HP Server Automation

for the HP-UX, IBM AIX, Red Hat Enterprise Linux, Solaris, SUSE Linux Enterprise Server, VMware, and Windows® operating systems

Software Version: 9.0

Upgrade Guide

Document Release Date: June 2010

Software Release Date: June 2010

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Document Changes

Chapter	Date	Version	Changes
	June 2010	9.0	Document Created

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1 SA 9.0 Upgrade Overview

This section describes the requirements and procedures for upgrading to SA 9.0.

Upgrade Paths

You can upgrade to SA 9.0 from the following releases:

- SA 7.50
- SA 7.50.0x (patch releases)
- SA 7.80
- SA 7.8x (minor release)
- SA 7.80.x (patch release)

Upgrading from SAS 6.x to SA 9.0

In order to upgrade to SA 9.0 from SAS 6.x, you must first upgrade to SA 7.50 or SA 7.80, then to SA 9.0.

Zero Operational Downtime Upgrade

The standard SA 9.0 upgrade procedure requires that your Multimaster Mesh be quiesced and shut down. However, an upgrade procedure with zero operational downtime is also available, but requires that you contact HP Professional Services for more information.

MBSA Patch Database Update

In previous upgrades, SA could update the MBSA patch database. As of SA 9.0, you must update the patch database using the SA Client or the `populate-opsware-update-library` script.

New SA Configuration Parameters

The following SA configuration parameters were new as of SA 7.80. If you are upgrading from SA 7.50, you must determine the values for these parameters and provide them during the installation interview. All new parameters, except `truth.host`, are seen only in the Advanced Interview Mode.

Table 1 New SA 9.0 Configuration Parameters

New Parameter	Description
`truth.host`	The hostname of the Model Repository Host.
`word.enable_content_mirroring`	Toggles Software Repository (word) mirroring (replication) on or off. **Valid Values**: Off - 0 / On - 1 **Default**: 1 - On
`hpln_user_name`	The username used to connect to HP Live Network. (Leave as "none" if HPLN is not being configured.)
`hpln_password`	The password associated with the username used to connect to HP Live Network. (Leave as "none" if HPLN is not being configured.)
`hpln_proxy`	The address of the proxy used to connect to the HP Live Network. (Leave as "none" if HPLN is not being configured or no proxy is needed to connect to HP Live Network.)
`hpln_proxy_user`	The username of the proxy user required to connect to the HP Live Network. (Leave as "none" if HPLN is not being configured, no proxy is configured or if no username is needed.)
`hpln_proxy_pwd`	The password of the proxy user required to connect to the HP Live Network. (Leave as "none" if HPLN is not being configured, no proxy is configured or if no username is needed.)

`hpln.uninstall.keepcontent`
`(Uninstall Parameter)`
	Specifies whether HP Live Network content should be preserved when a core is uninstalled.

Changes to the Database Statistics Job

The following changes have been made to the database statistics collection jobs. These jobs can be found in the dba_jobs table. These changes are only relevant to upgraded SA Cores.

To view the jobs you can run the following from SQL*Plus

```
# su - oracle
# sqlplus "/ as sysdba"
set line 200
col priv_user format a14
col what format a50
col job format 999
select job, priv_user, what from dba_jobs where priv_user in ('AAA','TRUTH');
```

Your output should be as follows:

SA 7.50:

```
## TRUTH DBMS_STATS.GATHER_SCHEMA_STATS(ownname=>'TRUTH', options=>'GATHER AUTO');
## AAA DBMS_STATS.GATHER_SCHEMA_STATS(ownname=>'AAA', options=>'GATHER AUTO');
```

SA 7.80 and above:

```
 ## TRUTH DBMS_STATS.GATHER_SCHEMA_STATS(ownname=>'TRUTH',
         estimate_percent=>dbms_stats.auto_sample_size,
         degree=>10, method_opt=>'FOR ALL COLUMNS SIZE AUTO',
         options=>'GATHER', cascade=>TRUE, gather_temp=>TRUE);
 ## AAA DBMS_STATS.GATHER_SCHEMA_STATS(ownname=>'AAA',
         estimate_percent=>dbms_stats.auto_sample_size,
         degree=>10, method_opt=>'FOR ALL COLUMNS SIZE AUTO',
         options=>'GATHER', cascade=>TRUE, gather_temp=>TRUE);
```

Backups of the dba_jobs.what information Table

During the SA 9.0 Model Repository Guide upgrade, the SA 7.50 dba_jobs.what information table is backed up and then replaced by the SA 7.8 dba_jobs.what table. You can view the backed up information by logging in to SQL*Plus and entering the following commands:

```
# su - oracle
# sqlplus "/ as sysdba"
SQL> set line 200
SQL> col ERR_ID format 999999
SQL> col ERR_USER format a8
SQL> col ERR_TABLE format a10
SQL> col ERR_TABLE_PK_ID format a10
SQL> col ERR_CODE format 9999999
SQL> col ERR_TEXT format a20
SQL> col ERR_INFO format a30

SQL> select ERROR_INTERNAL_MSG_ID ERR_ID,
SQL>  ERR_DATE,
SQL>  ERR_USER,
SQL>  ERR_TABLE,
SQL>  ERR_TEXT,
SQL>  ERR_INFO
SQL> from ERROR_INTERNAL_MSG where ERR_TEXT = 'SA7.8 Model Repository Upgrade'
order by ERR_DATE;
```

Output will look similar to the following:

```
 ERR_ID ERR_DATE  ERR_USER ERR_TABLE  ERR_TEXT               ERR_INFO
------- --------- -------- ---------- --------------------   ------------------------------
      6 07-MAY-09 TRUTH    DBA_JOBS   SA7.8 Model Repository Pre SA7.8 dba_jobs.what value
                                      Upgrade                was: DBMS_STATS.GATHER_SCHEMA_
                                                             STATS(ownname=>'TRUTH', options
                                                             =>'GATHER AUTO');

      5 07-MAY-09 AAA      DBA_JOBS   SA7.8 Model Repositryo Pre SA7.8 dba_jobs.what value
                                      Upgrade                was: DBMS_STATS.GATHER_SCHEMA_
                                                             STATS(ownname=>'AAA', options=
                                                             >'GATHER AUTO');
```

Running the dba_jobs manually

If you need to run the System/Schema Statistics and the Garbage Collection jobs manually, you must first grant the following privilege.

```
SQL> grant create session to truth, aaa, lcrep;
```

To run the statistics collection jobs manually in SQL*Plus, use the commands shown below.

If you copy and paste the following command examples, replace the variables like `schema_user_value` with the values of the `schema_user` column displayed by the preceding select statement. Substitute the variables such as `job_no_value` with the values of the `job` column displayed by the same select statement.

```
SQL> connect <schema_user_value>/<password>
SQL> exec dbms_job.run(<job_no_value>)
```

After you are done running the jobs, you should revoke the privileges granted above. Log in to SQL*Plus and enter the following command:

```
SQL> revoke create session from truth, aaa, lcrep;
```

Important Architectural Changes from SAS 6.x to SA 9.0

If you are upgrading from *SAS 6.6, SAS 6.61, or SAS 6.61.0x (patch release)* to SA 9.0, you must first upgrade to SA 7.50 or 7.80 and you must pay close attention to the following sections in the *SA 7.50 Upgrade Guide* that describe the new SA Core Component bundling architecture. It will affect how you design your new, upgraded system.

- *SA Core Component Bundling*
- *Implications of Upgrading to a Bundled Component Environment*
- *The SAS 6.x Standalone Core vs. the SA 7.50/7.80 First Core*
- *Planning your SA 7.x Layout*
- *Gateway Migration*

It is very important that you are familiar with the new bundled component architecture as described in the *SA Planning and Installation Guide* before attempting to upgrade a SAS 6.x non-bundled component environment to SA 9.0 as moving from an unbundled component environment to a bundled component environment requires redesigning your current component layout.

Note also that you cannot upgrade directly from SAS 6.6 to SA 9.0.

You must first upgrade to SA 7.50 or 7.80, then to SA 9.0.

Core components have changed in SA 7.50 and SA 7.80. For example, there is a new component called the Management Gateway that handles communications tasks previously handled by the Core Gateway (which still exists but with a somewhat different role). Another example of changing components is the elimination of the Global File Server. This functionality is now integrated into the Slice Component bundle.

2 SA 9.0 Upgrade Prerequisites

This section describes the prerequisites for upgrading to SA 9.0.

SA Upgrade Media

The SA Core upgrade media is provided on two DVDs:

- SA Core Component installation files are provided on the on the *SA 9.0 Primary DVD*.
- Software Repository upload content is located on the *SA 9.0 Agent and Utilities DVD*.

The SA Satellite upgrade and OS Provisioning media are provided on separate DVDs:

- *SA 9.0 Satellite Base DVD*
- *OS Provisioning DVD*

A fifth disk containing the HP-supplied Oracle database is not required for the upgrade process since the database cannot be upgraded by an SA upgrade.

Copying the DVDs to a Local Disk

HP recommends that you copy the contents of the SA DVDs to a local disk or to a network share and run the Installer from that location.

Dual Layer DVD Requirements

All SA installation DVDs require a DVD drive that supports dual layer. See the *SA Standard/ Advanced Installation Guide* for more information about the SA installation media.

Model Repository/Oracle Database DVD

As of SA 7.50, the *Oracle database* used by the Model Repository was moved from the Product Distribution media DVDs to its own DVD. This does not affect upgrade because the database cannot be upgraded by an SA upgrade. However, fresh installs of SA 9.0 require a different installation procedure than previous releases. For more information, see the *SA Simple/ Advanced Installation Guide*.

SA Upgrade Scripts

The SA upgrade script, /<distro>/opsware_installer/upgrade_opsware.sh, is provided on each product DVD. Which DVD you use to run the script depends on the components you are upgrading and is specified in the upgrade instructions.

Upgrade Script Command Line Syntax

Table 2 Shows the valid arguments for upgrade_opsware.sh:

Table 2 SA Installer Command Line Arguments

Argument	Description
-h	Display the Installer upgrade help for the command line options. *To display help during the interview, press ctrl-I.*
--resp_file=*file* (-r *file*)	Invoke the upgrade using the values in the specified response file. You will create and save the response file for an installation the first time you run the upgrade installer. The installer prompts for the component to install and then runs an interview that only prompts for data missing from the specified the response file. If the response file is incomplete, the installer prompts for the missing information. The installer keeps an inventory of the components that are installed on a given server.
--interview	Conduct the upgrade installation in interview mode. You will be prompted to provide values for a number of component parameters. At the end of the interview, the installer saves the response file. Typically, you specify this option when you run the Installer for the first time. You can also specify this option when you have an incomplete response file. If you specify both the --interview and --resp_file options, the installer runs the interview but uses the values in the response file you specified as the defaults.
--verbose	Run the upgrade installer in verbose mode which causes more information to be displayed on the console.

Uninstall Upgrade Script

If you must uninstall the upgrade after it has completed, you can run uninstall_opsware.sh script. This scripts takes no arguments. It is also found in the /<distro>/opsware_installer/ directory.

DNS Considerations

During the upgrade, most `cname` pointers are added to the `hosts` file automatically on all component hosts. These entries point to the server hosting the Infrastructure Component bundle (which includes the Management Gateway which has static port forwards for these services). During installation. you will be prompted to provide the value for `truth.host`, which is the hostname of the Model Repository host.

On the Slice Component bundle host, all the required entries are automatically added to the `hosts` file when the Slice Component bundle is installed.

On *Linux hosts*, entries are added to the `/etc/hosts` file.

On *SunOS hosts,* entries are added to the `/etc/inet/hosts` and `/etc/inet/ipnodes` file, if it exists. The `/etc/hosts` file is expected to be a symlink to `/etc/inet/hosts`.

➤ It is recommended that you remove all SAS 6.x-related DNS and `hosts` file entries before proceeding with the SA 9.0 upgrade.

Customized Configuration FIles

If you have created customized configuration files for your 6.x or later installation and want to continue using them with SA 7.x or 9.0, the SA Installer saves the configuration files in:

`/var/opt/opsware/install_opsware/config_file_archive/`

The files saved are:

- `/opt/opsware/oi_util/startup/components.config`
- `/opt/opsware/oi_util/startup/opsware_start.config`
- `/etc/opt/opsware/occ/psrvr.properties`
- `/etc/opt/opsware/dhcpd/dhcpd.conf`
- `/etc/opt/opsware/spin/spin.args`
- `/etc/opt/opsware/spin/srvrgrps_attr_map.conf`
- `/etc/opt/opsware/twist/twist.conf`
- `/etc/opt/opsware/twist/loginModule.conf`
- `/etc/opt/opsware/twist/twistOverrides.conf`
- `/etc/opt/opsware/vault/vault.conf`
- `/opt/opsware/waybot/etc/waybot.args`
- `/etc/opt/opsware/mm_wordbot/mm_wordbot.args`

The SA Installer does not automatically restore customizations made in configuration files; you must do that manually. If you move components to different hosts during the upgrade, you may want to copy your customized configuration files to the new host.

➤ To use WinPE-based Windows OS Provisioning on an upgraded core, make sure that the `authoritative` keyword in the `/etc/opt/opsware/dhcpd/dhcpd.conf` file on the boot server is uncommented. If you modify the `dhcpd.conf` file, you must restart the dhcp server, such as `/etc/init.d/opsware-sas restart dhcpd.`

SA 7.50 and Later Prerequisite Checking

Also new as of SA 7.50 and later is *prerequisite checking*. This check occurs before upgrade begins and verifies that all necessary packages/patches are installed on your system, as well as verifying certain environmental conditions (diskspace, locales, required directories, and so on). Most checks are advisory, not mandatory. If a prerequisite condition is not met by your system, you will see a warning and can either stop the upgrade to mitigate the problem or continue the upgrade.

If a required package is not installed on any machine that will host a SA Core Component, you must install the package before performing the upgrade.

For more information about required packages, see the *SA Simple/Advanced Installation Guide*.

Changing Component Layout

When you upgrade a core SA attempts to identify the component layout of your existing core. If SA cannot determine your core's component layout (typical or custom), you will be prompted to specify the component layout mode used during the core's installation. The layout must be the same as you chose when you installed the core. If you choose the incorrect layout and SA cannot determine the correct layout, the upgrade can result in an inoperable system due to mismatched component layout.

Required Oracle Versions

Fresh SA 9.0 installations will install Oracle 11g (11.1.0.7) if you choose to install the HP-supplied Oracle database for the Model Repository.

If you have an existing Oracle database that you plan to use with the Model Repository, you must ensure that it is Oracle version 10.2.0.2, 10.2.0.4, or 11.1.0.7 and that is configured as described in Appendix A: Oracle Setup for the Model Repository in the *SA Simple/Advanced Installation Guide*.

Required Packages for Oracle11g

SA 9.0 now ships with Oracle 11g as the HP-supplied database. Oracle 11g has different package requirements than Oracle 10g. You do not have to upgrade to Oracle 11g from 10g and the SA 9.0 upgrade process *does not* upgrade the Oracle database for the Model Repository, however, if you decide to upgrade your Oracle database to 11g from 10g, you must ensure that the new required packages are installed before upgrading the database.

The SA Installer Prerequisite Checker validates that the required packages are installed during the upgrade and if not, prompts you to install the packages. See *Appendix A: Oracle Setup for the Model Repository* in the *SA Standard/Advanced Installation Guide* for a list of these new required packages and instructions on setting up and configuring Oracle 11g.

Oracle Preparation

You must ensure that the Oracle environment has been prepared as described below. If changes are required, you can either make the changes manually or use the SA-provided script described below.

Oracle Parameters

The HP-supplied Oracle RDBMS that was installed with SA 7.50 contained a defect in which three `init.ora` parameters were set incorrectly. If you are upgrading from SA 7.50 you should ensure that the `init.ora` parameters are set correctly.

- `nls_length_semantics='CHAR'`
- `complex_view_merging = false`
- `event='12099 trace name context forever, level 1'`

open_cursors Value

The Oracle initialization parameter `open_cursors` must be set to 1000 or more for Oracle 11g. If you have an Oracle 10g database, the value must be 300 or more.

New Permissions Required for Database User opsware_admin

Prior to SA 9.0, Oracle's Export utility (`exp`) was used to extract the data from the SA Primary Core and the Import utility (`imp`) was used to inject the data into a Secondary Core. As of SA 9.0 the Oracle Export/Import utility is replaced by Oracle's Data Pump Export (`exmpdp`) and Import (`impdp`) utility. To accommodate the new utility, additional permissions are required for the database user `opsware_admin`. Therefore, prior to upgrading to SA 9.0, your DBA must grant the following permissions to the user `opsware_admin`.

```
grant create any directory to opsware_admin;

grant drop any directory to opsware_admin;
```

Script to Fix Oracle Parameters

If the parameters are not correct, you must run the change_init_ora.sh shell script on the Model Repository (truth)/Oracle database server before you upgrade the Model Repository. The shell script can be found on the *SA Primary DVD* the following directory:

```
/<distro>/opsware_installer/tools
```

You must run the script as root on the Oracle database.

Script usage:

```
# cd /<distro>/opsware_installer/tools
```

```
# ./change_init_ora.sh <oracle_home> <oracle_sid>
```

Compatibility with SAR/BSA Essentials, OO, and NA

SA 9.0 is compatible with:

- NA (Network Automation) - See the latest NA Release Notes
- OO (Operations Orchestrator) - See the latest OO Release Notes
- BSA Essentials - See the latest BSA Essentials Release Notes

Garbage Collection

Prior to SA 7.80 the following information was contained in the Model Repository:

- Garbage collection procedures and the dba_job table for old transactions
- The audit_params table, which included values for name='DAYS_TRAN' and 'LAST_DATE_TRAN,' that specified how long old transactions were retained.

In SA 9.0 this functionality has been moved to the Vault. The Vault now handles the garbage collection job for Transactions. By default the transaction data is retained for 7 days.

If you must modify how long these transactions are retained, you can do so using SA Configuration, Model Repository Multimaster Component, vault.garbageCollector.daysToPreserve.

Preparation for SA Upgrade

Preparation for All Upgrades to SA 9.0

Before you upgrade an Single Core or Multimaster Core, perform the following tasks:

- All CORD patch releases that have been applied to all core hosts must be uninstalled (for example CORD patch release 7.50.01, or minor release 7.8.1). See Upgrading a Single Core from 7.50 or SA 7.80 to SA 9.0 on page 27 or Upgrading a Multimaster Mesh from SA 7.50 or SA 7.80 to SA 9.0 on page 36 for instructions on removing CORD patches.

- Obtain the response files that were created when you deployed SA 7.50 or 7.80.

  By default, the SA Installer saves the response file in the following directory on the servers where you installed the SA components:

  ```
  /var/opt/opsware/install_opsware/resp/resp.<timestamp>
  ```

  By looking at the timestamp, choose the latest version of the response file.

- The Core Gateways and Management Gateway must be up and running and all other SA Core Components shut down for all SA upgrades.

- The core servers hosting the Model Repository and the Software Repository must have the `en_US.UTF-8` locale installed. To display data from Managed Servers in various locales, the core server hosting the Global File System (OGFS) (part of the Slice Component bundle), must also have those locales installed.

- Verify the response file:

  Check that the values in your response file match the actual core configuration. If you have changed any of the values that are used in the response file, update the response file accordingly.

  See Verify the Response File Before Upgrading on page 18.

- Notify SA users to cancel all scheduled **Remediate Patch Policy** jobs. After upgrading a Single Core or Multimaster Core to 9.0, SA users will not see their **Remediate Patch Policy** jobs in the Job Logs (SA Client) or the My Jobs list (SAS Web Client) that ran or are scheduled to run. (By default, the data about a job is cleared from the Job Logs (SA Client) and the My Jobs list (SAS Web Client) after 30 days.)

  After the upgrade, set up the scheduled **Remediate Patch Policy** jobs again by using the Remediate function in the SA Client.

Preparation for All Multimaster Upgrades to SA 9.0

Before you upgrade a Multimaster Core to SA 9.0, perform the following task:

- Log in to the SAS Web Client as a member of the *SA System Administrator group* and check for and resolve multimaster conflicts by using the Multimaster Tools.

See the *SA Administration Guide* for information about using the Multimaster Tools.

See the *SA Administration Guide* for information about the types of SA administrators — the SA Admin user and the SA System Administrators group.

You must not proceed with a core upgrade in a Multimaster Mesh if transaction conflicts are present.

The SA Installer checks for conflicts right after you run the upgrade script. If conflicts are present, the Installer displays the a message similar to the following:

```
[root@yellow1 root]# /var/opsware/disk001/opsware_installer/
upgrade_opsware.sh -r /OPSW/yellow_mm_601.resp
Distribution version = opsware_32.a

Verifying no conflicts exist in DB "yellow_truth": FAILURE (multiple rows
selected)
```

```
Conflicts were detected in the Truth database. Please re-start the core and
resolve the conflicts before attempting to perform this upgrade.

Upgrade aborted.
```

Where `yellow_truth` is the `tnsname` of the database.

Preparation for Server Automation Reporter (SAR)

If you have installed and are running Server Automation Reporter (SAR) in the SA 7.50 Core you will be upgrading, you must stop the SAR Data Miners before performing the SA 7.50 to SA 9.0 upgrade. After the SA Core upgrade is complete, you must then apply the SAR 9.0 patch to the core and upgrade any SAR Data Miners running in that Core. You can then restart the SAR Data Miners. See the *Server Automation Reporter (SAR) Installation Guide* for information about starting and stopping SAR Data Miners.

Preparation for Windows Patch Management for All Upgrades

For all upgrades, you must download the latest version of all required Windows Patch Management utilities. For SA 9.0, the required version for MBSA is 2.1.

The SA Windows Patch Management feature requires that, before running the Installer, you obtain several files from the Microsoft software download repository and copy them to a directory that will be accessible during the SA installation. During the installation process, the Installer will prompt you to enter the fully qualified path to the Microsoft files in this directory and will fail if the files do not exist at the specified location.

Installing MBSA 2.1 for SA 9.0

To obtain the required Windows patch management files, perform the following tasks:

1. Obtain the following files from Microsoft:

   - qchain.exe

     The `qchain.exe` utility is a command-line program that chains hotfixes together. When you chain updates, you install multiple updates without restarting the computer between each installation.

     To download the package containing `qchain.exe`, search for “`qchain.exe`” at *http://www.microsoft.com* . Install the package on a Windows machine and note the location of the `qchain.exe` file.

   - WindowsUpdateAgent-x86.exe

     The `WindowsUpdateAgent30-x86.exe` file is required by the `mbsacli.exe` utility. To download the package containing `WindowsUpdateAgent30-x86.exe`, search for "Windows Update Agent" at *http://www.microsoft.com*. After downloading, you must rename the file "`WindowsUpdateAgent-x86.exe`".

- WindowsUpdateAgent-x64.exe

  The `WindowsUpdateAgent30-x64.exe` file is required by the `mbsacli.exe` utility. To download the package containing `WindowsUpdateAgent30-x64.exe`, search for "Windows Update Agent" at *http://www.microsoft.com*. After downloading, you must rename the file "`WindowsUpdateAgent-x64.exe`".

- WindowsUpdateAgent-ia64.exe

  The `WindowsUpdateAgent30-ia64.exe` file is required by the `mbsacli.exe` utility. To download the package containing `WindowsUpdateAgent30-ia64.exe`, search for "Windows Update Agent" at *http://www.microsoft.com*. After downloading, you must rename the file "`WindowsUpdateAgent-ia64.exe`"..

2. Copy the files you obtained in the preceding steps to a directory that will be accessible by the SA Installer during the Software Repository installation. For example, you might copy the files to the following directory (this directory is user definable):

   ```
   /opsw/win_util
   ```

3. Verify that the destination directory contains all these files:

   ```
   WindowsUpdateAgent-x86.exe
   WindowsUpdateAgent-x64.exe
   WindowsUpdateAgent-ia64.exe
   qchain.exe
   ```

4. Write down the name of the directory containing the files. When you run the Installer, during the Software Repository installation, you will prompted to provide the fully qualified directory path. The location you provide will be stored in the parameter, `windows_util_loc`.

These patch management files will be copied to Windows servers during SA Agent deployment. If you upload newer versions of the files to the Software Repository later, they will be downloaded to the managed Windows servers during software registration. After the core is installed and running, you can upload new versions of these files with the Patch Settings window of the SAS Client.

For information on Windows Patch Management, see the *SA User's Guide: Application Automation*.

Verify the Response File Before Upgrading

The following table provides information about how to locate the values for the parameters in the SA 7.50 05 7.80 response file.

Table 3 Locating Parameter Values to Verify the Response File

parameter	how to find the current value
`cast.admin_pwd`	This parameter specifies the password for the SA Admin user. To verify that you have the correct value, log in to the SAS Web Client as the `Admin` user.
`decrypt_passwd`	This parameter contains the password to decrypt the database of crypto material. The value for this parameter does not change after installing SA. The value should be correct in the response file.
`truth.dcId`	Log in to the SAS Web Client, click **Facilities** in the **Navigation** panel and click the facility name for the facility you are upgrading to see its ID number.
`truth.dcNm`	The Facility's short name. Log in to the SAS Web Client, click **Facilities** in the **Navigation** panel and click the facility name for the Facility you are upgrading to see its short name.
`truth.dcSubDom`	Log in to the SAS Web Client, click **System Configuration** in the **Navigation** panel, and then click the facility name for the facility you are upgrading; look up the value for `opsware.core.domain`.
`truth.dest`	*This parameter is not required for upgrades.*

`truth.gcPwd`	The password for the Oracle `gcadmin` user. To verify that you have the correct value, log in to the Model Repository (truth) as the `gcadmin` user using this password. The Oracle `gcadmin` user does not have permission to log in to Oracle. If you have entered the correct password, the following message appears:
	`ORA-01045: user GCADMIN lacks CREATE SESSION privilege; logon denied`
	If you have entered an incorrect password, the following message appears:
	`ORA-01017: invalid username/password; logon denied`

Table 3 Locating Parameter Values to Verify the Response File (cont'd)

parameter	how to find the current value

`truth.lcrepPwd`	The password for the Oracle `lcrep` user. To verify that you have the correct value, log in to the Model Repository (truth) as `lcrep` using this password. The Oracle `lcrep` user does not have permission to log in to Oracle.
	If you have entered the correct password, the following message appears:
	`ORA-01045: user LCREP lacks CREATE SESSION privilege; logon denied`
	If you have entered an incorrect password, the following message appears:
	`ORA-01017: invalid username/password; logon denied`

`truth.oaPwd`	The password for the Oracle `opsware_admin` user. To verify that you have the correct value, log in to the Model Repository (truth) as `opsware_admin` with this password.

`truth.orahome`	The path for `ORACLE_HOME`. Log on to the server hosting the Model Repository (truth) and enter the following command:
	`su - oracle`
	`echo $ORACLE_HOME`

`truth.pubViewsPwd`	The value for this parameter does not change after installing SA. The value should be correct in the response file.
`truth.servicename`	This parameter contains the `tnsname` of the Model Repository (truth). Check `/var/opt/oracle/tnsnames.ora` on the server hosting the Model Repository (truth) to find the value.
`truth.sourcePath`	This parameter must point to an existing directory.
`truth.spinPwd`	The password for the Oracle `spin` user. To verify that you have the correct value, log in to the Model Repository (truth) as `spin` using this password
`truth.tnsdir`	The directory in which the `tnsnames.ora` file is located. Typically, this file is stored in the directory `/var/opt/oracle`.

Table 3 Locating Parameter Values to Verify the Response File (cont'd)

parameter	how to find the current value

`truth.aaaPwd`	The password for the Oracle `aaa` user. To verify that you have the correct value, log in to the Model Repository (truth) database as user `aaa` using this password. The Oracle `aaa` user does not have permission to log in to Oracle.
	If you have entered the correct password, the following message appears:
	`ORA-01045: user AAA lacks CREATE SESSION privilege; logon denied`
	If you have entered an incorrect password, the following message appears:
	`ORA-01017: invalid username/ password; logon denied`

`truth.truthPwd`	The password for the Oracle `truth` user. To verify that you have the correct value, log in to the Model Repository (truth) as `truth` using this password. The Oracle `truth` user does not have permission to log in to Oracle.
	If you have entered the correct password, the following message appears:
	`ORA-01045: user TRUTH lacks CREATE SESSION privilege; logon denied`
	If you have entered an incorrect password, the following message appears:
	`ORA-01017: invalid username/password; logon denied`

`truth.twistPwd`	The password for the Oracle `twist` user. To verify that you have the correct value, log in to the Model Repository (truth) as `twist` using this password.
`truth.vaultPwd`	The password for the Oracle `vault` user. To verify that you have the correct value, log in to the Model Repository (truth) as `vault` using this password. This parameter is only relevant to Multimaster Cores.
`twist.buildmgr.passwd`	On the server where the OS Provisioning Build Manager component is installed, check the file: `/var/opt/opsware/crypto/buildmgr/twist.passwd`

Table 3 Locating Parameter Values to Verify the Response File (cont'd)

parameter	how to find the current value
`twist.integration.passwd`	On the server where the SAS Web Client component is installed, check the file `/opt/opsware/twist/Defa...` In the file, locate the entry for the Integration password by searching for `uid=integration,ou=people` and note the `userpassword` attribute.
`twist.min_uid`	*Does not change from installation.*
`media_server.linux_media`	The location of your Linux OS media. Check the server where the OS Provisioning Media Server component is installed. Because this media is NFS exported, you can check the `/etc/exports` file (Linux) or the `/etc/dfs/dfstab` file (Solaris).
`media_server.sunos_media`	The location of your Solaris OS media. Check the server where the OS Provisioning Media Server component is installed. Because this media is NFS exported, you can check the `/etc/exports` file (Linux) or the `/etc/dfs/dfstab` file (Solaris).
`word.remove_files`	*This parameter is not required for upgrades.*
`media_server.windows_media`	The location of your Windows OS media. Check the server where the OS Provisioning Media Server component is installed. Check the file to see what this value is set to. `/etc/opt/opsware/samba/smb.conf`

`media_server.windows_share_name`	On the server where the OS Provisioning Media Server component is installed, see the file:
	`/opt/OPSWsamba/etc/smb.conf`
	for the value.

`media_server.windows_share_password`	This password is only used when importing Windows OS media; it is not used internally by SA. You cannot recover or validate the current Windows share password; however, you can set it or reset it during the upgrade.
`boot_server.buildmgr_host`	Log in to the SAS Web Client, click **Service Levels** in the **Navigation** panel, click **Opsware**, click **buildmgr**, and then click the **Members** tab.
`boot_server.speed_duplex`	On the server hosting the OS Provisioning Boot Server, check the file `/opt/OPSWboot/jumpstart/Boot/etc/.speed_duplex.state`
`truth.uninstall.needdata`	*This parameter is not required for upgrades. (It is only relevant when uninstalling SA.)*

Table 3 Locating Parameter Values to Verify the Response File (cont’d)

parameter	how to find the current value
`truth.uninstall.aresure`	*This parameter is not required for upgrades. (It is only relevant when uninstalling* SA.*)*
`truth.sid`	On the server hosting the Model Repository (truth), check the `tnsnames.ora` file; for example, if the file contains an entry similar to this: `devtruthac03 = (DESCRIPTION=(ADDRESS= (HOST=truth.XXX.dev.example.com)(PORT=1521) (PROTOCOL=tcp))(CONNECT_DATA= (SERVICE_NAME=truth)))` then, the SID for the Model Repository is `truth`.
`save_crypto`	*This parameter is not required for upgrades. (It is only relevant when uninstalling SA.)*

`agent_gw_list_args`	*This value is required only when upgrading a Satellite.*
	Obtain this value from the Gateway Properties file on the server hosting the Core Gateway.
	In the properties file, locate the values for the following parameters:
	`--GWAddress`
	the IP address of the server hosting the Core Gateway.
	`--ProxyPort`
	the port number used by Server Agents to communicate with the Core Gateway (port 3001 by default).

`default_locale`	Log in to the SAS Web Client to determine which locale is being used by SA (the locale value is apparent from the SAS Web Client UI).

Table 3 Locating Parameter Values to Verify the Response File (cont'd)

parameter	how to find the current value

`ogfs.store.host.ip`	**Linux**: on the server hosting the OGFS (Slice Component bundle), check the value in the `/etc/fstab` file. The entry is specified as follows:
	`# Begin Global Filesystem mounts`
	`<ogfs.store.host.ip>``:<ogfs.store.path> /`
	`var/opt/OPSWmnt/store nfs`
	`<ogfs.audit.host.ip>:<ogfs.audit.path> /`
	`var/opt/OPSWmnt/audit nfs`
	`# End Global Filesystem mounts`
	Solaris: on the server hosting the OGFS (Slice Component bundle), check the value in the `/etc/mnttab` file. The entry is specified as follows:
	`<`**`ogfs.store.host.ip`**`>:<ogfs.store.path>`
	`/var/opt/opsware/ogfs/mnt/store nfs`
	`intr,bg,xattr,dev=43c0003       1167864831`
	`<ogfs.audit.host.ip>:<ogfs.audit.path>`
	`/var/opt/opsware/ogfs/mnt/audit nfs`
	`rw,xattr,dev=43c0004    1167864831`

`ogfs.store.path`	**Linux**: on the server hosting the OGFS (Slice Component bundle), check the value in the file `/etc/fstab`. The entry is specified as follows:
	`# Begin Global Filesystem mounts`
	`<ogfs.store.host.ip>:`**`<ogfs.store.path>`**` /`
	`var/opt/OPSWmnt/store nfs`
	`<ogfs.audit.host.ip>:<ogfs.audit.path> /`
	`var/opt/OPSWmnt/audit nfs`
	`# End Global Filesystem mounts`
	Solaris: on the server hosting the OGFS (Slice Component bundle), check the value in the `/etc/mnttab` file. The entry is specified as follows:
	`<ogfs.store.host.ip>:<`**`ogfs.store.path`**`>`
	`/var/opt/opsware/ogfs/mnt/store nfs`
	`intr,bg,xattr,dev=43c0003       1167864831`
	`<ogfs.audit.host.ip>:<ogfs.audit.path>`
	`/var/opt/opsware/ogfs/mnt/audit nfs`
	`rw,xattr,dev=43c0004    1167864831`
	Note: The path for `ogfs.store.path` must be different from the path for `ogfs.audit.path`.

Table 3 Locating Parameter Values to Verify the Response File (cont'd)

parameter	how to find the current value

`ogfs.audit.host.ip`	**Linux**: on the server hosting the OGFS (Slice Component bundle), check the value in the file `/etc/fstab`. The entry is specified as follows:
	`# Begin Global Filesystem mounts`
	`<ogfs.store.host.ip>:<ogfs.store.path> /`
	`var/opt/OPSWmnt/store nfs`
	`<ogfs.audit.host.ip>``:<ogfs.audit.path> /`
	`var/opt/OPSWmnt/audit nfs`
	`# End Global Filesystem mounts`
	Solaris: on the server hosting the OGFS (Slice Component bundle), check the value in the `/etc/mnttab` file. The entry is specified as follows:
	`<ogfs.store.host.ip>:<ogfs.store.path>`
	`/var/opt/opsware/ogfs/mnt/store nfs`
	`intr,bg,xattr,dev=43c0003       1167864831`
	`<`**`ogfs.audit.host.ip`**`>:<ogfs.audit.path>`
	`/var/opt/opsware/ogfs/mnt/audit nfs`
	`rw,xattr,dev=43c0004    1167864831`
	Note: The path for `ogfs.audit.path` must be different from the path for `ogfs.store.path`.

`ogfs.audit.path`	**Linux**: on the server hosting the OGFS (Slice Component bundle), check the value in the file `/etc/fstab`. The entry is specified as follows:
	`# Begin Global Filesystem mounts`
	`<ogfs.store.host.ip>:<ogfs.store.path> /`
	`var/opt/OPSWmnt/store nfs`
	`<ogfs.audit.host.ip>:`**`<ogfs.audit.path>`**` /`
	`var/opt/OPSWmnt/audit nfs`
	`# End Global Filesystem mounts`
	Solaris: on the server hosting the OGFS (Slice Component bundle), check the value in the `/etc/mnttab` file. The entry is specified as follows:
	`<ogfs.store.host.ip>:<ogfs.store.path>`
	`/var/opt/opsware/ogfs/mnt/store nfs`
	`intr,bg,xattr,dev=43c0003       1167864831`
	`<ogfs.audit.host.ip>:<`**`ogfs.audit.path`**`>`
	`/var/opt/opsware/ogfs/mnt/audit nfs`
	`rw,xattr,dev=43c0004    1167864831`

`windows_util_loc`	The directory in which the Windows Patch Management utilities are located. See Preparation for Windows Patch Management for All Upgrades on page 16.

Table 3 Locating Parameter Values to Verify the Response File (cont'd)

parameter	how to find the current value

`cgw_admin_port`	On the server hosting the Core Gateway, check the files:
	`/etc/opt/opsware/opswgw-cgws-<truth.dcNm>/opswgw.properties`
	`/var/opt/opsware/crypto/opswgw-cgws-<truth.dcNm>/opswgw.pem`

`cgw_address`	On the server hosting the Core Gateway, check the files:
	`/etc/opt/opsware/opswgw-cgws-<truth.dcNm>/opswgw.properties`
	`/var/opt/opsware/crypto/opswgw-cgws-<truth.dcNm>/opswgw.pem`

`cgw_proxy_port`	On the server hosting the Core Gateway, check the files:
	`/etc/opt/opsware/opswgw-cgws-<truth.dcNm>/opswgw.properties`
	`/var/opt/opsware/crypto/opswgw-cgws-<truth.dcNm>/opswgw.pem`

`agw_proxy_port`	On the server hosting the Core Gateway, check the files:
	`/etc/opt/opsware/opswgw-agws-<truth.dcNm>/opswgw.properties`
	`/var/opt/opsware/crypto/opswgw-agws-<truth.dcNm>/opswgw.pem`

`cgw_slice_tunnel_listener_port`	On the server hosting the Core Gateway, check the files:
	`/etc/opt/opsware/opswgw-cgws-<truth.dcNm>/opswgw.properties`
	`/var/opt/opsware/crypto/opswgw-cgws-<truth.dcNm>/opswgw.pem`
	NOTE: The file might contain two entries for `opswgw.TunnelDst`. Use the value from the line that specifies `opswgw.pem`.

Table 3 Locating Parameter Values to Verify the Response File (cont'd)

parameter	how to find the current value

`mgw_tunnel_listener_port`	On the server hosting the Management Gateway, check the files:
	`/etc/opt/opsware/opswgw-mgws-<truth.dcNm>/opswgw.properties`
	`/var/opt/opsware/crypto/opswgw-mgws-<truth.dcNm>/opswgw.pem`

`masterCore.mgw_tunnel_listener_port`	On the server hosting the Management Gateway, check the files:
	`/etc/opt/opsware/opswgw-mgws-<truth.dcNm>/opswgw.properties`
	`/var/opt/opsware/crypto/opswgw-mgws-<truth.dcNm>/opswgw.pem`

`word_root`	*Does not change from installation.*

3 SA 9.0 Upgrade Procedure

This section describes the procedure for upgrading to SA 9.0 from SA 7.50 and 7.80 (includes 7.50.0x patch releases and the SA 7.8x minor releases).

Upgrading a Single Core from 7.50 or SA 7.80 to SA 9.0

This section provides a summary of a Single-Host Core or Multimaster Primary Core upgrade.

Phases of a Single Core Upgrade

The upgrade process can be subdivided into phases. You can use the right-hand column to indicate that a phase is completed:

Table 4 Phases of a Single Core Upgrade

Phase	Description	Complete
Pre-Upgrade	Complete the prerequisites for the SA 9.0 upgrade and uninstall all CORD patches.	
1	Invoke the Upgrade Installer and Complete the Interview	
2	Shut down the SAS 7.x Core Components and restart the Core and Management Gateways	
3	Upgrade the Core Components	
4	Upload the Software Repository Content	

➤ If you have installed and are running Server Automation Reporter (SAR) in the SA 7.50 Core you will be upgrading, you must stop the SAR Data Miners before performing the SA 7.50 to SA 9.0 upgrade. After the SA Core upgrade is complete, you must then apply the SAR 9.0 patch to the core and upgrade any SAR Data Miners running in that Core. You can then restart the SAR Data Miners. See the *Server Automation Reporter (SAR) Installation Guide* for information about starting and stopping SAR Data Miners.

To upgrade the components, perform the following steps:

Pre-Upgrade Phase

You must complete the following tasks before beginning the upgrade.

Uninstall All CORD Patches

!! Failure to remove any CORD patches from all core systems before beginning the upgrade can cause severe damage to your core.

If you have applied a CORD patch to any hosts in your Core (for example, SA CORD Patch release 7.50.01, 7.81 etc.), you must *uninstall* the patch from *all hosts* before beginning the upgrade procedure or the upgrade will fail.

Checking Whether CORD Patches have been Removed

You can run the SA Core Health Check Monitor (HCM) to check if all CORD patches have been removed from the First Core. To verify that all systems have had the patch removed, run the following command:

```
# /opt/opsware/oi_util/bin/run_all_probes.sh
```

Usage:

```
run_all_probes.sh run|list [<probe> [<probe>...][hosts="<system>[:<password>]
[<system>[:<password>]]..." [keyfile=<keyfiletype>:<keyfile>[:<passphrase>]]
```

Where:

Table 5 Health Check Monitor Arguments

Argument	Description
<system>	Name of a reachable SA Core system
<password>	Optional root password for <system>
<keyfiletype>	SSH keyfile type (rsa_key_file or dsa_key_file)
<keyfile>	Full path to the SSH keyfile
<passphrase>	Optional pass-phrase for <keyfile>

For <probe> specify check_opsware_version.

You should specify all servers hosting core components in the current core (hosts="<system>[:<password>) . There are a number ways to specify login credentials for those hosts. For example, if you were using passwords, the full command would be like this:

```
# /opt/opsware/oi_util/bin/run_all_probes.sh \
run check_opsware_version hosts="host1.company.com:s3cr3t \
host2company.com:pAssw0rd"
```

The hostnames and passwords, of course, should be replaced with your actual values.

Correct output looks similar to this:

```
Verify base version consistent on all systems: SUCCESS
Verifying patch versions...
*** 192.168.172.5: NO PATCHES INSTALLED
*** 192.168.172.6: NO PATCHES INSTALLED
*** 192.168.172.10: NO PATCHES INSTALLED
```

```
Verify consistent patch versions: SUCCESS
```

If the script is successful and it shows that no patches are installed as above, you can proceed with the upgrade.

If the script succeeds but there are patches installed, the output will look similar to this:

```
Verify base version consistent on all systems: SUCCESS
Verifying patch versions...
*** eggplant2.eggplant.qa.opsware.com: opsware_34.c.2999.0
*** eggplant4.eggplant.qa.opsware.com: opsware_34.c.2999.0
Verify consistent patch versions: SUCCESS
```

In this case, **do not** proceed with the upgrade without first uninstalling the patches.

For more detailed information about the The SA Core Health Check Monitor (HCM), see the *SA Administration Guide*.

Removing CORD Patches

The following steps must be done one core at a time (but can be performed at the same time for each machine in a single core). However, Satellite patches cannot be uninstalled in at the same time as the uninstallation of core server patches.

To remove any applied patches, perform the following tasks:

1 Run the uninstall patch script:

```
<distro>/opsware_installer/uninstall_patch.sh
```

2 If this is a patched system, the following will be displayed:

```
 You are about to remove an Opsware patch.  All core services
 must be running to successfully perform this operation.

 Continue (Y/N)?
```

Press Y to begin the patch uninstall. The script will display progress of the uninstallation and a success message upon completion. If the CORD patch uninstall is not successful, contact your HP Support Representative.

All core services on the target machine must be running to remove a patch otherwise the patch uninstall process will fail.

If you attempt to upgrade a server that has a CORD patch still installed, the software will abort with the following message:

```
  ATTENTION: This system contains a version of Opsware that has been
  patched - upgrading or uninstalling Opsware is not permitted until
  this patch has been removed.  Please use the following program
  to remove this patch from *all* core systems before attempting the
  upgrade:

    <distribution>/opsware_installer/uninstall_patch.sh
```

```
Failure to remove the patch from all systems before beginning the
upgrade may cause severe damage to the core.

Exiting Opsware Installer.
```

Additional Pre-Upgrade Tasks

You must have installed the MBSA 2.1 Windows Patch Management Utility before beginning the upgrade. See Preparation for Windows Patch Management for All Upgrades on page 16.

1 You will need the *SA 9.0 Primary* and *SA 9.0 Agent and Utilities* DVDs.

See SA Upgrade Media on page 9, including the recommendation, Copying the DVDs to a Local Disk on page 9.

2 On the server(s) where you will upgrade any SA Core Components to SA 9.0, mount the *SA Primary* DVD or NFS-mount the directory that contains a copy of the DVD contents.

The SA upgrade Installer must have *read/write root access* to the directories where it will upgrade the SA components, including NFS-mounted network appliances.

3 On the *Model Repository host*, open a terminal window and log in as root.

4 Change to the root directory:

cd /

Phase 1: Invoke the Upgrade Installer and Complete the Interview

1 On the *Model repository host*, from the *SA 9.0 Primary DVD*, invoke the SA Installer upgrade script with the `-r` (specify response file) argument. You must have the response file used to install either SAS 7.50 or SA 7.80 depending on which release you are upgrading from. Default file names:

Typical Interview: `oiresponse.slices_master_typical` or

Custom Interview: `oiresponse.slices_master_custom`.

```
/<distro>/opsware_installer/upgrade_opsware.sh -r
<full_path_to_response_file>
```

If you are not sure where the response file for your current SA Core is, use the latest dated file from this location:

```
/var/opt/opsware/install_opsware/resp
```

2 The SA Installer attempts to determine the component layout of your core (typical or custom). If it successfully determines your layout, go to step 5 on page 31. If not, go to step 3.

3 If the SA Installer *cannot determine* the component layout required by your core, the following menu is displayed:

```
Welcome to the Opsware Installer. Please select one of the following
installation options:

1 - Multimaster Opsware Core - First Core
```

```
2 - Multimaster Installation: Define New Facility; Export Model Repository
3 - Multimaster Opsware Core - Subsequent Core


Please enter a choice from the menu, 'h' for help, 'q' to quit: 1
```

Select `Multimaster Opsware Core - First Core`.

4 The following is displayed. Select the core component layout mode used to install the SA Core being upgraded:

Be sure to select the same component layout that you selected when installing the Core you are upgrading. If you select the wrong layout mode, the upgrade can render your core unusable.

```
Please select the component layout mode. In a "typical" install,
components are already bundled together in a pre-defined configuration.
"Custom" install allows you to install components "a la carte."

1 - Typical Component Layout Mode
2 - Custom Component Layout Mode

Please select the layout mode from the menu, type 'h' for help, 'q' to
quit:
```

5 The Interview Mode screen appears. At the Interview Mode prompt, select one of the following options:

```
1 - Simple Interview Mode
2 - Advanced Interview Mode
3 - Expert Interview Mode
```

Advanced and Expert Interview modes are typically only used for complex installations and troubleshooting purposes.

Choose Option 1 to use the default values for certain configuration parameters.

Choose Option 2 or 3 to specify advanced configuration parameters during the interview.

The Installer starts in interview mode.

6 Ensure that you have verified that the response file entries are correct and accept the parameter value defaults (which are taken from the response file you specified in step 1 on page 30). There are several new parameters in SA 9.0 that you will need to supply values for or confirm. See New SA Configuration Parameters on page 4.

7 Complete the interview and save the response file. Copy it to all the servers in the existing core that host a SA 7.50 or 7.80 Core Component. The default response file name for a Typical Interview is:

`/var/tmp/oiresponse.slices_master_typical`

or for a Custom Interview:

`/var/tmp/oiresponse.slices_master_custom.`

Phase 2: Shut down the SA 7.x Core Components/Restart the Core Gateway

1. Log on to *each Core Component host* and stop all SAS 7.x Core Components *including the Core Gateway* with the command:

   ```
   /etc/init.d/opsware-sas stop
   ```

   All components are stopped.

2. Start the Core Gateway:

   ```
   /etc/init.d/opsware-sas start opswgw-cgws mgw-cgws
   ```

➤ If you are upgrading from SA 7.50, you must run the following script on the Model Repository host before upgrading the Model Repository:

```
/<distro>/opsware_installer/tools/change_init_ora.sh
```

This scripts corrects several init.ora parameters. For more information, see Oracle Preparation on page 13.

1. Invoke the upgrade script as shown in step 2 on each of the Core servers. You must upgrade the SAS 7.x components to SA 9.0 in the following order:

   a. Model Repository

➤ As part of the Model Repository upgrade, custom attribute data is migrated to new tables. If you have many custom attributes, the Model Repository upgrade phase can take a long time to complete.

   b. Infrastructure Component bundle

   c. Slice Component bundle

   d. OS Provisioning Component bundle

2. On all servers that will host components for the SA 9.0 Core, invoke the SA 9.0 upgrade script with the `-r` (specify response file) argument. You must specify the response file you created in Phase 1, step 7 on page 31:

   ```
   <distro>/opsware_installer/upgrade_opsware.sh -r
   <full_path_to_response_file>
   ```

3. In **Typical Component Layout Mode**, the following screen displays (components must be installed in the order shown, selecting a installs all components in the correct order):

   ```
   Welcome to the Opsware Installer.
   Please select the components to install.

   1 ( ) Model Repository, First Core
   2 ( ) Core Infrastructure Components
   3 ( ) Slice
   4 ( ) OS Provisioning Components

   Enter a component number to toggle ('a' for all, 'n' for none).

   When ready, press 'c' to continue, or 'q' to quit
   ```

In **Custom Component Layout Mode**, the following screen displays (components must be installed in the order shown, selecting a installs all components in the correct order):

```
Welcome to the Opsware Installer.
Please select the components to install.

1 ( ) Model Repository, First Core
2 ( ) Multimaster Infrastructure Components
3 ( ) Software Repository Storage
4 ( ) Slice
5 ( ) OS Provisioning Media Server
6 ( ) OS Provisioning Boot Server

Enter a component number to toggle ('a' for all, 'n' for none).
When ready, press 'c' to continue, or 'q' to quit.
```

4 For **both Typical and Custom layout**, select `Model Repository`. Press `c` to install the component.

During the upgrade process, you may see a series of dialogues similar to the following:

```
1/6) ServiceLevel.Opsware.way way.max_remediations:
Deployed value: 100
New value: 50
Action: Change to new value (recommended)
Enter 't' to toggle behavior or 'c' to continue.
```

Other Service Level dialogues you may see are:

```
– ServiceLevel.Opsware.way way.max_remediations.action
– ServiceLevel.Opsware.word cache_max_size
– ServiceLevel.Opsware.word cache_min_size
– ServiceLevel.Opsware.buildmgr bm.reprovision_attributes_to_preserve
– ServiceLevel.Opsware.vault LedgerReaderInterval
- ServiceLevel.Opsware.spin spin.cronbot.delete_audits.cleanup_days
- ServiceLevel.Opsware.spin spin.cronbot.delete_snapshots.cleanup_days
- ServiceLevel.Opsware.way way.max_remediations
```

You should accept the defaults for these dialogues by pressing `c` to continue. The following or similar is displayed:

```
Summary of changes to be made:
1) ServiceLevel.Opsware.way way.max_remediations: Change from 100 to 50.
2) ServiceLevel.Opsware.way way.max_remediations.action:
Change from 300 to 100.
3) ServiceLevel.Opsware.word cache_max_size: Change from
2097152 to 10485760.
4) ServiceLevel.Opsware.word cache_min_size: Change from
1572864 to 8388608.
5) ServiceLevel.Opsware.buildmgr bm.reprovision_attributes_
to_preserve: Leave as boot_kernel boot_options kernel_
arguments ksdevice nfsv4_domain reboot_command system_locale
timezone.
6) ServiceLevel.Opsware.vault LedgerReaderInterval: Change
from 200000 to 600000.
Enter 'b' to go back or 'c' to continue with the above
action(s).
```

Press c to continue.

5. For **both Typical and Custom layout**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `Core Infrastructure Components`. Press `c` to upgrade the components. In Custom Layout, all infrastructure components are upgraded except for the Software Repository. This is typically so the Software Repository can be installed on a separate host.

6. For **Custom Layout only**: log on to the server that will host the *Software Repository Storage* and re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `Software Repository Storage`. Press `c` to continue. SA upgrades the component.

7. For **both Typical and Custom layout**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `Slice`. Press `c` to continue. SA upgrades the Slice Component bundle.

8. For **Typical layout only**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `OS Provisioning Components`. Press `c` to continue. SA upgrades the OS Provisioning components.

9. For **Custom layout only**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `OS Provisioning Media Server.` Press `c` to continue. SA upgrades the OS Provisioning Media Server.

10. For **Custom layout only**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `OS Provisioning Boot Server`. Press `c` to continue. SA upgrades the OS Provisioning Boot Server

Phase 4: Upload the Software Repository Content

Linux Media Verification (LMV) is a new installation component that checks the Linux/ESX Server OS media in the Media Server and removes SA OS Provisioning Stage2 images if necessary, making the Linux/ESX Server OS media compatible with SA 7.80 Linux/ESX Server OS provisioning. LMV updates all Linux/ESX Server MRLs for which the Infrastructure Component bundle (and/or `wordstore`) has NFS `RW` permission. Therefore, you must run OS Provisioning Linux Media Verification on the core (if you choose to upgrade the Satellite to SA 9.0).

In previous releases, you would have been required in this phase to upload the OS Provisioning Stage 2 Images due to certain modifications to Linux installation media that were necessary for compatibility with SA. As of SA 7.80, these modifications are no longer required so there is no longer a requirement to upload OS Provisioning Stage 2 Images.

If you must upgrade a mesh that has pre-SA 9.0 Satellite(s) but you do not want to upgrade the satellite to SA 9.0, you can choose to do either of the following:

- (Recommended) Run OS Provisioning Linux Media Verification option, but do not migrate the Satellite media:

    a. Ensure that the core host(s) on which you run Linux Media Verification does not have NFS read/write permission to the Linux / ESX Server OS media imported in the Satellite.

    b. Run the installer script and select OS Provisioning Linux Media Verification as shown is steps 1 and 2 below.

       You will now be able to perform Linux / ESX Server provision for both of the following:

  - Linux / ESX Server provision to an SA 9.0 Core's OS Provisioning `buildmgr` using the migrated media and newly imported media.
  - Linux / ESX Server provisioning behind a pre-SA 9.0 Satellite using previously imported media in the Satellite that have not been migrated.

Please note that the OS Provisioning job will fail under the following scenarios:

- Performing Linux / ESX Server OS Provisioning behind a pre-SA 9.0 Satellite using migrated media.
- Performing Linux / ESX Server OS Provisioning behind an SA 9.0 Core's `buildmgr` using non-migrated media.
- (*Not Recommended*) Skip the OS Provisioning Linux Media Verification step.

  By doing so, you will not be able to perform any Linux / ESX Server OS Provision in the mesh. You will only be able to perform Linux / ESX Server OS Provisioning behind a pre-SA 7.80 Satellite

---

1 Upgrade to the SA 9.0 content by performing the following tasks:

  a On the *Software Repository Word Storage server*, mount the *SA Agent and Utilities DVD* and invoke `upgrade_opsware.sh` script with the response file that you generated in Phase 1,
  step 7 on page 31.

  ```
  /<distro>/opsware_installer/upgrade_opsware.sh -r /
  <full_path_to_response_file>
  ```

  The following menu appears:

  ```
  Welcome to the Opsware Installer.
  Please select the components to install.

  1 ( ) Software Repository - Content (install once per mesh)
  2 ( ) OS Provisioning Linux Media Verification (required only for
  upgrades from pre-7.8 versions)

  Enter a component number to toggle ('a' for all, 'n' for none).
  When ready, press 'c' to continue, or 'q' to quit.
  ```

  b Select a to run both options: `OS Provisioning Linux Media Verification` which restores your Linux images to the vendor default and `Software Repository - Content` which uploads the upgrade content. Although you may have multiple Software Repositories, you only need to upload the content once. The content will be automatically replicated to all other Software Repositories in the Core. Press `c` to continue.

  c If you encounter *communication timeout errors* when installing the content, restart the Multimaster Software Repository component by entering the following commands; then repeat sub-step a and sub-step b in this step:

  ```
  /etc/init.d/opsware-sas restart mm_wordbot
  ```

  If restarting the Multimaster Software Repository component does not solve the problem, restart all the Core Components on the Software Repository server by entering the following command; then repeat sub-step a and sub-step b in this step:

```
/etc/init.d/opsware-sas restart
```

You can check the `verbose.log` to see if there are any upload retry errors. The SA Installer attempts three times to upload content. If any packages fail to upload, they will be listed in the log.

2 Verify that the core upgraded successfully. Log in to the SAS Web Client as a member of the *SA System Administrator group* and run the System Diagnosis tool on the core (from the Navigation panel, click **Administration ➤ System Diagnosis**. The **System Diagnosis: Perform Diagnosis** page appears.

   Select the components that you want to test. By default, all components are selected (the Data Access Engine, the Software Repository, Command Engine, and Web Services Data Access Engine).

   You should test all components. See the *SA Administration Guide* for information about running the SA System Diagnosis tool.

➤ After you upgrade to SA 9.0, you should upgrade the Server Agent on each Managed Server in the facility. The latest version of the Server Agent enables you to use new SA features. You can continue to use non-upgraded Agents, you will not be able to take advantage of all SA 9.0 functionality. See the *SA User's Guide: Server Automation* for information about the Agent Upgrade Tool.

Upgrading a Multimaster Mesh from SA 7.50 or SA 7.80 to SA 9.0

Perform the following tasks to upgrade the Subsequent Cores in a Multimaster Mesh.

➤ The SA Prerequisite checker runs before the upgrade of *each* component selected for upgrade to validate the required environment and SA prerequisites.If a required configuration or package is missing, the upgrade may prompt you to correct the problem before it can continue. Other messages are advisory and you can continue with the upgrade, if desired.

Phases of an SA 9.0 Multimaster Upgrade

This section provides a summary of the Multimaster Core upgrade process. You can use the right-hand column to indicate that a phase is completed:

Table 6 Phases of a Multimaster Upgrade

Phase	Description	Complete
Pre-Upgrade	Uninstall all CORD patches	
1	Invoke the SA Installer and Complete the Interview on First and Subsequent Cores	
2	Quiesce the Multimaster Mesh	

Table 6 Phases of a Multimaster Upgrade (cont'd)

Phase	Description	Complete
3	Stop All Core Components	
4	Start the Core and Management Gateways in all Cores	
5	Upgrade the First Core Components	
6	Upgrade All Subsequent Core Components	
7	Upload the Software Repository Content	

Pre-Upgrade Phase

You must have installed the MBSA 2.1 Windows Patch Management Utility before beginning the upgrade. See Preparation for Windows Patch Management for All Upgrades on page 16.

If you have applied a CORD patch to any hosts in your Core (for example, SA CORD Patch release 7.50.01 or 7.81, etc.), you must uninstall the patch from all hosts before beginning the upgrade procedure or the upgrade will fail.

Checking Whether CORD Patches have been Removed

You can run the SA Core Health Check Monitor (HCM) to check if all CORD patches have been removed from the First Core. To verify that all systems have had the patch removed, run the following command:

```
# /opt/opsware/oi_util/bin/run_all_probes.sh
```

Usage:

```
run_all_probes.sh run|list [<probe> [<probe>...][hosts="<system>[:<password>]
[<system>[:<password>]]..." [keyfile=<keyfiletype>:<keyfile>[:<passphrase>]]
```

Where:

Table 7 Health Check Monitor Arguments

Argument	Description
`<system>`	Name of a reachable UNIX system
`<password>`	Optional root password for `<system>`
`<keyfiletype>`	SSH keyfile type (`rsa_key_file` or `dsa_key_file`)
`<keyfile>`	Full path to the SSH keyfile
`<passphrase>`	Optional pass-phrase for `<keyfile>`

The probe to run is `check_opsware_version`.

All hosts in the current core should be given as arguments. There are a number ways to specify login credentials for those hosts. For example, if you were using passwords, the full command would be similar to this:

```
# /opt/opsware/oi_util/bin/run_all_probes.sh \
run check_opsware_version hosts="host1.company.com:s3cr3t \
host2company.com:pAssw0rd"
```

The hostnames and passwords should be replaced with the actual values.

Correct output looks similar to this:

```
Verify base version consistent on all systems: SUCCESS
Verifying patch versions...
*** 192.168.172.5: NO PATCHES INSTALLED
*** 192.168.172.6: NO PATCHES INSTALLED
*** 192.168.172.10: NO PATCHES INSTALLED
Verify consistent patch versions: SUCCESS
```

If the script is successful and it shows that no patches are installed as above, you can proceed with the upgrade.

If the script succeeds but there are patches installed, the output will look similar to this:

```
Verify base version consistent on all systems: SUCCESS
Verifying patch versions...
*** eggplant2.eggplant.qa.opsware.com: opsware_34.c.2999.0
*** eggplant4.eggplant.qa.opsware.com: opsware_34.c.2999.0
Verify consistent patch versions: SUCCESS
```

In this case, **do not** proceed with the upgrade without first uninstalling the patches.

For more detailed information about the The SA Core Health Check Monitor (HCM), see the *SA Administration Guide*.

Removing CORD Patches

➤ The following steps must be done one core at a time (but can be performed in parallel for each machine in a single core).However, patched Satellites cannot be uninstalled in parallel with the uninstallation of core servers.

To remove any applied patches, perform the following tasks:

1 Run the uninstall patch script:

```
<distro>/opsware_installer/uninstall_patch.sh
```

2 If this is a patched system, the following will be displayed:

```
 You are about to remove an Opsware patch.  All core services
 must be running to successfully perform this operation.

 Continue (Y/N)?
```

Press `Y` to begin the patch uninstall. The script will display progress of the uninstallation and a success message upon completion. If the CORD patch uninstall is not successful, contact your HP Support Representative.

➤ All core services on the target machine must be running to remove a patch otherwise the patch uninstall process will fail.

➤ Failure to remove any CORD patches from all core systems before beginning the upgrade can cause severe damage to your core.

If you attempt to upgrade a server that has a CORD patch still installed, the software will abort with the following message:

```
ATTENTION: This system contains a version of Opsware that has been
patched - upgrading or uninstalling Opsware is not permitted until
this patch has been removed.  Please use the following program
to remove this patch from *all* core systems before attempting the
upgrade:

  <distribution>/opsware_installer/uninstall_patch.sh

Failure to remove the patch from all systems before beginning the
upgrade may cause severe damage to the core.

Exiting Opsware Installer.
```

Phase 1: Invoke the SA Installer and Complete the Interview on First and Subsequent Cores

1 From the *Model Repository host*, mount the *SA 9.0 Primary DVD* and invoke the SA Installer upgrade script with the `-r` (specify response file) argument. You must have the response file you created when installing SA 7.50 or SA 7.80 depending on your Core's current version.

```
# /<distro>/opsware_installer/upgrade_opsware.sh -r
<full_path_to_response_file>
```

2 On the **First Core**, perform the following steps to complete the interview process:

a The SA Installer attempts to determine the component layout of your core (typical or custom). If it successfully determines your layout, go to step b. If not, you will see the following:

.

Select the component layout mode used to install the core then continue with step b:

```
Please select the component layout mode. In a "typical" install,
components are already bundled together in a pre-defined configuration.
"Custom" install allows you to install components "a la carte."

1 - Typical Component Layout Mode
2 - Custom Component Layout Mode

Please select the interview mode from the menu, type 'h' for help, 'q'
to quit:
```

You must select the same component layout that you selected when installing the Core you are upgrading. If you select the wrong layout mode, the upgrade can render your core unusable.

b The following menu is displayed:

```
Welcome to the Opsware Installer. Please select one of the following
installation options:

1 - Multimaster Opsware Core - First Core
2 - Multimaster Installation: Define New Facility; Export Model Repository
3 - Multimaster Opsware Core - Subsequent Core
```

```
Please enter a choice from the menu, 'h' for help, 'q' to quit:
```

- c Select `Multimaster Installation: First Core.`
- d The Interview Mode screen appears. At the Interview Mode prompt, select one of the following options:

  ```
  1 - Simple Interview Mode
  2 - Advanced Interview Mode
  3 - Expert Interview Mode
  ```

  Advanced and Expert Interview modes are typically only used for complex installations and troubleshooting purposes.

  Choose Option 1 to use the default values for certain configuration parameters.

  Choose Option 2 or 3 to specify advanced configuration parameters during the interview.

  The parameter values displayed during the interview are taken from the response file you specified when invoking the upgrade script. It is rare that you will need to change these values so you should accept the defaults during the interview.

  The Installer starts the interview mode.

- e Accept the defaults (which are taken from the response file you specified in step 1 on page 39). There are several new parameters in SA 9.0 that you will need to supply values for or confirm. See New SA Configuration Parameters on page 4.
- f Save the response file and copy it to all the servers in the core running a Core Component. You can accept the default response file name or provide your own. The default response file name for a Typical Interview is:

  ```
  /var/tmp/oiresponse.slices_master_typical
  ```

  or for a Custom Interview:

  ```
  /var/tmp/oiresponse.slices_master_custom
  ```

3 For each **Subsequent** Core in the mesh, as in the steps above, perform the following to complete the interview process:

- a Invoke the SA Installer upgrade script with the `-r` response file argument. The response file must be the response file you created when installing SA 7.50 or SA 7.80 Subsequent Core depending on your Core's current version

  ```
  # /<distro>/opsware_installer/upgrade_opsware.sh -r
  <full_path_to_response_file>
  ```

- b The SA Installer attempts to determine the component layout of your core (typical or custom). If it successfully determines your layout, go to step d. If not, go to step c.
- c The following is displayed, select a component layout mode:

  ```
  Please select the component layout mode. In a "typical" install,
  components are already bundled together in a pre-defined configuration.
  "Custom" install allows you to install components "a la carte."
  ```

```
1 - Typical Component Layout Mode
2 - Custom Component Layout Mode

Please select the interview mode from the menu, type 'h' for help, 'q'
to quit:
```

➤ Be sure to select the same component layout that you selected when installing the Core you are upgrading. If you select the wrong layout mode, the upgrade can render your core unusable.

d The following menu is displayed:

```
Welcome to the Opsware Installer. Please select one of the following
installation options:

1 - Multimaster Opsware Core - First Core
2 - Multimaster Installation: Define New Facility; Export Model
Repository
3 - Multimaster Opsware Core - Subsequent Core

Please enter a choice from the menu, 'h' for help, 'q' to quit:
```

Select `Multimaster Opsware Core - Subsequent Core`.

e The Interview Mode screen appears. At the Interview Mode prompt, select one of the following options:

```
1 - Simple Interview Mode
2 - Advanced Interview Mode
3 - Expert Interview Mode
```

Advanced and Expert Interview modes are typically only used for complex installations and troubleshooting purposes.

Choose Option 1 to use the default values for certain configuration parameters.

Choose Option 2 to specify advancedconfiguration parameters during the interview.

The parameter values displayed during the interview are taken from the response file you specified when invoking the upgrade script. It is rare that you will need to change these values so you should accept the defaults during the interview.

The Installer starts the interview mode.

f Accept the defaults and save the response file. Copy it to all servers in each **Subsequent** Core running a Core Component. The default response file name for a Typical Interview is:

```
/var/tmp/oiresponse.slices_slave_typical
```

or for a Custom Interview:

```
/var/tmp/oiresponse.slices_slave_custom
```

Phase 2: Quiesce the Multimaster Mesh

Examine the SAS Web Client **Multimaster State** page to ensure that there are no outstanding transactions or conflicts. If conflicts. exist, resolve them as described in the *SA Administration Guide*.

Phase 3: Stop All Core Components

1 *On all cores*, stop all Core Components except the Model Repository.

It is important that you do not stop the Oracle database.

a To stop the Core Components, on each Core Server, run the following command:

```
# /etc/init.d/opsware-sas stop
```

Phase 4: Start the Core and Management Gateways in all Cores

1 On *every Slice Component bundle host*, start the *Core Gateways*:

```
# /etc/init.d/opsware-sas start opswgw-cgws
```

2 On the *Infrastructure Component bundle host*, (or on the Multimaster Infrastructure Component bundle host, if you have a custom layout), start the *Management Gateway*:

```
# /etc/init.d/opsware-sas start opswgw-mgw
```

Phase 5: Upgrade the First Core Components

1 On the **First** Core, invoke the `upgrade_opsware.sh` script with the `-r <response_file>` option. Use the response file you created in Phase 1, step 2 on page 39.

```
# /<distro>/opsware_installer/upgrade_opsware.sh -r
<full_path_to_response_file>
```

The *Upgrade Component* menu is displayed (components must be installed in the order shown, selecting a installs all components in the correct order):

In **Typical Component Layout Mode**, the following screen displays:

```
Welcome to the Opsware Installer.
Please select the components to install.

1 ( ) Model Repository, First Core
2 ( ) Core Infrastructure Components
3 ( ) Slice
4 ( ) OS Provisioning Components

Enter a component number to toggle ('a' for all, 'n' for
none).

When ready, press 'c' to continue, or 'q' to quit
```

In **Custom Component Layout Mode**, the following screen displays (components must be installed in the order shown, selecting a installs all components in the correct order):

```
Welcome to the Opsware Installer.
Please select the components to install.

1 ( ) Model Repository, First Core
2 ( ) Multimaster Infrastructure Components
3 ( ) Software Repository Storage
4 ( ) Slice
5 ( ) OS Provisioning Media Server
6 ( ) OS Provisioning Boot Server, Slice version

Enter a component number to toggle ('a' for all, 'n' for none).
When ready, press 'c' to continue, or 'q' to quit.
```

Option 3 (Software Repository Storage) appears only when the script is invoked on an SA 7.50 *Software Repository* host.

You must run the following script on the Model Repository host before upgrading the Model Repository:

```
/<distro>/opsware_installer/tools/change_init_ora.sh
```

This scripts corrects several init.ora parameters. For more information, see Oracle Preparation on page 13.

2 Run the following script to set change the Oracle database parameter `nls_length_semantics` from BYTE to CHAR

```
<distro>/var/tmp/oitmp/opsware_installer/tools/change_init.ora.sh
```

3 For **both Typical and Custom layout**, select `Model Repository`. Press `c` to install the component.

While you upgrade the Model Repository, you might be prompted to confirm the SA configuration values.These values are taken from the response file, so you should accept the defaults.

As part of the Model Repository upgrade, custom attribute data is migrated to new tables. If you have many custom attributes, the Model Repository upgrade phase can take a long time to complete.

4 For **both Typical and Custom layout**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `Core Infrastructure Components`. Press `c` to upgrade the components.

5 For **Custom Layout only**: log on to the server that will host the *Software Repository Storage* and re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `Software Repository` Storage. Press `c` to continue. SA upgrades the component.

6 For **both Typical and Custom layout**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `Slice`. Press `c` to continue. SA upgrades the Slice Component bundle.

If you are upgrading multiple Slice Component bundles, they must be upgraded one-at-a-time. Simultaneous upgrade is not supported.

7 For **Typical layout only**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `OS Provisioning Components`. Press `c` to continue. SA upgrades the OS Provisioning components.

8 For **Custom layout only**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `OS Provisioning Media Server.` Press `c` to continue. SA upgrades the OS Provisioning Media Server.

9 For **Custom layout only**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `OS Provisioning Boot Server`. Press `c` to continue. SA upgrades the OS Provisioning Boot Server

If the upgrade takes more than an hour from the time the Data Access Engine (`spin`) starts up, some managed devices may be marked unreachable. Run the communications test to resolve this.

Phase 6: Upgrade All Subsequent Core Components

1 Invoke the upgrade script as shown in step 3 on page 44 on each of the Core servers. You must upgrade the SAS 7.x components to SA 9.0 in the following order:

a Model Repository

As part of the Model Repository upgrade, custom attribute data is migrated to new tables. If you have many custom attributes, the Model Repository upgrade phase can take a long time to complete.

b Infrastructure Component bundle

c Slice Component bundle

d OS Provisioning Component bundle

2 Run the following script to set change the Oracle database parameter `nls_length_semantics` from BYTE to CHAR

```
<distro>/var/tmp/oitmp/opsware_installer/tools/change_init.ora.sh
```

3 On all **Subsequent** Cores, invoke `upgrade_opsware.sh script` with the `-r` (specify response file) argument using the response file you created in Phase 1, step 3 on page 40.

```
# /<distro>/opsware_installer/upgrade_opsware.sh -r
<full_path_to_response_file>
```

The *Upgrade Components* menu is displayed:

In **Typical Component Layout Mode**, the following screen displays (components must be installed in the order shown, selecting a installs all components in the correct order):

```
Welcome to the Opsware Installer.
Please select the components to install.

1 ( ) Model Repository, additional core
2 ( ) Core Infrastructure Components
```

```
3 ( ) Slice
4 ( ) OS Provisioning Components

Enter a component number to toggle ('a' for all, 'n' for
none).

When ready, press 'c' to continue, or 'q' to quit
```

In **Custom Component Layout Mode**, the following screen displays (components must be installed in the order shown, selecting a installs all components in the correct order):

```
Welcome to the Opsware Installer.
Please select the components to install.

1 ( ) Model Repository, additional core
2 ( ) Multimaster Infrastructure Components
3 ( ) Software Repository Storage
4 ( ) Slice
5 ( ) OS Provisioning Media Server
6 ( ) OS Provisioning Boot Server, Slice version

Enter a component number to toggle ('a' for all, 'n' for none).
When ready, press 'c' to continue, or 'q' to quit.
```

Option 3 (Software Repository Storage) appears only when the upgrade script is invoked on an SA 7.50 *Software Repository* host.

4 Log on to the *Model Repository host* and select `Model Repository` from the menu then press `c` to continue.

When upgrading Subsequent Cores, you can simultaneously upgrade multiple cores.

5 Upgrade the remaining **Subsequent Core Components** in the following order. Make sure to invoke the `upgrade_opsware.sh` script with the `-r <response_file>` option. Use the response file you created in Phase 1, step 3 on page 40.

```
# /<distro>/opsware_installer/upgrade_opsware.sh -r
<full_path_to_response_file>
```

6 For **both Typical and Custom layout**, select `Model Repository`. Press `c` to install the component.

While you upgrade the Model Repository, you might be prompted to confirm the SA configuration values.These values are taken from the response file, so you should accept the defaults.

As part of the Model Repository upgrade, custom attribute data is migrated to new tables. If you have many custom attributes, the Model Repository upgrade phase can take a long time to complete.

7 For **both Typical and Custom layout**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `Core Infrastructure Components`. Press `c` to upgrade the components.

8 For **Custom Layout only**: log on to the server that will host the *Software Repository Storage* and re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `Software Repository` `Storage`. Press `c` to continue. SA upgrades the component.

9 For **both Typical and Custom layout**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `Slice`. Press `c` to continue. SA upgrades the Slice Component bundle.

➤ If you are upgrading multiple Slice Component bundles, they must be upgraded one-at-a-time. Simultaneous upgrade is not supported.

10 For **Typical layout only**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `OS Provisioning Components`. Press `c` to continue. SA upgrades the OS Provisioning components.

11 For **Custom layout only**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `OS Provisioning Media Server.` Press `c` to continue. SA upgrades the OS Provisioning Media Server.

12 For **Custom layout only**, re-invoke the `upgrade_opsware.sh` script, specifying the same response file and select `OS Provisioning Boot Server`. Press `c` to continue. SA upgrades the OS Provisioning Boot Server

➤ If the upgrade takes more than an hour from the time the Data Access Engine (`spin`) starts up, some managed devices may be marked unreachable. Run the communications test to resolve this.

Phase 7: Upload the Software Repository Content

You need only upload Software Repository content to a Multimaster Mesh's First Core, the content will be replicated automatically to your Subsequent Cores. You must, however, run the OS Provisioning Linux Media Verification option on the First Core and all of the Subsequent Cores.

➤ If you are upgrading a Multimaster Mesh with more than three cores, you must have completed the upgrade of each core's Infrastructure Component bundle host before beginning content upload.

➤

Linux Media Verification (LMV) is a new installation component that checks the Linux/ESX Server
OS media in the Media Server and removes SA OS Provisioning Stage2 images if necessary, making the Linux/ESX Server OS media compatible with SA 7.80 Linux/ESX Server OS provisioning. LMV updates all Linux/ESX Server MRLs for which the Infrastructure Component bundle (and/or `wordstore`) has NFS `RW` permission. Therefore, you must run OS Provisioning Linux Media Verification on the First Core, all of the Subsequent Cores, and Satellite(s) (if you choose to upgrade the Satellite to SA 9.0).

In previous releases, you would have been required in this phase to upload the OS Provisioning Stage 2 Images due to certain modifications to Linux installation media that were necessary for compatibility with SA. As of SA 7.80, these modifications are no longer required so there is no longer a requirement to upload OS Provisioning Stage 2 Images.

If you must upgrade a mesh that has pre-SA 7.80 Satellite(s) but you do not want to upgrade the satellite to SA 7.80, you can choose to do either of the following:

- (Recommended) Run OS Provisioning Linux Media Verification option, but do not migrate the Satellite media:

  a. Ensure that the core host(s) on which you run Linux Media Verification does not have NFS read/write permission to the Linux / ESX Server OS media imported in the Satellite.

  b. Run the installer script and select OS Provisioning Linux Media Verification as shown is steps 1 and 2 below.

     You will now be able to perform Linux / ESX Server provision for both of the following:

     - Linux / ESX Server provision to an SA 7.80 Core's OS Provisioning `buldmgr` using the migrated media and newly imported media.
     - Linux / ESX Server provisioning behind a pre-SA 7.80 Satellite using previously imported media in the Satellite that have not been migrated.

Please note that the OS Provisioning job will fail under the following scenarios:

- Performing Linux / ESX Server OS Provisioning behind a pre-SA 7.80 Satellite using migrated media.
- Performing Linux / ESX Server OS Provisioning behind an SA 7.80 Core's `buildmgr` using non-migrated media.

---

1. Install the SA 9.0 content on the **First** Core by performing the following steps:

   a. From the *Infrastructure Component bundle* host, mount the *Agent and Utilities DVD* and invoke `upgrade_opsware.sh` script with the response file that you generated in Phase 1, step 3 on page 40.

   ```
   # /<distro>/opsware_installer/upgrade_opsware.sh -r /
   <full_path_to_response_file>
   ```

   The following Menu appears:

   ```
   Welcome to the Opsware Installer.
   Please select the components to install.

   1 ( ) Software Repository - Content (install once per mesh)
   2 ( ) OS Provisioning Linux Media Verification (required only for
   upgrades from pre-7.8 versions)

   Enter a component number to toggle ('a' for all, 'n' for none).
   When ready, press 'c' to continue, or 'q' to quit.
   ```

   b. Select a to perform `OS Provisioning Linux Media Verification` (this step restores your Linux images to the vendor default) and `Software Repository – Content` to upload the upgrade content. Press c to continue. SA performs the verification and uploads the Software Repository content.

   c. If you encounter communication timeout errors when installing the content, restart the Multimaster Software Repository component by entering the following commands; then repeat sub-step a and sub-step b in this step:

```
# /etc/init.d/opsware-sas restart mm_wordbot
```

If restarting the Multimaster Software Repository component does not solve the problem, restart all the SA components on the Software Repository server by entering the following command; then repeat sub-step a in this step:

```
# /etc/init.d/opsware-sas restart
```

You need to *perform this step only once* when upgrading the cores in a multimaster mesh; for example, if you installed the content component in the First Core, you do *not* need to install the content in each Subsequent Core. The content is replicated automatically.

2 Verify that the core upgraded successfully. Log in to the SAS Web Client as a member of the *SA System Administrator group* and run the System Diagnosis tool on the core (from the Navigation panel, click Administration ➤ System Diagnosis. The **System Diagnosis: Perform Diagnosis** page appears.

Select the components that you want to test. By default, all components are selected (the Data Access Engine, the Software Repository, Command Engine, and Web Services Data Access Engine.

You should test all components. See the *SA Administration Guide* for information about running the SA System Diagnosis tool.

Upgrading a Satellite from SA 7.50 or SA 7.80 to SA 9.0

You are not required to upgrade your Satellites immediately after a Core upgrade to SA 9.0.

Phases of an SA 9.0 Satellite Upgrade

This section provides a summary of the Satellite upgrade process. You can use the right-hand column to indicate that a phase is completed:

Table 8 Phases of a Satellite Upgrade

Phase	Description	Complete
1	Invoke the SA Installer and Complete Satellite Upgrade Interview	
2	Upgrade the Satellite	
4	(Optional) Upgrade the OS Provisioning Components	

If you used the *SA Satellite Base DVD* to install your Satellite(s), you must use the *SA 7.80 Satellite Base DVD* to perform the Upgrade. If you used the *Satellite Base Including OS Provisioning DVD* to install your Satellite(s), you must use the SA 7.80 *Satellite Base Including OS Provisioning DVD* to perform the Upgrade.

Phase 1: Invoke the SA Installer and Complete Satellite Upgrade Interview

1 Mount the *SA 9.0 Satellite Base DVD* (or *Satellite Base Including OS Provisioning DVD* if you have the OS Provisioning feature installed in the Satellite core) and invoke the SA Installer upgrade script by entering the following command. You must have the response file used to install the Satellite.

```
# /<distro>/opsware_installer/upgrade_opsware.sh -r
<full_path_to_response_file>
```

2 The Interview Mode screen appears. At the Interview Mode prompt, select one of the following options:

```
1 - Simple Interview Mode
2 - Advanced Interview Mode
3 - Expert Interview Mode
```

Advanced and Expert Interview modes are typically only used for complex installations and troubleshooting purposes.

Choose Option 1 to use the default values for certain configuration parameters.

Choose Option 2 to specify advanced configuration parameters during the interview.

The installer will take all values from the response file.

Save the response file.

Phase 2: Upgrade the Satellite Gateway

1 The Upgrade Component Menu is displayed (the OS Provisioning components are not displayed when you use the *SA 9.0 Satellite Base DVD*):

```
Welcome to the Opsware Installer.
 Please select the components to install.
 1. ( ) Satellite (Interactive Install)
 2. ( ) OS Provisioning Boot Server
 3. ( ) OS Provisioning Media Server
Enter a component number to toggle ('a' for all, 'n' for none).
When ready, press 'c' to continue, or 'q' to quit.

Selection: 1
```

2 Select `Satellite (Interactive Install)`. Press `c` to continue.

3 The Installer launches the Gateway Interview, which then displays the following banner:

```
************************************************************
*                                                          *
*                Satellite Installer                       *
*         Copyright (C) 2004-2010: Hewlett Packard         *
*                                                          *
*                                                          *
************************************************************
```

4 The following is displayed:

```
Are you ready to proceed? [y/n] y
```

Press y to proceed.

5 The following is displayed:

```
This server has version <old_version> of the Opsware Gateway installed.  Do
you want to uninstall that version and install version <new_version>?
[y/n] y
```

`Press y to continue.`

6 The following is displayed:

```
Should I try and shut them all down before the upgrade? [y/n] y
```

Press Y to continue.

7 The upgrade proceeds. Upon completion, the following is displayed:

```
This Opsware Gateway has been upgraded to the current version.  Would you
like to continue and either add a new instance on this server or edit the
configuration of an existing instance? [y/n] n
```

Select `n`. The Satellite installation will continue in the background and will display a success message when the Satellite is installed.

Phase 4: (Optional) Upgrade the OS Provisioning Components

1 If you have OS Provisioning installed in the Satellite Core, using the *Satellite Base Including OS Provisioning DVD*, invoke the `upgrade_opsware.sh` script with the response file you generated and from the component menu, and select OS Provisioning Boot Sever to upgrade that component.

2 After the Boot Server is upgraded, again using the *Satellite Base Including OS Provisioning DVD*, invoke the `upgrade_opsware.sh` script with the response file you generated and from the component menu, and select OS Provisioning Media Server to upgrade that component.

When the Media Server is upgraded, the Linux Verification Utility automatically converts the OS Provisioning Stage2 images to the SA 7.80 default Linux images.

4 SA 9.0 Post-Upgrade Tasks

This section describes the tasks required after upgrading to SA 9.0.

Updated Waypurge Garbage Collection Procedure

In SA 9.0 the Garbage Collection was modified so that all eligible child records are completely deleted from the SESSION_SERVICE_INSTANCES table which improves performance.

After you have upgraded to SA 9.0, you should perform the following tasks to complete the update to the Waypurge Garbage Collection procedure. You will run a script that will delete any existing child records in your SESSION_SERVICE_INSTANCES table which reduces the size of the table.

Perform the following on the Model Repository host (or hosts in a Multimaster Mesh):

1 Log in to SQL*Plus and check how many records are expected to be deleted (The SQL gives the number of session trees to be deleted):

```
SQLPLUS> SELECT count(session_id) FROM sessions
          WHERE (parent_session_id IS NULL OR
              parent_session_id IN (SELECT session_id FROM sessions WHERE
              parent_session_id IS NULL AND status = 'RECURRING')) AND
              status <> 'PENDING' AND status <> 'RECURRING' AND
              trunc(nvl(signoff_dt, nvl(end_dt,start_dt))) <
             (trunc(sysdate) - (SELECT value FROM audit_params WHERE name = 'DAYS_WAY'))
                  AND NOT EXISTS (SELECT reconcile_session_id FROM device_role_classes
              WHERE reconcile_session_id IS NOT NULL AND
                  reconcile_session_id = sessions.session_id);
```

2 Manually run the WAYPURGE.GC_SESSIONS dba_job.

```
sqlplus "/ as sysdba"
SQLPLUS> grant create session to gcadmin;
SQLPLUS> connect gcadmin/<password_for_gcadmin>
SQLPLUS> col schema_user format a10
SQLPLUS> col what format a50
SQLPLUS> set line 200
SQLPLUS> select job, schema_user, last_date, this_date, next_date, broken, what from
user_jobs where what LIKE '%WAYPURGE%';
```

Sample output:

```
JOB        SCHEMA_USE LAST_DATE       THIS_DATE       NEXT_DATE       BRO WHAT
---------- ---------- --------------- --------------- --------------- --- ----------------------_
    189 GCADMIN    14-APR-10                      15-APR-10       N   WAYPURGE.GC_SESSIONS;
```

Note the job number.

```
SQLPLUS>  exec dbms_job.run(189);
```

Note the time taken by the manual job run and increase the value of WAY_GC_SESSIONTREES_DELETE_MAX accordingly. You should gradually increase the WAY_GC_SESSIONTREES_DELETE_MAX value and monitor the time taken to run the job. WAY_GC_SESSIONTREES_DELETE_MAX can be increased to 300, 500, 1000, 3000 and so on.

```
sqlplus "/ as sysdba"
SQLPLUS> grant create session to lcrep;
SQLPLUS> connect lcrep/<password for lcrep>
SQLPLUS> UPDATE audit_params SET value = 1000 WHERE name = 'WAY_GC_SESSIONTREES_DELETE_MAX';
SQLPLUS> commit;
```

Perform step 1 again to monitor the number of records that must be deleted.

> You can run the WAYPURGE.GC_SESSIONS dba_job manually or use the nightly dba_job run to delete child records. Note that the garbage collection nightly DBA job is run only once a day, so it may take several days for it to delete all the child records. HP recommends a combination of manual and nightly job runs.

3 After all child records are removed, delete the WAY_GC_SESSIONTREES_DELETE_MAX value from the AUDIT_PARAMS table.

```
sqlplus "/ as sysdba"
SQLPLUS> grant create session to lcrep;
SQLPLUS> connect lcrep/<password for lcrep>
SQLPLUS> DELETE FROM audit_params WHERE name = 'WAY_GC_SESSIONTREES_DELETE_MAX';
SQLPLUS> Commit;
SQLPLUS> select AUDIT_PARAM_ID, NAME, VALUE from audit_params;
```

4 Ensure that the WAY_GC_SESSIONTREES_DELETE_MAX value was removed.

Monitoring the ERROR_INTERNAL_MSG Table

Various SA internal PL/SQL procedures write exceptions to the truth.ERROR_INTERNAL_MSG table. You should monitor this table for errors (daily checks are recommended) on all Model Repository (Oracle) databases.

Executing the SQL below lists the data in error_internal_msg from the last fifteen days.

> You can remove the WHERE clause if you want to display all data in the truth.ERROR_INTERNAL_MSG table.

```
# Su - oracle
# Sqlplus "/ as sysdba"
SQL> set line 200
SQL> col ERR_ID format 999999
SQL> col ERR_USER format a8
SQL> col ERR_TABLE format a25
SQL> col ERR_TABLE_PK_ID format a10
SQL> col ERR_CODE format 9999999
SQL> col ERR_TEXT format a20
SQL> col ERR_INFO format a30

SQL> select ERROR_INTERNAL_MSG_ID ERR_ID,
ERR_DATE,
ERR_USER,
ERR_TABLE,
ERR_TABLE_PK_ID,
ERR_CODE,
ERR_TEXT,
DELETE_FLG,
ERR_INFO
from ERROR_INTERNAL_MSG
where ERR_DATE > sysdate - 15
order by ERR_DATE;
```

Rebuilding the SHADOW_FOLDER_UNIT Table

The procedure SHADOW_FOLDER_UNIT_RELOAD is provided in case the contents of SHADOW_FOLDER_UNIT table becomes out of synchronization or there are multiple records of the type (`shadow_folder_unit.folder_id = -1`).

The table can be rebuilt without stopping the system. Simply connect as user `TRUTH`, `TWIST`, `SPIN`, or `OPSWARE_ADMIN` and issue the command:

```
exec SHADOW_FOLDER_UNIT_UTIL.SHADOW_FOLDER_UNIT_RELOAD
```

Check the results from monitoring the `ERROR_INTERNAL_MSG` table. If the results contain:

```
'ERR_TABLE' = 'UNIT_RELATIONSHIPS'
```

do the following:

1 Check if there are records in `truth.SHADOW_FOLDER_UNIT` of the type (`folder_id = -1`).

```
SQL> connect / as sysdba
SQL>  select count(*) from shadow_folder_unit where folder_id = -1;
```

2 If the above SQL returns more than zero rows, then run the following during low database usage time:

```
SQL> grant create session to truth;
SQL> connect truth/<password>
SQL> exec SHADOW_FOLDER_UNIT_UTIL.SHADOW_FOLDER_UNIT_RELOAD;
```

3 Run the SQL from Monitoring the ERROR_INTERNAL_MSG Table on page 52 and check if the procedure has listed any faulty records. `SHADOW_FOLDER_UNIT_UTIL.SHADOW_FOLDER_UNIT_RELOAD` is idem potent therefore the faulty records can be fixed and you can rerun `SHADOW_FOLDER_UNIT_UTIL.SHADOW_FOLDER_UNIT_RELOAD`.

HP recommends that you gather table statistics after the data reload:

```
SQL> connect truth/<password>
SQL> exec dbms_stats.gather_table_stats (
                ownname=> 'TRUTH',
                tabname=> 'SHADOW_FOLDER_UNIT',
                estimate_percent=> DBMS_STATS.AUTO_SAMPLE_SIZE,
                cascade => true);
```

4 Revoke the permissions given to user truth:

```
SQL> connect / as sysdba
SQL> revoke create session to truth;
```

OS Provisioning Build Manager Customizations

During the upgrade to SA 9.0, the system configuration values for the OS Build manager (`bm.reprovision_attributes_to_preserve`) are updated with new required SA 9.0 values.

If you modified the `bm.reprovision_attributes_to_preserve` values prior to the upgrade, your changes are lost during upgrade, therefore, you must modify `bm.reprovision_attributes_to_preserve` after upgrade to respecify your customized values.

If you do not respecify these custom values after upgrade, any Linux or Solaris managed servers you provision will lose the custom attributes assigned using the modified `bm.reprovision_attributes_to_preserve` values that existed before upgrade.

You can respecify your custom values by appending the custom attribute names and values that should be used during reprovisioning to `bm.reprovision_attributes_to_preserve` on the System Configuration page in the SAS Web Client. Remember to click the Save button at the bottom of the page to apply your changes.

Content Migration

You may need to perform tasks in the *SA Content Migration Guide*. Not all upgrades will have required content migration tasks.

Server Automation Reporter (SAR) and BSA Essentials 2.0

Upgrading from SA 7.50

If you are upgrading from SA 7.50 to SA 9.0 and have Server Automation Reporter (SAR) installed, you must complete the SA 9.0 Core upgrade, then apply the SAR 7.80 patch to the upgraded core, upgrade any SAR Data Miners running in the core and restart the Data Miners. See the SAR 7.80 *Technical Note: Installing SAR 7.80* for information about applying the SAR patch to the core and see the *Server Automation Reporter (SAR) Installation Guide* for information about starting and stopping SAR Data Miners. Once you have upgraded to SAR 7.80, you can upgrade to BSA Essentials 2.0.

Download the SAR 7.80 Compliance Reports

After upgrading to SA 7.80 and applying the SAR 7.80 patch to the core, you must also download the SAR 7.80 Compliance Reports. The SAR 7.50 Compliance Reports are not supported with SA/SAR 7.80. For information on configuring the Live Network Connector and SAR to download the updated Compliance Reports, see the *Server Automation (SAR) 7.80 Patch Release Notes* and the *Server Automation Reporter (SAR) Installation Guide*.

Upgrading from 7.80

If you are upgrading from SA 7.80 to SA 9.0, you must install BSA Essentials 2.0. See the *BSA Essentials Installation Guide*. SAR 7.80 is not compatible with SA 9.0.

New Installations

You should install BSA Essentials 2.0 in an SA 9.0 environment. See the *BSA Essentials Installation Guide*.

Storage Visibility and Automation

If you plan to upgrade the Application Storage Automation System (ASAS) product to the Storage Visibility and Automation feature in Server Automation (SA), see the *Storage Visibility and Automation Upgrade Guide*.

Post-Upgrade Migration of Windows Server Objects

After upgrading to SA 9.0, if there are any Windows Server Objects in the Library (including Windows Registry, Windows Services, IIS Metabase, and COM+ objects), you must perform a manual migration step to upgrade these objects so that they are compatible with SA 9.0.

The migration is performed by a script called `ssr-migrate.sh`.

Usage

```
/opt/opsware/twist/migration/ssr-migrate.sh -u detuser
```

Options

Table 9 Windows Server Objects Migration Utility Options

option	description
`-u username`	Specifies the username to use when authenticating to SA. Use `detuser` under normal circumstances.
`-p password`	Allows the password to be given on the command line. If a password is not given on the command line, the program will prompt you for the password.
`-f`	Forces the script to perform the migration on all Windows Server Objects, even if the object appears to have been previously migrated.
`-m maxsize`	Specify the maximum size (in mb) for Windows Server Objects to be migrated. By default, the utility will not attempt to migrate objects larger than 50 megabytes.
`-h`	Display help.

To migrate the Window Server objects, perform these tasks:

1. Log in to any server that hosts a *Slice Component bundle*.
2. Run the following command:

   ```
   /opt/opsware/twist/migration/ssr-migrate.sh -u detuser
   ```

3. The `ssr-migrate.sh` utility prompts you for the password for the `detuser` account. Enter the password
4. The utility then migrates all Windows Server Objects, making them compatible with SA 9.0.

Configuring Contact Information in SA Help

To configure the SA administrator contact information that appears on the SA Help page, perform the following tasks:

1. In the SA Core, log on as `root` to the server running the Command Center (Slice Component bundle).
2. Change to the following directory:

   ```
   /etc/opt/opsware/occ
   ```

3. Open the `psrvr.properties` file in a text editor.
4. Modify the values in the following fields to change the contact information in the SAS Web Client Help:

   ```
   pref.occ.support.href
   pref.occ.support.text
   ```

5. Save the file and exit.
6. Restart the Command Center component by entering the following command:

   ```
   /etc/init.d/opsware-sas restart occ.server
   ```