© 2016 by Pulse Secure, LLC. All rights reserved

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

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

Pulse Connect Secure / Pulse Policy Secure
Virtual Appliance Service Provider Virtual Appliance Deployment Guide

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

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.pulsesecure.net/support/eula.

By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Revision History
2014-12-15 – Changes for rebranding
Abbreviated Table of Contents

Table of Contents .......................................................................................................................... ii
List of Tables ................................................................................................................................. iv
About This Guide ........................................................................................................................... v
PART 1 Virtual Appliances ............................................................................................................ 1
CHAPTER 1 Virtual Appliances Overview ..................................................................................... 2
CHAPTER 2 Deploying Virtual Appliances on VMware ESXi Through vCenter Using OVF Properties .......................................................................................................................... 8
CHAPTER 3 Deploying Virtual Appliances in VMware vSphere Using the Serial Port ........... 16
CHAPTER 4 Using NETCONF Perl Client to Configure the Virtual Appliance ....................... 20
CHAPTER 5 Deploying on a Kernel-Based Virtual Machine ...................................................... 23
CHAPTER 6 Deploying Pulse Virtual Appliance on Hyper-V ...................................................... 28
PART 2 Index ................................................................................................................................. 36
PART 2 Index ................................................................................................................................. 37
# Table of Contents

Table of Contents ........................................................................................................................ ii

List of Tables ................................................................................................................................. iv

About This Guide ............................................................................................................................. v

Related Documentation and Release Notes .................................................................................. v

Document Conventions ................................................................................................................... v

Requesting Technical Support ......................................................................................................... vi

Self-Help Online Tools and Resources ......................................................................................... vi

Opening a Case with PSGSC ........................................................................................................... vi

PART 1 Virtual Appliances ............................................................................................................... 1

CHAPTER 1 Virtual Appliances Overview ..................................................................................... 2

Virtual Appliance Editions and Requirements ................................................................................ 2

Hardware and Software Requirements ......................................................................................... 2

Upgrading from a Previous Version .............................................................................................. 3

Supported Features on Virtual Appliances .................................................................................. 3

Virtual Appliance Package Information .......................................................................................... 4

SPE Virtual Appliance Utility Scripts ............................................................................................. 6

CHAPTER 2 Deploying Virtual Appliances on VMware ESXi Through vCenter Using OVF Properties .......................................................................................................................... 8

Overview of Deploying Virtual Appliances on VMware ESXi ....................................................... 8

Using the Deployment Script to Define the Initial Configuration Parameters ................................ 8

Example Output ............................................................................................................................ 13

Verifying Your Deployment with vmware-cmd ............................................................................. 14

CHAPTER 3 Deploying Virtual Appliances in VMware vSphere Using the Serial Port .............. 16

Overview of Scripts for Deploying Through the VMware ESX Hypervisor Serial Port ................. 16

Using the init-network-config.exp and create-va.exp Scripts ..................................................... 16

init-network-config.exp Parameters .............................................................................................. 17

create-va.exp Parameters ............................................................................................................. 18

CHAPTER 4 Using NETCONF Perl Client to Configure the Virtual Appliance ......................... 20

Installing the NETCONF Perl Client ............................................................................................. 20

Verifying the Installation and the Version of Perl ....................................................................... 20

Installation of NETCONF Perl Client ............................................................................................ 21

Using the VA-SPE Sample Scripts ............................................................................................... 21

Using the get_active_users.pl Script ......................................................................................... 21

Using the edit_config_ive.pl Script ........................................................................................... 22

Enabling the VMXNET3 Driver ..................................................................................................... 22

CHAPTER 5 Deploying on a Kernel-Based Virtual Machine ...................................................... 23

About a Kernel-Based Virtual Machine ....................................................................................... 23

Limitations .................................................................................................................................... 24

Installing the KVM Modules ........................................................................................................ 24
Deploying a KVM Virtual Appliance ................................................................................................. 26

CHAPTER 6 Deploying Pulse Virtual Appliance on Hyper-V ...................................................... 28
Overview of PCS Hyper-V Enablement .............................................................................................. 28
Deploying a Hyper-V VA-SPE/VA-DTE through the Hyper-V Manager: ...................................... 28
Deploying a Hyper-V VA-SPE/VA-DTE through Powershell cmdlets ........................................ 34

PART 2 Index ...................................................................................................................................... 36

PART 2 Index ...................................................................................................................................... 37
List of Tables

Table 1: Notice Icons ........................................................................................................... v
Table 2: VMware Qualified System ......................................................................................... 3
Table 3: KVM Qualified System ............................................................................................... 3
Table 4: create-va.pl Parameters ........................................................................................... 9
Table 5: Management Port Behavior While Deploying a Template ....................................... 11
Table 6: Internal Port Behavior While Deploying a Template .................................................. 11
Table 7: External Port Behavior While Deploying a Template ............................................... 11
Table 8: Management Port Behavior During a New Deployment ........................................... 12
Table 9: Internal Port Behavior During a New Deployment ..................................................... 12
Table 10: External Port Behavior During a New Deployment .................................................. 13
Table 11: init-network-config.exp Parameters ....................................................................... 17
Table 12: create-va.exp Parameters ....................................................................................... 18
Table 13: kvm-va.conf Parameters .......................................................................................... 26
About This Guide

- Related Documentation and Release Notes
- Document Conventions
- Requesting Technical Support

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 http://www.pulsesecure.net/techpubs/.

Document Conventions

Table 1 defines notice icons used in this guide.

Table 1: Notice Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![i]</td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>![exclamation mark]</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>![warning]</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>![laser]</td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
</tbody>
</table>
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 http://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: http://www.pulsesecure.net/support
- Search for known bugs: http://www.pulsesecure.net/support
- Find product documentation: http://www.pulsesecure.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://www.pulsesecure.net/support
- Download the latest versions of software and review release notes: http://www.pulsesecure.net/support
- Search technical bulletins for relevant hardware and software notifications: http://www.pulsesecure.net/support
- Open a case online in the CSC Case Management tool: http://www.pulsesecure.net/support

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: http://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 http://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 http://www.pulsesecure.net/support.
PART 1 Virtual Appliances

- Virtual Appliances Overview
- Deploying Virtual Appliances on VMware ESXi Through vCenter Using OVF Properties
- Deploying Virtual Appliances in VMware vSphere Using the Serial Port
- Using NETCONF Perl Client to Configure the Virtual Appliance
- Deploying on a Kernel-Based Virtual Machine
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
- SPE Virtual Appliance Utility Scripts

Virtual Appliance Editions and Requirements

Two types of virtual appliances are available:

- Demonstration and Training Edition (DTE)
- Service Provider Edition (SPE)

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.

The SPE 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

<table>
<thead>
<tr>
<th>VMware Tools Version</th>
<th>vCenter/ESXi Version</th>
<th>Qualified Pulse Connect Secure and Secure Access System Versions</th>
<th>Qualified Pulse Policy Secure and Access Control System Versions</th>
<th>Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.4.0</td>
<td>ESXi 5.5, 5.5 U3</td>
<td>8.2</td>
<td>5.3</td>
<td>IBM BladeServer H chassis</td>
</tr>
<tr>
<td>9.4.0.25733</td>
<td>4.1U3</td>
<td>8.1</td>
<td>5.1</td>
<td>BladeCenter HS blade server</td>
</tr>
<tr>
<td>9.4.0.25733</td>
<td>5.5</td>
<td>8.0R5</td>
<td>5.0R5</td>
<td></td>
</tr>
<tr>
<td>9.4.0.25733</td>
<td></td>
<td>7.4R10</td>
<td>4.4R10</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: VMware's HA feature is qualified; VMware's DRS & Fault Tolerance features are not qualified.

Table 3: KVM Qualified System

<table>
<thead>
<tr>
<th>QEMU/KVM Version</th>
<th>Qualified Pulse Connect Secure and Secure Access System Versions</th>
<th>Qualified Pulse Policy Secure and Access Control System Versions</th>
<th>Hardware Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>QEMU emulator version 2.3.0</td>
<td>8.2</td>
<td>5.3</td>
<td>Linux Server Release 6.4 on an Intel Xeon CPU L5640 @ 2.27GHz</td>
</tr>
<tr>
<td>v1.4.0</td>
<td>8.1</td>
<td>5.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8.0R5</td>
<td>5.0R5</td>
<td>NFS storage mounted in host</td>
</tr>
<tr>
<td></td>
<td>7.4R10</td>
<td>4.4R10</td>
<td>24GB memory in host</td>
</tr>
</tbody>
</table>

Upgrading from a Previous Version

If you are upgrading the Pulse Connect Secure software on your SPE 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)
• Clustering
• User record synchronization

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 SPE downloadable zip contains the following files:

• README-SPE.txt—A quick start guide for the SPE virtual appliance.
• README-scripts.txt—Up-to-date information on the contents of the zip file and how to run the scripts.
• VA-SPE-release-buildnumber-serial-disk1.vmdk—A virtual disk file that contains the Pulse Connect Secure or Pulse Policy Secure software. The SERIAL version assumes using a serial port to set up the initial network configuration.
• VA-SPE-release-buildnumber-serial.ovf—An Open Virtualization Format (OVF) specification that defines the virtual appliance and contains a reference to the disk image.
• VA-SPE-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-SPE-release-buildnumber-vt.ovf—An OVF specification that defines the virtual appliance and contains a reference to the disk image.
• init-network-config.exp—A script to configure the initial network settings.
• create-va.exp—A script to import the OVF file into the ESX server and configure the initial network settings (the create-va.exp script is a superset of the init-network-config.exp script).
• setupva.conf—An example configuration file for the create-va.exp and init-network-config.exp scripts.
• 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 SPE virtual appliance. Cannot be used for configuring the SPE 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 SPE virtual appliance configuration.

The DTE downloadable zip contains the following files:
• README-DTE.txt—a quick start guide for the SPE 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:
• 20-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:
• 20-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.

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 ESX server.

The OVF file does not include any virtual serial port configuration. If the SERIAL OVF image is used, the virtual machine specification needs to be updated with the desired virtual serial port configuration before the virtual appliance is powered on for the first time.

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 SPE virtual appliance, clone it to a template and export that template. From the template, you can then instantiate additional SPE virtual appliances.

**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 Solution Guide

**SPE Virtual Appliance Utility Scripts**

Several utility scripts are included with the SPE virtual appliance package. These scripts assist with:

- Deployment
- Initial setup of the SPE virtual appliance
• Configuring the SPE 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 SPE 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 ESX to run the virtual appliance, you can use these scripts for deployment. These scripts use the service console of ESX 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

• Overview of Scripts for Deploying Through the VMware ESX Hypervisor Serial Port

• Installing the VA-SPE Sample Scripts
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 ESX, is a hypervisor that installs on top of a physical server and partitions it into multiple virtual machines. VMware ESXi does not contain the ESX’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 VA-SPE 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 4 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 4: create-va.pl Parameters**

<table>
<thead>
<tr>
<th>vCenter-Related Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>- -vCenterServer</td>
<td>Hostname or IP address of the vCenter Server.</td>
</tr>
<tr>
<td>- -vCenterUsername</td>
<td>Username for logging in to the VMware vCenter Server.</td>
</tr>
<tr>
<td>- -vCenterPassword</td>
<td>Password for logging in to the VMware vCenter Server. Special characters in the password must be escaped with a backslash (). For example, Pulsesecure123$</td>
</tr>
<tr>
<td>- -datacenterName</td>
<td>Data center under which the Cluster/ESXi Host is present or added.</td>
</tr>
<tr>
<td>- -clusterorHostName</td>
<td>Name of the VMware cluster where the virtual appliance is to be deployed.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>When deploying the virtual appliance in an ESXi server, this parameter must following the format ESXi-server-name. For example, mydev.pulsesecure.net.</td>
</tr>
<tr>
<td>- -datastore</td>
<td>Name of the datastore where the virtual appliance is to be deployed.</td>
</tr>
<tr>
<td>- -vaname</td>
<td>Name of the virtual appliance to create.</td>
</tr>
</tbody>
</table>

**Pulse Connect Secure and Policy Secure-Related Parameters**

| - -ipAddress              | IP address to assign to the internal port of the Pulse Connect Secure virtual appliance. |
| - -netmask                | Netmask to assign to the internal port of the virtual appliance. |
| - -gateway                | Gateway to assign to the internal port of the virtual appliance. |
| - -adminUsername          | Username for the default administrator account for the virtual appliance. |
| - -adminPassword          | Password for the default administrator account for the virtual appliance. |
| - -primaryDNS             | IP address for the primary DNS server. |
| - -secondaryDNS           | IP address for the secondary DNS server. |
| - -domain                 | Domain name for the virtual appliance. |
- -wins  Windows Internet Name Service (WINS) hostname or IP address.
- -commonName  Common name for the default device certificate.
- -organization  Organization for the default device certificate.
- -randomText  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.

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
- -mgmtipAddress  Management network IP address.
- -mgmtnetmask  Management network netmask address.
- -mgmtgateway  Management network gateway address.

- -managementPortReconfigWithValueInVAppProperties  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 5 and Table 8.

- -internalPortReconfigWithValueInVAppProperties  The internal port overwrite property. If set to 1, overwrite the virtual appliance’s internal port settings with the ones specified during deployment. See Table 6 and Table 9.

Virtual Appliance External Interface Parameters
- -extipAddress  External network IP address.
- -extnetmask  External network netmask address.
- -extgateway  External network gateway address.

- -externalPortReconfigWithValueInVAppProperties  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 7 and Table 10.

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

### Table 5: Management Port Behavior While Deploying a Template

<table>
<thead>
<tr>
<th>Management Port Overwrite Value</th>
<th>Management Port Configuration Values</th>
<th>Pulse Connect Secure and Pulse Policy Secure Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The management port IP address, netmask address and gateway address are valid values.</td>
<td>Because <code>managementPortReconfigWithValueInVAppProperties</code> is 0, the management port-related parameters are retained and are not overwritten with values in the passed configuration.</td>
</tr>
<tr>
<td>0</td>
<td>The management port IP address, netmask address and gateway address are not valid values.</td>
<td>Because <code>managementPortReconfigWithValueInVAppProperties</code> is 0, the management port-related parameters are retained and are not overwritten with values in the passed configuration.</td>
</tr>
<tr>
<td>1</td>
<td>The management port IP address, netmask address and gateway address are valid values.</td>
<td>You can configure the management port with the new values passed while deploying. The existing cache value is overwritten with new values.</td>
</tr>
<tr>
<td>1</td>
<td>The management port IP address, netmask address and gateway address are not valid values.</td>
<td>During the boot process, the administrator is asked whether to configure the management port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter <strong>N</strong> to skip the management port configuration. Enter <strong>Y</strong> to specify valid values for the management port.</td>
</tr>
</tbody>
</table>

### Table 6: Internal Port Behavior While Deploying a Template

<table>
<thead>
<tr>
<th>Internal Port Overwrite Value</th>
<th>Internal Port Configuration</th>
<th>Pulse Connect Secure and Pulse Policy Secure Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Valid or invalid configuration</td>
<td>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.</td>
</tr>
<tr>
<td>1</td>
<td>Valid configuration</td>
<td>Use the new values passed while deploying and configure the internal port.</td>
</tr>
<tr>
<td>1</td>
<td>Invalid configuration</td>
<td>During the boot process, the administrator is asked whether to configure the internal port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enter <strong>N</strong> to skip the internal port configuration. Enter <strong>Y</strong> to specify valid values for the internal port.</td>
</tr>
</tbody>
</table>

### Table 7: External Port Behavior While Deploying a Template

<table>
<thead>
<tr>
<th>External Port Overwrite Value</th>
<th>Management Port Configuration Values</th>
<th>Pulse Connect Secure and Pulse Policy Secure Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The external port IP address, netmask address and gateway address are valid values.</td>
<td>Because <code>externalPortReconfigWithValueInVAppProperties</code> is 0, the external port-related parameters are retained and are not overwritten with values in the passed configuration.</td>
</tr>
</tbody>
</table>
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.

The external port IP address, netmask address and gateway address are not valid values.

You can configure the external port with the new values passed while deploying. The existing cache value is overwritten with new values.

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 8 and Table 9.

Table 8: Management Port Behavior During a New Deployment

<table>
<thead>
<tr>
<th>Management Port Overwrite Value</th>
<th>Management Port Configuration Values</th>
<th>Pulse Connect Secure and Pulse Policy Secure Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The management port IP address, netmask address and gateway address are valid values.</td>
<td>Valid management configuration is available. Configure the Pulse Connect Secure or Pulse Policy Secure with these values.</td>
</tr>
<tr>
<td>0</td>
<td>The management port IP address, netmask address and gateway address are not valid values.</td>
<td>Invalid management configuration is present. Do not configure the management port properties.</td>
</tr>
<tr>
<td>1</td>
<td>The management port IP address, netmask address and gateway address are valid values.</td>
<td>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.</td>
</tr>
<tr>
<td>1</td>
<td>The management port IP address, netmask address and gateway address are not valid values.</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 9: Internal Port Behavior During a New Deployment

<table>
<thead>
<tr>
<th>Internal Port Overwrite Value</th>
<th>Internal Port Configuration</th>
<th>Pulse Connect Secure and Pulse Policy Secure Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 or 1</td>
<td>Valid configuration</td>
<td>Configure the internal port based on the passed configuration values.</td>
</tr>
<tr>
<td>0 or 1</td>
<td>Invalid configuration</td>
<td>During the boot process, the administrator is asked whether to configure the internal port.</td>
</tr>
</tbody>
</table>
### Table 10: External Port Behavior During a New Deployment

<table>
<thead>
<tr>
<th>External Port Overwrite Value</th>
<th>External Port Configuration Values</th>
<th>Pulse Connect Secure and Pulse Policy Secure Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The external port IP address, netmask address and gateway address are valid values.</td>
<td>Valid external configuration is available. Configure the Pulse Connect Secure or Pulse Policy Secure with these values.</td>
</tr>
<tr>
<td>0</td>
<td>The external port IP address, netmask address and gateway address are not valid values.</td>
<td>Invalid external configuration is present. Do not configure the management port properties.</td>
</tr>
<tr>
<td>1</td>
<td>The external port IP address, netmask address and gateway address are valid values.</td>
<td>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.</td>
</tr>
<tr>
<td>1</td>
<td>The external port IP address, netmask address and gateway address are not valid values.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

**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.

```plaintext
perl create-va.pl --configFile /root/darumuga/ovf_dir/va_config_files/7.2R4_va_spe.conf
```

Your output will look similar to the following:

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

**OVF File:** /root/darumuga/ovf_dir/7.2/VA-SPE-SA-7.2R4-21662.1/VA-SPE-SA-21662.1-vT.ovf

**VA Name:** "7.2R4_VA_SPE_125_10"

**vCenter Server:** 10.204.54.201
**vCenter Username:** darumuga
**vCenter Password:** Pulsesecure123\$

**Datacenter Name:** PBU-QA
**Cluster / Host Name:** Dharma_ESXi_5_Cluster/asgdevesx3.bngrd.pulsesecure.net

**IP Address:** 3.3.125.10
**Netmask:** 255.0.0.0
**Gateway:** 3.0.0.1
**Management IP Address:** 10.209.125.10
**Management Netmask:** 255.255.240.0
```
Management Gateway: 10.209.127.254
Reconfigure Internal Port with value in VAapp properties: 0
Reconfigure Management Port with value in VAapp properties: 0
Primary DNS: 10.209.194.50
Secondary DNS: 1.1.1.1
DNS Domains: pulsesecure.net
WINS: WINSServer
Admin Username: admin
Admin Password: neoteris
Organization: Pulse
Common Name: secure.pulsesecure.net
ExternalNetwork Mapped to: "IPv6-Ext"
InternalNetwork Mapped to: "IPv6-Int"
ManagementNetwork Mapped to: "ASG QA"

Command = ovftool --skipManifestCheck --name="7.2R4_VA_SPE_125_10" --prop:vaIVEConfig="vaIPAddress=3.3.125.10; vaNetmask=255.0.0.0; vaGateway=3.0.0.1; vaManagementIPAddress=10.209.125.10; vaManagementNetmask=255.255.240.0; vaManagementGateway=10.209.127.254; vaInternalPortReconfigWithValueInVAppProperties=0; vaManagementPortReconfigWithValueInVAppProperties=0; vaPrimaryDNS=10.209.194.50; vaSecondaryDNSs=1.1.1.1; vaDNSDomain=pulsesecure.net; vaWINSServer=WINSServer; vaCommonName=secure.pulsesecure.net; vaOrganization=Pulse; vaRandomText=Pulse_your_Net; vaAdminUsername=admin; vaAdminPassword=neoteris " --net:ExternalNetwork="IPv6-Ext" --net:ManagementNetwork="ASG QA" --datastore=devesx3 --powerOn /root/darumuga/ovf_dir/7.2/VA-SPE-SA-7.2R4-21662.1/VA-SPE-SA-21662.1-VT.ovf.ovf vi://darumuga/Pulse123\$010.204.54.201/PBU- QA/host/Dharma_ESXi_5_Cluster/asgdevesx3.bngrd.pulsesecure.net

Status: Task completed
[root@NFS_Server_117_74_Dharma VA-SPE-SA-7.2R4-21662.1]#

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 Deploying Virtual Appliances in VMware vSphere Using the Serial Port

- Overview of Scripts for Deploying Through the VMware ESX Hypervisor Serial Port
- Using the init-network-config.exp and create-va.exp Scripts

Overview of Scripts for Deploying Through the VMware ESX Hypervisor Serial Port

The following scripts are included in the VA-SPE package for deploying a virtual appliance through the serial port of a VMware ESX hypervisor.

- **init-network-config.exp** – An `expect` script that performs initial network configuration of newly instantiated SPE virtual appliances.

- **create-va.exp** – This script is a superset of the `init-network-config.exp` script. It instantiates an SPE virtual appliance and performs the initial network configuration. The `create-va.exp` script is not needed if you instantiate the virtual appliance another way.

**NOTE:** These scripts are not supported on the VMware ESXi hypervisor.

Prerequisites for these scripts are:

- Scripts must be installed and run on a Linux or UNIX system.
- The Linux or UNIX system must have the VMware Tcl/Tk Expect toolkits installed.
- The virtual appliance must be configured to use a serial console. The serial console must be accessible from the system running the scripts either through a direct connection or by telnet to a terminal server.
- (create-va.exp Script Only) The SPE ovf and vmdk files must be on the VMware ESX server where the virtual appliance is to be instantiated. You must use the serial version; the VT version is not supported.
- (create-va.exp Script Only) The OVF Tool must be installed on the VMware ESX server.

Related Documentation

- Using the init-network-config.exp and create-va.exp Scripts

Using the init-network-config.exp and create-va.exp Scripts

The `init-network-config.exp` and `create-va.exp` scripts accept input from either the command line, a configuration file, or both.
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.

Configuration file parameters use the following format:

```
paramname: paramvalue
```

A configuration file is specified using the - - file parameter. If no configuration file is specified, the script looks for a setupva.conf file in the current directory.

Each parameter must be on a separate line. Lines starting with a pound sign (#) are treated as comments.

If a parameter appears on both the command line and in the configuration file, the command line value is used.

NOTE: The init-network-config.exp and create-va.exp scripts neither validate parameters nor verify connectivity of the serial connection to the virtual appliance.

**init-network-config.exp Parameters**

The init-network-config.exp script configures the initial network configuration once the SPE virtual appliance is instantiated.

Table 11 lists all parameters for the init-network-config.exp script.

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

**Table 11: init-network-config.exp Parameters**

<table>
<thead>
<tr>
<th>Parameters for Configuration File</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- -file filename</td>
<td>The configuration file. If this parameter is not present, setupva.conf is used. Specifying a configuration file is optional.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameters for Serial Console Access</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- -ctype connecttype</td>
<td>The serial console connection. Valid values are &quot;terminal server&quot; or &quot;serial&quot;. You must place the value in double-quotes. For example, - -ctype &quot;serial&quot;. Use &quot;terminal server&quot; if the virtual appliance serial console is accessed through a telnet connection to a terminal server. Use &quot;serial&quot; if the virtual appliance serial console is accessed by directly opening a serial device at the system running the script.</td>
</tr>
<tr>
<td>- -tsip terminal server ip</td>
<td>The terminal service IP address. This parameter is valid only when ctype is set to &quot;terminal server&quot;.</td>
</tr>
<tr>
<td>- -tsport terminal server port</td>
<td>The telnet port at the terminal server used to access the virtual appliance serial console.</td>
</tr>
<tr>
<td>- -cport serial port device</td>
<td>The serial device to open to access the virtual appliance serial console. This parameter is valid only when ctype is set to &quot;serial&quot;.</td>
</tr>
</tbody>
</table>
Parameters for Virtual Appliance Initial Configuration

- `-ip ipaddress` IP address for the virtual appliance internal port.
- `-mask netmask` Virtual appliance internal port netmask.
- `-dgw default gateway` Default gateway for the virtual appliance internal port.
- `-pridns primary dns` IP address of the primary DNS server for the virtual appliance.
- `-secdns secondary dns` Optional IP address of the secondary DNS server for the virtual appliance.
- `-domain domain` Domain name for the virtual appliance.
- `-wins wins` Optional WINS server IP address.
- `-cname common name` Common name for the virtual appliance.
- `-orgname organization name` Organization name for the virtual appliance.
- `-rtxt random text` Random text used for generating a self-signed certificate.
- `-adminusr adminuser` Administrator username for the virtual appliance.
- `-adminpwd adminuser` Administrator password for the administrator account at the virtual appliance.

create-va.exp Parameters

The `create-va.exp` script accepts all the `init-network-config.exp` script parameters in Table 11. In addition, the `create-va.exp` script accepts the parameters shown in Table 12 for instantiating the virtual appliance.

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

Table 12: create-va.exp Parameters

<table>
<thead>
<tr>
<th>ESX Server-Related Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-esxhost esxhost</code> DNS name or the IP address of the ESX server where the virtual appliance is to be instantiated.</td>
</tr>
<tr>
<td><code>-exadmin ESX username</code> ESX administrator username. The script uses this username to log in to the ESX server. This user must have super user privileges.</td>
</tr>
<tr>
<td><code>-esxpasswd ESX password</code> Administrator password to log in to the VMware ESX server.</td>
</tr>
</tbody>
</table>

Parameters to Locate Resources at the ESX Server

| `-ovfpath ovf path` The location of the OVF image at the VMware ESX server. |
| `-esxserial serialdevice` Path to the serial port device on the VMware ESX server; for example, /dev/ttyS0. This value creates the virtual serial port in the virtual appliance by editing the vmx file. |
The mapping of a logical network name in the OVF specification to an actual network on the VMware ESX server. You can use the following values for ovfnet: InternalNetwork, ExternalNetwork, and ManagementNetwork.

Multiple network maps can be specified by repeating the netmap parameter.

If there are multiple target datastores on the ESX server, this parameter specifies the datastore where the virtual appliance is to be created.

Name of the virtual appliance to create.

Switches console from serial to terminal service after configuring the virtual appliance. The default is "yes", meaning switch to terminal service.

The following example uses the create-va.exp script:

```
/create-va.exp --ip 100.10.11.11 --mask 255.255.255.0 --dgw 100.10.11.1 --pridns 100.50.10.1 --secdns 100.20.10.1 --domain company.com --wins 111.11.1.11 --cname aaa.company.com --orgname "Company Inc" --rtxt "Somewhere in text123" --adminusr admin --adminpwd Password --ctype "terminal server" --tsip ts.comp.com --tsport 9999 --esxhost 10.20.50.1 --esxadmin root --esxpasswd pswd --vaname VA-SPE1 --ovfpath /root/ovfs/build12345.ovf --esxserial /tmp/ttyS0 --netmap "InternalNetwork"="ESXInternalNetwork" --netmap "ExternalNetwork"="ESXExternalNetwork" --netmap "ManagementNetwork"="ESXManagementNetwork" storage=datastore1
```

Related Documentation

* Overview of Scripts for Deploying Through the VMware ESX Hypervisor Serial Port
CHAPTER 4 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 VA-SPE 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 VA-SPE 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:

```bash
$ 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:

   ```bash
   linux# ./configure --prefix=/usr/libssh2
   (by default, libssh2 gets installed under /usr/local/include 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)

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

3. Install CPAN

   ```bash
   linux# yum install cpan
   ```

4. Install Netconf from CPAN:

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

5. Install Term::Readkey from CPAN:

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

Related Documentation

- Using the VA-SPE Sample Scripts

Using the VA-SPE Sample Scripts

After you download and install the VA-SPE 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.

```bash
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 SPE virtual appliance configuration and has the following syntax:

```
perl edit_config_ive.pl options request target
```

where:

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

<table>
<thead>
<tr>
<th>request</th>
<th>Name of the file containing the configuration in XML format. An example of the contents of a configuration file is:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>&lt;configuration&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>  &lt;system&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>    &lt;network&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>       &lt;network-overview&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>         &lt;settings&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>           &lt;node&gt;localhost2&lt;/node&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>           &lt;hostname&gt;pcs-hostname.mycompany.com&lt;/hostname&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>       &lt;/settings&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>       &lt;/network-overview&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>    &lt;/network&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>  &lt;/system&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;/configuration&gt;</code></td>
</tr>
</tbody>
</table>

| 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 5 Deploying on a Kernel-Based Virtual Machine

- About a Kernel-Based Virtual Machine
- Installing the KVM Modules
- Deploying a KVM Virtual Appliance

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
```
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 a KVM Virtual Appliance

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/kernel/arch/x86/kvm/kvm.ko
[root@localhost ~]# insmod lib/modules/KernelVersion/kernel/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.
CHAPTER 5: Deploying on a Kernel-Based Virtual Machine

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: 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
  inet addr:10.204.56.142  Bcast:10.204.63.255  Mask:255.255.240.0
  inet6 addr: fe80::230:48ff:fe32:e04e/64 Scope:Link
  UP BROADCAST RUNNING PROMISC 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:1000
  RX bytes:4082423409 (3.8 GiB)  TX bytes:158009811 (150.6 MiB)
  Interrupt:18 Memory:d8000000-d8020000
lo       Link encap:Local Loopback
  inet addr:127.0.0.1  Mask:255.0.0.0
```

© 2016 by Pulse Secure, LLC. All rights reserved
Related Documentation

- About Kernel-based Virtual Machine
- Deploying a KVM Virtual Appliance

Deploying a KVM Virtual Appliance

The `kvm-create-img.pl` script is included in the VA-SPE package for deploying a Pulse Secure virtual appliance image as a guest OS on a KVM machine.

The `kvm-create-img.pl` script accepts input from either the command line, a configuration file, or both. 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 complete list of parameters is shown in Table 13.

Table 13: `kvm-va.conf` Parameters

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>Number of GB of host virtual space (physical memory) to allocate for the guest. The default is 2 GB.</td>
</tr>
<tr>
<td>IntMapBridge</td>
<td>Bridge internal port gateway. The default is br0.</td>
</tr>
<tr>
<td>ExtMapBridge</td>
<td>Bridge external port gateway. The default is br0.</td>
</tr>
<tr>
<td>MgtMapBridge</td>
<td>Bridge management port gateway. The default is br0.</td>
</tr>
<tr>
<td>IntTapInterface</td>
<td>Internal tap networking device in the host. The default is tap1.</td>
</tr>
<tr>
<td>ExtTapInterface</td>
<td>External tap networking device in the host. The default is tap2.</td>
</tr>
<tr>
<td>MgtTapInterface</td>
<td>Management tap networking device in the host. The default is tap3.</td>
</tr>
<tr>
<td>IntMacAddr</td>
<td>Guest internal port MAC address. The default value is no MAC address.</td>
</tr>
<tr>
<td>ExtMacAddr</td>
<td>Guest external port MAC address. The default value is no MAC address.</td>
</tr>
<tr>
<td>MgtMacAddr</td>
<td>Guest management port MAC address. The default value is no MAC address.</td>
</tr>
</tbody>
</table>
CHAPTER 5: Deploying on a Kernel-Based Virtual Machine

Consoletype Serial console interface to directly access the KVM guest. The default is telnet:localhost:9999,server,nowait.

| Interfaceup | Location and name of script to a tap to an existing bridge when the guest starts. The default is /root/kvm-rli/ifupNew. |
| Interfacedown | Location and name of script to remove a tap when the guest exits. The default is /root/kvm-rli/ifdownNew. |
| Monitorva | Interface to access the virtual machine monitor. The default is telnet:localhost:8888,server,nowait. |

If a parameter appears on both the command line and in the configuration file, the command line value is used. The `kvm-create-img.pl` script neither validates parameters nor verifies connectivity to the virtual appliance.

The script format is:

```
./kvm-create-img.pl -paramname paramvalue configurationFile -valimage imageName
```

The following two examples show how to run the `kvm-create-img.pl` script.

```
./kvm-create-img.pl -configFile kvm_va.conf -valimage VA-SPE-SA-26686.1-SERIAL.img
./kvm-create-img.pl -Memory 2G -IntMapBridge br0 -Consoletype telnet::9999,server,nowait -valimage VA-SPE-SA-26686.1-SERIAL.img
```

Each parameter must be on a separate line. Lines starting with a pound sign (#) are treated as comments.

The following example shows the default `kvm-va.conf` file.

```
Memory = 2G
IntMapBridge = br0
ExtMapBridge = br0
MgtMapBridge = br0
IntTapInterface = tap1
ExtTapInterface = tap2
MgtTapInterface = tap3
IntIfMacAddr =
ExtIfMacAddr =
MgtIfMacAddr =
Consoletype = telnet:localhost:9999,server,nowait
Interfaceup = /root/kvm-rli/ifupNew
Interfacedown = /root/kvm-rli/ifdownNew
Monitorva = telnet:localhost:8888,server,nowait
```

Related Documentation

- About Kernel-based Virtual Machine
- Installing the KVM Modules
CHAPTER 6 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.

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 VA-SPE/VA-DTE through the Hyper-V Manager:

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

1. Copy the Hyper-V VA-SPE/VA-DTE Package to the Hyper-V Server
2. Open Hyper-V Manager.
3. Deploy Hyper-V VA-SPE|VA-DTE

![Hyper-V Manager](image)

4. Select Generation 1 as Hyper-V VA-SPE|VA-DTE does not support Generation 2 and click on Next.
5. Now assign the appropriate memory. Enter **2048 MB** for VA-SPE 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 opens. Check the **Use an existing virtual hard disk** button and provide the location of the Hyper-V VA-SPE/VA-DTE package.vhdx (step 1)
8. Click on Finish. Hyper-V Server creates an entry under Virtual Machines.

   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 VA-SPE|VA-DTE before powering on the VM. Adding network adapters after powering-on the Hyper-V VA-SPE|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.
   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 VA-SPE/VA-DTE through Powershell cmdlets

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

2. Open PowerShell as administrator.
3. Enter the vn-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 VA-SPE|VA-DTE on the Hyper-V Server

For example for deploying the VA-SPE:

PS> New-VM -Name hyper-v-va -MemoryStartupBytes 2048MB -VHDPath F:\hyper_v_packages\VA-SPE-SA-b1d42698.1-VT.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\VA-DTE-SA-b1d42698.1-VT.vhdx -SwitchName Int_Network_Switch -Generation 1


<table>
<thead>
<tr>
<th>Port</th>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>External</td>
<td>PS&gt; ADD-VMNetworkAdapter -VMName &lt;vm-name&gt; -SwitchName &lt;External Network Switch Name&gt;</td>
<td>PS&gt; ADD-VMNetworkAdapter -VMName hyper-v-va -Switchname Ext_Network_Switch -Name External_Port</td>
</tr>
<tr>
<td>Management Port</td>
<td>PS&gt; ADD-VMNetworkAdapter -VMName &lt;vm-name&gt; -Switchname &lt;Management Network Switch Name&gt;</td>
<td>PS&gt; ADD-VMNetworkAdapter -VMName hyper-v-va -Switchname Mgmt_Network_Switch -Name</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>IsManagementOs</th>
<th>VMName</th>
<th>SwitchName</th>
<th>MacAddress</th>
<th>Status</th>
<th>IPAddresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Adapter False hyper-v-va IntSwitch 000000000000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ext_Port False hyper-v-va ExtSwitch 000000000000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mgmt_Port False hyper-v-va MgmtSwitch 000000000000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Now, change the name of Internal Network Adapter:

PS> Rename-VMNetworkAdapter -VMName darumuga_VA_SPE_115_132 -Name "Network Adapter" -NewName "Int_Portal"

Sample Output:

<table>
<thead>
<tr>
<th>Name</th>
<th>IsManagementOs</th>
<th>VMName</th>
<th>SwitchName</th>
<th>MacAddress</th>
<th>Status</th>
<th>IPAddresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Int_Portal False hyper-v-va IntSwitch 000000000000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ext_Port False hyper-v-va ExtSwitch 000000000000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mgmt_Port False hyper-v-va MgmtSwitch 000000000000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

PS> Start-VM -name <vm-name>
PART 2 Index

- Index
PART 2 Index

C
configuration file
va.conf ............................................. 13
create-va.exp script .................................. 4
create-va.pl script ..................................... 4

G
get_active_users.pl ........................................ 4
get_active_users.xml .................................... 5
get_active_users.xsl .................................... 4

I
init-network-config.exp script ............................. 4
install-prereqs.pl script ................................ 23
ive.pm .................................................. 4
ive_methods.pl .......................................... 4

K
kvm-create-img.pl script .................................. 32

R
requirements

S
script
create-va.exp ............................................. 4
create-va.pl ............................................. 4
init-network-config.exp ................................ 4
install-prereqs.pl ....................................... 23
kvm-create-img.pl ....................................... 32
supported features ....................................... 3

T
technical support ........................................... vii
contacting PSGSC ....................................... vii

V
va.conf configuration file .................................. 13
vmware-cmd ............................................. 14

Z
zip file
contents ................................................. 4