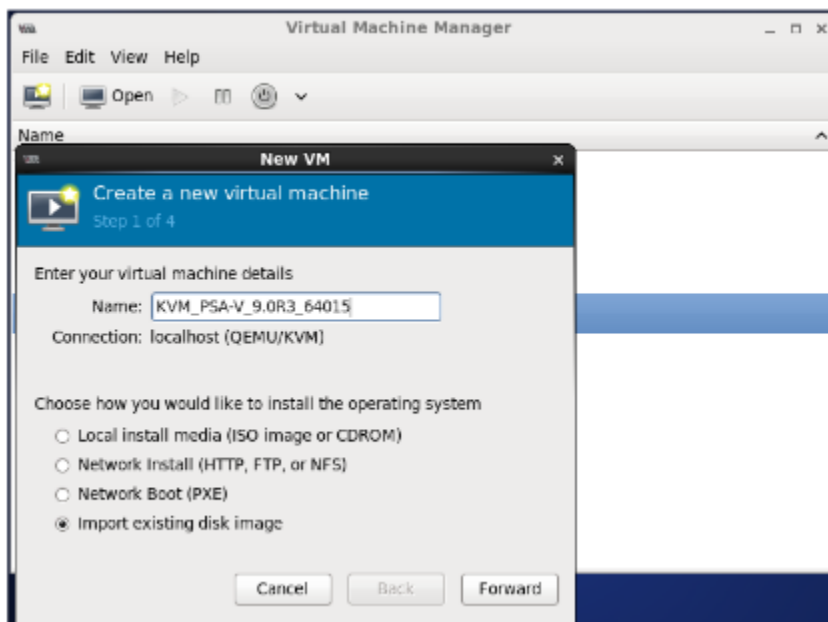
8. Click on **Browse** and select the PSA-V VT image. Click on **Forward** button.
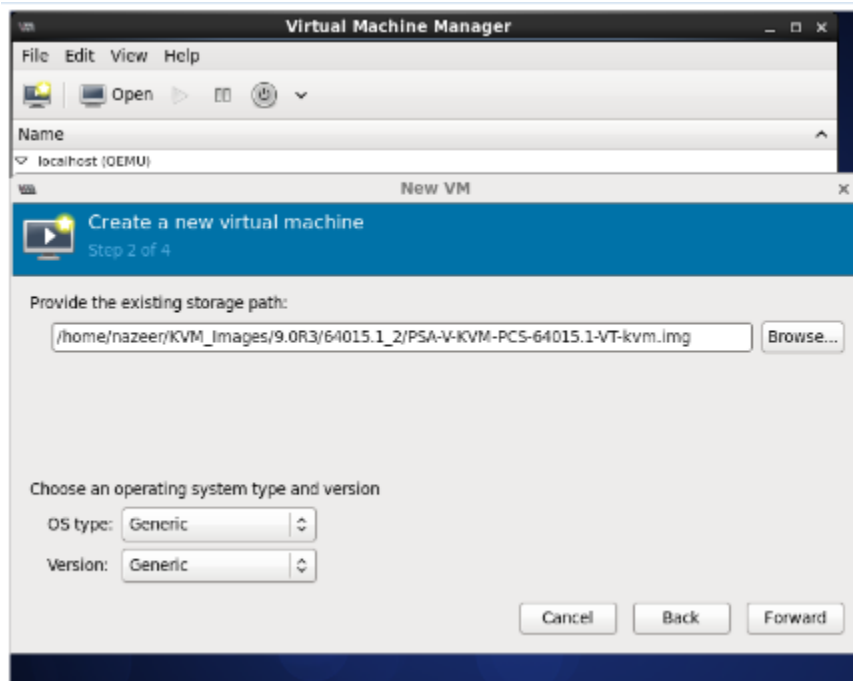
9. Set **Memory** to *2048MB* and **CPUs** to *2*. Click on **Forward** button.
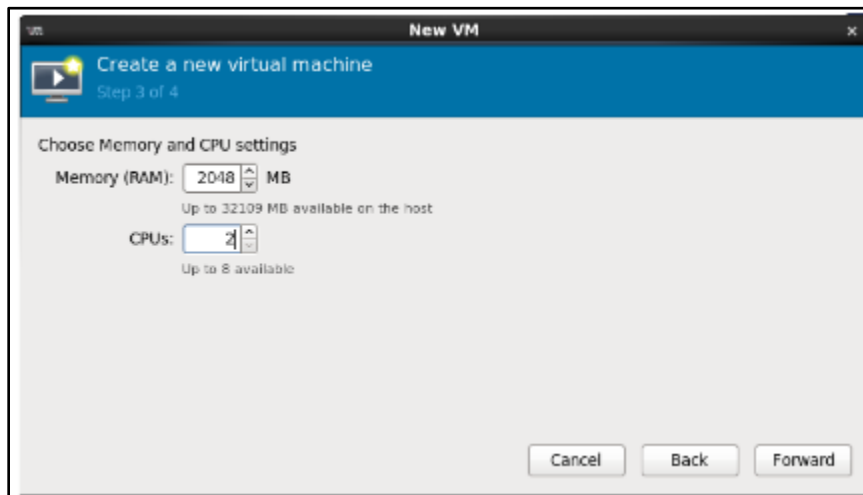
10. Select **Customize configuration before install** and click on **Finish** button.
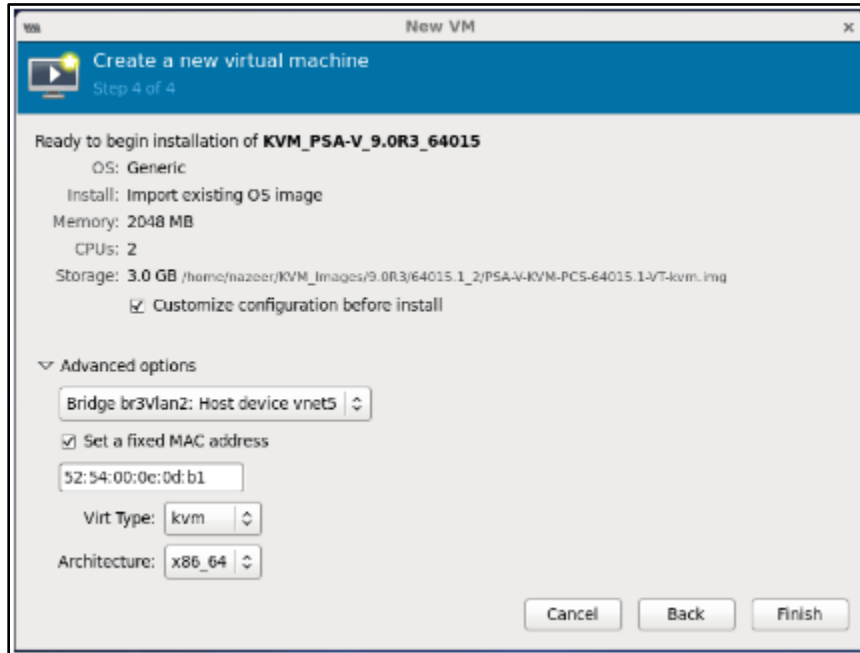
11. The following window appears.
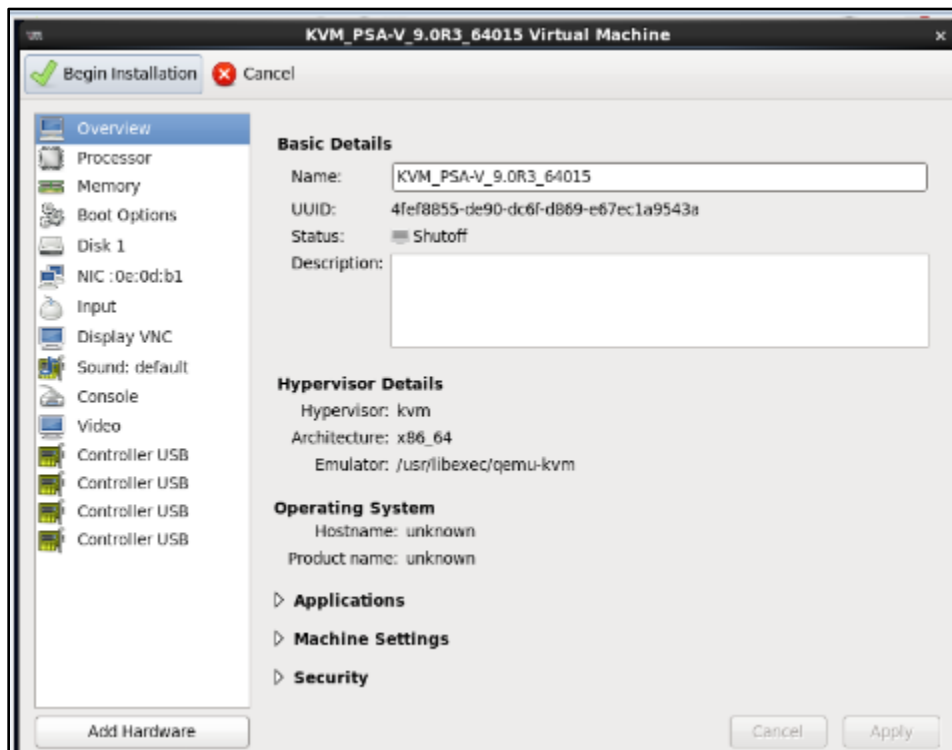
12. Select the NIC Card and set **Device model** to *virtio* (from Hypervisor default). This will be the internal port of the PSA-V.
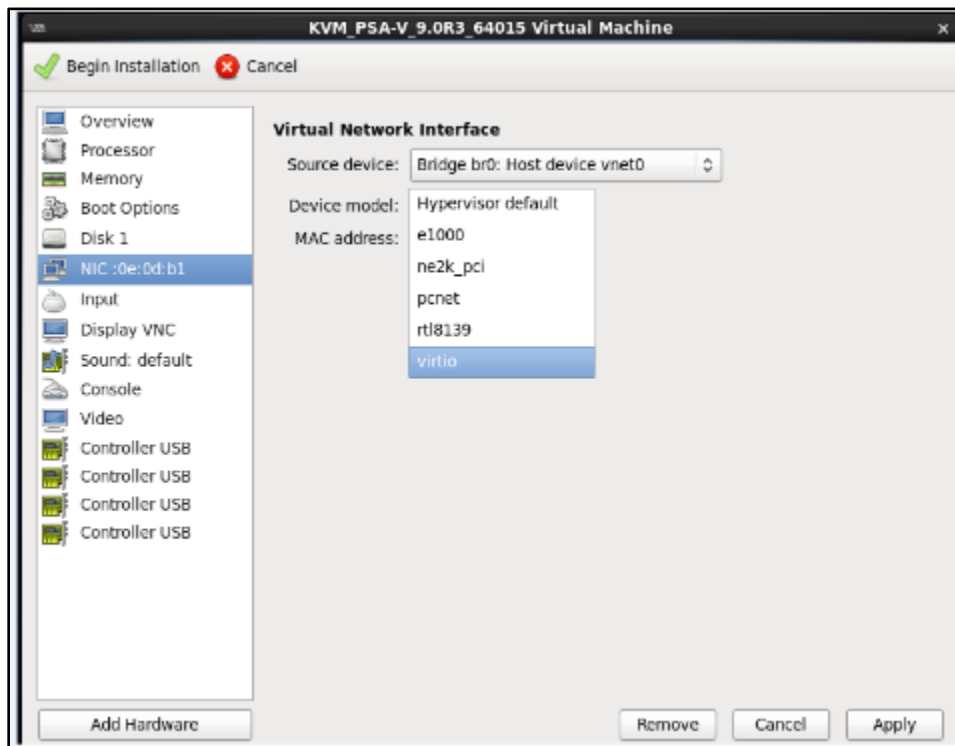
13. Click on **Add Hardware**, select **Network** in the left panel.

    a. Set **Host Device** to the required physical interface.

    b. Set **Device Model** to virtio and click on **Finish**. This will be the external network port.

14. Click on **Add Hardware**, select **Network** in the left panel

   a. Set **Host Device** to the required physical interface

   b. Set **Device Model** to *virtio* and click on **Finish**. This will be the management network port.
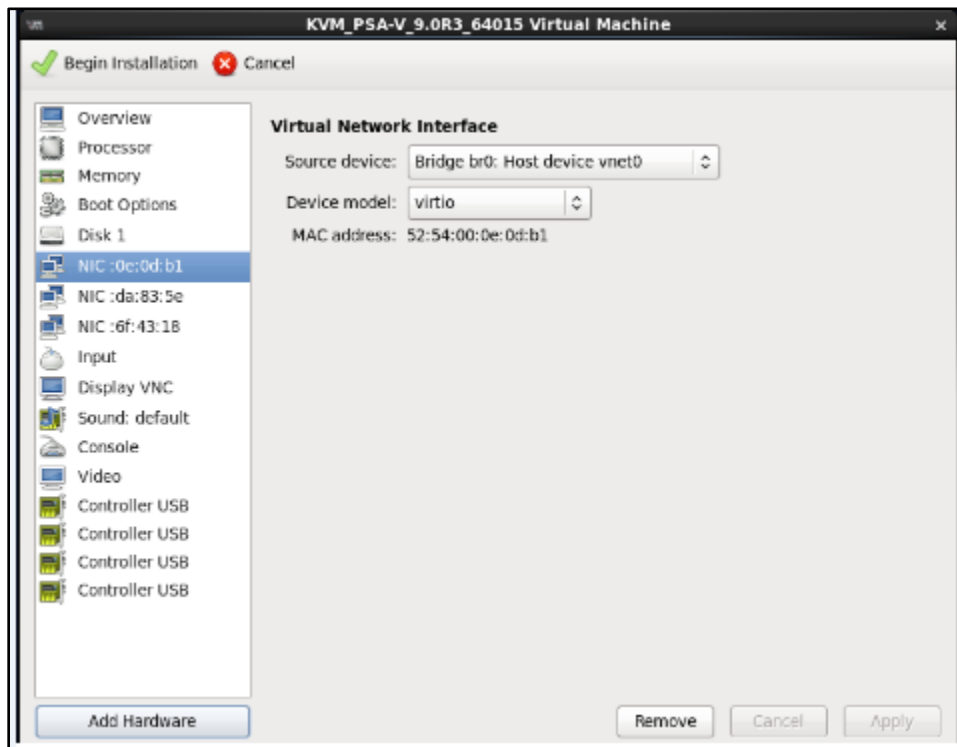
15. Select the **Disk bus** as *Virtio*.
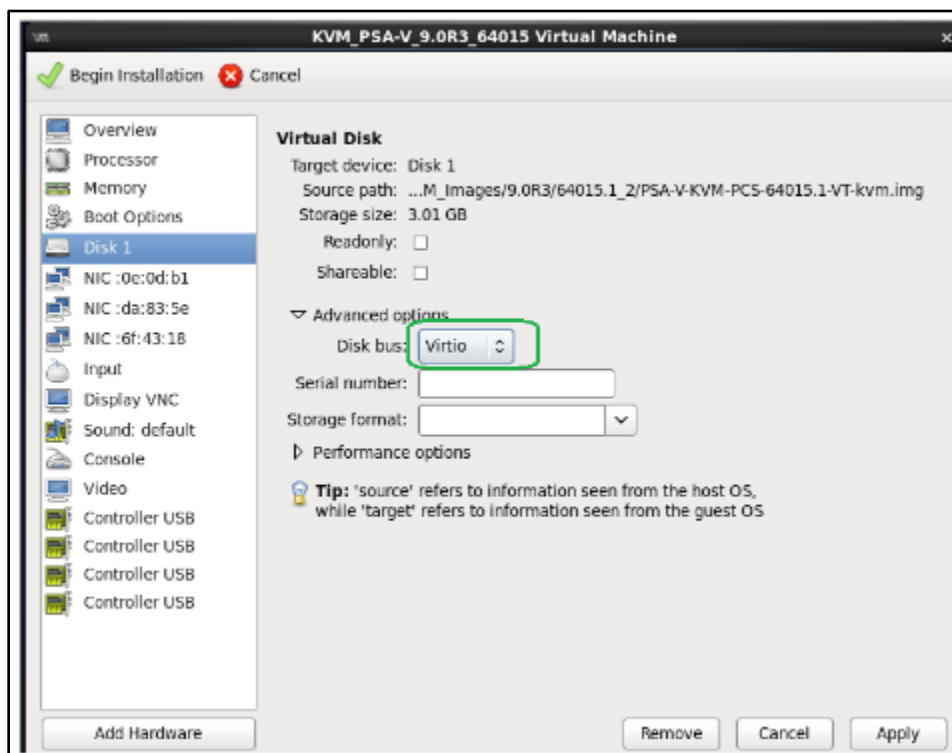
16. Select the **Storage format** as *qcow2*.
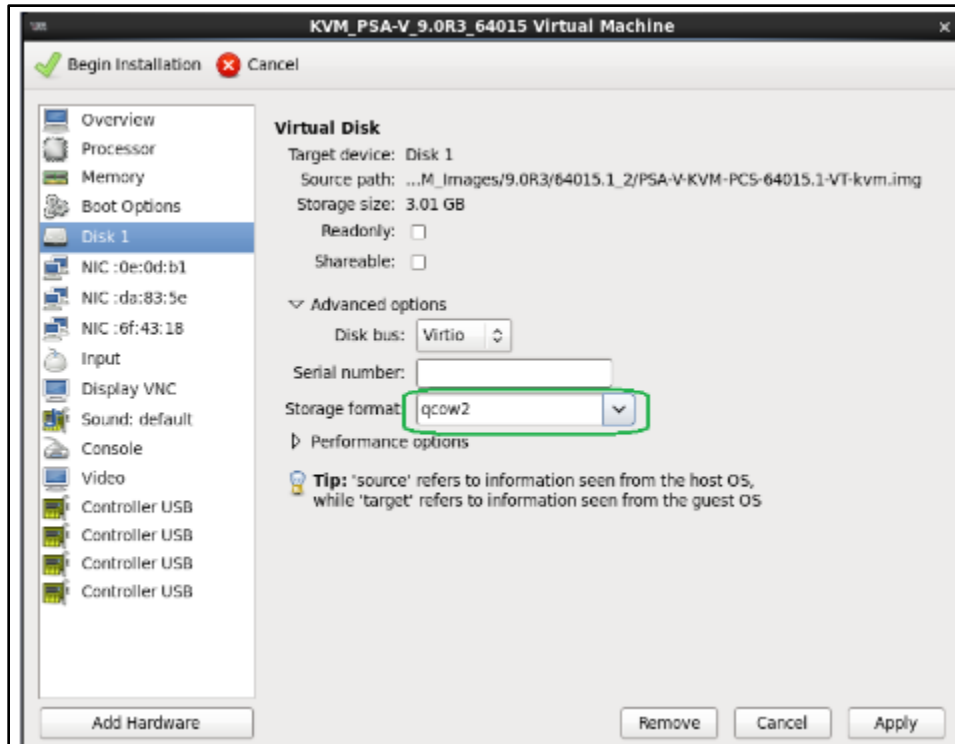
17. Click on **Begin Installation**.
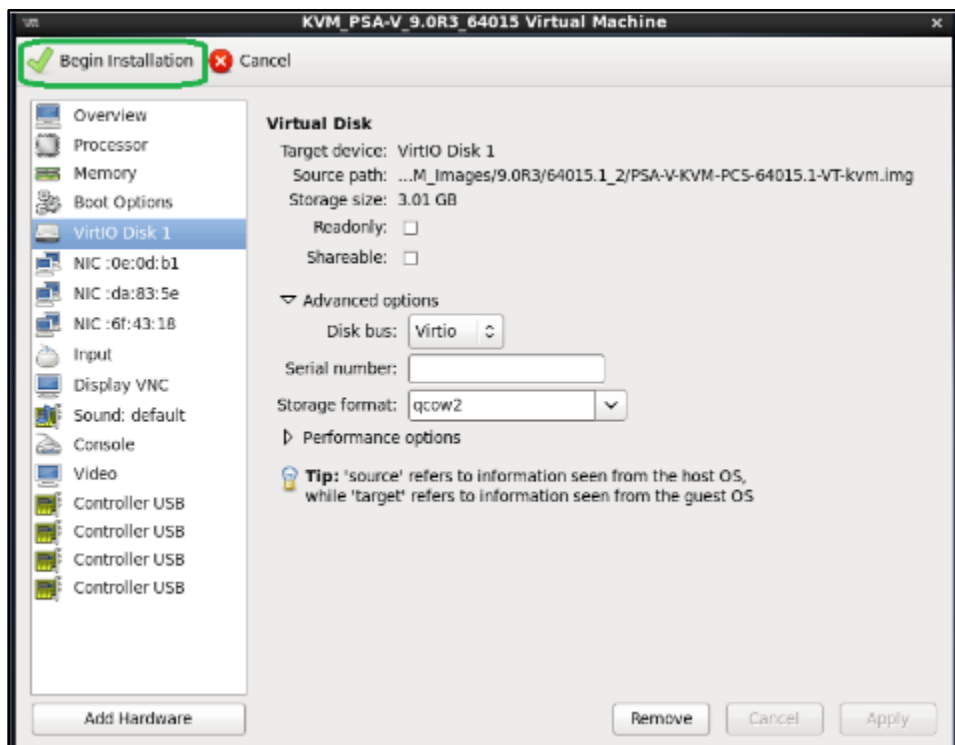
18. Appearance of LILO menu.

19. Display of PCS Initial Configuration Menu (installation complete).
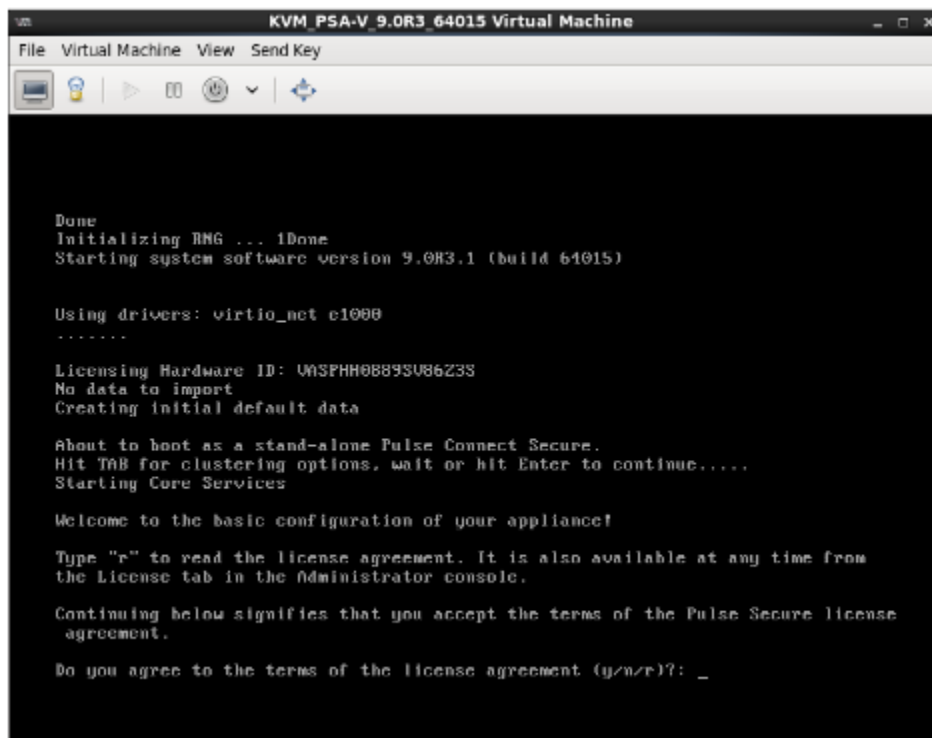
Related Documentation

- **About a Kernel-Based Virtual Machine**

- **Installing the KVM Modules**

CHAPTER 5 Deploying Pulse Virtual Appliance on Hyper-V

Overview of PCS Hyper-V Enablement

Pulse Virtual Appliances are now supported on Microsoft's Hyper-V hypervisor in addition to VMWare and KVM hypervisor platforms.

Table 13: Number of cores to be allocated to each Hyper-V model.

Platform	Cores Per VM
PSA3000-V	2
PSA5000-V	4
PSA7000-V	8

Limitations

- Hyper-V does not support more than one VLAN on a Network Adapter. Due to this limitation, VLAN functionality provided by PCS cannot be used on Hyper-V VA. Please refer to the 'To allow a virtual machine to use a VLAN' section from **https://technet.microsoft.com/en-us/library/cc816585(v=ws.10).aspx**.

- The image supports only IDE disks and will support only the 'Generation 1' type of Virtual machine in Hyper-V Manager due to the above limitation.

Deploying a Hyper-V/PSA-V/VA-DTE through the Hyper-V Manager

To deploy a Pulse virtual appliance through the Hyper-V Manager:

1. Copy the Hyper-V PSA-V|VA-DTE Package to the Hyper-V Server

2. Open Hyper-V Manager.

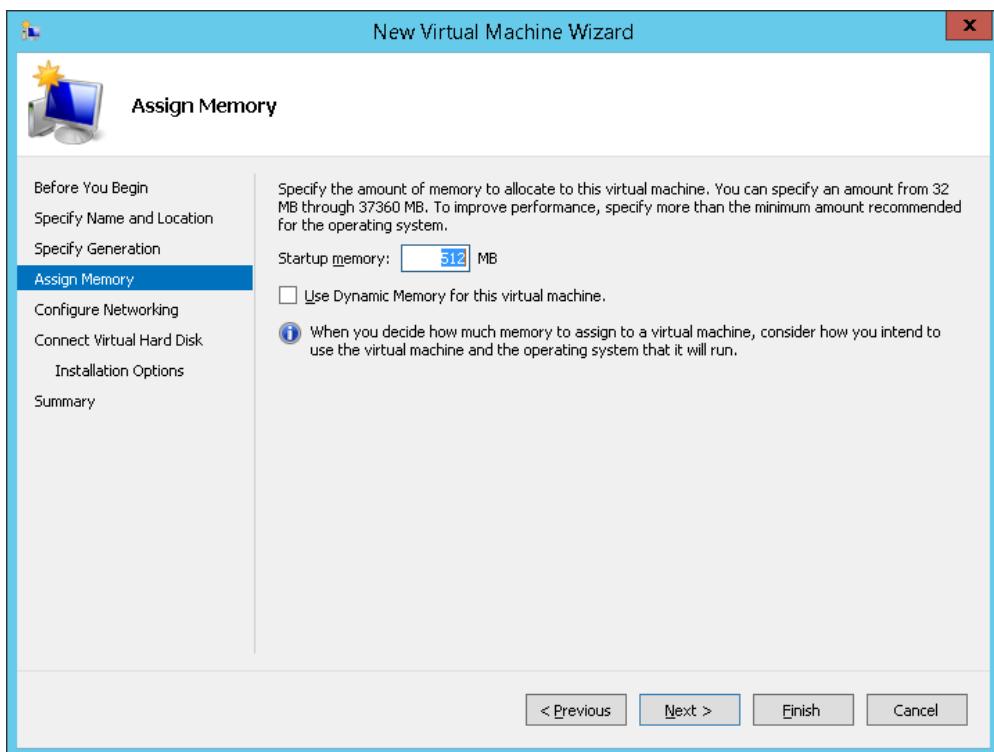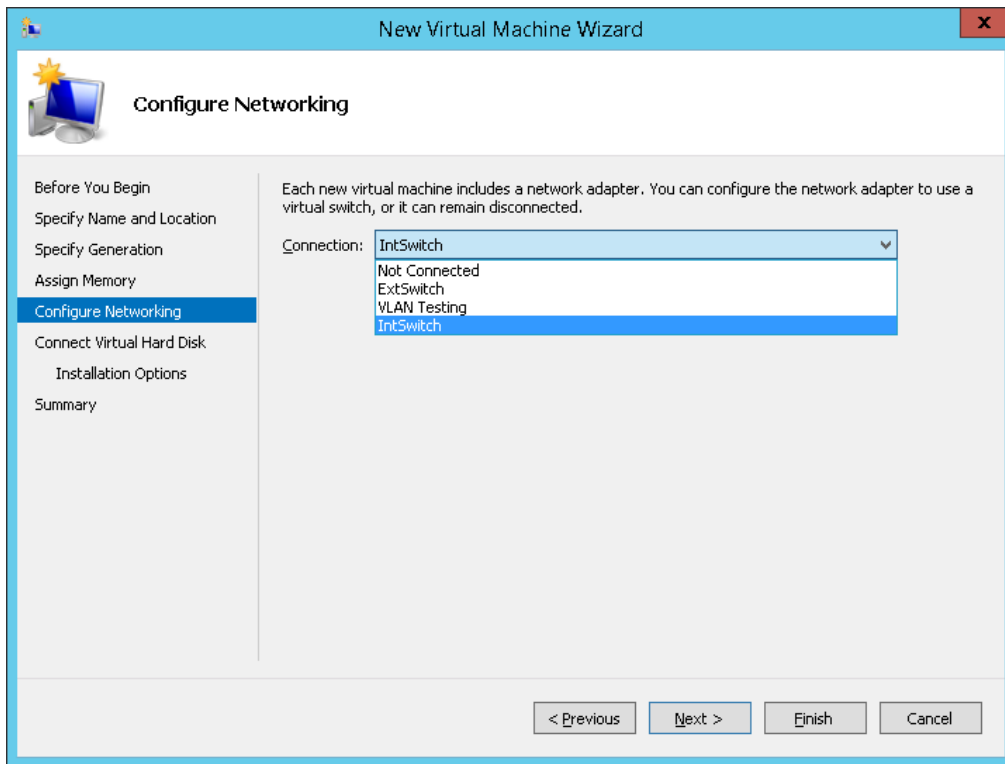3. Deploy Hyper-V PSA-V|VA-DTE
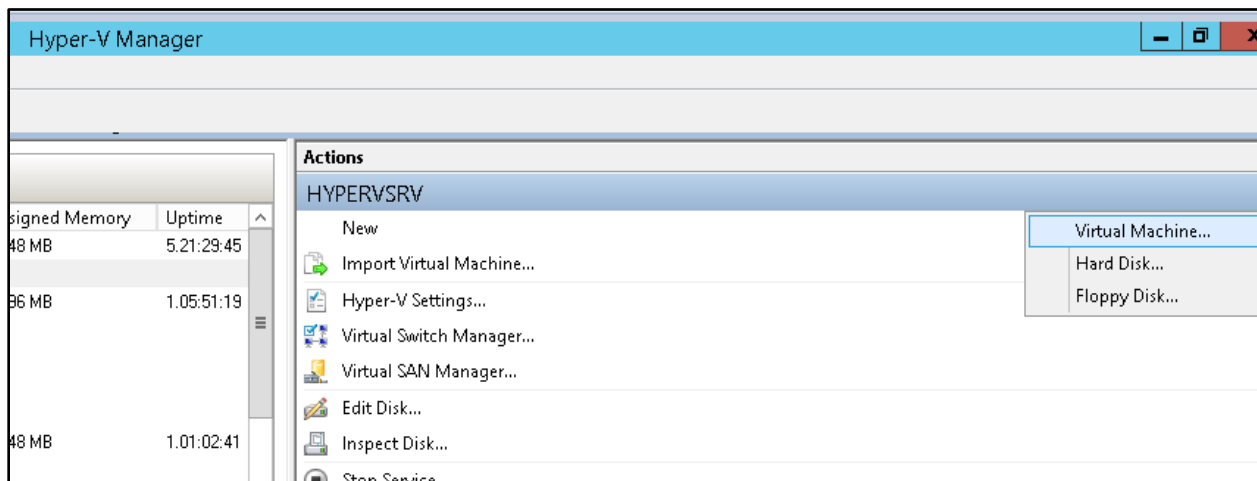
4. Select Generation 1 as Hyper-V PSA-V|VA-DTE does not support Generation 2 and click on Next.
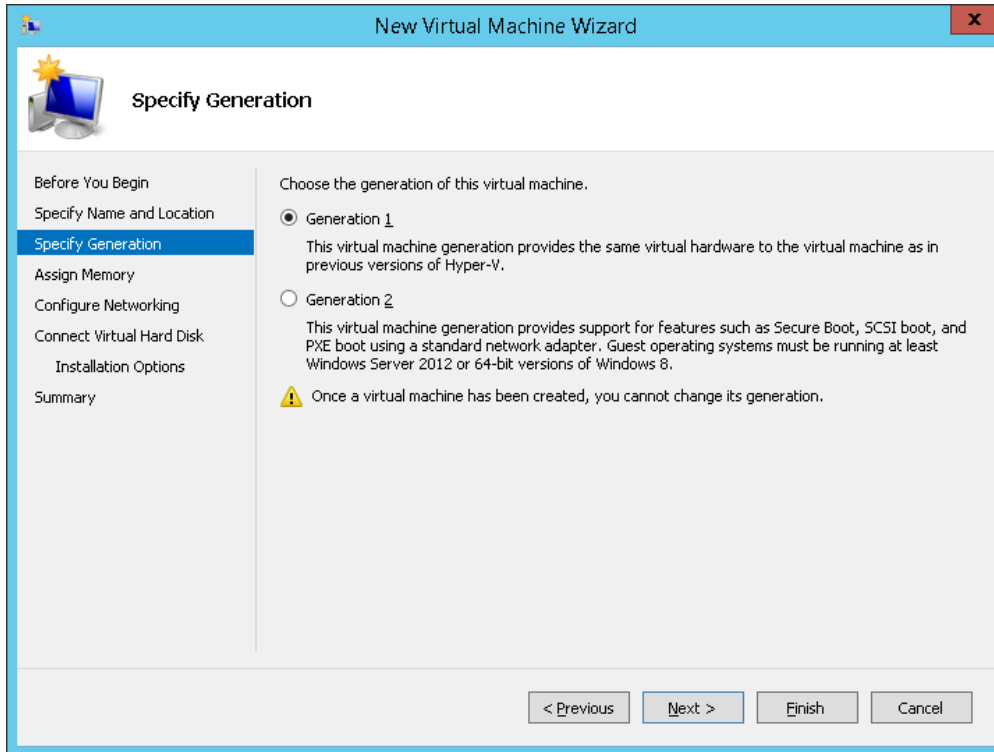

5. Now assign the appropriate memory. Enter 2048 MB for PSA-V and 2048 MB for VA-DTE and click on Next.

6. The Configure Networking page opens. Select a virtual switch to be used by the network adapter and click on Next.

7. The Connect Virtual Hard Disk page appears. Select the **Use an existing virtual hard disk** button and provide the location of the Hyper-V PSA-V|VA-DTE package.vhdx(step 1)
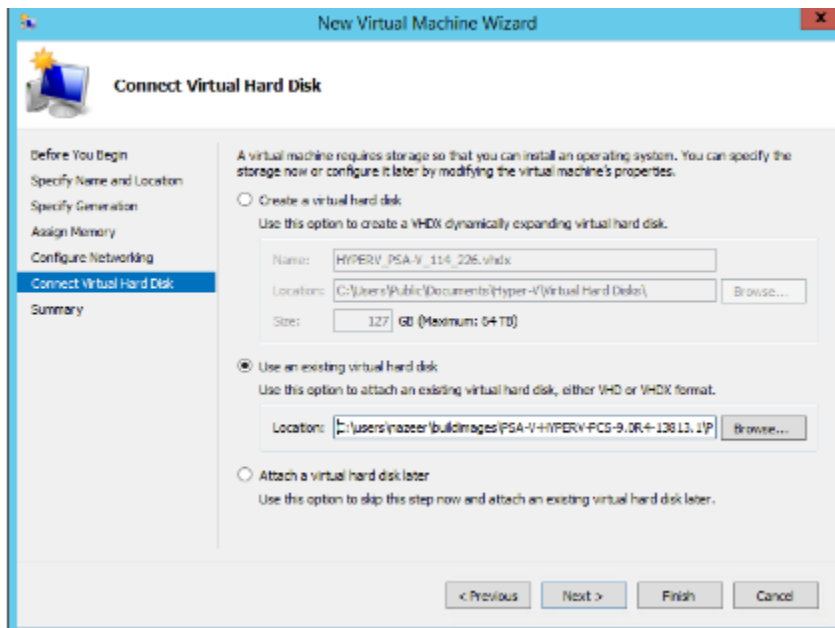
8. Click on **Finish**. Hyper-V Server creates an entry under Virtual Machines.

9. Now, add a network adapter for External Port and Management Port.

    a.   Right Click on the VM Name and click on **Settings**.

    b.   In the dialog box that opens, click on **Add Hardware** in the left pane.

    c.   On the right pane, select **Network Adapter**.

d. Click on **Add**.

ⓘ **Note:** It is important to add all the three network adapters to Hyper-V PSA-V|VA-DTE before powering on the VM. Adding network adapters after powering-on the Hyper-V PSA-V|VA-DTE may result in network connectivity issues. The following list indicates the order of virtual adapters:
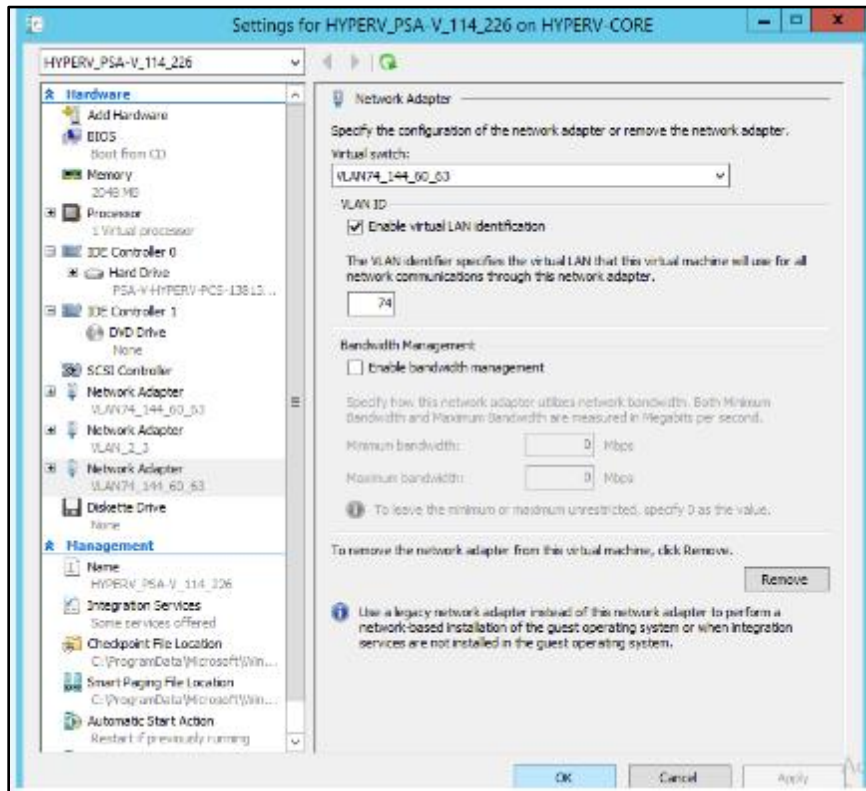
1. Network Adapter: Internal
2. Network Adapter 2: External
3. Network Adapter 3: Management

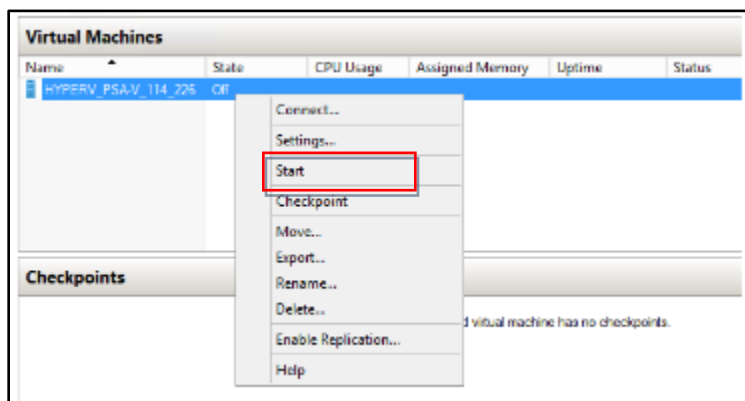10. Select the virtual switch for the External Port. Click on **apply**.
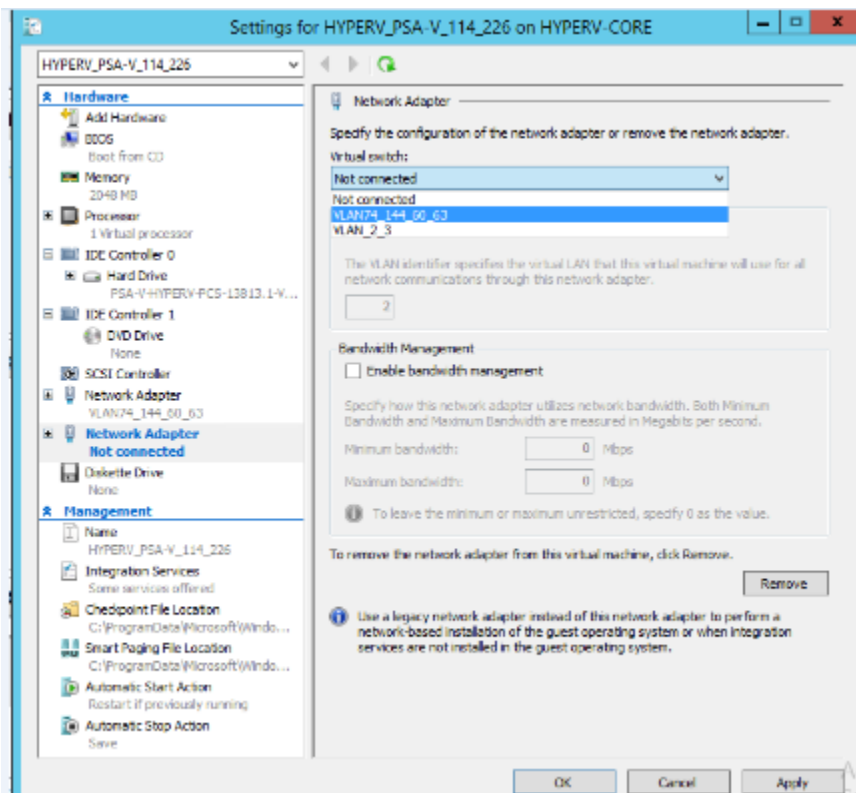
11. Now add network adapter for management port.

    a. Click on **Add Hardware** on the left pane. Select **Network Adapter**. Click on **Add**.

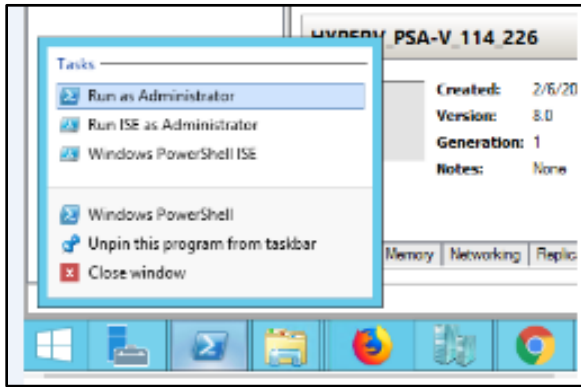   b. Select the Virtual Switch for the Management Port. Click on **Apply**.

12. Select **Start** to power on the virtual machine.

Deploying a Hyper-V PSA-V/VA-DTE through Powershell cmdlets

To deploy a Hyper-V PSA-V/VA-DTE through Powershell cmdlets:

1. Copy the Hyper-V PSA-V|VA-DTE Package to the Hyper-V Server.

2. Open PowerShell as administrator.

3. Enter the vm-name, memory (in MB), location of VHDx file, and the internal network switch name. Use the example below to perform this step. Create a Hyper-VA PSA-V|VA-DTE on the Hyper-V Server

   For example, for deploying the PSA-V:

   ```
   PS> New-VM -Name hyper-v-va -MemoryStartupBytes 2048MB -VHDPath F:\hyper_v_packages/PSA-V-
   HYPERV-PCS-<Version No.>-VT-hyperv.vhdx -SwitchName Int_Network_Switch -Generation 1
   ```

   For example, for deploying the VA-DTE

   ```
   PS> New-VM -Name hyper-v-va -MemoryStartupBytes 2048MB -VHDPath F:\hyper_v_packages/PSA-V-
   HYPERV-DTE-PCS-<Version No.>-VT-hyperv.vhdx -SwitchName Int_Network_Switch -Generation 1
   ```

4. Now, add two network adapters for the External Port and Management Port.

Port	Format	Example
External Port	`PS> ADD-VMNetworkAdapter -VMName <vm-name> -Switchname <External Network Switch Name>`	`PS> ADD-VMNetworkAdapter -VMName hyper-v-va -Switchname Ext_Network_Switch -Name External_Port`
Management Port	`PS> ADD-VMNetworkAdapter -VMName <vm-name> -Switchname <Management Network Switch Name>`	`PS> ADD-VMNetworkAdapter -VMName hyper-v-va -Switchname Mgmt_Network_Switch -Name`

5. Set the number of processors to assign to the Hyper-V

   ```
   PS> SET-VMProcessor -VMName <vm-name> -count <cpu-count>
   ```

   For example:

   ```
   PS> SET-VMProcessor -VMName hyper-v-va -count 1
   ```

6. Perform the following steps to change the name of internal network adapter:

   ```
   PS> Get-VMNetworkAdapter -VMName <vm-name>
   ```

Sample Output:

Name	IsManagementOs	VMName	SwitchName	MacAddress	Status	IPAddresses
Network Adapter	False	hyper-v-va	IntSwitch	000000000000		{}
Ext_Port	False	hyper-v-va	ExtSwitch	000000000000		{}
Mgmt_Port	False	hyper-v-va	MgmtSwitch	000000000000		{}

Now, change the name of Internal Network Adapter:

PS> Rename-VMNetworkAdapter -VMName user1_PSA-V_115_132 -Name "Network Adapter" -NewName "Int_Port"

Sample Output

PS> Get-VMNetworkAdapter -VMName <vm-name>

Name	IsManagementOs	VMName	SwitchName	MacAddress	Status	IPAddresses
Int_Port	**False**	**hyper-v-va**	**IntSwitch**	**000000000000**		**{}**
Ext_Port	**False**	**hyper-v-va**	**ExtSwitch**	**000000000000**		**{}**
Mgmt_Port	**False**	**hyper-v-va**	**MgmtSwitch**	**000000000000**		**{}**

7. To power on the Hyper-V VA enter:

```
PS> Start-VM –name <vm-name>
```

CHAPTER 6 Obtaining Licenses through PCLS for PSA-V

- **Overview**
- **Obtaining license keys from PCLS**
- **Virtual Appliance Platform Licensing**

Overview

Prior to 8.3R3, VMware PSA-Vs depend on a physical/virtual license server to lease license counts. In 8.3R3, the PCS VMs are enabled to provision licenses through the Pulse Cloud Licensing Service (PCLS) and periodically send heartbeat messages to PCLS for auditing purposes.

A virtual appliance downloads licenses from Pulse Cloud Licensing Service through authentication codes. The virtual machine sends heartbeats every 10 hours to the Pulse Cloud Licensing Service. If it is not able to connect to Pulse Cloud Licensing Service for 30 days, in the case of PSA-Vs, all the installed licenses get disabled. They get re-enabled only when the communication with PCLS is restored. PCS will log this information under Event Logs. To know more about the license configuration for PSA-V appliances refer to the **License Configuration for PSA-V Appliances Deployment Guide**.

Obtaining license keys from PCLS

This section covers the following topics:

Authorizing a PCS-VM

An admin obtains an authentication code for his entitlement externally via e-mail. The PCS VM first contacts the PulseOne Cloud License Service (PCLS) and the licenses get installed on the PSA-V. The license summary page shows the installed licenses. If the authentication code is not valid, PCLS will send appropriate error message, which gets logged in PCS-VM logs.

In addition to functioning as PCS, the virtual machine periodically sends heartbeat messages to the PulseOne Cloud License Service (PCLS). The heartbeat message includes various attributes of the VM like, machine-id, uuid, mac-addr, external-ip, internal-ip, internal-mac, external-mac, nc-count, number of-nodes, version-number, build-number, heartbeat-token, ipv4-addr, node-state, active-sessions, pulse-count, pulse-version and so on. This helps PCLS to identify duplicate/cloned VM instances.

ⓘ **Note:** In the initial release of PCLS, there is no enforcement. It just collects the data and stores in its database. But, first version of PCS VM can understand stop command from PCLS and disable itself.


Obtaining License Keys

An admin obtains an authentication code for his entitlement externally via e-mail. The admin must enter the authentication code in the License Server download page to validate and fetch license keys. If validation is successful, the admin receives the license keys in return.

To obtain license keys:

1. Go to **System > Configuration > Download Licenses**. See Figure below.

2. Under On demand license downloads, enter the authentication code in the text box.

3. Click on Download and Install.
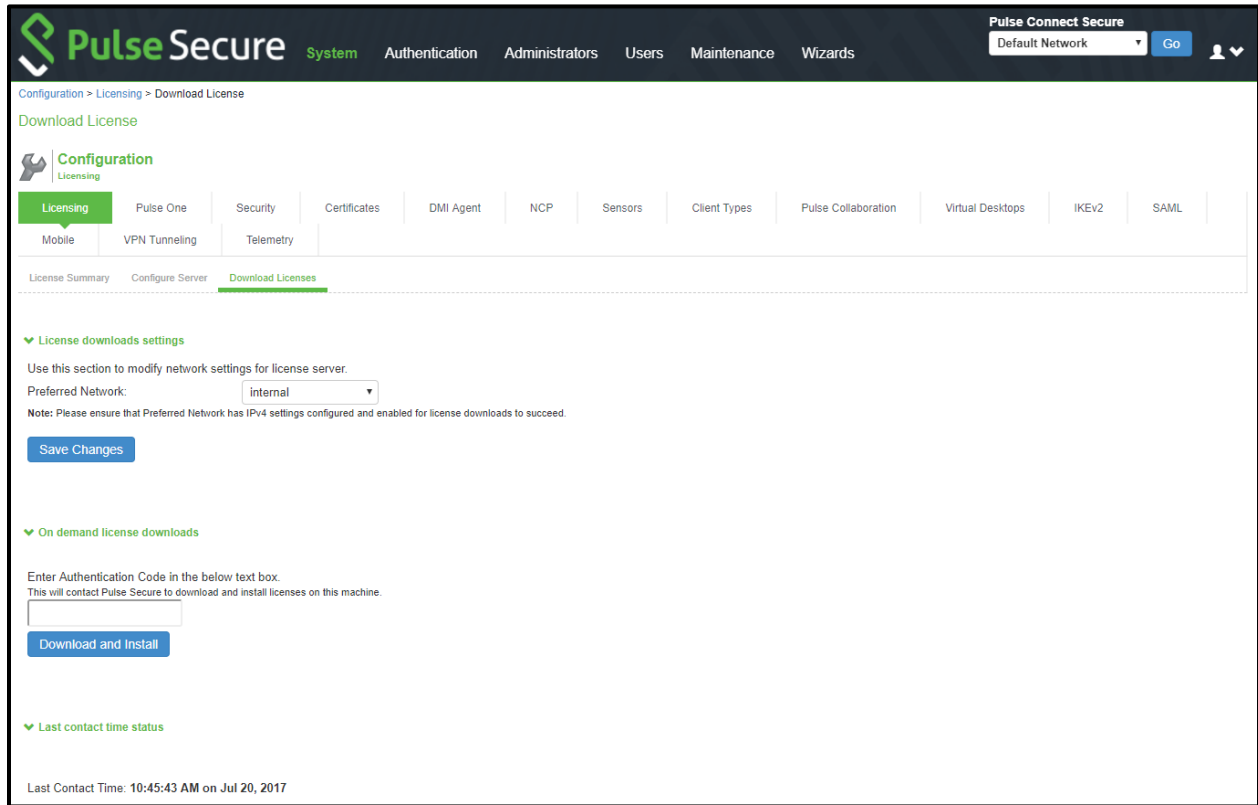
4. Now, go to the License Summary tab to view a list of the licenses installed.

Viewing the License Summary

To view the licensing summary:

1. Go to **System > Configuration > Licensing > Licensing Summary**.

2. Under the Installed license details, admin can see the license keys obtained through PCLS. Admin can copy these license keys in a backup file and re-paste it on the text box, without having to contact PCLS again.

Note: PCS VM needs to be able to connect to PCLS through port 443. It can lease licenses from a license server and also get license keys from PCLS. In this case, the licenses leased and license keys obtained from PCLS will get added.

Virtual Appliance Platform Licensing

To define similar level of hardware sizing on VMs, we need to enforce the number of cores currently admins can assign to the system. Even if admins assign more cores to the system we have to enforce only the allowed number of cores by the platform licenses. To do this new SKUs have been added to the licensing SKUs as features and will be enforced by the licensing framework.

> (i) **Note:** On upgrade from an older version to PCS 8.3R3/PPS 5.4R3, core licenses are NOT enforced. Customer need not install any core licenses. The behavior of the VA/PSA is similar to 8.3R1. The customer can lease the user licenses from license server or get licenses using authorization codes from the PCLS.

Since a licensing server cannot give out these licenses while launching the VMs the admin needs to register with PCLS and fetch the required licenses from PCLS. New SKUs have been added to the number of cores. VMs can fetch the licenses required for the assigned cores by the hypervisor when the VM is registered with PCLS. While launching, platforms are required to fetch the core licenses before the first use if the PSA-V doesn't have the licenses to use the cores, it would be required to talk to PCLS to fetch license, if the license is not assigned at the PCLS VM would turn off all the other cores and only enables the admin login and no user login will be allowed

If fewer core licenses are fetched from the PCLS, VM would turn off the rest of the cores that didn't get any license. There will not be any enforcement on the memory side, VMs will be allowed to use any memory required. But the minimum required memory that a VM needs will be published after the testing completes based on test results.

Below, is the list of new SKUs that have been added:

- PSA3000-V-EVAL-2W : Virtual Appliance allow Usage of two CPU cores - 2 week license
- PSA3000-V-EVAL-4W : Virtual Appliance allow Usage of two CPU cores - 4 week license
- PSA3000-V-EVAL-8W : Virtual Appliance allow Usage of two CPU cores - 8 week license
- PSA3000-V-1YR : Virtual Appliance allow Usage of two CPU cores - Subscription 1 years
- PSA3000-V-1YR-R : Virtual Appliance allow Usage of two CPU cores - Subscription 1 years Renewal
- PSA5000-V-EVAL-2W : Virtual Appliance allow Usage of four CPU cores - 2 week license
- PSA5000-V-EVAL-4W : Virtual Appliance allow Usage of four CPU cores - 4 week license
- PSA5000-V-EVAL-8W : Virtual Appliance allow Usage of two four cores - 8 week license
- PSA5000-V-1YR : Virtual Appliance allow Usage of four CPU cores - Subscription 1 years
- PSA5000-V-1YR-R : Virtual Appliance allow Usage of four CPU cores - Subscription 1 years Renewal
- PSA7000-V-EVAL-4W : Virtual Appliance allow Usage of eight CPU cores - 4 week license
- PSA7000-V-EVAL-8W : Virtual Appliance allow Usage of two eight cores - 8 week license
- PSA7000-V-1YR : Virtual Appliance allow Usage of eight CPU cores - Subscription 1 years
- PSA7000-V-1YR-R : Virtual Appliance allow Usage of eight CPU cores - Subscription 1 years Renewal
- PSA3000-V-3YR : Virtual Appliance allow Usage of two CPU cores - Subscription 3 years

- PSA3000-V-3YR-R : Virtual Appliance allow Usage of two CPU cores - Subscription 3 years Renewal

- PSA5000-V-3YR : Virtual Appliance allow Usage of four CPU cores - Subscription 3 years

- PSA5000-V-3YR-R : Virtual Appliance allow Usage of four CPU cores - Subscription 3 years Renewal

- PSA7000-V-3YR : Virtual Appliance allow Usage of eight CPU cores - Subscription 3 years

- PSA7000-V-3YR-R : Virtual Appliance allow Usage of eight CPU cores - Subscription 3 years Renewal

To enable required performance VM should be assigned the required number of cores. The following table gives approximate cores to assign to get the required performance

Table 14: Number of cores to be allocated to each PSA-x000V model.

Platform	Cores Per VM	Maximum Concurrent Users	Maximum Installed Count
PSA-V	-	2	25000
PSA-3000V	2	200	25000
PSA-5000V	4	2500	25000
PSA-7000V	8	25000	25000