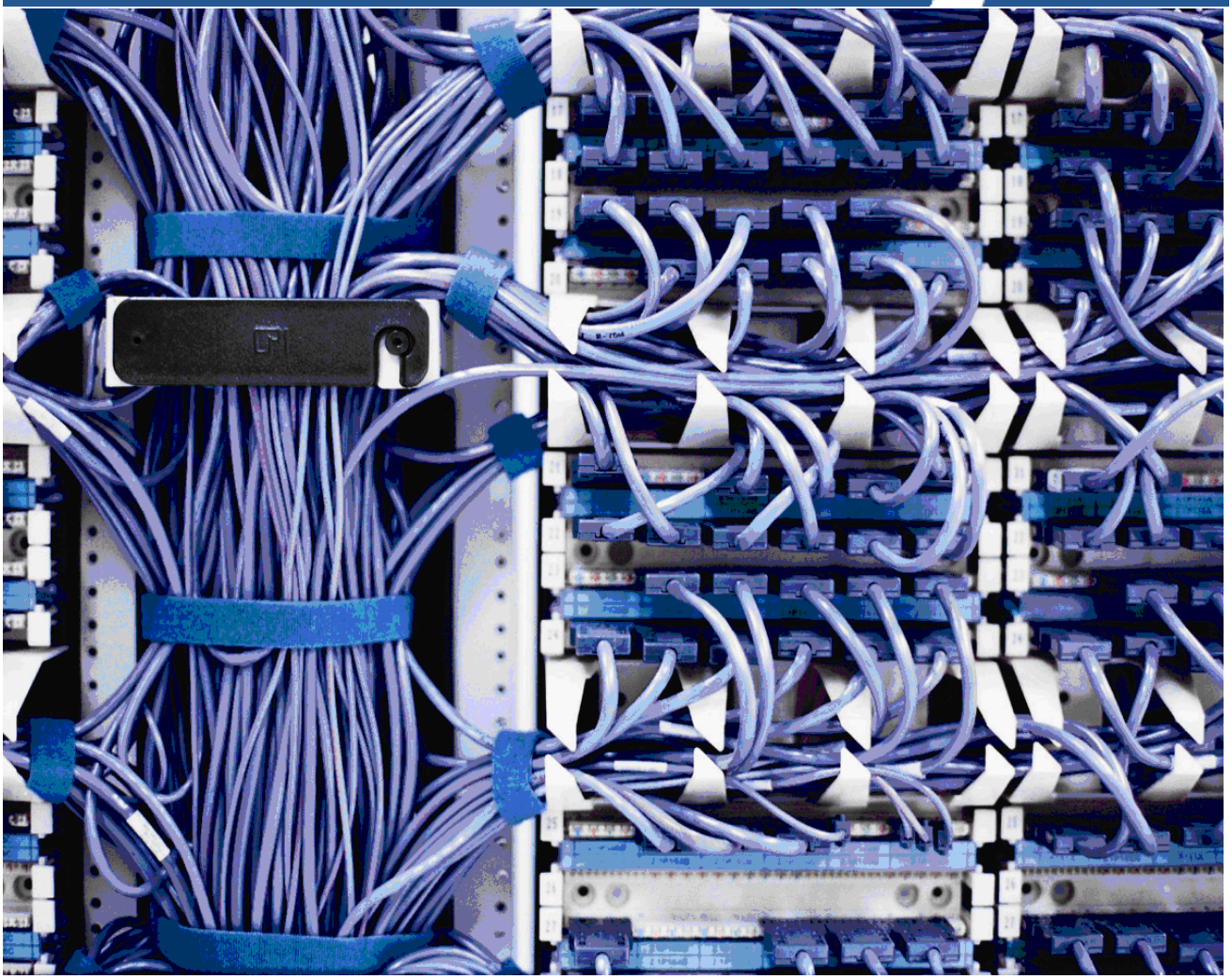
# HPSA - VPN SVP V7.0

## Installation Guide



Reference number: p180-000404

Updated edition: Jan 2015

### 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 ©(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©(1,2).

#### Copyright Notices



#### Trademark Notices

Jboss is a registered trademark of Red Hat, Inc.

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

Oracle® and Java™ are registered trademarks of Oracle and/or its affiliates.

EnterpriseDB is a registered trademark of EnterpriseDB Corporation.

UNIX® is a registered trademark of the Open Group.

Windows® and Windows NT® 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.

Printed in DK

# Contents

1 Introduction
1-1 In This Guide ..... 4
1-2 Audience ..... 4
1-3 Manual Organization ..... 4
1-4 Install Location Descriptors ..... 5
1-5 Solution Structure ..... 5
1-6 References ..... 7
2 Introduction to VPN SVP
2-1 What is the VPN Service Value Pack? ..... 8
3 VPN SVP Installation
3-1 Prerequisites ..... 9
3-2 Installation of VPN SVP ..... 10
3-2-1 New Installation of VPN SVP ..... 10
3-2-2 Post-install Configuration of VPN SVP ..... 13
3-2-3 Configuration of VPN SVP CRM Portal ..... 15
3-3 Re-installation of VPN SVP ..... 16
3-3-1 Cleaning up existing jobs ..... 16
3-4 Upgrade Installation of VPN SVP ..... 17
3-4-1 Upgrade Procedure ..... 17
3-4-2 Post-Upgrade Configuration of VPN SVP ..... 19
3-4-3 Post-Upgrade Configuration of CRM Portal ..... 19
3-5 Verification of Installation and Configuration ..... 19
3-6 Uninstalling VPN SVP and CRM Portal ..... 20
3-6-1 Uninstall without preserving existing data ..... 20
3-6-2 Uninstall preserving existing data ..... 21
4 VPN SVP Installation in Cluster Environment
4-1 Prerequisites ..... 22
4-2 First Cluster Node Installation of VPN SVP ..... 22
4-3 Following Cluster Node Installation of VPN SVP ..... 22
4-3-1 Configuration of VPN SVP. ..... 23
4-4 Verification of Installation and Configuration in a Cluster Environment ..... 23
5 Code Signing
5-1 Installing and Configuring Gnu Privacy Guard ..... 24
5-2 Verifying the Authenticity and Integrity of the Software ..... 24
Appendix A

# 1 Introduction

## 1-1 In This Guide

This guide contains installation information for the HP Service Activator VPN Service Value 7.0 (VPN SVP) which is provided as an application using the HP Service Activator (HPSA) version 7.0 framework.

The guide contains detailed information about:

- Prerequisites
- Installation of VPN SVP
- Re-installation of VPN SVP
- Upgrade installation of VPN SVP on previous versions of VPN SVP, V6.2-1A, V6.2-1B, V6.2-1C and V6.2-2A.
- Verification of a VPN SVP installation
- Un-installation of VPN SVP
- Installation of VPN SVP in cluster environment

## 1-2 Audience

The audience for this guide is:

- Systems Administrator or the installer of the VPN SVP

The installer must understand the architecture, tools, and service delivery processes described in [*HPSA_OVERVIEW*] and must in general be familiar with the HP Service Activator version 7.0 solution concept.

The installer must have a basic understanding of the OS on which the installation is done. No prior knowledge of the VPN SVP product is assumed.

In addition, the installer must have a combination of some or all of the following:

- Basic knowledge of Network configuration tasks
- Please note that the installer must have Administrator privileges to perform this installation.

## 1-3 Manual Organization

This guide contains the following chapters:

Chapter 1: “Introduction”, presenting an overview of this document.

Chapter 2: “Introduction to VPN SVP”, presenting an overview of the VPN SVP solution structure and its features.

Chapter 3: “VPN SVP Installation”, which provides detailed instructions on how make a fresh install of VPN SVP, a re-installation, an upgrade installation as well as un-installation of VPN SVP.

Chapter 4: “VPN SVP Installation in Cluster Environment”, which provides detailed instructions on how to setup VPN SVP in a Clustered environment.

Chapter 5: “Verifying the Authenticity and Integrity of the Solution” provides instructions on assessing the integrity of the delivered product before installing it, by verifying the signature of the software packages.

# 1-4 Install Location Descriptors

The following names are used to define install locations throughout this guide.

**Table 1-1** Install Location Descriptors

| Descriptor | What the Descriptor Represents |
|---|---|
| *$ACTIVATOR_OPT* | The base installation location of Service Activator.<br>The UNIX location is `/opt/OV/ServiceActivator`<br>The Windows location is<br>`<install drive>:\HP\OpenView\ServiceActivator` |
| *$ACTIVATOR_VAR* | The install location of specific Service Activator files.<br>The UNIX location is `/var/opt/OV/ServiceActivator`<br>The Windows location is<br>`$ACTIVATOR_OPT\var` |
| *$ACTIVATOR_BIN* | The install location of specific Service Activator files.<br>The UNIX location is `$ACTIVATOR_OPT/bin`<br>The Windows location is<br>`$ACTIVATOR_OPT\bin` |
| *$ACTIVATOR_ETC* | The install location of specific Service Activator files<br>The UNIX Location is `/etc/opt/OV/ServiceActivator`<br>The Windows location is<br>`$ACTIVATOR_OPT\etc` |
| *$JBOSS_HOME* | The install location for JBoss.<br>The UNIX location is `/opt/HP/jboss`<br>The Windows location is `<install drive>:\HP\jboss` |
| *$JBOSS_DEPLOY* | The install location of the Service Activator J2EE components.<br>The UNIX location is `$JBOSS_HOME/standalone/deployments`<br>The Windows location is<br>`$JBOSS_HOME\standalone\deployments` |
| *$SOLUTION* | The install location of the VPN SVP solution.<br>The location is `$ACTIVATOR_OPT/solutions/SAVPN` |

# 1-5 Solution Structure

VPN SVP 7.0 is available in the form of a zip file, VPNSVP-V70-1A.zip. Once VPN SVP is successfully imported using the Deployment Manager (DM), it extracts the files in a solution specific directory structure, `$ACTIVATOR_OPT/solutions/SAVPN`. Now the DM can be used to deploy the solution into the run-time execution environment.

The DM expects a file/directory structure as illustrated below and a `deploy.xml` descriptor adhering to the `deploy.dtd` provided by HP Service Activator 7.0.

```
SAVPN/
        |-3rd-party/
        |       |-lib/
        |       |-inventory/
        |       |-src/
        |-bin/
        |       |-ServiceUpload/
        |       |-SQLDeployer/
        |       |-XMLConverter/
        |-docs/
        |-crm.ear/
        |       |-crm.war/
        |       |-lib/
        |-etc/
        |   |-config/
        |   |       |-error_code_bundle
        |   |               |-majorcodes
        |   |               |-minorcodes
        |   |       |-inventoryTree
        |   |       |-service_upload
        |   |       |-menus
        |   |-designer/
        |   |       |-handlers/
        |   |       |-nodes/
        |   |-MigrateScripts/
        |   |-scripts/
        |   |-sql/
        |   |-template_files/
        |   |       |-Cisco
        |   |       |-Common
        |   |       |-jtp
        |   |       |-Juniper
        |   |-tests/
        |   |      |-messages/
        |   |-workflows/
        |-install/
        |-inventory/
        |-log/
        |-UI/
```

# 1-6 References

**List of References**

| Reference | Document Title | FileName |
|---|---|---|
| *HPSA_USR* | HP Service Activator User's and Administrator's Guide. Edition V70-1A | HPSA-User.pdf |
| *HPSA_MIGRATE* | HP Service Activator Migration Guide Version 6.2 to 7.0. Edition V70-1A | MigrationGuide.pdf |
| *HPSA_INSTALL* | HP Service Activator Installation Guide. Edition V70-1A | InstallationGuide.pdf |
| *HPSA_OVERVIEW* | HP Service Activator System Integrator's Overview Edition V70-1A | Overview.pdf |
| *HPSA_DEPLOY* | HP Service Activator Solution Separation and the Deployment Manager Edition V70-1A | DeploymentManager.pdf |

**NOTE:** Above documents are available in the HP Service Activator 7.0 docs folder.

# 2 Introduction to VPN SVP

The HP Service Activator VPN Service Value implements a multi vendor MPLS based VPN provisioning solution which automates repetitive task and which provides a convenient collection of tools to ease the daily work of a Service Provider.

## 2-1 What is the VPN Service Value Pack?

The VPN Service Value Pack software extends the value and benefits of the HP Service Activator framework.

The objective of the VPN Service Value is to:

- Provide an easy-to-use platform for VPN provisioning and management which enhances the effectiveness of the provider's operations and lowers the risk of configuration errors and service outages
- Reduced time to deployment through pre-implemented workflows and configuration templates
- Facilitate integration with the multi vendor equipment
- Include VPN Service Management expertise, recommendations, and best practices
- Provide an operational foundation for a solution that can easily be customized and extended to map specific customer contexts
- Include a multi-vendor catalogue of solutions and components that constantly develop in line with new services
- Integrates with the HP Network Node Manager (HP NNMi) to perform dataload of the discovered Network Elements into the VPN SVP solution
- VPN SVP supports both IPv4 and IPv6 L3 VPN/MPLS services
- VPN SVP supports the Flow-Through-Activation (FTA) requiring no operator interactions
- VPN SVP provides the North Bound Interfaces to integrate with the 3rd-party Order Management systems

The VPN SVP normally requires some customization and extensions to provide the precise services and facilities requested by a particular customer. The flexibility and openness of the HPSA framework and of VPN SVP provides an ideal environment for customer specific modifications and extensions.

# 3 VPN SVP Installation

This chapter describes how to install VPN SVP Service Pack V7.0-1A and contains the exact instructions for the installation, configuration and verification of a VPN Service Value Pack V7.0(VPN SVP) along with CRM Portal system.

## 3-1 Prerequisites

Prerequisites for VPN SVP and VPN SVP CRM Portal are:

- HP Service Activator (HPSA) 7.0 installed and configured.
- Common Resource Model Solution CRModel 7-0-0 installed and deployed.
  - To determine the version of CRModel, open the file $ACTIVATOR_OPT\solutions\CRModel\version.xml

```
<Version type="solution">
   <Solution-Name>CRModel</Solution-Name>
   <Label>CRModel</Label>
   <Major>7</Major>
   <Minor>0</Minor>
   <Revision>0</Revision>
</Version>
```

- Cygwin must be installed on windows platforms. For instruction on cygwin installation, refer to the "**Installing and Configuring Secure Shell**" section of the [*HPSA_INSTALL*]. While installing cygwin, the bash package in the Base category must be selected for installation. Note, that you must include cygwin in your System variable 'Path', e.g. as …;`C:\cygwin\bin`;..
- Bash shell should be installed on HP UX. To install GNU bash on HP-UX, download the installable from http://hpux.connect.org.uk/hppd/hpux/Shells/. Follow the instructions in these packages to complete the installation of bash.
- The database installation must include the Commandline Client programs. For instructions on oracle installation, refer to the "**Installing Database software"** section of the [*HPSA_INSTALL*].
- VPN SVP executes some external scripts from the deployment manager. On windows installations, to enable external script execution from the deployment manager, a mapping between file extensions and the interpreter to be used for should be made in the file `$ACTIVATOR_ETC/config/dm.xml`. The following snippet should be sufficient:

```
<File-Extensions>
  <Extension script_type="sh">C:\cygwin\bin\bash.exe -l</Extension>
</File-Extensions>
```

For more information on how to add the mapping, refer to the "**Deployment Manager Configuration Parameters",** sub section **"File Extensions".**

---

**WARNING:** Other solutions if deployed already may use database table names, constraint names etc that could clash with the names used by VPN SVP, in which case these will need to be resolved before deployment may succeed.

---

- For liaison between HPSA and NNM/NA, refer to the [*HPSA_INSTALL*] and [*HPSA_OVERVIEW*] for the configuration changes required.

**NOTE:** After the HPSA is installed, verify that the $ACTIVATOR_VAR/log directory has the subdirectory created with hostname (without domain) $ACTIVATOR_VAR/log/<hostname>. If such a directory does not exist, create the directory with hostname manually.
**NOTE:** Use cygwin 1.7.x or later when the product is used with Windows 2008 R2.
**NOTE:** VPN SVP liaison with NNM has not been validated for IPv6 services.

# 3-2 Installation of VPN SVP

The VPN Service Value Pack ISO file is organized as follows:

| | |
|---|---|
| /Opensource/ | Location of the 3rd-party sources and their licenses. |
| /Binaries/ | Location of the installation zip for VPN SVP and digitally signed certificate. |
| /Documentation/ | Location of the VPN SVP product documentation. |
| /Readme/ | Location of end user license agreement. |

Extract the contents of the ISO file to fetch the VPN SVP installation zip, VPNSVP-V70-1A.zip, in the Binaries folder.

**NOTE:** Binaries folder contains the VPN SVP solution and certificate file. Refer to the section 5 for instructions on verifying the authenticity of the software.

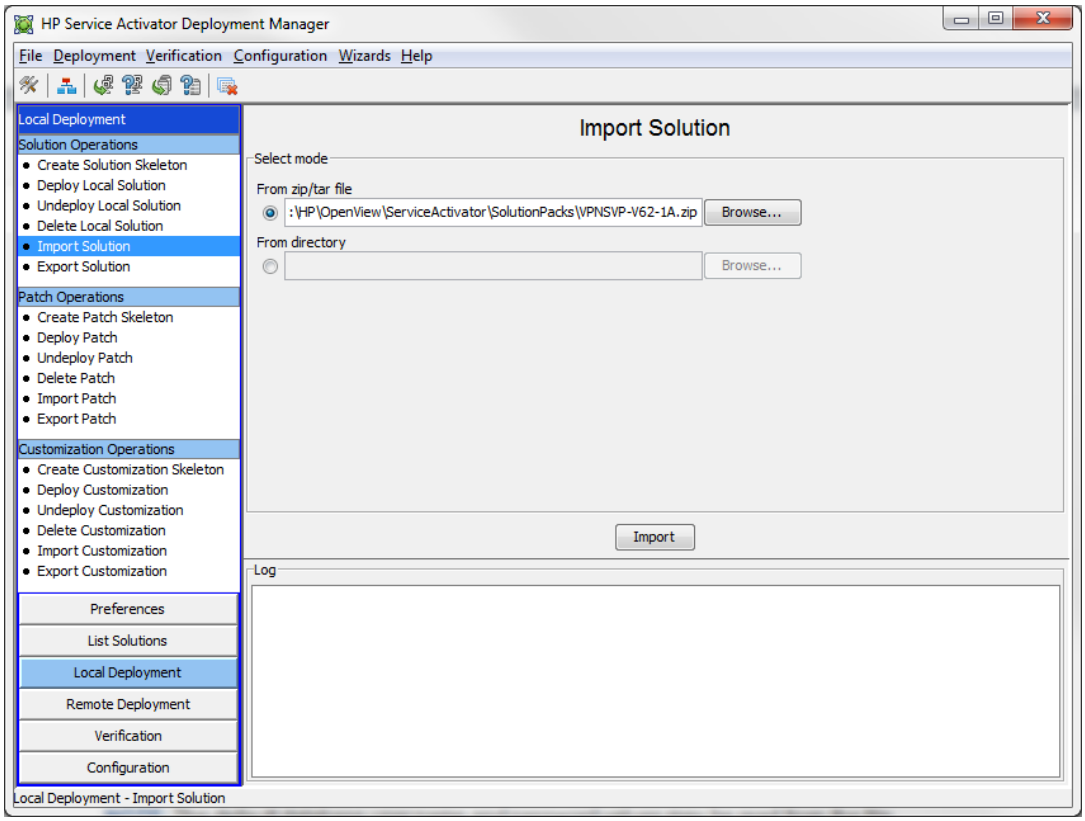
## 3-2-1 New Installation of VPN SVP

Do the following:

1. Make sure that the prerequisites described above in section 3-1 are all in place.

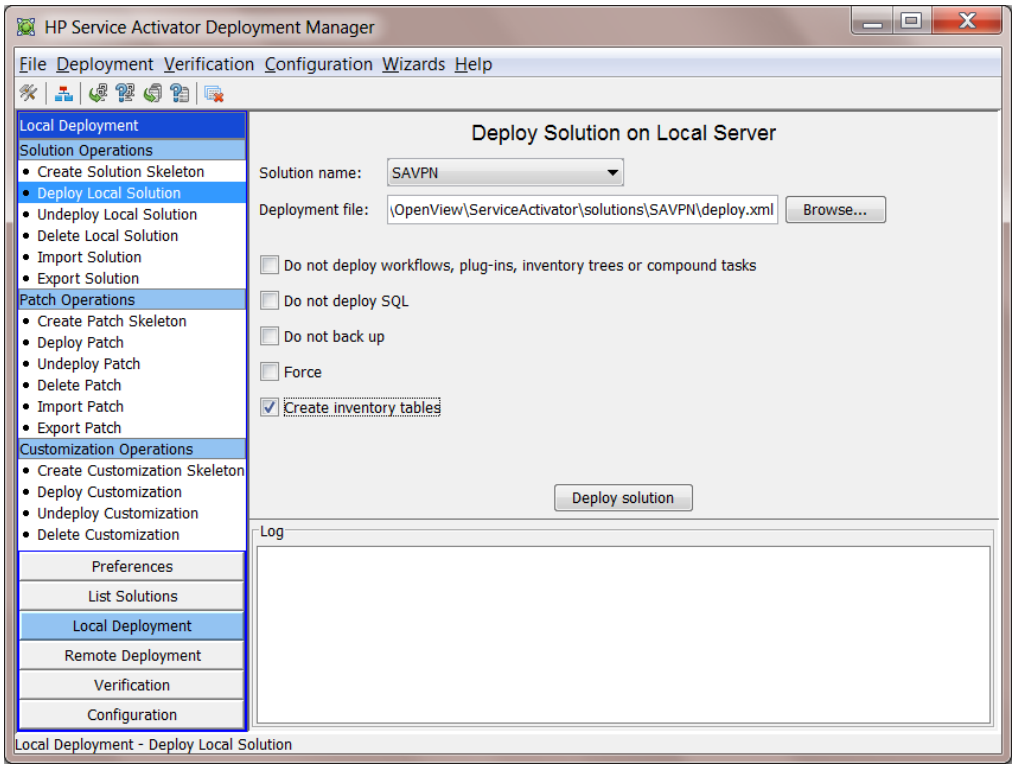
**NOTE:** During installation and configuration of HPSA, the system user and password is specified. The system user is used for all internal communication, e.g. between cluster nodes and will also be the only login available on HPSA before more users are configured. Do not use 'admin' as the system user. It may cause problems in VPN SVP.

2. Make sure the Service Activator service is not running, otherwise stop it. Refer to the section "**Starting and Stopping Service Activator**" of the [*HPSA_INSTALL*] for more details.
3. Extract the contents of the ISO file to fetch the VPN SVP installation zip, VPNSVP-V70-1A.zip, in Binaries folder.
4. Copy the installation file `VPNSVP-V70-1A.zip` into `$ACTIVATOR_OPT/SolutionPacks` directory.
5. Launch the `$ACTIVATOR_OPT/bin/deploymentmanager[.bat]`, and select the solution VPNSVP-V70-1A.zip for import, as shown in the following figure




**NOTE:** The default database user name and password values may be read from the file `$ACTIVATOR_ETC/config/dbAccess.cfg`. If the DB username and password are not configured in this file, then in the DM tool GUI → File → Preferences, Configure System Database Connection accordingly.

6. Click on the Import button to extract the solution SAVPN from the zip. This step creates the SAVPN folder under $ACTIVATOR_OPT/solutions and extracts the solution structure, as described in section 1-5 Solution Structure. This operation may take a while to complete.
7. Deploy the SAVPN solution by selecting SAVPN in the DM tool, as shown in the following figure. Since it is a new installation of SAVPN, select the check box “Create Inventory Tables”.




8. Configure VPN SVP (see section 3-2-2 Post-install Configuration of VPN SVP).
9. Configure CRM portal (see section 3-2-3 Configuration of VPN SVP CRM Portal).
    - The configuration (section 3-2-2 and/or 3-2-3 ) can be executed again manually after the product is installed if changes to the initial provided values are required. The configuration scripts suggest default values for database parameters, activator host, activator port, CRM host and CRM port. It is recommended that you use default values when being prompted.
10. After completion of the installation and configuration steps, start the Service Activator service. Refer to section "**Starting and Stopping Service Activator**" of the [*HPSA_INSTALL*] for more details.
11. The installation is complete and is ready for use.

## 3-2-2 Post-install Configuration of VPN SVP

This section describes the necessary post-install configuration of VPN SVP.

Configuration is done by a number of scripts, located in directory `$SOLUTION/etc/config`. To ease the configuration process, a single `config.sh` script executes all these scripts.

If a configuration script introduces changes to any existing HPSA configuration file, it is assumed that this file is in its original state (as left by the HPSA installation).

**NOTE:** Any existing configuration file will be backed up in the same directory with the name `<filename>.original`.

**NOTE:** Repeated execution of the configuration scripts will reuse the information in `<filename>.original`. Hence, changes made manually to `<filename>` may be lost.

**NOTE:** The changes made to following configuration files are logged in files placed in `$ACTIVATOR_VAR/log/`:

*savpnsp.install.$time.log*

*savpnsp.mwfm.xml.diff*

*savpnsp.web.xml.diff*

*savpnsp.jboss-services.xml.diff*

**NOTE:** The changes are made to following configuration files:
*$JBOSS_DEPLOY/hpsa.ear/META-INF/jboss-deployment-structure.xml*

*$JBOSS_DEPLOY/hpsa.ear/activator.war/META-INF/MANIFEST.MF*

The configuration can be done from a command line prompt on all platforms. For windows, the command can be run from the bash prompt. This description uses the command line interface:

1. Make sure that the HPSA service is stopped.
2. When HPSA service is completely stopped, execute – as root – (or as Administrator, in Windows) the configuration by issuing the following commands.

   ```
   cd $SOLUTION/etc/config
   ./config.sh
   ```

   For Windows, the commands need to be executed from the bash command prompt.

   During the configuration, the installer will be asked for the ip-address/-port of the CRM web portal. Specify required values.
3. Initialize the VPN SVP solution DB structure following the below steps.

**NOTE:** Only execute this step, if keeping the existing inventory data is not required as part of an upgrade or re-install, as the VPN SVP database structures will be cleared and reset!

In order to deploy and initialize the database structures needed by VPN SVP, execute the following:

```
cd $SOLUTION/etc/config
./resetVPNDB.sh
```

If running the above script generates errors, please check the database user name, password and instance name. Database parameters can be changed manually running Service Activator

configuration program `$ACTIVATOR_BIN/ActivatorConfig` and followed by repeating all steps from the beginning of this section as described.

**NOTE:** If it is necessary to re-configure HPSA e.g. due to other applications, VPN SVP must be un-installed first as re-configuration of ServiceActivator may remove all files used by VPN SVP.

**NOTE:** If VPN SVP is re-configured, it may overwrite changes that other ServiceActivator applications installed after VPN SVP may have added to the HPSA installation and configuration files (as the `<filename>.original` version will be used by VPN SVP as described above).

4. The VPN SVP configuration is completed.

**NOTE:** Ensure that the auditor module in $ACTIVATOR_ETC/config/mwfm.xml is not commented. This module is required for the NNM integration to work.

```
<Module>
  <Name>auditor</Name>
  <Class-Name>com.hp.ov.activator.mwfm.engine.module.DBAuditModule</Class-Name>
  <Param name="db" value="db"/>
  <Param name="store_audit" value="true"/>
  <Param name="store_statistics" value="false"/>
</Module>
```

# 3-2-3 Configuration of VPN SVP CRM Portal

**NOTE:** If the CRM Portal system is not required, the same can be removed from the Jboss application space. The CRM Portal Link on HPSA left pane can be deconfigured using HPSA's menu configuration option. For more details see Appendix A

The configuration framework of the CRM Portal resembles that of VPN SVP, i.e. individual scripts conducting self-contained parts of the configuration and a config script for a complete configuration.

Do the following:

1. Execute:

```
cd $JBOSS_DEPLOY/crm.ear/crm.war/WEB-INF/config
./config.sh
```

   During the configuration, the installer will be asked for the

   - Database connection line. Format: Server:Port:Database. Recommended to accept the suggested values.
   - Database User. Recommended to accept the suggested value.
   - Database password. Recommended to accept the suggested value.
   - Service Activator Host. Recommended to accept the suggested value.
   - Service Activator Port. Recommended to accept the suggested value.
   - Portal synchronization Socket Listener Port. Recommended to accept the suggested value.

2. Initialize the VPN SVP CRM Portal DB structure following the below steps.

**NOTE:** Only execute this step, if keeping the existing inventory data is not required as part of an upgrade or re-install, as the VPN SVP database structures will be cleared and reset!

   In order to initialize and deploy the necessary database structure needed by VPN SVP CRM Portal, execute the following

```
cd $JBOSS_DEPLOY/crm.ear/crm.war/WEB-INF/config
./resetVPNDB.sh
```

   The `resetVPNDB.sh` script may output numerous errors during its first invocation due to the attempt to remove not yet configured tables. Execute the script again to reset the database with no error messages.

   If running the script a second time still generates errors, please check database user name, password and instance name. Database parameters can be changed manually repeating all described steps from the beginning of this section.

**NOTE:** It is a prerequisite for executing the database reset script of VPN SVP CRM Portal that the VPN SVP already is installed and configured.

3. The VPN SVP CRM Portal configuration is completed.

**NOTE:** The changes are made to following configuration file:
*$JBOSS_HOME/bin/standalone.conf[.bat]* to create a deployment marker file *$JBOSS_DEPLOY/crm.ear.dodeploy*

# 3-3 Re-installation of VPN SVP

Normally, when re-installing VPN SVP, there may be a need of preserving the existing inventory data from the current installation of the product. In this case the existing data must be left in the database during de-install so that all inventory data is available again after installing the (possibly new version of the) product.

The re-installation of VPN SVP is a two step process. First step is to undeploy SAVPN, and the second step is to deploy SAVPN.

---

**NOTE:** Do not run `resetVPNDB.sh` or `initVPNDB.sh` during or after the installation as this will erase all data.

---

1. Stop all the pending jobs, jobs that are scheduled and the backup scheduler. Refer to section 3-3-1 Cleaning up existing jobs.
2. Before re-installing the VPN SVP, the existing version must be undeployed. Follow the de-installation procedure, described in section 3-6-2 Uninstall preserving existing data.
3. After this, deploy the product as described in section 3-2-1 New Installation of VPN SVP Step 7. Keep in mind to uncheck the 'create inventory tables' option.
4. When the new version is successfully installed, make sure that the HPSA service is completely stopped. Refer to the section: "**Starting and Stopping Service Activator**" of the [*HPSA_INSTALL*] for more details.

## 3-3-1 Cleaning up existing jobs

1. If there are any jobs pending, make sure that you stop them.
   - Open HPSA window.
   - Click on Jobs in the Work Area.
   - Select each job, right click and choose **'stop job'** action under each job tab except **'scheduled job'** tab.
   - The state of such jobs is set to 'Fail' in CRM Portal; you can either delete them or resubmit after the migration depending on your requirement.
2. Stop the backup scheduler if running.
   - In the tools menu, if scheduler is set to `'ON'`, click on scheduler to turn it `'OFF'`.
3. Make sure that there are no services in 'scheduled' state.
   - In the HPSA window, click on Jobs in the work area.
   - Check the 'scheduled jobs' tab.
   - If there are any services in scheduled state, follow the steps below stop the services.
     - Right click and choose **'modify job'** option. A new window pops up.
     - Modify the value of the **'Status'** to **'STOP'**.
     - Modify the **'Schedule Time'** to a little ahead of the current time.
     - Wait for all the scheduled jobs to be stopped.
     - After the migration is done, you must schedule the jobs again from CRM portal.

# 3-4 Upgrade Installation of VPN SVP

This section describes how to install VPN SVP as an upgrade to a previously installed version of VPN SVP using the VPN SVP V70-1A kit.

HPSA VPN SVP 7.0-1A is based on HPSA 7.0 and HPSA VPN SVP V62-1A/1B/1C is based on HPSA 6.2. This implies, upgrading also means upgrading the HPSA version from 6.2 to 7.0. This includes migration of the data from previous version.

Upgrade of the following VPN SVP versions is supported:

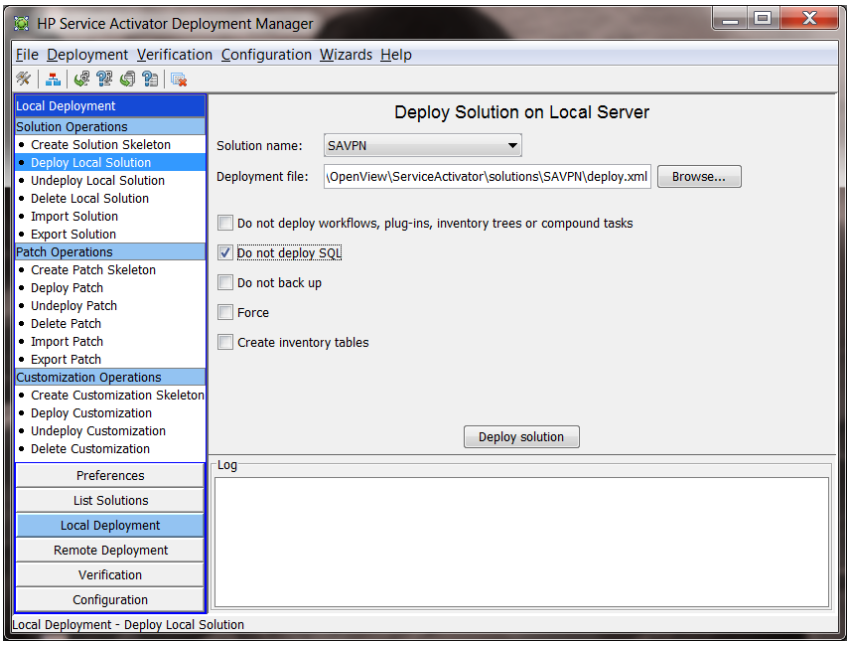
- HPSA VPN SVP V62-1A
- HPSA VPN SVP V62-1B
- HPSA VPN SVP V62-1C
- HPSA VPN SVP V62-2A

**NOTE:** If the upgrade installation is about to be done from a not supported version, please refer first to the SAVPN support team.

## 3-4-1 Upgrade Procedure

In order to upgrade from HPSA 6.2 to 7.0 followed by upgrading VPN SVP, do the following:

1. Stop all the pending jobs, jobs that are scheduled and the backup scheduler of the existing version (like section 3-3-1 Cleaning up existing jobs for this version).
2. Take a backup of the VPN SVP 6.2 database, including the HPSA 6.2 and CRModel database using standard Oracle/EnterpriseDB utilities.
3. Uninstall HPSA 6.2.
4. Delete all HPSA directories. In Windows, it is `<Drive>:\HP` folder, and in Unix, they are `/opt/HP/jboss`, `/opt/OV/ServiceActivator`, `/etc/opt/OV/ServiceActivator` and `/var/opt/OV/ServiceActivator`
5. Follow the steps specified in the [*HPSA_MIGRATE*] in order to migrate from HPSA 6.2 to HPSA 7.0.
6. Import and deploy CRModel.
   - Launch Deployment Manager UI and import CRModel.zip
   - Deploy CRModel and select the proper update deploy xml file according to your database.
7. ***Impor***t SAVPN Solution VPNS*VP-V70-1A.zip.* It will extract solution into SAVPN folder.
8. Deploy SAVPN. Check the ***'Do not deploy SQL'*** option and click on *Deploy solution* button. This step also results in migration of the VPN SVP data from the previous version of VPN SVP.




9. Configure VPN SVP. Refer to section 3-2-2 Post-install Configuration of VPN SVP
10. Configure CRM. Refer to section 3-2-3 Configuration of VPN SVP CRM Portal
11. After completion of the upgrade, start the HPSA service. Refer to the **section ”Starting and Stopping Service Activator”** of the [*HPSA_INSTALL*] for more details.
12. The upgrade installation is complete and is ready for use.

### 3-4-2 Post-Upgrade Configuration of VPN SVP

This section is common to a new installation; refer to section 3-2-1 above. But please be careful and pay attention to the following note in step 3 of the referred procedure:

**NOTE:** Only execute this step, if keeping the existing inventory data is not required as part of an upgrade or re-install, as the VPN SVP database structures will be cleared and reset!

So do not execute the `resetVPNDB.sh` script as it will cleanup preserved data.

### 3-4-3 Post-Upgrade Configuration of CRM Portal

This section is common to a new installation; refer to section 3-2-1 above. But please be careful and pay attention to the following note in step 3 of the referred procedure:

**NOTE:** Only execute this step, if keeping the existing inventory data is not required as part of an upgrade or re-install, as the VPN SVP database structures will be cleared and reset!

So do not execute the CRM Portal's `resetVPNDB.sh` script as it will cleanup preserved data.

## 3-5 Verification of Installation and Configuration

In order to verify that the VPN SVP is installed and configured correctly, do the following:

1. Start HPSA service. Refer to section "**Starting and Stopping Service Activator**" of the [*HPSA_INSTALL*] for more details.

**NOTE:** Complete start of JBoss service may take several minutes after its restart. You may verify that JBoss has completely started by monitoring the $JBOSS_HOME/standalone/log/server.log

2. Log into VPN SVP:
   - Start a browser and direct it to the URL of Service Activator login page: http://<computer name>:<port>/activator/jsp/login.jsp
   - Log in as the system user and password created when installing HPSA.
   - ServiceActivator Active Jobs page should appear in the browser.
3. Log into VPN SVP CRM portal by selecting CRM Portal from Service Activator main page, left menu:
   - Expand **Tools** menu
   - Select item **CRM Portal**
   - CRM Portal welcome page should appear in a new browser window.

# 3-6 Uninstalling VPN SVP and CRM Portal

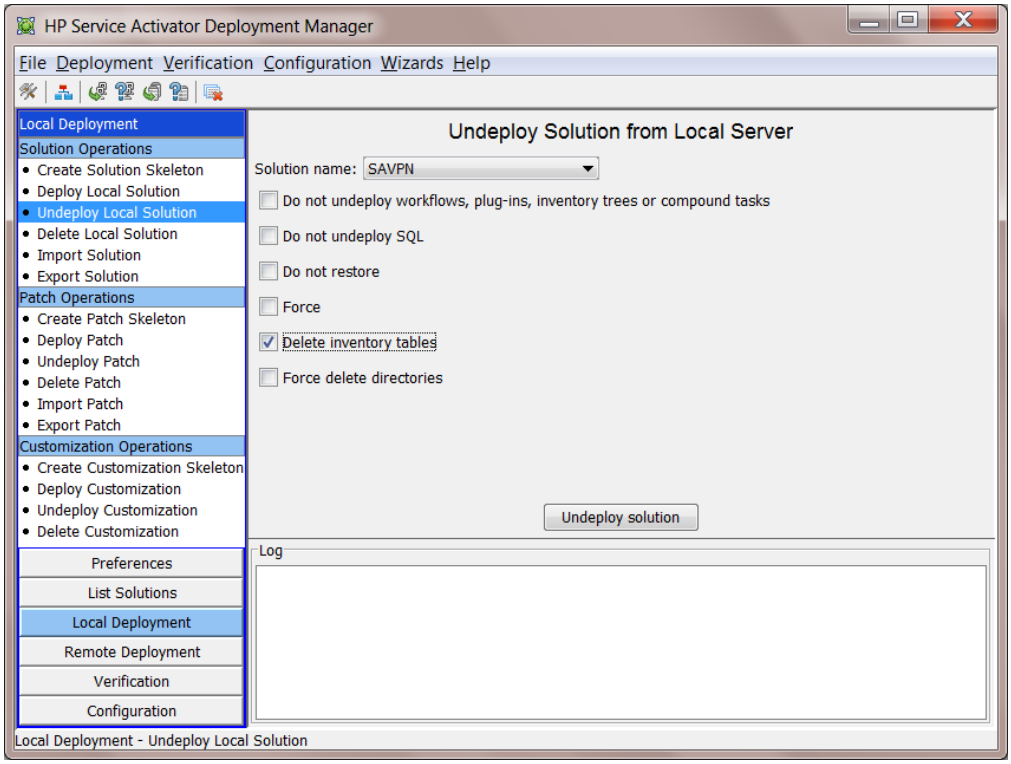
While uninstalling the VPN SVP, you may either want to preserve the existing DB schema and data, or you may not want the data. You may want to preserve the data in situation where you want to reinstall or upgrade VPN SVP.

Following sections explain both the processes.

## 3-6-1 Uninstall without preserving existing data

1. Launch the `$ACTIVATOR_OPT/bin/deploymentmanager`, and select “Undeploy Local Solution”.
2. Select the Solution name SAVPN.
3. Check the option “Delete inventory tables”, as shown in the below figure
4. Click on “Undeploy solution” to undeploy VPN SVP.

**NOTE:** If you want to re-install or upgrade your solution, you probably want to preserve your DB data. See 3-6-2 Uninstall preserving existing data

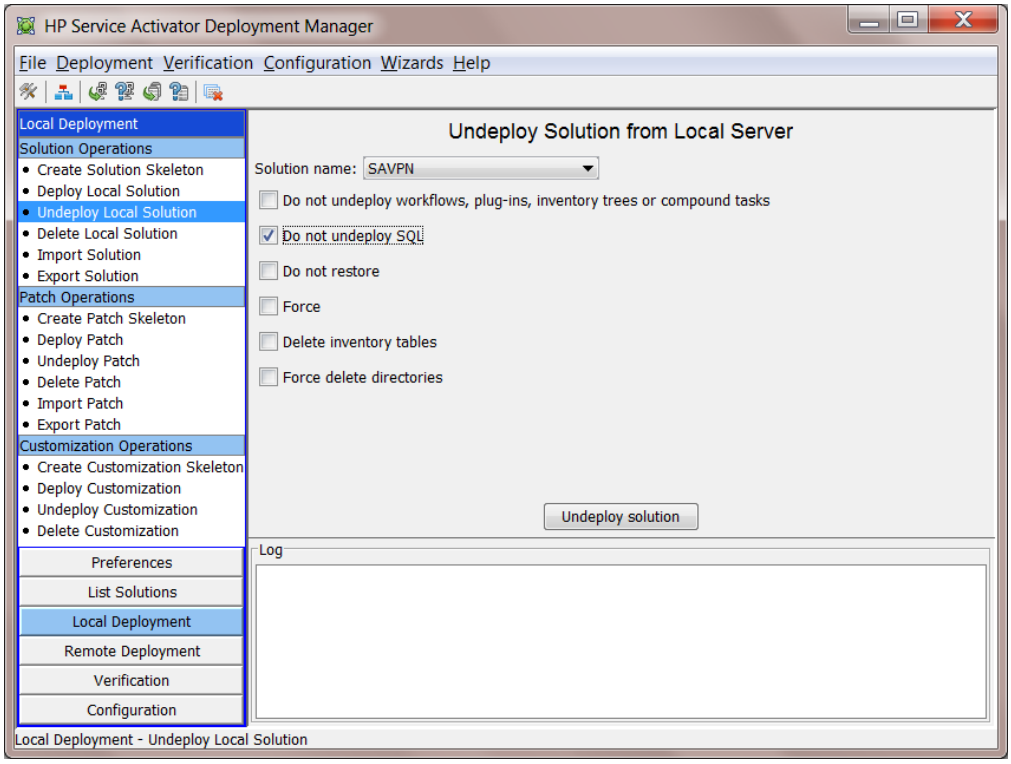



**NOTE:** The default database user name and password values may be read from the file `$ACTIVATOR_ETC/config/dbAccess.cfg`. If the DB username and password are not configured in this file, then in the DM tool GUI → File → Preferences, Configure Database Connection accordingly.

5. When the script completes running successfully, the VPN SVP solution is un-deployed, and the solution and CRM Portal are de-configured successfully.

## 3-6-2 Uninstall preserving existing data

1. Launch the `$ACTIVATOR_OPT/bin/deploymentmanager`, and select “Undeploy Local Solution”.
2. Select the Solution name SAVPN.
3. Check the option “Do not undeploy SQL”, as shown in the below figure
4. Click on “Undeploy solution” to undeploy VPN SVP. The DB tables are not dropped.




**NOTE:** The default database user name and password values may be read from the file `$ACTIVATOR_ETC/config/dbAccess.cfg`. If the DB username and password are not configured in this file, then in the DM tool GUI → File → Preferences, Configure Database Connection accordingly.

5. When the script completes successfully, the VPN solution has been un-deployed, and the solution and CRM portal have been de-configured successfully. But all the existing data are preserved in the db tables.

# 4 VPN SVP Installation in Cluster Environment

## 4-1 Prerequisites

The prerequisites for VPN SVP and VPN SVP CRM Portal in a clustered environment are as described in Prerequisites.

## 4-2 First Cluster Node Installation of VPN SVP

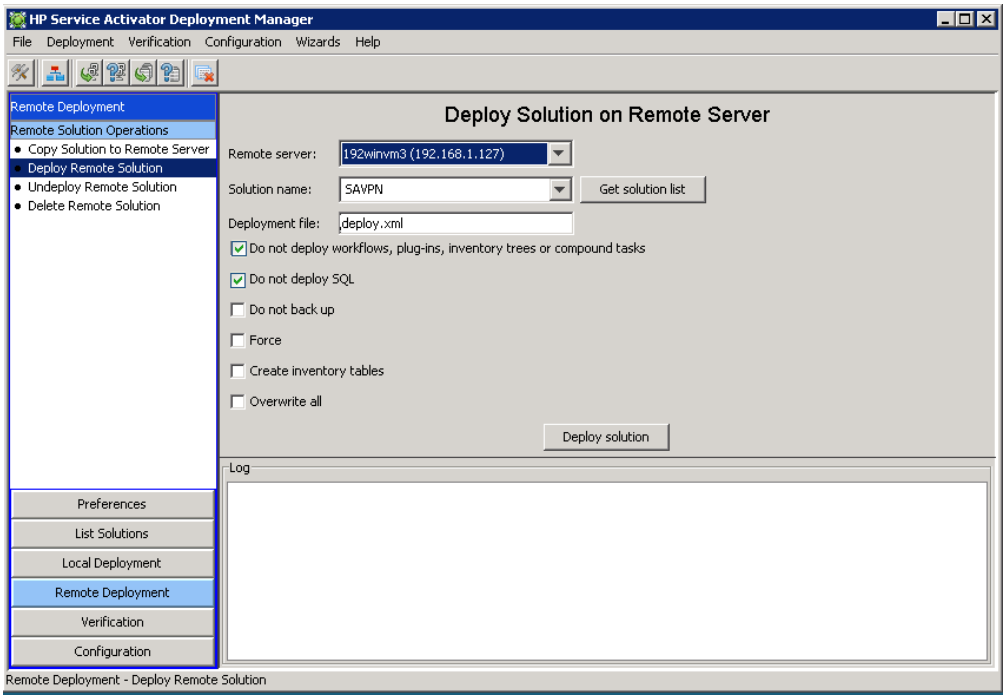
The first cluster node installation and the non-clustered installation procedures are identical. It is described in Chapter 3 VPN SVP Installation.

## 4-3 Following Cluster Node Installation of VPN SVP

This section describes the procedure of installing the VPN SVP on the second or following nodes of a cluster.

Do the following:

1. Execute steps 1 to 3 as described in section 3-2-1 New Installation of VPN SVP.
2. In a cluster setup, the solution can be deployed from the local server to other nodes using the deployment manager UI. Deployment in a cluster setup needs to be done for one node at a time. Deploying to a remote server involves two steps, copying the solution to the remote server and deploying the solution on the remote server.
    i. To copy a solution to a remote server, select the Deployment tab in the Deployment Manager and select the “Copy Solution to Remote Server” option. Select the solution from the dropdown list, then select the remote server, and finally click the [Copy solution] button. For more details on copying solution to remote server, refer to the [*HPSA_DEPLOY*] section “**Copy Solution to Remote Server**”.
    ii. After the copy is successful, select the “Deploy Remote Solution” option. The first step is selecting the remote server from the drop-down list. Then you need to click the [Get solution list] button to connect to the remote server and retrieve a list of not deployed solutions on the remote server. Select the SAVPN solution. The name of the deployment file must then be entered manually; the Deployment Manager does not provide a function to retrieve a list of deployment files from the remote server.
    iii. Select the “Do not deploy workflows, plug-ins, inventory trees or compound tasks” as well as the “Do not deploy SQL” checkboxes (these components have typically already been deployed while deploying in the local server) and uncheck the “Create Inventory Tables”. Click on [Deploy solution] button, as shown in the following figure. For more details on deploying solution to remote server, refer to the [*HPSA_DEPLOY*] section “**Deploy Remote Solution**”.




## 4-3-1 Configuration of VPN SVP

The configuration must be done from a command line prompt on all platforms. On windows, the command must be run from the bash prompt.

1. Configuration of VPN SVP: Follow the procedure describe in section 3-2-2 Post-install Configuration of VPN SVP

   During the configuration, the installer will be asked for the ip-address/-port of the CRM web portal.

   Do not change the suggested values and make sure to use localhost as the ip address and the same port number on all nodes.

2. Configuration of VPN SVP CRM Portal: Follow the procedure describe in section 3-2-3 Configuration of VPN SVP CRM Portal

   During the configuration, the installer will be asked for database related parameters as well as ip-address/-port of the Service Activator host.

   Do not change the suggested values as the database parameters must be the same on each node.

   Make sure to use localhost as the ip address and the same port number on all nodes.

The above configuration assures that the CRM portal and the HPSA service both have a floating IP address (localhost) that may be used independently of which nodes are active.

# 4-4 Verification of Installation and Configuration in a Cluster Environment

In order to make a simple and necessary (but not always a sufficient) verification that the VPN SVP is installed and configure correctly in a clustered environment, the verification procedure described in section 3-5 Verification of Installation and Configuration may be executed on each node.

Additionally, the HPSA service provides tools to e.g. view that status of the nodes in a cluster that may be used to verify the correct installation. Consult the [*HPSA_INSTALL*], [*HPSA_USR*] and [*HPSA_DEPLOY*] for more on these features.

# 5 Code Signing

This Software Product from HP is digitally signed and accompanied by Gnu Privacy Guard (GnuPG) signatures. HP strongly recommends using signature verification on its products, but there is no obligation. Customers will have the choice of running this verification or not as per their IT Policies.

## 5-1 Installing and Configuring Gnu Privacy Guard

If you do not already have GnuPG installed, you will first need to download and install it. For information about obtaining and installing GnuPG, see http://www.gnupg.org

Before verifying the signatures delivered on the HP Service Activator VPN SVP DVD, you need to configure GnuPG for accepting the HP signature. To do this, follow these steps:

1. Log on your system
2. Get the HP public key from following location: https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPLinuxCodeSigning and save the key as hpPublicKey.pub.
3. Import the key into GnuPG by running this command:

   *gpg --import hpPublicKey.pub*

## 5-2 Verifying the Authenticity and Integrity of the Software

The procedures listed below allow you to assess the integrity of the software before installing it, by verifying the signatures of the software packages.

The same signature file can be used for verifying the authenticity on HP-UX 11i v3, RHEL 6.1, MS Windows Server 2008 R2.

From a command prompt, go to the /Binaries directory on the DVD and run the following commands:

*gpg --verify VPNSVP-V70-1A.zip.sig VPNSVP-V70-1A.zip*

Look for the following output from the gpg command:

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

# Appendix A

**NOTE:** Take a backup of the files and directories mentioned in below steps, before attempting to make the changes.

Following are the steps to be followed if CRM portal needs to be removed.

1. Delete the directory crm.ear from $JBOSS_HOME/standalone/deployments.
2. Delete crm.ear.deployed directory from $JBOSS_HOME\standalone\deployments.
3. In $JBOSS_HOME/bin modify standalone.conf[.bat] to remove following entries

*set CRM_EAR_DODEPLOY=C:/HP/jboss/standalone/deployments/crm.ear.dodeploy*

*set CRM_EAR_DEPLOYED=C:/HP/jboss/standalone/deployments/crm.ear.deployed*

*set CRM_EAR_FAILED=C:/HP/jboss/standalone/deployments/crm.ear.failed*

*if exist "%CRM_EAR_DEPLOYED%" (*

*del "%CRM_EAR_DEPLOYED%"*

*)*

*if exist "%CRM_EAR_FAILED%" (*

*del "%CRM_EAR_FAILED%"*

*)*

*if exist "%CRM_EAR_DODEPLOY%" (*

*del "%CRM_EAR_DODEPLOY%"*

*)*

*echo crm > %CRM_EAR_DODEPLOY%*

4. Modify $JBOSS_HOME/standalone/deployments/hpsa.ear/META-INF/jboss-deployment-structure.xml to remove following entries

*<module name="org.apache.xalan" services="export" />*

5. Modify $JBOSS_HOME/standalone/deployments/hpsa.ear/activator.war/META-INF to remove following entries

*org.apache.xalan services export*

6. Modify $ACTIVATOR_ETC/config/menus/SAVPN_menu.xml to remove following entries

*<Item>*

*<Id>1200</Id>*

*<Label>CRM portal</Label>*

*<Url popup="true" multiple="false" menubar="true" location="true">/crm/LoginSubmit.do?userId=#user#&passWord=default</Url>*

*<SessionKeys>user</SessionKeys>*

*</Item>*

7. Modify $ACTIVATOR_HOME/solutions/SAVPN/etc/VPNDemo/resetVPNDemoAll.sh to remove the following entries

```
echo
echo "Reset CRM db ..."
echo "========================"

cd $JBOSS_HOME/standalone/deployments/crm.ear/crm.war/WEB-INF/config
./resetVPNDB.sh << EOF

EOF

echo
echo "Load portal demo data..."
echo "========================"

cd ../examples
./DeployStaticPortalData.sh NoPrompt << EOF
EOF
```