HPSP VPN Technology Extension

V7.0

Release Notes

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

Trademark Notices

Java™ is a registered trademark of Oracle and/or its affiliates.

Linux is a U.S. registered trademark of Linus Torvalds

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of the Open Group.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Table of Contents

In This Guide

This document aims to give a brief description of all the features included in the version 7.0 of the HPSP VPN Technology Extension. For more information on the details of each feature, see the referenced documentation.

Audience

The primary audience for this guide is the user community in the organization of the CSP where HPSP VPN TE is deployed.

In addition this guide will serve as a general description of the HPSP VPN TE for system integrators and other audiences with a general interest, such as the CSP's IT experts.

References

Manuals for HPSP VPN Technology Extension v7.0:

- HPSP VPN Technology Extension v7.0 – User's Guide
- HPSP VPN Technology Extension v7.0 - Delivery Guide

Acronyms

HPSP: HP Service Provisioner
HPSP VPN TE: HP Service Provisioner Technology Extension
HP TV: HP Trueview resource inventory
HPSA VPN: HPSA VPN activation solution
HP SR: HP Subscription Repository

1 Product Identification

Product: HPSP VPN Technology Extension
Version: V7.0
Released: January 2015

2 Features

Built on top of the HP Service Provisioner, the HPSP VPN TE includes all the required components to provision L3 VPN Services, from the order entry process to the low level activation on the network.

The following components are included in the solution:

- Customer agent UI, through which VPN Services can be managed and monitored.
- VPN Product and Service Catalog, including the decomposition of the customer services in technical services.
- Workflows in charge of managing the provisioning process, associated to the technical services in the catalog.
- Out-of-the-box adaptor to interact with HP TV, in charge of the network resource inventory.
- Out-of-the-box adaptor to interact with HPSA VPN, in charge of the service activation.

Once installed, the HPSP VPN TE is ready to be used.

3 Installation notes

The solution is built on HPSP V7.0. Please refer to the HPSA documentation to see the system requirements.

For concrete information on the installation guide, please refer to the document 'HPSP VPN Technology Extension v7.0 - Delivery Guide'.

4 Verification of signed binary

HP products deliver on our 'trustworthy and reliable' brand promise. Creating and delivering an electronic cryptographic "signature" for HP code will give our customers an industry standard method to verify the integrity and authenticity of the code they received from HP before deployment.

The verification of the signed binary will be done by using GnuPG.

For RHEL (Red Hat Enterprise Linux) the GnuPgG is installed by default. You can check check the "gnupg" rpm package is installed with the following command line:

rpm -qa "gnupg*" .

If it is not installed, you can install it from your RHEL media via rpm or yum command.

To verify the signed code, you can use the following command:

gpg –verify <.sig file obtained from HPCSS> <input file>*.

The output should be as shown similar to one given bellow.

gpg: Signature made Mon 28 Jan 2013 10:40:32 AM CET using DSA key ID 2689B887

gpg: Good signature from "Hewlett-Packard Company (HP Codesigning Service)"

gpg: WARNING: This key is not certified with a trusted signature!

gpg: There is no indication that the signature belongs to the owner.

Primary key fingerprint: FB41 0E68 CEDF 95D0 6681 1E95 527B C53A 2689 B887

NOTE: message "Good signature from "Hewlett-Packard Company (HP Codesigning Service)" "indicates the code sign verification is successful.