HP Server Automation

Ultimate Edition

Software Version: 10.22

Upgrade Guide

Document Release Date: June 2, 2016
Software Release Date: December 11, 2015

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

Adobe® is a trademark of Adobe Systems Incorporated.

Intel® and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft®, Windows®, Windows® XP are U.S. registered trademarks of Microsoft Corporation.

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

UNIX® is a registered trademark of The Open Group.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Support

Visit the HP Software Support Online website at:

https://softwaresupport.hp.com/

This website 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 website 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:

https://hpp12.passport.hp.com/hppcf/createuser.do

To find more information about access levels, go to:

https://softwaresupport.hp.com/web/softwaresupport/access-levels

Support Matrices

For complete support and compatibility information, see the support matrix for the relevant product release. All support matrices and product manuals are available here on the HP Software Support Online website:

https://softwaresupport.hp.com/group/softwaresupport/support-matrices

You can also download the *HP Server Automation Support and Compatibility Matrix* for this release from the HP Software Support Online Product Manuals website:

https://softwaresupport.hp.com/

This site requires that you register for an HP Passport and sign in. After signing in, click the **Search** button and begin filtering documentation and knowledge documents using the filter panel.

Documentation Updates

All the latest Server Automation product documentation for this release is available from the SA Documentation Library:

https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00417675

Use the SA Documentation Library to access any of the guides, release notes, support matrices, and white papers relevant to this release or to download the full documentation set as a bundle. The SA Documentation Library is updated in each release and whenever the release notes are updated or a new white paper is introduced.

How to Find Information Resources

You can access the information resources for Server Automation using any of the following methods:

Method 1: Access the latest individual documents by title and version with the new SA Documentation Library

Method 2: Use the complete documentation set in a local directory with All Manuals Downloads

Method 3: Search for any HP product document in any supported release on the HP Software Documentation Portal

To access individual documents:

1. Go to the SA 10.x Documentation Library:

   https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00417675

2. Log in using your HP Passport credentials.
3. Locate the document title and version that you want, and then click **go**.

To use the complete documentation set in a local directory:

1. To download the complete documentation set to a local directory:
   a. Go to the SA Documentation Library:

      https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00417675

   b. Log in using your HP Passport credentials.
   c. Locate the All Manuals Download title for the SA 10.1 version.
   d. Click the **go** link to download the ZIP file to a local directory.
   e. Unzip the file.
2. To locate a document in the local directory, use the Documentation Catalog (docCatalog.html), which provides an indexed portal to the downloaded documents in your local directory.
3. To search for a keyword across all documents in the documentation set:
   a. Open any PDF document in the local directory.
   b. Select **Edit > Advanced Search** (or Shift+Ctrl_F).
   c. Select the All PDF Documents option and browse for the local directory.
   d. Enter your keyword and click Search.

To find additional documents on the HP Software Documentation Search Portal:

Go to the HP Software Documentation Search Portal:

https://softwaresupport.hp.com/

This site requires that you register for an HP Passport and sign in. After signing in, click the **Search** button and begin filtering documentation and knowledge documents using the filter panel.

To register for an HP Passport ID, click the **Register** link on the HP Software Support Online login page.

You can also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details. See Documentation Change Notes for a list of any revisions.

Product Editions

There are two editions of Server Automation:

- Server Automation (SA) is the Ultimate Edition of Server Automation. For information about Server Automation, see the SA Release Notes and the SA User Guide: Server Automation.
- Server Automation Virtual Appliance (SAVA) is the Premium Edition of Server Automation. For more information about what SAVA includes, see the SAVA Release Notes and the SAVA at a Glance Guide.

Document Change Notes

The following table indicates changes made to this document since the last released edition.

Date	Changes
December 2014	Original version of this document for release with SA 10.2.
May 2015	Modified instructions to account for the ability to install as non-root user who has root privileges. Previously, only root user could perform the installation.

Contents

1 SA 10.2 Upgrade Overview

This section describes the requirements and procedures for upgrading to SA 10.2.

Upgrade Paths

You can upgrade to SA 10.2 from the following releases:

- SA 9.10
- SA 9.1x
- SA 10.0
- SA 10.0x (patch release)
- SA 10.1x

Warning: After the standard SA Core upgrade is initiated, there is no procedure available to roll back to the previous version. For complex SA installations (multiple SA Cores, distributed core components, etc.), HP strongly recommends that you contact HP Professional Services (PSO) for assistance and consider a PSO-supported rolling upgrade procedure which does provide some rollback capabilities.

SA Core Configurations Supported for Customer Upgrade

This section describes the SA Core configurations that are supported for customer upgrade.

The *first upgrade of an SA Core to SA 10.1* from a previous version must be performed by HP Professional Services or an HP certified consultant unless your core matches one of the SA Core configurations supported for customer upgrade described in Chapter 2: *SA Core Configurations* in the *SA Standard/Advanced Installation Guide*. After the core has been upgraded to SA 10.0, HP supports customer-performed upgrades to SA 10.1 or later as long as your core configuration is one of the supported configurations. All other core configurations will continue to require the services of HP Professional Services. If you are uncertain whether you can upgrade an existing SA Core yourself, contact HP Technical Support.

These configurations include:

- SA Core with a Local HP-supplied Oracle Database
- SA Core with a Remote Customer-supplied Oracle Database
- SA Core with a Remote Model Repository and HP-supplied Oracle Database
- SA Core with a Remote Model Repository and HP-supplied Oracle Database and Additional Slice Component Bundle Instances
- SA Core with a Remote Customer-supplied Oracle Database and Additional Slice Component Bundles
- SA Core with a Remote Model Repository and HP-supplied Oracle Database, Additional Slice Component Bundle Instances and Satellites
- SA Core with a Remote Customer-supplied Oracle Database, Additional Slice Component Bundles and Satellites
- Advanced Installation: SA First (Primary) Core with a Secondary Core (Multimaster Mesh) - a set of two or more SA Cores that communicate through Management Gateways and that can perform synchronization of data about their respective Managed Servers

The SA Interview and the Core Definition File (CDF)

SA 10.0 and later transitions from the Response Files used with previous versions to the new Core Description File (CDF), an XML based configuration file. The first time you upgrade a core or satellite to this release, the upgrade script uses the SA core parameter/configuration defaults from your existing response files in `/var/opt/opsware/install_opsware/resp` on Model Repository component host of the core being upgraded and stores them in a new default `cdf.xml` file. In subsequent upgrades, you will specify this CDF file using the `-c` argument when invoking the script. See Core Definition Files on page 31 and The SA Interview and the Core Definition File (CDF) on page 20.

If, for security reasons, you have stored your response file in a location other than the default location on the host being upgraded, you can copy the files to the Model Repository component host directory `/var/opt/opsware/install_opsware/resp` for the core to be upgraded.

During upgrade, you are required to provide values for certain SA parameters used to configure your SA installation. This process is known as the *SA Interview.* As of this release, the values you provide are saved to a Core Definition File (*CDF)* which replaces the response file of previous SA versions.

SA creates the first CDF when you upgrade an SA Primary or Secondary Core or Satellite. The CDF is saved in:

`/var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml`

Windows Patch Database Update

In previous upgrades, SA could update the Windows patch database. As of SA 9.0 and later, you must update the patch database using the SA Client as described in the *SA User's Guide: Server Automation* or by using the `populate-opsware-update-library` script.

Updated Cryptographic Material

The cryptographic material file, `/var/opt/opsware/crypto/cadb/realm/opsware-crypto.db.e`, used by SA for secure communication between core components and managed servers has been updated as of this release in order to reset the required expiration date. The new cryptographic file is installed automatically when you upgrade and no further action is required on your part.

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 `db.host`, are seen only in the Advanced Interview Mode.

table 1 New SA Configuration Parameters

New Parameter	Description
`db.host`	Was `truth.host`. The hostname of the Model Repository Host.
`db.sid`	Was `truth.sid`.
`db.orahome`	Was `truth.orahome`.
`db.port`	Was `truth.port`.
`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.)

table 1 New SA Configuration Parameters (cont'd)

New Parameter	Description
hpln_proxy_user	The proxy user username 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 proxy user password 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.

There are also several new Satellite parameters introduced in this release. For a list of these parameters and information about their use, see Upgrading a Satellite on page 69.

Changes to Oracle Initialization Parameters

During upgrade, SA makes the following changes to certain Oracle initialization parameters. These changes only occur if you have installed the HP-supplied Oracle database. If you are using a non-HP-supplied Oracle database, you must make these updates manually.

Oracle 11g Only

```
nls_length_semantics='CHAR'
optimizer_mode=all_rows
"_complex_view_merging"=false
event='12099 trace name context forever, level 1'
remote_login_passwordfile=EXCLUSIVE
```

- if open_cursors < 1000 then the open_cursors is set to 1000

Oracle 12c Only

```
nls_length_semantics='CHAR'
optimizer_mode=all_rows
remote_login_passwordfile=EXCLUSIVE
```

- if open_cursors < 1500 then the open_cursors is set to 1500

Note: The parameters _complex_view_merging and event are not required for Oracle 12c.

The following permissions are granted to the database user opsware_admin:

- grant create any directory to opsware_admin;
- grant drop any directory to opsware_admin;
- grant create job to opsware_admin with admin option;

Changes to the Database Jobs

Oracle has introduced `dba_scheduler_jobs` scheduling which is more robust and fully-featured than `dba_jobs` scheduling used in previous SA versions. Oracle recommends the use of the `dba_scheduler_jobs` package for releases 10g and later since Oracle will not add new features to `dba_jobs` and its continued use could run into limitations. All SA jobs that were performed using the `dba_jobs` scheduler are ported to the new `dba_scheduler_jobs` package during upgrade to SA 10.0 or later.

To verify that existing jobs are executing correctly, perform the following tasks.

Enter the following commands in SQL*Plus:

```
# su - oracle
# sqlplus "/ as sysdba"
set line 200
col job_name format a50
col owner format a14
col last format a17
col next format a17
col state format a10
col job_action format a50

select job_name, owner, to_char(LAST_START_DATE, 'MM/DD/YY HH:MI:SS')
last, to_char(next_run_date, 'MM/DD/YY HH:MI:SS') next, state, job_action
from dba_scheduler_jobs where owner in ('OPSWARE_ADMIN', 'LCREP',
'GCADMIN');
```

In the output generated from the preceding statement, the value of the `JOB_ACTION` column indicates the type of job. The jobs owned by `GCADMIN` perform the garbage collection. The job owned by `LCREP` performs index statistics collection and the job owned by `OPSWARE_ADMIN` performs system statistics collection. Sample output will appear similar to this:

```
JOB_NAME                  OWNER   LAST              NEXT              STATE     JOB_ACTION
------------------------- ------- ----------------- ----------------- -----     ----------------------------
WLMPURGE_GC               GCADMIN 04/02/12 09:00:02 04/04/12 09:00:00 SCHEDULED WLMPURGE.GC_JOBS
STORAGEINITIATORPURGE_GC  GCADMIN 04/02/12 09:47:30 04/03/12 10:47:30 SCHEDULED STORAGEINITIATORPURGE.GC_
                                                                                STORAGEINITIATORS
AUDITPURGE_GC             GCADMIN 04/02/12 09:00:02 04/04/12 09:00:00 SCHEDULED AUDITPURGE.GC_AUDITLOGS
CHANGELOGPURGE_GC         GCADMIN 04/02/12 09:00:02 04/04/12 09:00:00 SCHEDULED CHANGELOGPURGE.GC_CHANGELOGS
WAYPURGE_GC               GCADMIN 04/02/12 09:00:02 04/04/12 09:00:00 SCHEDULED WAYPURGE.GC_SESSIONS
LCREP_INDEX_STATS         LCREP   04/02/12 11:00:00 04/03/12 11:00:00 SCHEDULED gather_lcrep_stats
OPSWARE_ADMIN_SYSTEM_     OPSWARE 04/02/12 06:00:00 04/03/12 06:00:00 SCHEDULED gather_opsware_admin_
STATS                     _ADMIN                                                sys_stats


7 rows selected.
```

where:

JOB_NAME - name of the job

OWNER - the user who with permissions to run the job

LAST_DATE - last date-time when the job was run

NEXT_DATE - next date the job will run

STATE - The status of the scheduled job:

- disabled - The job is disabled

- scheduled - The job is scheduled to be executed
- running - The job is currently running
- completed - The job has completed, and is not scheduled to run again
- broken - The job is broken
- failed - The job was scheduled to run once and failed
- retry scheduled - The job has failed at least once and a retry has been scheduled to be executed
- succeeded - The job was scheduled to run once and completed successfully
- JOB_ACTION - the procedure that the job runs

Changes to the Database Statistics Job

Oracle documentation advises that you enable Automatic Optimizer statistics collection. When you have the optimizer enabled, the database can automatically collect optimizer statistics for tables with absent or stale statistics. If fresh statistics are required for a table, the database collects them both for the table and its associated indexes.

Oracle claims that automatic statistics collection eliminates many manual tasks associated with managing the optimizer and significantly reduces the risks of generating poor execution plans because of missing or stale statistics.

SA's schema collection jobs (performed in previous versions by the `TRUTH`, `AAA` and `LCREP` users) is now removed and SA now relies on Oracle's Automatic Optimizer statistics collection to collect the schema statistics. By default Oracle's Automatic Optimizer statistics collection is enabled.

To verify that the Oracle Automatic optimizer statistics collection is turned on, perform the following steps:

Execute the following commands in SQL*Plus:

```
# su - oracle
# sqlplus "/ as sysdba"

set line 200
col status format a10

SELECT status FROM dba_autotask_client where client_name='auto optimizer
stats collection';
```

The output from the above statement should be as follows:

```
STATUS
----------
ENABLED
```

If the status is not set to `ENABLED`, execute the following statement to enable Oracle's Automatic Optimizer statistics collection.

```
EXEC DBMS_AUTO_TASK_ADMIN.ENABLE(client_name => 'auto optimizer stats
collection',operation => NULL, window_name => NULL);
```

2 Using the SA Installer

This section describes SA Installer syntax, interview modes, and installation logs.

Download the SA Installation Files

This process describes the electronic download files and the decompression and reassembly steps you must take to prepare the SA installation files prior to performing the SA installation.

The this process will take approximately 83GB of space in total. Ensure you have enough free disk space available where you extract the install files.

Electronic Download Files

(~26.6 GB total size to download)

1. Software_SA_Product_Software_10.20_Part_1_T8900-15063-01.setup
2. Software_SA_Product_Software_10.20_Part_2_T8900-15063-02.tar.gz
3. Software_SA_Product_Software_10.20_Part_3_T8900-15063-03.tar.gz
4. Software_SA_Product_Software_10.20_Part_4_T8900-15063-04.tar.gz
5. Software_SA_Product_Software_10.20_Part_5_T8900-15063-05.tar.gz
6. Software_SA_Product_Software_10.20_Part_6_T8900-15063-06.tar.gz
7. Software_SA_Product_Software_10.20_Part_7_T8900-15063-07.tar.gz
8. Software_SA_Product_Software_10.20_Part_8_T8900-15063-08.tar.gz

Download Verification and Reassembly

1. All Server Automation 10.2 downloaded files must be placed in the same directory (for example, /cust/SA)
2. Run the setup script

   ```
   # sh Software_SA_Product_Software_10.20_Part_1_T8900-15063-01.setup
   ```

   a. `Software_SA_Product_Software_10.20_Part_1_T8900-15063-01.setup` will perform the following:

   - Check the downloaded file integrity
   - Assemble the split files
   - Extract Server Automation 10.2 bits into a directory called T8900-15063 (~30GB extracted).
   - Provide needed information for Server Automation 10.2 Installation and/or Upgrade

b Successful execution of setup script should create an assembled tar.gz package called `T8900-15063.tar.gz` (~26GB in size) and also extract its contents into directory T8900-15063 (~30GB in size)

Server Automation Distribution Contents

Server Automation electronic distributions contents in directory T8900-15063 are as follows:

```
T8900-15063-oracle_sas
T8900-15063-primary
T8900-15063-sat_base
T8900-15063-sat_osprov
T8900-15063-upload
```

Server Automation Distribution Handling

You can ship the distribution package file (`T8900-15063.tar.gz`) to a Linux server location where you want to install Server Automation and then extract the package `T8900-15063.tar.gz`.

For example:

```
mkdir /mnt; cd /mnt;
tar xvfz /{path}/T8900-15063.tar.gz
```

GNU tar tool usually supports the "z" to extract gzip file. If tar tool doesn't support "z", do this:

```
gunzip -dc /{path}/T8900-15063.tar.gz | tar xvf -
```

where:

- `{path}` is the path to the directory containing the shipped distribution package, (i.e., `T8900-15063.tar.gz`)

(Optional) Directly Extract SA Distribution via Script

As an alternative to the default SA distribution handling described under Server Automation Distribution Handling on page 18, you can export the Server Automation distribution directory extracted by the setup script and mount at a remote Linux location for remote access (NFS export)

A directory of the Server Automation distribution will be created where the setup script was run.

For example:

If the setup script was run at `/cust/SA`, then the extracted SA distribution and its package are found at `/cust/SA/T8900-15063` and `/cust/SA/T8900-15063.tar.gz`.

You will then be able to install or upgrade HP Server Automation 10.2 from the directory `/cust/SA/T8900-15063`.

Invoking the SA Installer

You invoke an upgrade using the SA Installer with one of the following scripts from a mounted copy of the upgrade media. For example:

`/<mountpoint>/hpsa-primary/disk001/opsware_installer/hpsa_upgrade.sh`

Do not invoke the SA Installer from any other distribution:

- `hpsa_upgrade.sh`— upgrades the SA Core Components for a Primary Core, upgrades the components for Secondary Cores.
- `hpsa_upgrade_satellite.sh` — upgrades the components for an SA Satellite.

`hpsa_upgrade.sh` and `hpsa_upgrade_satellite.sh` accept the command line arguments shown in Table 2:

table 2 SA Installer Command Line Arguments

Argument	Description
`-h`	Display the Installer help for the command line options. *To display help during the interview, press* `ctrl-I`.
`-c <cdf_filename>`	Invoke the Installer using the SA installation configuration parameter values in a specified saved Core Definition File (CDF. If you do not specify a CDF, you must provide the values for certain configuration parameters or accept the SA default values. The SA configuration parameter values you provide during the installation interview are used for the current installation and are automatically saved into an initial CDF that is used later during SA Core upgrades and installation of Secondary SA Cores.
`--pwsave`	Specifies that the root passwords for all servers specified during installation are to be encrypted and accessed by a master password that you specify. See Master Passwords on page 21.
`--verbose | --debug`	Run the installer in verbose or debug mode which causes more information to be displayed on the console. See also Installer Logs on page 26.

Best Practice: Using the screen Utility for SA Upgrades

The `screen` utility for Linux enables you to safely run the SA Installer and recover from interruptions such as a network disconnection. If, for some reason, you are disconnected from an installation session, you can log back into the machine and use screen to reattach to your installation session.

SA recommends that you invoke the SA Installer using the `screen` utility in order to minimize the impact of an installation problem due to a network failure.

Red Hat Enterprise Linux, SUSE Linux Enterprise Server and Oracle Enterprise Linux distributions include the `screen` package but you must explicitly install it (the `screen` package is not available by default).

SA Installer Installation Modes

Depending on how you invoke the SA Installer, you are prompted to provide values for a number of parameters, for example, passwords, file locations, and so on. The number of parameters you are prompted for varies depending on the installation method you choose.

Simple Installation Modes

If you choose a Simple Installation, the default values for certain parameters that are rarely modified will be used (you will not be prompted to specify values for these parameters). These parameters include the various Oracle passwords used internally by the Core Components.

Advanced and Expert Interview modes should be used only by HP technical services.

Advanced Installation Modes

If you choose the Advanced Installation, the installer prompts you to supply values for those parameters not modifiable in the Simple Installation.

Expert Installation Mode

Used by HP Technical Staff

The SA Interview and the Core Definition File (CDF)

During an upgrade, you may need to provide values for certain SA parameters used to configure your SA upgrade. This process is known as the *SA Interview.* The values you provide are saved to a Core Definition File (CDF) which replaces response files.

SA creates the first CDF when you upgrade a pre-SA 10.1 SA Primary Core. You will use this CDF later to perform future upgrade. See Reusing a Core Definition File (CDF) on page 24.

SA 10.0 and later transitions from the Response Files used with previous versions to the new Core Description File (CDF), an XML based configuration file. The first time you upgrade a core or satellite to a 10.x release, the upgrade script uses the SA core parameter/configuration defaults from your existing response files in `/var/opt/opsware/install_opsware/resp` on Model Repository component host of the core being upgraded and stores them in a new default `cdf.xml` file. In subsequent upgrades, you will specify this CDF file using the `-c` argument when invoking the script. See Core Definition Files on page 31 and The SA Interview and the Core Definition File (CDF) on page 20.

If, for security reasons, you have stored your response file in a location other than the default location on the host being upgraded, you can copy the files to the Model Repository component host directory `/var/opt/opsware/install_opsware/resp` for the core to be upgraded.

The CDF is saved in:

`/var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml`

In some cases, when you provide a parameter value, the SA Installer validates the response (for example, a directory or path that does not exist or an invalid value or range); you are asked to re-enter a value if the installer is not able to validate your response. Some parameters are also revalidated during the actual upgrade of the Core Components. If a response to a prompt cannot be validated at time of upgrade, the installer runs a mini-interview during which you can provide a valid response.

Master Passwords

As of SA 10.2 and later, you can specify a master password to be used to access the encrypted root passwords of all core hosts specified during the installation of a new SA Core.

To encrypt server root passwords specified during installation, invoke the installation with the `--pwsave` argument. When you begin an installation with the `--pwsave` argument specified, the installer encrypts root passwords and saves them in the final CDF on completion of the installation whether a successful or failed install. See Invoking the SA Installer on page 19.

The Master Password (MP) is saved as a hash of hash SHA(SHA(MP)). SA uses this key to encrypt the root passwords of all servers that are specified as part of a new core installation and secure hash SHA(MP) is used to generate a 1024 character key and an encrypted password string which is saved on each host as `root_user_password`.

You specify the master password when you see this prompt at the end of the installation, specify “none” if you do not want to create a master password:

```
Creating temporary CDF [/var/tmp/cdf_tmp.xml]

master.password []:


Specify a master password. This password will enable encryption of the
server(s) password. If "none" is specified then server(s) password will not be
saved.


master.password []: *******
```

Invoking the Installer on an SA Core that Uses a Master Password

When you begin an upgrade that on a core that uses a master password, you are prompted to provide the password before continuing:

```
Specify a master password. This password will enable decryption of the
server(s) password. Enter "none" to provide the server(s) password again.


master.password []:
```

The installer will use the encrypted passwords for the core hosts that were stored when you created the master password. If you specify “none” as the master password, the installer prompts you to provide passwords for each core server.

The SA Password Utility

When you use master passwords, as described above, there may be circumstances, such as an installation interrupted after the root passwords of the core host servers were encrypted and the root password of any of the host servers has changed, in which you must manually enter the encrypted passwords in the CDF in order to continue the installation. Were you to simply restart the installation without manually entering the encrypted passwords, you would be prompted to again enter the root password for any servers on which the password had changed.

SA provides an encrypted password utility that you can use to regenerate the encrypted passwords and manually enter the results into the CDF.

The SA Password Management utility takes a file with master password and root passwords (comma separated values) in the plain text format and writes back what we expect them to be in a same file. It is up to user to manually replace the old values in CDF with new ones to keep it updated.

Invoke the password utility as follows:

`<distro>/opsware_Installer/hpsa_password_utility.sh <csv_file>`

where `<distro>` is the full path to the distribution media, for example:

`/<mountpoint>/hpsa-primary/`

SA Core Installation by Root or Non-root Users

Multiple types of users can perform installations and upgrades on SA Cores.

Previously, only root ssh users with *root ssh login* enabled could perform installations on SA Cores. That is no longer required.

Types of Install Users

The following users are supported when using the SA installer to install, or upgrade SA on a local machine:

- root user
- regular user who has permissions to invoke commands with *su*
- regular user who has permissions to invoke commands as root with *sudo* capabilities

When you use a regular user for performing the installation or upgrade of a core, make sure you invoke the command using *sudo*. For example: `sudo <distro>/ opsware_installer/hpsa_install.sh`

The following users are supported when using the SA installer to install SA on remote machines:

- root user (including *root ssh* access)
- regular user with *sudo* capabilities (including *user ssh* access)

Password-less *sudo* is not supported for regular users with *sudo* capabilities.

Settings Required for Regular Users with sudo Capabilities

Make the following changes to the `/etc/sudoers` file on every machine where the user (in this case *Bob*) installs SA:

```
Defaults       lecture=never
Bob      ALL=(ALL)     ALL
```

General Settings for User Names

This section describes general rules for user names in SA.

User names should have the following characteristics:

- Be portable across systems conforming to the *POSIX.1-2008* standard for portable OS interfaces. The value is composed of characters from the portable filename character set.
- Not contain a hyphen (-) character as the first character of a portable user name.
- Use the following set of characters if it is a portable filename:
  `A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k l m n o p q r s t u v w x y z 0 1 2 3 4 5 6 7 8 9 . _`

Help

At any time during the interview, you can press `ctrl-I` to display help for the current interview prompt. A brief description of the prompt and the expected responses will be displayed.

How and When CDFs are Saved

During upgrade, the SA Installer saves a temporary CDF after you press `c` to continue in the Upgrade Components screen:

```
Upgrade components
==================
Components to be Upgraded
-------------------------
Model Repository, First Core
Core Infrastructure Components
Slice
OS Provisioning Components
Software Repository - Content (install once per mesh)
Up-to-date Components (will not upgrade)
----------------------------------------
Oracle RDBMS for SAS

Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

The temporary CDF is saved in `/var/tmp/cdf_<timestamp>_temp.xml`. This file can be used to resume an interrupted upgrade. See Restarting an Interrupted Upgrade. This temporary file is updated as each component is processed thus maintaining the setup state as of the most recent action.

If you delete CDFs for security purposes, this file should be deleted as well.

Concluding the Interview

After you have provided values for all the SA configuration parameters, the SA Installer automatically saves the CDF at the end of the installation. The location of the CDF is determined by:

- whether the infrastructure component bundle host is known at the point of exit, if so, the CDF is saved on that host under `/var/opt/opsware/install_opsware/cdf` as `cdf.xml`. CDF backups are saved as `cdf_<timestamp>.xml`.
- if the Infrastructure host is unknown at the point of exit, the CDF is saved as `cdf_tmp.xml` under `/var/tmp` on the server on which the installer was invoked.

Reusing a Core Definition File (CDF)

You can specify a CDF to use for an upgrade by invoking the installer using the `-c <cdf_filename>` argument. The installer reads the contents of CDF and uses the parameter values stored in that file as the defaults. Use the latest CDF as determined by the time stamp. The CDF is saved as described in How and When CDFs are Saved. For example:

`/var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml`

Restarting an Interrupted Upgrade

Should the SA Installer encounter a correctable error, the installation stops. Correct the error and retry the installation. To restart an interrupted installation after you have corrected any errors, perform the following tasks:

1. Invoke the SA Installer using the temporary CDF that was created by the interrupted installation, for example:

   `/<mountpoint>/hpsa-primary/disk001/opsware_installer/hpsa_upgrade.sh -c /var/tmp/cdf_ts_temp.xml`

   Use the latest CDF as determined by the time stamp. See How and When CDFs are Saved on page 23.

2. You see a screen similar to the following:

```
Specify Hosts to Install
========================

Currently specified hosts:

<IP_address> (oracle_sas)
<IP_address> (word_store)
<IP_address> (gateway_master, osprov_boot_slice, slice, osprov_media)

Please select one of the following options:

1. Add/edit host(s)
2. Delete host(s)

Enter the option number or one of the following directives
```

```
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

where <IP_address> is the IP address for the host(s) you specified during the interrupted upgrade (taken from the CDF).

Press c to continue.

3 You see a screen similar to the following:

```
Host Passwords
==============

Parameter 1 of 3
<IP_address> password []:
```

Enter the credentials for each host specified as part of the upgrade.

When all passwords have been entered, press Y to continue.

```
All values are entered.  Do you wish to continue? (Y/N) [Y]:
End of interview.
```

At this point, the SA Installer will check the state of any components already upgraded before the upgrade was interrupted.

4 Select the Install Type when prompted (must be the same as the Install Type selected for the interrupted upgrade).

5 You see a screen similar to the following:

```
Host/Component Layout
=====================

Installed Components

Oracle RDBMS for SAS                                : <IP_address>
Model Repository, First Core                        : <IP_address>
Multimaster Infrastructure Components               : <IP_address>
Software Repository Storage                         : <IP_address>
Slice                                               : <IP_address>
OS Provisioning Media Server                        : <IP_address>
OS Provisioning Boot Server, Slice version          : <IP_address>
Software Repository - Content (install once per mesh): <IP_address>

-----------------------------------------

Select a component to assign

1. Slice

Enter the number of the component or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

Press c to continue.

6 You see a screen similar to the following:

```
Interview Parameters
====================

Navigation keys:
Use <ctrl>P to go to the previous parameter.
```

```
Use <ctrl>N to go the next parameter.
Use <tab> to view help on the current parameter.
Use <ctrl>C to abort the interview.



All prompts have values.  What would you like to do:

1. Re-enter values
2. Continue

Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

The SA Installer uses the parameter values specified in the CDF from the interrupted upgrade. You should not need to change these values. Press `c` to continue.

7 After the installer completes some preparation, you see a screen similar to the following:

```
Upgrade components
==================

Components to be Upgraded
-------------------------
OS Provisioning Boot Server, Slice version: <IP_address>

Up-to-date Components (will not upgrade)
----------------------------------------
Oracle RDBMS for SAS                                 : <IP_address>
Model Repository, First Core                         : <IP_address>
Multimaster Infrastructure Components                : <IP_address>
Software Repository Storage                          : <IP_address>
Slice                                                : <IP_address>
OS Provisioning Media Server                         : <IP_address>
Software Repository - Content (install once per mesh): <IP_address>


Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

Note that the components that had been upgraded before the installation was interrupted are listed under `Up-to-date Components (will not upgrade)`.

The uninstalled components are listed under `Components to be Upgraded`.

Press c to continue the upgrade from the point it was interrupted.

When resuming an interrupted upgrade, you must not change the hosts or component host assignments you specified during the original installation.

Installer Logs

The HPSA Installer logs component installation output to a standard log file:

`/var/log/opsware/install_opsware/hpsa_installer_<timestamp>.log`

If the `--verbose` argument is specified, the installer generates verbose logs for various component installations to: `/var/log/opsware/install_opsware/`. For example:

- `<ip_address>-install-infrastructure-<timestamp>.verbose.log`
- `<ip_address>-install-osprov-<timestamp>.verbose.log`
- `<ip_address>-install-slice-<timestamp>.verbose.log`
- `<ip_address>-install-word_uploads-<timestamp>.verbose.log`

Console output is logged to:

`/var/log/opsware/install_opsware/hpsa_installer-<timestamp>.log`

If you specify the `--verbose` and `--debug` options, the output to the console will be more verbose while the contents of the standard and verbose log files will remain the same.

Some SA Core Components have supplementary logs that contain additional details about the installation of those components.

See the *SA Administration Guide* for information about SA Core Component logs.

The following log files are created during the installation of the Model Repository:

`/var/log/opsware/install_opsware/truth/truth_install_<number>.log`
`/var/log/opsware/install_opsware/truth/truth_install_<number>_sql.log`

SA Parameter Password Security

During the SA installation or upgrade process, some cleartext passwords specified for core parameters are automatically obfuscated and some are not. Some passwords are obfuscated when SA Core Components start up, such as the OS Provisioning Build Manager password when the Web Services Data Access Engine server starts up. Passwords in some files must be manually obfuscated, such as passwords in the installation logs and Installer response files.

There are several ways to manually secure cleartext passwords. Which you choose will depend on your security requirements:

- Encrypt the response files and installation logs.
- Purge sensitive information from the Installer response files.
- Store the Installer response files and logs on a secure server.

Table 3 lists cleartext passwords that are automatically obfuscated and passwords that must be manually secured.

table 3 Cleartext Passwords

Cleartext Password	Filename	Automatically Obfuscated	Manually Secured
admin	/var/opt/opsware/twist/?DefaultAuthenticatorInit.ldift	✔	
buildmgr	/var/opt/opsware/crypto/buildmgr/twist.passwd /var/opt/opsware/crypto/occ/twist.passwd /var/opt/opsware/twist/?DefaultAuthenticatorInit.ldift	✔ ✔ ✔	
cleartext admin	/etc/opt/opsware/twist/startup.properties	✔	
detuser	/var/opt/opsware/crypto/twist/detuserpwd /var/opt/opsware/crypto/OPSWhub/twist.pwd	✔ ✔	
integration	/var/opt/opsware/twist/?DefaultAuthenticatorInit.ldift	✔	
root	/var/log/opsware/agent/agent.err		✔

table 3 Cleartext Passwords (cont'd)

Cleartext Password	Filename	Automatically Obfuscated	Manually Secured
	Installer response files:		
	/var/opt/opsware/install_opsware/cdf/* (infrastructure component host)	✔	
	/var/tmp/cdf_tmp.xml (on host where installer invoked)	✔	
	/var/opt/opsware/install_opsware/resp (pre-10.0 response files)		✔
	/var/opt/opsware/install_opsware/install_opsware*		✔
	/var/tmp/@*		✔
	/var/opt/opsware/install_opsware/truth/truth_install_*	✔	
	/var/log/opsware/install_opsware/hpsa_console_logs	✔	
spin	/etc/opt/opsware/spin/spin.args	✔	
vault	/var/opt/opsware/crypto/vault/vault.pwd	✔	

Securing Installer Log and CDFs

Depending on the level of your security requirements, it is recommended that the installation or upgrade team encrypt or move installation logs files to a secure server and, if necessary, encrypt, move to a secure server, and/or purge sensitive information from the Installer CDF. Remember that certain CDFs are needed for SA Core upgrades and Secondary Core installations and the log files are useful for troubleshooting so completely removing them is not recommended.

3 SA 10.2 Upgrade Prerequisites

This section describes the prerequisites for upgrading to SA 10.2.

➤ In an SA Core, servers that host a core's components must all be running the same operating system. Different update levels (for example, Red Hat Enterprise Linux 6 U2 and SUSE 10) are supported on hosts within the same core. In a multiple core mesh, each distinct core can be running under a different operating system (for example, Core 1 running Red Hat Enterprise Linux 6 U2 and Core 2 running SUSE 10) but all hosts in each distinct core must be running the same operating system.

SA Upgrade Files

SA is delivered as electronic files that need to be downloaded locally and reassembled as the first prerequisite step in the installation or upgrade. For instructions on this prerequisite step, see Download the SA Installation Files on page 17.

SA Internal Directory Naming

During installation, the SA Installer creates a number of default directories/folders with a default naming format. For example:

```
/var/opt/opsware/word/Package Repository
```

These directory/folder names are required and must not be changed. If changed, you may have problems when upgrading your SA Core.

Core Definition Files

During upgrade, you are required to provide values for certain SA parameters used to configure your SA installation. The values you provide are saved to a Core Definition File (CDF). SA creates the first CDF when you install the SA Primary Core. You will use this CDF later add a Secondary Core for a Multimaster Mesh (multiple core SA installation) or perform an upgrade.

In some cases, when you provide a parameter value, the HPSA Installer validates the response (for example, a directory or path that does not exist or an invalid value or range); you are asked to re-enter a value if the installer is not able to validate your response. Some parameters are also revalidated during the actual installation of the Core Components. If a response to a prompt cannot be validated at time of installation, the installer runs a mini-interview during which you can provide a valid response.

CDFs and the First Upgrade from 9.x to SA 10.2

When you upgrade from SA 9.x, you will not have a CDF to specify since previous versions used a response file to store core parameter values.

If you know the core to be upgraded has the latest response files, the installer will attempt to aggregate the response files found on the Model Repository component host in `/var/opt/opsware/install_opsware/resp` and use the core parameter values from those files to create the initial CDF.

If you have moved the existing core's response file for security reasons, you can copy them to `/var/opt/opsware/install_opsware/resp` or specify the full path to the response file when invoking the installer by using the `-r` argument.

If you do not have the response files for the core to be upgraded, you will be required to manually provide the core parameter values.

For subsequent upgrades, you can specify the CDF created during the previous upgrade.

Parameter Values

If you initiate an upgrade without specifying a response file or CDF, you will be required to provide values for all SA Core Component parameters during the upgrade process. You may also be prompted to supply values for parameters that have been introduced in the release you are upgrading to.

SA Upgrade Script

The SA upgrade script is located in

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

where `<distro>` is the full path to the distribution media. For example:

`/<mountpoint>/hpsa-primary/`

Upgrade Script Command Line Syntax

Table 4 Shows the valid arguments for hpsa_`upgrade.sh`:

table 4 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`.
`-c cdf_filename`	(Optional) Invoke the upgrade using the values in the specified Core Configuration File (CDF). This version of SA transitions from the Response Files used with previous versions to the new Core Description File (CDF), an XML based configuration file. The first time you upgrade a core or satellite to an SA 10.x release from an earlier release, the upgrade script uses the SA core parameter/configuration defaults from your existing response files in `/var/opt/opsware/install_opsware/resp` on Model Repository component host of the core being upgraded and stores them in a new default `cdf.xml` file. In subsequent upgrades, you will specify this CDF file using the `-c` argument when invoking the script. See Core Definition Files on page 31 and CDFs and the First Upgrade from 9.x to SA 10.2 on page 32. If, for security reasons, you have stored your response file in a location other than the default location on the host being upgraded, you can copy the files to the Model Repository component host directory `/var/opt/opsware/install_opsware/resp` for the core to be upgraded.
`--verbose`	Run the upgrade installer in verbose mode which causes more information to be displayed on the console.

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 `db.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`.

To use WinPE-based Windows OS Provisioning on an upgraded core, ensure that the `authoritative` keyword in the `/etc/opt/opsware/dhcpd/dhcpd_custom.conf` file on the boot server is uncommented. If you modify the `dhcpd_custom.conf` file, you must restart the DHCP server:

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

Customized Configuration Preservation After Upgrade to SA 10.x

After upgrading to SA 10.x, SA preserves certain changes you make to SA component configuration files during subsequent upgrades.

However, if you are upgrading from SA 9.x to SA 10.x, you must follow the procedure in Configuration Files Backed Up During Upgrade to SA10.x on page 35 to retain backups of your current modified component configuration files.

SA preserves configuration files for the following components:

- Data Access Engine (`spin`)
- Web Services Data Access Engine (`twist`)
- Component of the Global File System (`spoke`)
- Model Repository (`word`)
- Command Engine (`occ`)
- Deployment Automation (`da`)
- Component of the Global File System (`hub`)
- Command Engine component (`way`)
- Model Repository Multimaster component (`vault`)
- Gateways (`opswgw`)

SA Gateway configuration files have been customizable since SA 9.0. Gateway customizations are made in `/etc/opt/opsware/opswgw-<gateway_name>/opswgw.custom`.

To preserve your modifications, SA creates a configuration file named with `_custom` appended to the name of the source file, for example:

- `<component_name>_custom.conf`
- `<component_name>_custom.properties`
- `<component_name>_custom.args`

You can modify these files to override default component configuration specifications, for example:

- `twist_custom.conf` is created for `twist.conf`
- `psrvr_custom.properties` is created for `psvr.properties`
- `waybot_custom.args` is created for `waybot.args`

New Configuration Files Created During SA 10.x Upgrade

The SA component configuration files created during this upgrade are:

- `/etc/opt/opsware/spin/spin_custom.args`
- `/etc/opt/opsware/twist/twist_custom.conf`
- `/etc/opt/opsware/spoke/spoke_custom.conf`
- `/etc/opt/opsware/mm_wordbot/mm_wordbot_custom.args`
- `/etc/opt/opsware/occ/psrvr_custom.properties`
- `/etc/opt/opsware/da/da_custom.conf`
- `/etc/opt/opsware/hub/hub_custom.conf`
- `/etc/opt/opsware/waybot/waybot_custom.args`
- `/etc/opt/opsware/vault/vault_custom.conf`
- `/etc/opt/opsware/opswgw-<gateway_name>/opswgw.custom`

Configuration Files Backed Up During Upgrade to SA10.x

During the upgrade to SA 10.x, the SA Installer saves a copy of the previous SA installation's component configuration files in:

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

If you have made modifications to any of these configuration files, you can use these backup as a reference for modifications you may have made.

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/twistOverrides.conf is saved as twist.conf`
- `/etc/opt/opsware/vault/vault.conf`

- `/opt/opsware/waybot/etc/waybot.args`
- `/etc/opt/opsware/mm_wordbot/mm_wordbot.args`

During the upgrade to SA 10.x, the SA Installer does not automatically restore customizations made in configuration files; you must do that manually by making your modifications to the new `<component_name>_custom.conf` files. Also, If you move components to different hosts during the upgrade, you will need to supply modified `<component_name>_custom.conf` (or `.args` or `.properties`) files on the new host.

The configuration file `/etc/opt/opsware/twist/loginModule.conf` is not saved during upgrade. If you have modified this file, you must manually recreate any modifications you want carried over to your upgraded core. You can find a backup of the pre-upgrade `loginModule.conf` file in `/var/opt/opsware/install_opsware/config_file_archive/`.

LDAP Configuration After Upgrade from SA 7.x and Earlier to SA10 10.x

As of SA 10.0 and later, the method used to import LDAP users and groups changed. In these later releases, the script `ldap_config.sh` must be used to import LDAP users and groups into the SA Core.

After upgrading to SA 10.x, you must re-import your LDAP users and groups as described in the *SA Administration Guide*, "Authenticating with an External LDAP Directory Service" and "Importing External LDAP Users and User Groups".

SA 7.50 and Later Prerequisite Checking

As of SA 7.50 and later *prerequisite checking* is automated. 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 Planning and 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.

In SA cores with distributed core components, all components must be of the same SA version. Mixed SA version core components are not supported.

Oracle Database

This section discusses information that is relevant to the Oracle Database.

See the *SA Oracle Setup for the Model Repository* guide for more information.

Required Oracle Versions

If you have an existing Oracle database that you plan to use with the Model Repository, you must ensure that it is an Oracle version that is supported by SA 10.x as shown in the supported database section of the *SA Compatibility Matrix*. Also ensure that is configured as described in Appendix A: *Oracle Setup for the Model Repository* in the *SA Standard/Advanced Installation Guide*.

Upgrading SA does not affect your existing Oracle installation. Fresh SA 10.1 installations will install Oracle 12c (12.1.0.1) if you choose to install the HP-supplied Oracle database for the Model Repository.

Required Packages for Oracle12c

SA 10.1 now ships with Oracle 12c as the HP-supplied database. Oracle 12c has different package requirements than Oracle 11g. You do not have to upgrade to Oracle 12c from 11g and the SA 10.1 upgrade process does not upgrade the Oracle database for the Model Repository, however, if you decide to upgrade your Oracle database to 12c from 11g, you must ensure that the new required packages are installed before upgrading the database.

The SA Installer Prerequisite Checker validates the database parameters and ensures that they are set according to SA requirements. 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 12c.

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.

Oracle 11.2.0.x

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

Oracle 12.1.0.x

- `nls_length_semantics='CHAR'`

Note: Do not specify the `_complex_view_merging` and the `event` parameters for Oracle 12C.

Also verify that the following initialization (`init.ora`) parameters are specified correctly. For parameters not listed, SA assumes that the default Oracle parameters are used:

Oracle 11.2.0.x

```
compatible := required to be >= 11.2.0
cursor_sharing := required to be = FORCE
db_file_multiblock_read_count := suggested to be >= 16
db_block_size := required to be >= 8192
deferred_segment_creation := required to be = FALSE
event := required to be = 12099 trace name context forever, level 1
job_queue_processes := required to be >= 1000
log_buffer := required to be >= 5242880
memory_target := required to be >= 1879048192 (1.75GB)
nls_length_semantics := required to be = CHAR
nls_sort := required to be = GENERIC_M
open_cursors := required to be >= 1500
optimizer_index_cost_adj := required to be = 20
optimizer_index_caching := required to be = 80
optimizer_mode := 'required to be = ALL_ROWS
processes := required to be >= 1024
recyclebin := required to be = OFF
remote_login_passwordfile := required to be = EXCLUSIVE
session_cached_cursors := required to be >= 50
undo_tablespace := should be = UNDO or other UNDO tablespace
undo_management := should be = AUTO
_complex_view_merging := required to be = FALSE
```

Oracle 12.1.0.x

```
compatible := required to be >= 12.1.0
cursor_sharing := required to be = FORCE
db_block_size := required to be >= 8192
db_file_multiblock_read_count := suggested to be >= 16
deferred_segment_creation := required to be = FALSE
job_queue_processes := required to be >= 1000
max_string_size := required to be = STANDARD
memory_target := required to be >= 2684354560 (2.5GB)
nls_length_semantics := required to be = CHAR
nls_sort := required to be = GENERIC_M
open_cursors := required to be >= 1500
optimizer_index_cost_adj := required to be = 100
optimizer_index_caching := required to be = 0
optimizer_mode := 'required to be = ALL_ROWS
processes := required to be >= 1024
recyclebin := required to be = OFF
remote_login_passwordfile := required to be = EXCLUSIVE
session_cached_cursors := required to be >= 50
undo_tablespace := should be = UNDO or other UNDO tablespace
```

Note: The parameters _complex_view_merging and event are no longer required for Oracle 12c.

open_cursors Value

The Oracle initialization parameter open_cursors must be set to 1000 or more for Oracle 11g. If you have an Oracle 12c database, the value must be 1500 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 10.0 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 10.2, 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;
```

Note: If you are upgrading from SA 10.0, these grants should have already been granted and need not be granted again.

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 in the following directory:

`/<distro>/opsware_installer/tools`

where `<distro>` is the full path to the distribution media. For example:

`/<mountpoint>/hpsa-primary/`

You must run the script as a user with root privileges on the Oracle database.

Script usage:

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

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

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 and later this functionality has been moved to the `vault` component. The `vault` component now handles the garbage collection job for Transactions. By default the transaction data is retained for seven 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`.

Oracle RAC

In an Oracle RAC environment, only one of the RAC nodes is used during the installation/upgrade process. The SA Installer connects to only one Oracle instance to modify the Model Repository. During normal SA operations, all the RAC nodes are used.

To accommodate the remote Model Repository install/upgrade process in Oracle RACed environment, the following two `tnsnames.ora` files are required on the SA server. By default, SA expects the `tnsnames.ora` file to be located in `/var/opt/oracle`

- `tnsnames.ora-install_upgrade`

  This copy of `tnsnames.ora` is used during SA installation/upgrade. The file can be renamed.

  During the upgrade process, you can use soft links to point `tnsnames.ora` to `tnsnames.ora-install_upgrade`. During install-upgrade the installer connects to the database through only one RACed node.

  The `tnsnames.ora` links can be changed as follows:

  a. Make sure that none of the clients are connected to the Oracle RACed database.

  b. Use soft links to point `tnsnames.ora` to `tnsnames.ora-install_upgrade`.

     For example: `$ln –s tnsnames.ora-install_upgrade tnsnames.ora`

- `tnsnames.ora-operational`

  This copy of `tnsnames.ora` is used during normal SA operation. This file can be renamed.

  After the SA upgrade is completed, change the soft link and point `tnsnames.ora` to `tnsnames.ora-operational`. During normal SA operation, the installer connects to the database through all the active RACed nodes.

  The `tnsnames.ora` links can be changed as follows:

  a. Make sure that none of the clients are connected to the Oracle RACed database.

  b. Use soft links to point `tnsnames.ora` to `tnsnames.ora-operational`.

     For example: `$ln –s tnsnames.ora-operational tnsnames.ora`

     For more information, see the *SA Oracle Setup for the Model Repository* guide, *Oracle RAC Support* section.

Preparation for SA Upgrade

Preparation for All Upgrades to SA 10.x

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 9.14). See Uninstall All CORD Patches on page 50 for instructions on removing CORD patches.
- Gather the correct values for the parameters shown in Core Parameter Values Required for Upgrade on page 42.
- The Core Gateways, Management Gateway and core services must be up and running.
- 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.

- Notify SA users to cancel all scheduled **Remediate Patch Policy** jobs. After upgrading a Single Core or Multimaster Core to 10.2, 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 10.x

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

Before you upgrade a Multimaster Core to SA 10.x you must ensure that there are no conflicts in the mesh. You should follow the procedures described in the *SA Administration Guide*. "Viewing the State of the Multimaster Mesh - SA Client" to determine what transaction conflicts exist in the mesh, if any. If there are conflicts, follow the procedure described in the *SA Administration Guide*, "Resolving Mesh Conflicts - SA Client".

Server Automation Reporter (SAR)

If you have been using Server Automation Reporter (SAR) or BSAE reports, SAR and BSAE are not supported for use with SA 10.x and later.

Compatibility with OO and NA

SA 10.x is compatible with:

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

Windows Patch Management Utilities

The SA Windows Patch Management feature requires several files from the Microsoft software download repository. These files can be installed during Core installation.

If you do not plan to use SA to manage Windows servers, you can optionally choose not to install these files and successfully complete installation. However, if these files are not installed, *no operations against Windows servers should be performed*. These files are required for many Windows-based operations other than Windows patching including Windows OS Provisioning.

Installing the Required Windows Patch Management Files in an Existing Core

Should you decide later that you need to perform Windows patching, you will need to install the required Windows Patch Management files either by using the SA Client's Import feature or the `populate-opsware-update-library` command line script.

See the *SA User Guide: Server Patching* for more information about manually downloading the Windows Patching Utilities.

Core Parameter Values Required for Upgrade

The following table lists the core parameters that require values during upgrade whether specified manually or taken from an existing CDF.

table 5 Required Upgrade Parameter Values

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 SA 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 SA Client, select the **Administration** tab, then select Facilities. Select the facility you are upgrading to see its ID number.

table 5 Required Upgrade Parameter Values (cont'd)

Parameter	How to Find the Current Value
truth.dcNm	The Facility's short name. Log in to the SA Client, select the **Administration** tab, then select Facilities. Select the facility you are upgrading to see its short name.
truth.dcSubDom	Log into the SA Client, select the **Administration** tab, select System Configuration in the navigation panel, and then select 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
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 **Note**: After upgrade, this parameter name will be db.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

table 5 Required Upgrade Parameter Values (cont'd)

Parameter	How to Find the Current Value
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.
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.

table 5 Required Upgrade Parameter Values (cont'd)

Parameter	How to Find the Current Value
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
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).
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.

table 5 Required Upgrade Parameter Values (cont'd)

Parameter	How to Find the Current Value
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.)*
truth.uninstall.aresure	*This parameter is not required for upgrades. (It is only relevant when uninstalling* SA.*)*
truth.sid **Note**: After upgrade, this parameter name will be db.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.
truth.port **Note**: After upgrade, this parameter name will be db.port	Port on which the database host is being monitored and accepts connections.
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 SA Client to determine which locale is being used by SA (the locale value is apparent from the SA Client UI).

table 5 Required Upgrade Parameter Values (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
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
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
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
windows_util_loc	The directory in which the Windows Patch Management utilities are located unless you choose not to install them. See Windows Patch Management Utilities on page 42.
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

table 5 Required Upgrade Parameter Values (cont'd)

Parameter	How to Find the Current Value
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.
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.*

4 SA 10.2 Upgrade Procedure

This section describes the procedures for upgrading a Single Core (including distributed core component cores), Multimaster Mesh First and Secondary Cores, and Satellites to SA 10.2 from SA 9.x (includes patch releases and the minor releases).

Warning: After the standard SA Core upgrade is initiated, there is no procedure available to roll back to the previous version. For complex SA installations (multiple SA Cores, distributed core components, etc.), HP strongly recommends that you contact HP Professional Services (PSO) for assistance and consider a PSO-supported rolling upgrade procedure which does provide some rollback capabilities.

Supported Upgrade Paths

You can upgrade to SA 10.2 from the following releases:

- SA 9.10
- SA 9.1x
- SA 10.0
- SA 10.0x (patch release)
- SA 10.1x

CORD patches are rolled back to nearest major release either automatically during the upgrade or manually, if necessary.

New HPSA Upgrade Installer

As of SA 10.0, SA provides a simplified, enhanced, more flexible upgrade installation script. For information about the new installation procedure, see Upgrading a Single-host Core on page 55, Upgrading a Single Core with Distributed Components on page 58, Upgrading the First Core of a Multimaster Mesh on page 61 and Upgrading a Secondary Core of a Multimaster Mesh on page 64. If you have Satellite installations, see Upgrading a Satellite on page 69.

Before the Upgrade

Review and perform the tasks in this section before beginning the upgrade.

Uninstall All CORD Patches

You must uninstall any CORD patches that have been applied to any core including Single Core hosts, Multimaster Mesh First and Secondary Cores, and Satellites.

SA 9.1x: To roll back 9.1x to 9.1 before upgrade, see the patch roll back instructions in the SA 9.1x CORD release notes.

SA 10.0x: To rollback from 10.0x to 10.0 before upgrade, see the patch roll back instructions in the SA 10.0x CORD release notes.

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

For a *Single Core host* (no distributed core components), the SA Installer can automatically remove any CORD patches you have installed. However, in a distributed component core or Multimaster Mesh with CORD patches installed on core hosts (for example, SA CORD Patch release 7.50.01, 7.81, 9.02 etc.), you must *manually uninstall* the patch from *all hosts* using the procedure shown below 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 verify that all CORD patches have been removed from the First Core. To verify that all systems have had the patch removed, from the SA 10.1 media 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 6 Health Check Monitor Arguments

Argument	Description
`<system>`	Name of a reachable SA Core system
`<password>`	Optional password for user with root privileges on `<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 from a Standalone or Single-Host Core

The SA Installer will automatically roll back any applied CORD patches when invoked on a standalone or single-host core. No manual intervention is required.

Removing CORD Patches from First and Secondary Cores in a Multimaster Mesh

CORD patches must be uninstalled on one core at a time. If the core has distributed components, you can simultaneously uninstall the CORD patches from all machines in that core that host core components.

Satellite CORD patches, however, cannot be uninstalled in at the same time as the uninstallation of core server CORD patches.

1. Remove any applied CORD patches from the *Secondary Core(s)* (one core at a time):
   a. From the SA 10.1 media, Run the uninstall patch script on the Secondary Core:

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

      where `<distro>` is the full path to the distribution media. For example:

      `/<mountpoint>/hpsa-primary/`

   b. 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.
```

2 Remove any applied CORD patches from the *First (Primary) Core*:

a From the SA 10.1 media, run the uninstall patch script on the First (Primary) Core:

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

where `<distro>` is the full path to the distribution media. For example:

```
/<mountpoint>/hpsa-primary/disk001/opsware_installer/uninstall_patch.sh
```

b 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.
```

Uninstall Database Patches

Before you begin any core upgrade, you must first run the following script to uninstall database patches. On each model repository component host, run the following script:

```
<distro>/opsware_installer/uninstall_patch_db.sh --force_run
```

In addition to this, a resp file is required:

```
<distro>/opsware_installer/uninstall_patch_db.sh --force_run -r
<resp_file>:
```

`<distro>` is the full path to the distribution media. For example:

`/<mountpoint>/hpsa-primary/`

Additional Pre-Upgrade Requirements

1. Ensure that the SA Installation Files are downloaded locally.

   See SA Upgrade Files on page 31.

➤ The SA Upgrade Installer must have *read/write root privileges* to any mounted directories used during the upgrade of SA components, including any NFS-mounted network appliances.

2. Open a terminal window and log in as a user with root privileges.
3. Change to the root directory:

   ```
   cd /
   ```

➤ 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.

➤ Should the SA Upgrade Installer encounter a correctable error, the installation stops. Correct the error and retry the installation. The SA Installer will restart at the point that the error occurred.

Upgrading Supported SA Core Configurations

The *first upgrade of an SA Core to SA 10.x* from a previous version must be performed by HP Professional Services or an HP certified consultant unless your core matches one of the SA Core configurations supported for customer upgrade described in Chapter 2: *SA Core Configurations* in the *SA Planning and Installation Guide*. After the core has been upgraded to SA 10.x, HP supports customer-performed upgrades as long as your core configuration is one of the supported configurations. All other core configurations will continue to require the services of HP Professional Services. If you are uncertain whether you can upgrade an existing SA Core yourself, contact HP Technical Support.

The following sections provide instructions for each of the supported SA Core configurations documented in the *SA Planning and Installation Guide*.

➤ The Oracle database is not upgraded during an SA Core upgrade.

SA Core with a Local HP-supplied Oracle Database

1. Ensure that all upgrade prerequisites have been met.
2. Ensure that all CORD patches have been uninstalled from any server to be upgraded. See Uninstall All CORD Patches on page 50.
3. Use the instructions in Upgrading a Single-host Core on page 55 to upgrade the core.

SA Core with a Remote Customer-supplied Oracle Database

1. Ensure that all upgrade prerequisites have been met.
2. Ensure that all CORD patches have been uninstalled from any server to be upgraded. See Uninstall All CORD Patches on page 50.
3. Use the instructions in Upgrading a Single-host Core on page 55 to upgrade the core.

SA Core with a Remote Model Repository and HP-supplied Oracle Database

1. Ensure that all upgrade prerequisites have been met.
2. Ensure that all CORD patches have been uninstalled from any server to be upgraded. See Uninstall All CORD Patches on page 50.
3. Use the instructions in Upgrading a Single Core with Distributed Components on page 58 to upgrade the core.

SA Core with a Remote Model Repository and HP-supplied Oracle Database and Additional Slice Component Bundle Instances

1. Ensure that all upgrade prerequisites have been met.
2. Ensure that all CORD patches have been uninstalled from any server to be upgraded. See Uninstall All CORD Patches on page 50.
3. Use the instructions in Upgrading a Single Core with Distributed Components on page 58 to upgrade the core.

SA Core with a Remote Customer-supplied Oracle Database and Additional Slice Component Bundles

1. Ensure that all upgrade prerequisites have been met.
2. Ensure that all CORD patches have been uninstalled from any server to be upgraded. See Uninstall All CORD Patches on page 50.
3. Use the instructions in Upgrading a Single Core with Distributed Components on page 58 to upgrade the core.

SA Core with a Remote Model Repository and HP-supplied Oracle Database, Additional Slice Component Bundle Instances and Satellites

1. Ensure that all upgrade prerequisites have been met.
2. Ensure that all CORD patches have been uninstalled from any server to be upgraded. See Uninstall All CORD Patches on page 50.
3. Use the instructions in Upgrading a Single Core with Distributed Components on page 58 to upgrade the core.
4. Use the instructions in Upgrading a Satellite on page 69 to upgrade the Satellite(s).

SA Core with a Remote Customer-supplied Oracle Database, Additional Slice Component Bundles and Satellites

1. Ensure that all upgrade prerequisites have been met.
2. Ensure that all CORD patches have been uninstalled from any server to be upgraded. See Uninstall All CORD Patches on page 50.
3. Use the instructions in Upgrading a Single Core with Distributed Components on page 58 to upgrade the core.
4. Use the instructions in Upgrading a Satellite on page 69 to upgrade the Satellite(s).

Advanced Installation: SA First (Primary) Core with a Secondary Core (Multimaster Mesh)

1. Ensure that all upgrade prerequisites have been met.
2. Ensure that all CORD patches have been uninstalled from any server to be upgraded. See Uninstall All CORD Patches on page 50.
3. Use the instructions in Upgrading the First Core of a Multimaster Mesh on page 61 to upgrade the First Core.
4. Use the instructions in Upgrading a Secondary Core of a Multimaster Mesh on page 64 to upgrade the Secondary Core.

Upgrading a Single-host Core

➤ If you are upgrading a Multimaster Mesh, use the instructions shown in Upgrading the First Core of a Multimaster Mesh on page 61.

➤ Ensure that all CORD patches have been uninstalled, see Uninstall All CORD Patches on page 50.

1. On the core host, invoke the SA upgrade script as a user with root privileges:

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

   where `<distro>` is the full path to the distribution media. For example:

   `/<mountpoint>/hpsa-primary/`

SA 10.0 and later transitions from the Response Files used with previous versions to the new Core Description File (CDF), an XML based configuration file. The first time you upgrade a core or satellite to an SA 10.x release from an earlier release, the upgrade script uses the SA core parameter/configuration defaults from your existing response files in `/var/opt/opsware/install_opsware/resp` on Model Repository component host of the core being upgraded and stores them in a new default cdf.xml file. In subsequent upgrades, you will specify this CDF file using the -c argument when invoking the script. See Core Definition Files on page 31 and CDFs and the First Upgrade from 9.x to SA 10.2 on page 32.

If, for security reasons, you have stored your response file in a location other than the default location on the host being upgraded, you can copy the files to the Model Repository component host directory `/var/opt/opsware/install_opsware/resp` for the core to be upgraded.

2 The SA Upgrade script determines the component layout of your core and the Specify Hosts to Upgrade screen displays. It will look similar to the following:

```
Specify Hosts to Upgrade
========================

Currently specified hosts:

        <localhost_IP>

Please select one of the following options:

1. Add/edit host(s)
2. Delete host(s)

Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

Since this is a single core upgrade (all components to be upgraded are installed on the `localhost`), enter `c` and Enter to continue.

3 When you are prompted to enter the credentials for the server, enter the username and password credentials and press Enter. You are asked to re-enter the password for confirmation. When all passwords have been entered and verified, you see the message:

```
All values are entered. Do you wish to continue (Y/N) [Y]:
```

Press Enter to accept the default (`Y`) or `N` to re-enter values.

4 A screen similar to the following displays:

```
Host/Component Layout
=====================

Installed Components

Oracle RDBMS for SA                                    : <localhost_IP>
Model Repository, First Core                           : <localhost_IP>
Multimaster Infrastructure Component                   : <localhost_IP>
Software Repository Storage                            : <localhost_IP>
Slice                                                  : <localhost_IP>
OS Provisioning Media Server                           : <localhost_IP>
OS Provisioning Boot Server, Slice version             : <localhost_IP>
Software Repository - Content (install once per mesh)  : <localhost_IP>

Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

You may also see an entry similar to the following if any components do not require upgrade:

```
Up-to-date Components (will not upgrade)
----------------------------------------
Oracle RDBMS for SA
```

5 The following prompt displays:

```
 (windows_util_loc)
Please enter the directory path containing the Microsoft patching
utilities. Press Control-I for a list of required files or enter "none" if
you do not wish to upload the utilities at this time [none]:
```

Enter the fully qualified path to the Microsoft patching utilities or `none`.

The Microsoft patching utilities are required if you plan to use SA to install Windows operating system patches/hotfixes and/or to manage Windows-based servers with SA. If you do not intend to use SA for these tasks, you can bypass the upload of these files by entering "`none`". However, if in future you decide to use SA for Windows patching or to manage Windows servers, you will be required to install these utilities from the SA Client. For information about uploading these utilities from the SA Client, see the *User Guide: Server Patching*.

6 The Host Component Layout screen displays again. Press `c` to continue.

7 At this point, a prerequisite check is performed to ensure the host meets certain basic SA requirements. You may see a display similar to the following:

```
Prerequisite Checks
===================

Results for <IP_address>

WARNING Insufficient swap space (2 GBytes).
        4 GBytes is the recommended for core_inst.
        File system '/' has XXXXX Mbytes available and XXXXXX is
        recommended.

Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

You should attempt to meet the requirements specified in these warnings, however, you may be able to continue the upgrade if you are unable to meet the recommended settings. Press `c` to continue.

8 At this point the upgrade begins and you will see a series of informational messages displayed on the screen as the upgrade progresses. On completion of the upgrade, a success message displays.

9 You should now upgrade the SA Agents installed on managed servers as described in the *SA User's Guide: Server Automation*, "SA Agent Management".

You are not required to upgrade the agents, but in order to take advantage of the latest functionality that may have been added in the new release, agents must be upgraded. If you continue using an older agent, certain new functionality may not be available on the server managed by that agent. See the *SA Release Notes* for Agent compatibility issues.

Since support for Windows Server 2012 x64 as a managed platform was added in a CORD patch release to 9.1x, when the upgrade rolls the SA Core version back to SA 9.10, any Windows Server 2012 x64 managed servers you have in your core may not be recognized as having a valid operating system during hardware registration. After upgrading the managed server's agent, you can either manually run hardware registration or wait for it to run automatically (within 12 hours) after which the Windows Server 2012 x64 managed servers will be recognized correctly. Note that any managed platform added as part of a CORD release may be subject to similar core rollback before upgrade issues.

Upgrading a Single Core with Distributed Components

➤ If you are upgrading a Multimaster Mesh, use the instructions shown in Upgrading the First Core of a Multimaster Mesh on page 61.

➤ Ensure that all CORD patches have been uninstalled, see Uninstall All CORD Patches on page 50.

1 On the core's Infrastructure Component bundle host, invoke the SA upgrade script as a user with root privileges.

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

where `<distro>` is the full path to the distribution media. For example:

```
/<mountpoint>/hpsa-primary/
```

➤ SA 10.0 and later transitions from the Response Files used with previous versions to the new Core Description File (CDF), an XML based configuration file. The first time you upgrade a core or satellite to an SA 10.x release from an earlier release, the upgrade script uses the SA core parameter/configuration defaults from your existing response files in `/var/opt/opsware/install_opsware/resp` on Model Repository component host of the core being upgraded and stores them in a new default cdf.xml file. In subsequent upgrades, you will specify this CDF file using the -c argument when invoking the script. See Core Definition Files on page 31 and CDFs and the First Upgrade from 9.x to SA 10.2 on page 32.

If, for security reasons, you have stored your response file in a location other than the default location on the host being upgraded, you can copy the files to the Model Repository component host directory `/var/opt/opsware/install_opsware/resp` for the core to be upgraded.

2 The Specify Hosts to Upgrade screen displays. It will look similar to the following:

```
Specify Hosts to Upgrade
========================

Currently specified hosts:

        <localhost_IP>

Please select one of the following options:

1. Add/edit host(s)
2. Delete host(s)

Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

Since this core has distributed components, you must add all servers that host a core component(s). Enter 1, to Add/Edit hosts in the Currently Specified Hosts list.

3 You are prompted to specify the number of server addresses you want to add. Enter the number and press Enter.

4 You see a screen similar to the following:

```
Adding Hosts
============

Parameter 2 of 3
FQDN Hostname / IP []:
```

Enter the hostname or IP address of the first host to add and press enter. Repeat for all the hosts you are adding.

When you have added the specified number of hosts, you see this message:

```
All values are entered. Do you wish to continue (Y/N) [Y]:
```

Press Enter to accept the default (`Y`) or `N` to re-enter values.

5 When you are prompted to enter the credentials for each specified host, enter the username and password credentials and press Enter. You are asked to re-enter the password for confirmation. When all passwords have been entered and verified, you see the message:

```
All values are entered. Do you wish to continue (Y/N) [Y]:
```

Press Enter to accept the default (`Y`) or `N` to re-enter values.

6 The SA Upgrade script determines the component layout of your core. A screen similar to the following displays:

```
Host/Component Layout
=====================

Installed Components

Oracle RDBMS for SA                                    : 192.168.100.101
Model Repository, First Core                           : <localhost_IP>
Multimaster Infrastructure Component                   : <localhost_IP>
Software Repository Storage                            : 192.168.100.112
Slice                                                  : 192.168.100.113
OS Provisioning Media Server                           : 192.168.100.114
OS Provisioning Boot Server, Slice version             : 192.168.100.115
Software Repository - Content (install once per mesh)  : 192.168.100.116

Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

You may also see an entry similar to the following if any components do not require upgrade:

```
Up-to-date Components (will not upgrade)
----------------------------------------
Oracle RDBMS for SA (192.168.100.101)
```

7 The following prompt displays:

```
 (windows_util_loc)
Please enter the directory path containing the Microsoft patching
utilities. Press Control-I for a list of required files or enter "none" if
you do not wish to upload the utilities at this time [none]:
```

Enter the fully qualified path to the Microsoft patching utilities or `none`.

The Microsoft patching utilities are required if you plan to use SA to install Windows operating system patches/hotfixes and/or to manage Windows-based servers with SA. If you do not intend to use SA for these tasks, you can bypass the upload of these files by entering "`none`". However, if in future you decide to use SA for Windows patching or to manage Windows servers, you will be required to install these files from the SA Client. For information about uploading these files from the SA Client, see the *User Guide: Server Patching*.

8 The Host Component Layout screen displays again. Press `c` to continue.

9 At this point, a prerequisite check is performed on each specified host to ensure the hosts meet certain basic SA requirements. You may see notifications similar to the following for each host:

```
Prerequisite Checks
===================

Results for <IP_address>

WARNING Insufficient swap space (2 GBytes).
        4 GBytes is the recommended for core_inst.
        File system '/' has XXXXX Mbytes available and XXXXXX is
        recommended.

Enter one of the following directives
(<c>continue, <p>revious, <h>elp, <q>uit):
```

You should attempt to meet the requirements specified in these warnings, however, you may be able to continue the upgrade if you are unable to meet the recommended settings. Press `c` to continue.

At this point the upgrade begins and you will see a series of informational messages displayed on the screen as the upgrade progresses. On completion of the upgrade, a success message is displayed.

10 You should now upgrade the SA Agents installed on managed servers as described in the *SA User's Guide: Server Automation*, "SA Agent Management".

You are not required to upgrade the agents, but in order to take advantage of the latest functionality that may have been added in the new release, agents must be upgraded. If you continue using an older agent, certain new functionality may not be available on the server managed by that agent. See the *SA Release Notes* for Agent compatibility issues.

Upgrading the First Core of a Multimaster Mesh

This procedure assumes that the First Core has distributed Core Components. If the core does not have distributed components, the list shown in step 6 will display hostname or the IP address of the First Core for all components.

➤ Ensure that all CORD patches have been uninstalled from all mesh core hosts (First, Secondary and Satellite) using the procedure described in Uninstall All CORD Patches on page 50 before beginning the upgrade.

1 Shut down all Secondary Core services in the Multimaster Mesh by issuing the following command as a user with root privileges on each Secondary Core host:

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

2 Start the Management and Core Gateways on the Secondary Core host

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

3 On the Primary Core's Infrastructure Component bundle host, invoke the SA upgrade script as a user with root privileges.

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

where, `<distro>` is the full path to the distribution media. For example,

```
/<mountpoint>/hpsa-primary/
```

➤ SA 10.0 and later transitions from the Response Files used with previous versions to the new Core Description File (CDF), an XML based configuration file. The first time you upgrade a core or satellite to an SA 10.x release from an earlier release, the upgrade script uses the SA core parameter/configuration defaults from your existing response files in `/var/opt/opsware/install_opsware/resp` on Model Repository component host of the core being upgraded and stores them in a new default cdf.xml file. In subsequent upgrades, you will specify this CDF file using the -c argument when invoking the script. See Core Definition Files on page 31 and CDFs and the First Upgrade from 9.x to SA 10.2 on page 32.

If, for security reasons, you have stored your response file in a location other than the default location on the host being upgraded, you can copy the files to the Model Repository component host directory `/var/opt/opsware/install_opsware/resp` for the core to be upgraded.

4 The Specify Hosts to Upgrade screen displays. It will look similar to the following:

```
Specify Hosts to Upgrade
========================

Currently specified hosts:

        <localhost_IP>

Please select one of the following options:
```

```
1. Add/edit host(s)
2. Delete host(s)

Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

Since this core has distributed components, you must add all servers that host a core component(s). Enter 1, to Add/Edit hosts in the Currently Specified Hosts list.

5 You are prompted to specify the number of server addresses you want to add. Enter the number and press Enter.

6 You see a screen similar to the following:

```
Adding Hosts
============

Parameter 2 of 3
FQDN Hostname / IP []:
```

Enter the hostname or IP address of the first host to add and press enter. Repeat for all the hosts you are adding.

When you have added the specified number of hosts, you see this message:

```
All values are entered. Do you wish to continue (Y/N) [Y]:
```

Press Enter to accept the default (Y) or N to re-enter values.

7 When you are prompted to enter the credentials for each specified host, enter the username and password credentials and press Enter. You are asked to re-enter the password for confirmation. When all passwords have been entered and verified, you see the message:

```
All values are entered. Do you wish to continue (Y/N) [Y]:
```

Press Enter to accept the default (Y) or N to re-enter values.

8 The SA Upgrade script determines the component layout of your core. A screen similar to the following displays:

```
Host/Component Layout
=====================

Installed Components

Oracle RDBMS for SA                                    : 192.168.100.101
Model Repository, First Core                           : <localhost_IP>
Multimaster Infrastructure Component                   : <localhost_IP
Software Repository Storage                            : 192.168.100.112
Slice                                                  : 192.168.100.113
OS Provisioning Media Server                           : 192.168.100.114
OS Provisioning Boot Server, Slice version             : 192.168.100.115
Software Repository - Content (install once per mesh)  : 192.168.100.116

Enter one of the following directives
(<c>continue, <p>revious, <h>elp, <q>uit):
```

You may also see an entry similar to the following if any components do not require upgrade:

```
Up-to-date Components (will not upgrade)
----------------------------------------
Oracle RDBMS for SA (192.168.100.101)
```

9 The following prompt displays:

```
 (windows_util_loc)
Please enter the directory path containing the Microsoft patching
utilities. Press Control-I for a list of required files or enter "none" if
you do not wish to upload the utilities at this time [none]:
```

Enter the fully qualified path to the Microsoft patching utilities or `none`.

The Microsoft patching utilities are required if you plan to use SA to install Windows operating system patches/hotfixes and/or to manage Windows-based servers with SA. If you do not intend to use SA for these tasks, you can bypass the upload of these files by entering "`none`". However, if in future you decide to use SA for Windows patching or to manage Windows servers, you will be required to install these files from the SA Client. For information about uploading these files from the SA Client, see the *User Guide: Server Patching*.

10 The Host Component Layout screen displays again. Press `c` to continue.

11 At this point, a prerequisite check is performed on each specified host to ensure the hosts meet certain basic SA requirements. You may see notifications similar to the following for each host:

```
Prerequisite Checks
===================

Results for <IP_address>

WARNING Insufficient swap space (2 GBytes).
        4 GBytes is the recommended for core_inst.
        File system '/' has XXXXX Mbytes available and XXXXXX is
        recommended.

Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

You should attempt to meet the requirements specified in these warnings, however, you may be able to continue the upgrade if you are unable to meet the recommended settings. Press `c` to continue.

At this point the upgrade begins and you will see a series of informational messages displayed on the screen as the upgrade progresses. On completion of the upgrade, a success message is displayed. When the upgrade completes, the Core Description File (CDF) is automatically saved in

```
/var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml
```

12 You should now upgrade all Secondary Cores, see the next section and, after upgrading the Secondary Cores, you should upgrade the SA Agents installed on managed servers as described in the *SA User's Guide: Server Automation*, "SA Agent Management".

You are not required to upgrade the agents, but in order to take advantage of the latest functionality that may have been added in the new release, agents must be upgraded. If you continue using an older agent, certain new functionality may not be available on the server managed by that agent. See the *SA Release Notes* for Agent compatibility issues.

Upgrading a Secondary Core of a Multimaster Mesh

- Ensure that all CORD patches have been uninstalled from all mesh core hosts (First, Secondary and Satellite) using the procedure described in Uninstall All CORD Patches on page 50 before beginning the upgrade.

- 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.

- You can upgrade the Secondary Cores in a mesh one at a time or upgrade multiple Secondary Cores concurrently. After each Secondary Core has been upgraded, its services will be restarted and can remain running while you upgrade the other Secondary Cores.

  Perform the following tasks to upgrade a Secondary Core (you will do this for all Secondary Cores in the Multimaster Mesh).

  1. Ensure that there are no outstanding transactions or conflicts in the mesh before upgrading any Secondary Core as described in "Viewing the State of the Multimaster Mesh - SA Client" in the *SA Administration Guide*. If conflicts exist, resolve them as described in "Resolving Mesh Conflicts - SA Client" in the *SA Administration Guide*.
  2. Ensure that all Secondary Core services, including the Management and Core Gateways are up and running.

- **Note**: If you need to start the Management and Core Gateways on the Secondary Core host issue the following command on each Secondary Core host:

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

  3. On the Secondary Core host, invoke the SA upgrade script as a user with root privileges.

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

     where `<distro>` is the full path to the distribution media. For example:

     ```
     /<mountpoint>/hpsa-primary/
     ```

- SA 10.0 and later transitions from the Response Files used with previous versions to the new Core Description File (CDF), an XML based configuration file. The first time you upgrade a core or satellite to an SA 10.x release from an earlier release, the upgrade script uses the SA core parameter/configuration defaults from your existing response files in `/var/opt/opsware/install_opsware/resp` on Model Repository component host of the core being upgraded and stores them in a new default cdf.xml file. In subsequent upgrades, you will specify this CDF file using the -c argument when invoking the script. See Core Definition Files on page 31 and CDFs and the First Upgrade from 9.x to SA 10.2 on page 32.

  If, for security reasons, you have stored your response file in a location other than the default location on the host being upgraded, you can copy the files to the Model Repository component host directory `/var/opt/opsware/install_opsware/resp` for the core to be upgraded.

  4. The Specify Hosts to Upgrade screen displays. It will look similar to the following:

     ```
     Specify Hosts to Upgrade
     ========================

     Currently specified hosts:

             localhost_IP

     Please select one of the following options:
     ```

```
1. Add/edit host(s)
2. Delete host(s)

Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

Since this is a single core upgrade (all components to be upgraded are installed on the `localhost`), enter `c` and Enter to continue.

If you are upgrading multiple Secondary Cores, you can upgrade the cores simultaneously. Of course, the prerequisites shown in Before the Upgrade on page 50 must have been met and the upgrade script must be run on each Secondary Core. Hosts added in Step 2 above are servers that host components of a single Secondary Core, not separate Secondary Cores.

5 The SA Upgrade script determines the component layout of your core. A screen similar to the following displays:

```
Host/Component Layout
=====================

Installed Components

Oracle RDBMS for SA                                    : <localhost_IP>
Model Repository, First Core                           : <localhost_IP>
Multimaster Infrastructure Component                   : <localhost_IP>
Software Repository Storage                            : <localhost_IP>
Slice                                                  : <localhost_IP>
OS Provisioning Media Server                           : <localhost_IP>
OS Provisioning Boot Server, Slice version             : <localhost_IP>
Software Repository - Content (install once per mesh)  : <localhost_IP>

Enter one of the following directives
(<c>continue, <p>revious, <h>elp, <q>uit):
```

You may also see an entry similar to the following if any components do not require upgrade:

```
Up-to-date Components (will not upgrade)
----------------------------------------
Oracle RDBMS for SA
```

6 The following prompt displays:

```
 (windows_util_loc)
Please enter the directory path containing the Microsoft patching
utilities. Press Control-I for a list of required files or enter "none" if
you do not wish to upload the utilities at this time [none]:
```

Enter the fully qualified path to the Microsoft patching utilities or `none`.

The Microsoft patching utilities are required if you plan to use SA to install Windows operating system patches/hotfixes and/or to manage Windows-based servers with SA. If you do not intend to use SA for these tasks, you can bypass the upload of these files by entering "`none`". However, if in future you decide to use SA for Windows patching or to manage Windows servers, you will be required to install these files from the SA Client. For information about uploading these files from the SA Client, see the *User Guide: Server Patching*.

7 The Host Component Layout screen displays again. Press `c` to continue.

8 At this point, a prerequisite check is performed to ensure the host meets certain basic SA requirements. You may see a display similar to the following:

```
Prerequisite Checks
===================

Results for <IP_address>

WARNING Insufficient swap space (2 GBytes).
        4 GBytes is the recommended for core_inst.
        File system '/' has XXXXX Mbytes available and XXXXXX is
        recommended.

Enter one of the following directives
(<c>continue, <p>revious, <h>elp, <q>uit):
```

You should attempt to meet the requirements specified in these warnings, however, you may be able to continue the upgrade if you are unable to meet the recommended settings. Press `c` to continue.

At this point the upgrade begins and you will see a series of informational messages displayed on the screen as the upgrade progresses. On completion of the upgrade, a success message is displayed. When the upgrade completes, the Core Description File (CDF) is automatically saved in

`/var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml`

9 You should now upgrade the SA Agents installed on managed servers as described in the *SA User's Guide: Server Automation*, "SA Agent Management".

You are not required to upgrade the agents, but in order to take advantage of the latest functionality that may have been added in the new release, agents must be upgraded. If you continue using an older agent, certain new functionality may not be available on the server managed by that agent. See the *SA Release Notes* for Agent compatibility issues.

Upgrading a Secondary Core with Distributed Components

Ensure that all CORD patches have been uninstalled from all mesh core hosts (First, Secondary and Satellite) using the procedure described in Uninstall All CORD Patches on page 50 before beginning the upgrade.

1 On the Secondary Core host, invoke the SA upgrade script as a user with root privileges.

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

where `<distro>` is the full path to the distribution media. For example:

`/<mountpoint>/hpsa-primary/`

SA 10.0 and later transitions from the Response Files used with previous versions to the new Core Description File (CDF), an XML based configuration file. The first time you upgrade a core or satellite to an SA 10.x release from a earlier release, the upgrade script uses the SA core parameter/configuration defaults from your existing response files in `/var/opt/opsware/install_opsware/resp` on Model Repository component host of the core being upgraded and stores them in a new default cdf.xml file. In subsequent upgrades, you will specify this CDF file using the -c argument when invoking the script. See Core Definition Files on page 31 and CDFs and the First Upgrade from 9.x to SA 10.2 on page 32.

If, for security reasons, you have stored your response file in a location other than the default location on the host being upgraded, you can copy the files to the Model Repository component host directory `/var/opt/opsware/install_opsware/resp` for the core to be upgraded.

2 The Specify Hosts to Upgrade screen displays. It will look similar to the following:

```
Specify Hosts to Upgrade
========================

Currently specified hosts:

        <localhost_IP>

Please select one of the following options:

1. Add/edit host(s)
2. Delete host(s)


Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

Since this core has distributed components, you must add all servers that host a core component(s). Enter 1, to Add/Edit hosts in the Currently Specified Hosts list.

3 You are prompted to specify the number of server addresses you want to upgrade. Enter the number and press Enter.

4 You see a screen similar to the following:

```
Adding Hosts
============

Parameter 2 of 7
FQDN Hostname / IP []:
```

Enter the hostname or IP address of the first host to add and press enter. Repeat for all the hosts you are adding.

When you have added the specified number of hosts, you see this message:

```
All values are entered. Do you wish to continue (Y/N) [Y]:
```

Press Enter to accept the default (`Y`) or `N` to re-enter values.

5 When you are prompted to enter the credentials for each specified host, enter the username and password credentials and press Enter. You are asked to re-enter the password for confirmation. When all passwords have been entered and verified, you see the message:

```
All values are entered. Do you wish to continue (Y/N) [Y]:
```

Press Enter to accept the default (`Y`) or `N` to re-enter values.

6 The SA Upgrade script determines the component layout of your core. A screen similar to the following displays:

```
Host/Component Layout
=====================

Installed Components

Oracle RDBMS for SA                                  : 192.168.100.101
Model Repository, First Core                         : <localhost_IP>
Multimaster Infrastructure Component                 : <localhost_IP>
Software Repository Storage                          : 192.168.100.112
Slice                                                : 192.168.100.113
OS Provisioning Media Server                         : 192.168.100.114
OS Provisioning Boot Server, Slice version           : 192.168.100.115
```

```
Software Repository - Content (install once per mesh)    : 192.168.100.116

Enter one of the following directives
(<c>continue, <p>revious, <h>elp, <q>uit):
```

You may also see an entry similar to the following if any components do not require upgrade:

```
Up-to-date Components (will not upgrade)
----------------------------------------
Oracle RDBMS for SA (192.168.100.101)
```

7 The following prompt displays:

```
 (windows_util_loc)
Please enter the directory path containing the Microsoft patching
utilities. Press Control-I for a list of required files or enter "none" if
you do not wish to upload the utilities at this time [none]:
```

Enter the fully qualified path to the Microsoft patching utilities or `none`.

The Microsoft patching utilities are required if you plan to use SA to install Windows operating system patches/hotfixes and/or to manage Windows-based servers with SA. If you do not intend to use SA for these tasks, you can bypass the upload of these files by entering "`none`". However, if in future you decide to use SA for Windows patching or to manage Windows servers, you will be required to install these files from the SA Client. For information about uploading these files from the SA Client, see the *User Guide: Server Patching*.

8 The Host Component Layout screen displays again. Press `c` to continue.

9 At this point, a prerequisite check is performed on each specified host to ensure the hosts meet certain basic SA requirements. You may see notifications similar to the following for each host:

```
Prerequisite Checks
===================

Results for <IP_address>

WARNING Insufficient swap space (2 GBytes).
        4 GBytes is the recommended for core_inst.
        File system '/' has XXXXX Mbytes available and XXXXXX is
        recommended.

Enter one of the following directives
(<c>continue, <p>revious, <h>elp, <q>uit):
```

You should attempt to meet the requirements specified in these warnings, however, you may be able to continue the upgrade if you are unable to meet the recommended settings. Press `c` to continue.

At this point the upgrade begins and you will see a series of informational messages displayed on the screen as the upgrade progresses. On completion of the upgrade, a success message is displayed. When the upgrade completes, the Core Description File (CDF) is automatically saved in

```
/var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml
```

10 You should now upgrade the SA Agents installed on managed servers as described in the *SA User's Guide: Server Automation*, "SA Agent Management".

You are not required to upgrade the agents, but in order to take advantage of the latest functionality that may have been added in the new release, agents must be upgraded. If you continue using an older agent, certain new functionality may not be available on the server managed by that agent. See the *SA Release Notes* for Agent compatibility issues.

Upgrading a Satellite

You are not required to upgrade your Satellites immediately after a Core upgrade to SA 10.2.

During the Simple upgrade interview, you will not be prompted for new parameter values and defaults will be used. If you need to specify values for these new parameters, you must select the advanced upgrade interview. After upgrade the Satellite parameters are the following:

table 7 Satellite Parameters

Parameter	Requirement	Description
`truth.oaPwd`	`opsware_admin` user access	The opsware_`admin` password.
`cast.admin_pwd`	SA Administrator's access	The SA Administrator's password
`NEW satellite.dcNm`	The Satellite Facility identification	The name of the new Satellite's facility.
`NEW satellite.realm_name`	Realm name	The name of the new Realm to be serviced by the Satellite. SA uses the Realm name and the IP address of a managed server to uniquely identify a managed server. The Gateway Installer assigns the Realm name to the new Satellite facility. The Core and Satellite facility names must be different. The Realm name cannot contain spaces.
`satellite.host.ip`	Satellite host's network location	The IP address of the server on which you will install the Satellite
`NEW satellite.gateway_name`	The name for a new or existing Satellite Gateway (name cannot contain spaces)	The name of the Gateway the Satellite will use for communications with the First Core management Gateway or other Satellite Gateways (in a cascaded Satellite topology).
`NEW satellite.proxy_port`	The port used by Agents to contact the new Satellite.	The port number on which agents can contact the Satellite Gateway. (Default: 3001).
`NEW satellite.parentgw.ip`	A Core Management Gateway IP address	The IP address of a server running a Management Gateway.

table 7 Satellite Parameters (cont'd)

Parameter	Requirement	Description
NEW satellite.parentgw. tunnel_listener_port	The Management Gateway's listener port	The port number through which tunnel connections to the Management Gateway will pass. (The default port is 2001.) The Management Gateway listens on this port for connection requests from the Satellite. In the Management Gateway Properties File, this port specified with the opswgw.TunnelDst parameter The path to the Core's Gateway Properties file is: /etc/opt/opsware/ opswgw-mgw0-<facility>/ opswgw.properties
NEW satellite.parentgw. proxy_port	The port on which a Core's Management Gateway listens for connection requests.	The port number on which a Core's Management Gateway listens for connection requests from Satellite Gateways to SA Core Components (default 3003) or the port on which a Satellite Gateway listens for connection requests from other Satellite Gateways to SA Core Components (cascading Satellite links) (default 3001).
decrypt_passwd	Accessing Core cryptographic material	The password required to access the Core's cryptographic material.
word_root	Package Repository location (OS Provisioning)	The root directory for the Package Repository. For example: /var/opt/opsware/word
media_server. linux_media	Linux media location (OS Provisioning)	The pathname to the Linux media. For example: /media/opsware/linux
media_server. sunos_media	Solaris media location (OS Provisioning)	The pathname to the Solaris media. For example: /media/opsware/sunos
media_server. windows_media	Windows media location (OS Provisioning)	The pathname to the Windows media. For example: /media/opsware/windows
bootagent.host	OS Provisioning Boot Server	The OS Provisioning Boot Server IP or hostname.

table 7 Satellite Parameters (cont'd)

Parameter	Requirement	Description
`agent_gw_list_args`	Agent- Gateway communications	The list of Gateways on which the the Satellite's agent will be installed. Specified by the IP address and port number (`ip:port`) on which Agents can contact the Gateway in the Satellite facility. Default <*satellite_gateway*>:3001.

Phases of an SA 10.2 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 Satellite upgrade script and specify Satellite hosts	
2	Supply Satellite parameter values	
3	Upgrade the Satellite components	
4	(Optional) Upgrade the OS Provisioning Components	
5	Upgrade SA Agents	

Satellite Upgrade Procedures

The following sections cover:

- 1. Single-Host Satellite Upgrade (OS Provisioning Not Installed)
- 2. Single-Host Satellite with OS Provisioning Components
- 3. Satellite with OS Provisioning Components on a Separate Host Upgrade

1. Single-Host Satellite Upgrade (OS Provisioning Not Installed)

This procedure upgrades a Satellite installed with all Satellite components on the same host, OS Provisioning components are not installed.

Phase 1: Invoke the SA Upgrade Script and Specify Satellite Hosts

1 If you have installed any patches to the Satellite you are upgrading, you must remove them before starting the upgrade. See Uninstall All CORD Patches on page 50.

2 Invoke the SA Installer upgrade script by entering the following command. You must have the path to the response file used to install the Satellite.

```
/<distro>/opsware_installer/hpsa_upgrade_satellite.sh -r <response_file>
```

where `<distro>` is the full path to the distribution media. For example:

```
/<mountpoint>/hpsa-primary/
```

SA 10.0 ad later transitions from the Response Files used with previous versions to the new Core Description File (CDF), an XML based configuration file. The first time you upgrade a core or satellite to an SA 10.x release from an earlier release, the upgrade script uses the SA core parameter/configuration defaults from your existing response files in `/var/opt/opsware/install_opsware/resp` on Model Repository component host of the core being upgraded and stores them in a new default cdf.xml file. In subsequent upgrades, you will specify this CDF file using the -c argument when invoking the script. See Core Definition Files on page 31 and CDFs and the First Upgrade from 9.x to SA 10.2 on page 32.

If, for security reasons, you have stored your response file in a location other than the default location on the host being upgraded, you can copy the files to the Model Repository component host directory `/var/opt/opsware/install_opsware/resp` for the core to be upgraded.

3 The following menu displays:

```
Specify Host(s) for Satellite Upgrade
=====================================

Currently specified hosts:

   <IP_address> (localhost)

Please select one of the following options:

1. Add/edit host(s)
2. Delete host(s)

Enter the option number or one of the following directives
(<c>ontinue, <h>elp, <q>uit): c
```

Since this example Satellite upgrade uses the host that the upgrade script is invoked on for all components, type `c` and press Enter to continue. You can invoke the upgrade from a remote machine by selecting `2` to delete the localhost IP address followed by `1` to add the remote host IP address.

The upgrade script displays messages as it prepares the Satellite host for upgrade.

4 The following menu displays:

```
Host/Component Layout
=====================

Installed Components

Satellite

Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

Since only the Satellite components are installed, `Satellite` is the only component listed.

Type `c` and press Enter to continue.

Phase 3: Supply Satellite Parameter Values

1 The following menu displays:

```
Interview Parameters
====================

Navigation keys:
Use <ctrl>p to go to the previous parameter.
Use <ctrl>n to go the next parameter.
Use <tab> to view help on the current parameter.
Use <ctrl>c to abort the interview.


All prompts have values.  What would you like to do:

1. Re-enter values
2. Continue

Enter the option number or one of the following directives
(<c>ontinue, <h>elp, <q>uit):
```

The SA upgrade script takes the default values for the Satellite parameters from the response file or CDF you specified. Be very careful changing these values but if you have a valid reason to do so, select 1. Each parameter and its assigned value is displayed and you can change the value if necessary.

Type `c` and press Enter to continue.

Phase 4: Upgrade the Satellite

1 At this point, the Prerequisite Check begins.

Before SA begins the upgrade, it performs a prerequisite check that validates that the host on which you are upgrading the Satellite meets the minimum requirements. The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on. If your host fails the prerequisite check, the upgrade can fail or core performance may be negatively affected. If your host fails the prerequisite check or displays warnings, correct the problem(s) or contact HP support services.

The prerequisite check may display messages similar to the following:

```
Prerequisite Checks
==============

Results for <IP_address>:

        WARNING Insufficient swap space (18 GBytes).
                24 Gbytes is the recommended for Oracle.

        WARNING File system '/' has 29447 MBytes available and 154050 is
                recommended.

Enter the option number or one of the following directives:
(<c>ontinue, <p>revious, <h>elp, <q>uit)
```

The Prerequisite check identifies WARNINGs and/or FAILUREs. FAILUREs can cause a failed or incomplete upgrade and must be resolved before continuing. WARNINGs allow you to continue the upgrade, however, Satellite performance may be negatively affected if you continue without resolving them.

If your server passes the prerequisite check, enter `c` and press Enter to begin the Satellite upgrade.

2. You see many messages displayed as the upgrade progresses. Unless the upgrade fails, these messages are purely informational. When the upgrade completes, the Core Description File (CDF) is automatically saved.
3. You must now upgrade your SA Agents. See Phase 4: Upgrade the SA Agents on page 80.

2. Single-Host Satellite with OS Provisioning Components

This procedure upgrades a Satellite installed with all Satellite and OS Provisioning components on the same host.

Phase 1: Invoke the SA Upgrade Script and Specify Satellite Host

1. Invoke the SA Installer upgrade script by entering the following command. You must have the path to the response file used to install the Satellite.

   ```
   /<distro>/opsware_installer/hpsa_upgrade_satellite.sh -r <response_file>
   ```

   where `<distro>` is the full path to the distribution media. For example:

   ```
   /<mountpoint>/hpsa-primary/
   ```

SA 10.0 and later transitions from the Response Files used with previous versions to the new Core Description File (CDF), an XML based configuration file. The first time you upgrade a core or satellite to an SA 10.x release from an earlier release, the upgrade script uses the SA core parameter/configuration defaults from your existing response files in `/var/opt/opsware/install_opsware/resp` on Model Repository component host of the core being upgraded and stores them in a new default cdf.xml file. In subsequent upgrades, you will specify this CDF file using the -c argument when invoking the script. See Core Definition Files on page 31 and CDFs and the First Upgrade from 9.x to SA 10.2 on page 32.

If, for security reasons, you have stored your response file in a location other than the default location on the host being upgraded, you can copy the files to the Model Repository component host directory `/var/opt/opsware/install_opsware/resp` for the core to be upgraded.

2 The following menu displays:

```
Specify Host(s) for Satellite Upgrade
=====================================

Currently specified hosts:

   <IP_address> (localhost)

Please select one of the following options:

1. Add/edit host(s)
2. Delete host(s)

Enter the option number or one of the following directives
(<c>ontinue, <h>elp, <q>uit): c
```

Since this example Satellite upgrade uses the host that the upgrade script is invoked on for all components, type `c` and press Enter to continue. You can invoke the upgrade from a remote machine by selecting `2` to delete the localhost IP address followed by `1` to add the remote host IP address.

The upgrade script displays messages as it prepares the Satellite host for upgrade.

3 The following menu displays:

```
Host/Component Layout
=====================

Installed Components

Satellite
OS Provisioning Boot Server
OS Provisioning Media Server

Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

Type `c` and press Enter to continue.

Phase 2: Supply Satellite Parameter Values

1 The following menu displays:

```
Interview Parameters
====================

Navigation keys:
Use <ctrl>p to go to the previous parameter.
Use <ctrl>n to go the next parameter.
Use <tab> to view help on the current parameter.
Use <ctrl>c to abort the interview.


All prompts have values.  What would you like to do:

1. Re-enter values
2. Continue
```

```
Enter the option number or one of the following directives
(<c>ontinue, <h>elp, <q>uit):
```

The SA upgrade script takes the default values for the Satellite parameters from the response file or CDF you specified. Be very careful changing these values but if you have a valid reason to do so, select 1. Each parameter and its assigned value is displayed and you can change the value if necessary.

Type `c` and press Enter to continue.

Phase 3: Upgrade the Satellite

1. At this point, the Prerequisite Check begins.

Before SA begins the upgrade, it performs a prerequisite check that validates that the host on which you are upgrading the Satellite meets the minimum requirements. The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on. If your host fails the prerequisite check, the upgrade can fail or core performance may be negatively effected. If your host fails the prerequisite check or displays warnings, correct the problem(s) or contact HP support services.

The prerequisite check may display messages similar to the following:

```
Prerequisite Checks
==============

Results for <IP_address>:

        WARNING Insufficient swap space (18 GBytes).
                24 Gbytes is the recommended for Oracle.

        WARNING File system '/' has 29447 MBytes available and 154050 is
                recommended.

Enter the option number or one of the following directives:
(<c>ontinue, <p>revious, <h>elp, <q>uit)
```

The Prerequisite check identifies WARNINGs and/or FAILUREs. FAILUREs can cause a failed or incomplete upgrade and must be resolved before continuing. WARNINGs allow you to continue the upgrade, however, Satellite performance may be negatively affected if you continue without resolving them.

If your server passes the prerequisite check, enter `c` and press Enter to begin the Satellite upgrade.

2. You see many messages displayed as the upgrade progresses. Unless the upgrade fails, these messages are purely informational. When the upgrade completes, the Core Description File (CDF) is automatically saved.
3. You must now upgrade your SA Agents. See Phase 4: Upgrade the SA Agents on page 80.

3. Satellite with OS Provisioning Components on a Separate Host Upgrade

This procedure upgrades a Satellite installed with the Satellite components on one host and the OS Provisioning components on another host.

Phase 1: Invoke the SA Upgrade Script and Specify Satellite Hosts

1. Invoke the SA Installer upgrade script by entering the following command. You must have the path to the response file used to install the Satellite.

```
/<distro>/opsware_installer/hpsa_upgrade_satellite.sh -r <response_file>
```

where <distro> is the full path to the distribution media. For example:

/<*mountpoint*>/hpsa-primary/

SA 10.0 and later transitions from the Response Files used with previous versions to the new Core Description File (CDF), an XML based configuration file. The first time you upgrade a core or satellite to an SA 10.x release from an earlier release, the upgrade script uses the SA core parameter/configuration defaults from your existing response files in /var/opt/opsware/install_opsware/resp on Model Repository component host of the core being upgraded and stores them in a new default cdf.xml file. In subsequent upgrades, you will specify this CDF file using the -c argument when invoking the script. See Core Definition Files on page 31 and CDFs and the First Upgrade from 9.x to SA 10.2 on page 32.

If, for security reasons, you have stored your response file in a location other than the default location on the host being upgraded, you can copy the files to the Model Repository component host directory /var/opt/opsware/install_opsware/resp for the core to be upgraded.

2 The following menu displays:

```
Specify Host(s) for Satellite Upgrade
=====================================

Currently specified hosts:

   <IP_address> (localhost)

Please select one of the following options:

1. Add/edit host(s)
2. Delete host(s)

Enter the option number or one of the following directives
(<c>ontinue, <h>elp, <q>uit): c
```

Since the OS Provisioning components are installed on a separate server from the Satellite components, you must specify the IP address for the server that hosts the OS Provisioning components.

3 Press 1 to add the host IP address.

The following prompt displays:

```
Enter number of hosts to add:
```

Enter the appropriate number. For this example, we use two hosts:

```
Enter number of hosts to add: 2
```

For this example, we add the hosts:

- 192.168.136.36
- 192.168.136.39

4 The following screen displays:

```
Adding Hosts
============

Parameter 1 of 2
Hostname/IP []:
```

Enter the hostname or IP address of the first server that will host an SA Core Component(s) and press Enter.

Do the same for the second host. You see this message:

```
All values are entered.  Do you wish to continue? (Y/N) [Y]:
```

Enter `Y` to continue.

5 A screen similar to the following displays:

```
Specify Hosts to Install
========================

Currently specified hosts:

        192.168.136.36
        192.168.136.39


Please select one of the following options:

1. Add/edit host(s)
2. Delete host(s)

Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

6 At this point you can press `2` to delete a host or `0` to add/edit a hostname/IP address.

```
Enter number of hosts to add (or enter "0" to edit the list):
```

Or, if you are satisfied with the entries, press `C` to continue.

7 You are asked to provide the credentials for each host in the list shown in Step 4:

```
Host Passwords
==============

Parameter 1 of 5

192.168.136.36 password []:
Enter the value again:
```

You are prompted for the password for each specified host. You are asked to re-enter each password for confirmation. After you provide all required passwords, you see the message:

```
All values are entered.  Do you wish to continue? (Y/N) [Y]:
```

Enter `Y` to continue.

The upgrade script displays messages as it prepares the Satellite hosts for upgrade.

8 The following menu displays:

```
Host/Component Layout
=====================

Installed Components

Satellite
OS Provisioning Boot Server
OS Provisioning Media Server

Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

Type `c` and press Enter to continue.

Phase 2: Supply Satellite Parameter Values

1 The following menu displays:

```
Interview Parameters
====================

Navigation keys:
Use <ctrl>p to go to the previous parameter.
Use <ctrl>n to go the next parameter.
Use <tab> to view help on the current parameter.
Use <ctrl>c to abort the interview.


All prompts have values.  What would you like to do:

1. Re-enter values
2. Continue

Enter the option number or one of the following directives
(<c>ontinue, <h>elp, <q>uit):
```

The SA upgrade script takes the default values for the Satellite parameters from the response file or CDF you specified. Be very careful changing these values but if you have a valid reason to do so, select 1. Each parameter and its assigned value is displayed and you can change the value if necessary.

Type `c` and press Enter to continue.

Phase 3: Upgrade the Satellite

1 At this point, the Prerequisite Check begins.

Before SA begins the upgrade, it performs a prerequisite check that validates that the host on which you are upgrading the Satellite meets the minimum requirements. The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on. If your host fails the prerequisite check, the upgrade can fail or core performance may be negatively effected. If your host fails the prerequisite check or displays warnings, correct the problem(s) or contact HP support services.

The prerequisite check may display messages similar to the following:

```
Prerequisite Checks
==============

Results for <IP_address>:

        WARNING Insufficient swap space (18 GBytes).
                24 Gbytes is the recommended for Oracle.

        WARNING File system '/' has 29447 MBytes available and 154050 is
                recommended.

Enter the option number or one of the following directives:
(<c>ontinue, <p>revious, <h>elp, <q>uit)
```

The Prerequisite check identifies WARNINGs and/or FAILUREs. FAILUREs can cause a failed or incomplete upgrade and must be resolved before continuing. WARNINGs allow you to continue the upgrade, however, Satellite performance may be negatively affected if you continue without resolving them.

If your server passes the prerequisite check, enter `c` and press Enter to begin the Satellite upgrade.

2 You see many messages displayed as the upgrade progresses. Unless the upgrade fails, these messages are purely informational. When the upgrade completes, the Core Description File (CDF) is automatically saved.

3 You must now upgrade your SA Agents. See Phase 4: Upgrade the SA Agents on page 80.

Phase 4: Upgrade the SA Agents

You should now upgrade the SA Agents installed on managed servers as described in the *SA User's Guide: Server Automation*, "SA Agent Management".

You are not required to upgrade the agents, but in order to take advantage of the latest functionality that may have been added in the new release, agents must be upgraded. If you continue using an older agent, certain new functionality may not be available on the server managed by that agent. See the *SA Release Notes* for Agent compatibility issues.

5 SA 10.2 Post-Upgrade Tasks

This section describes the tasks that may be required after upgrading to SA 10.2.

Upgrade SA Agents

If you have not already done so in Phase 4 of the upgrade procedure, you should now upgrade the SA Agents installed on managed servers as described in the *SA User Guide: Server Automation*, "SA Agent Management."

You are not required to upgrade the agents, but in order to take advantage of the latest functionality that may have been added in the new release, agents must be upgraded. If you continue using an older agent, certain new functionality may not be available on the server managed by that agent.

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 81 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 10.2, the system configuration values for the OS Build manager (`bm.reprovision_attributes_to_preserve`) are updated with new required SA 10.2 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`.

To modify this system configuration parameter, in the SA Client select the **Administration** tab, then select System Configuration in the navigation pane. In the list of SA components, select OS Build Manager. This displays the system configuration parameters for this component. Locate and modify the value of `bm.reprovision_attributes_to_preserve`. Select the Revert button to discard your changes or the Save button to save your changes.

Content Migration

You may need to perform tasks described in the *SA Content Utilities Guide*.

Not all upgrades will have required content migration tasks. Any required content migration tasks will be documented in this section, if any.

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 SA10.2, 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 10.x.

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 10.2.

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 a user with root privileges 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
```

Virtualization Integration and Upgrade

This section describes how to upgrade your virtualization inventory from HP SA 9.*x* to HP SA 10.*x*. This process is only needed if you are managing Virtualization Services (VSs) such as VMware vCenter Server, or hypervisors such as ESX, ESXi, or Hyper-V with any HP SA 9.*x* versions.

You must perform these upgrade tasks to manage your virtualization inventory on HP SA 10.*x*.

Summary of the Migration Process

1 Run the migration script with the `--list` option to get a summary of your virtualization environment. See Prepare to Migrate - Use the --list Option on page 85.

2 Examine the output of the --list option. See Examine the Output from the --list Option on page 86.

3 If you have any VSs on servers not managed by an SA agent, manually install the SA agent on those servers. For details, see Migrate Virtualization Services Not Managed by an Agent on page 87.

4 If you have any individual SA managed hypervisors, manually add those hypervisors to a VS, then add those VSs to SA. For details, see Migrate Individually Managed Hypervisors on page 87.

5 Run the migration script with the `--migrate` option. See Migrate with the --migrate Option on page 88.

6 Optionally run the migration script with the `--clean_all` option. See Clean Up with the --clean_all Option on page 88.

7 Examine and verify your virtualization environment in the SA Client.

Prepare to Migrate - Use the --list Option

After you upgrade your SA cores to SA 10.*x*, prepare for the migration by running the migrate script with the `--list` option. This displays the current VS configuration to help you determine what you need to do. For example:

```
/opt/opsware/bin/python2 v12n_migrate.py --list
```

For details on the migration script, see Migration Script Reference on page 88.

The `--list` option displays the following:

- All the VSs you have running.
- For each VS, whether or not it is running on an agent-managed server.
- All the hypervisors running under the VS.
- All your individually managed hypervisors: ESX, ESXi, and Hyper-V.

Examine the Output from the --list Option

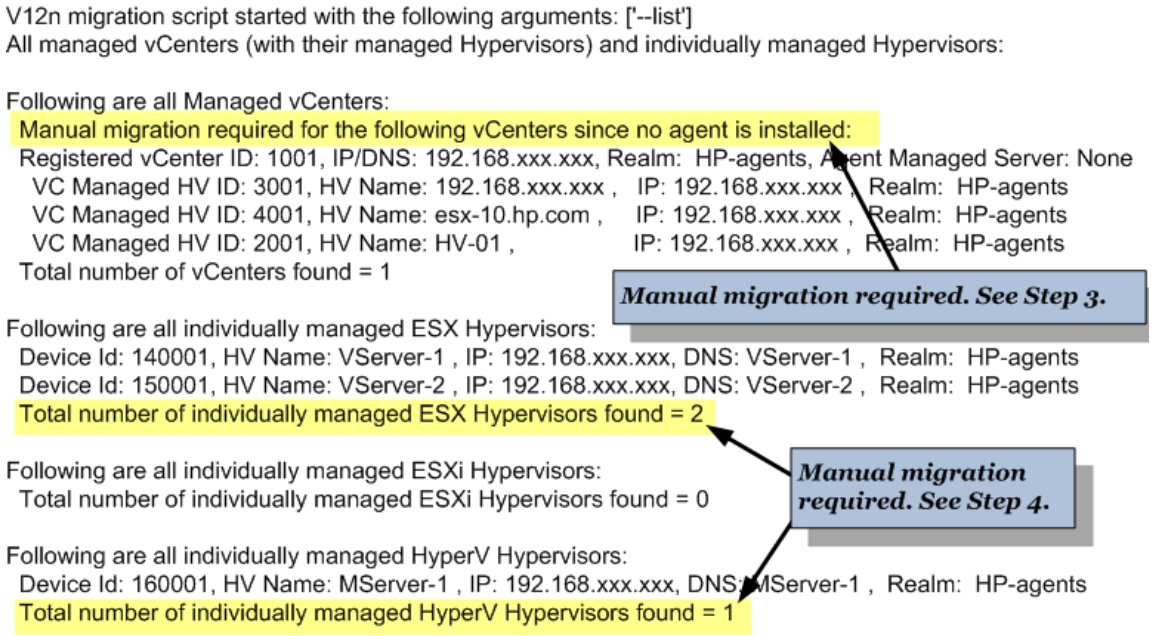
This section describes the output of the `--list` option and the steps to take based on that output. The `--list` option gives the following output:

- **All Managed vCenter Servers** lists the VSs being managed by SA and whether or not manual migration is required for them. If you have any VSs that require manual migration, migrate them as described in Migrate Virtualization Services Not Managed by an Agent on page 87.
- **Individually Managed Hypervisors** lists the hypervisors being managed by SA. If you have any individually managed hypervisors, you must migrate them as described in Migrate Individually Managed Hypervisors on page 87.

Sample Output 1 - Manual Migration Required

The following is sample output with yellow highlighting added to show one vCenter server that requires manual migration and three individually managed hypervisors that require manual migration:

figure 1 Sample Output of the Migration Script with the --list Option



Sample Output 2 - No Manual Migration Required

The following is sample output with yellow highlighting added to show one vCenter server that does not require manual migration because it is running on an agent-managed server, and no individually managed hypervisors:

figure 2 Sample Output of the Migration Script with the --list Option

```
V12n migration script started with the following arguments: ['--list']
All managed vCenters (with their managed Hypervisors) and individually managed Hypervisors:

Following are all Managed vCenters:
 Registered vCenter ID: 31001, IP/DNS: 192.168.xxx.xxx, Realm: HP-agents, Agent Managed Server: 30001
   VC Managed HV ID: 15001, HV Name: 192.168.xxx.xxx , IP: 192.168.xxx.xxx ,  Realm:  HP-agents
   VC Managed HV ID: 16001, HV Name: 192.168.xxx.xxx , IP: 192.168.xxx.xxx ,  Realm:  HP-agents
   VC Managed HV ID: 13001, HV Name: ESX-5.hp.com ,    IP: 192.168.xxx.xxx ,  Realm:  HP-agents
 Total number of vCenters found = 1

Following are all individually managed ESX Hypervisors:
 Total number of individually managed ESX Hypervisors found = 0

Following are all individually managed ESXi Hypervisors:
 Total number of individually managed ESXi Hypervisors found = 0

Following are all individually managed HyperV Hypervisors:
 Total number of individually managed HyperV Hypervisors found = 0
```

No manual migration required. See Step 5.

Migrate Virtualization Services Not Managed by an Agent

If you have Virtualization Services managed by SA but not agent-managed, you must install an SA agent on those servers. For instructions on installing the SA agent on servers, see “Installing the SA Agent” in the *SA User Guide: Server Automation*.

If you integrated using the hostname, SA may be unable to correlate the VS with the agent-managed device. If you integrated with the hostname, you must perform the Add VS step as a post-upgrade task. For further information about adding a VS, see Chapter 5, Virtualization Service Tasks, on page 37

If you have no VSs managed by SA or all your VSs are on agent-managed servers, skip this step.

Migrate Individually Managed Hypervisors

If you have hypervisors managed by SA, such as VMware ESX, ESXi or Microsoft Hyper-V, you must manage them under a Virtualization Service.

If you have no hypervisors individually managed by SA, skip this step.

1. For the ESX and ESXi servers, bring them under management of a VMware vCenter Server. For instructions, see the VMware documentation.
2. For the Hyper-V servers, bring them under management of a Microsoft System Center Virtual Machine Manager (SCVMM). For instructions, see the Microsoft documentation.
3. Use the SA Client to add the VSs to SA management. For instructions, see Add Virtualization Service on page 39.

Migrate with the --migrate Option

To migrate all your virtualization data, run the migration script with the `--migrate` option. For example:

```
/opt/opsware/bin/python2 v12n_migrate.py --migrate --user <SA username>
  --password <password>
```

For details on the migration script, see Migration Script Reference on page 88.

This migrates your existing virtualization inventory to the HP SA 10.1 format.

Clean Up with the --clean_all Option

After performing the migration, old data remains in the SA database. Leaving this data in the SA database will not cause any problems, however you can safely remove this data by using the `--clean_all` option.

Use the `--clean_all` option only after using the `--migrate` option. Once you use the `--clean_all` option, no further migration can be performed.

The following is an example command with the `--clean_all` option:

```
/opt/opsware/bin/python2 v12n_migrate.py --clean_all --user <SA username>
  --password <password>
```

This removes all the old virtualization data from the SA database.

For details on the migration script and the `--clean_all` option, see Migration Script Reference on page 88.

Migration Script Reference

This section describes the virtualization migration script and all its options.

Location of the Migration Script

The migration script is on your SA product distribution located at `/<distro>/opsware_installer/tools/v12n_migrate.py`.

The python interpreter is on your SA core server at `/opt/opsware/bin/python2`.

For more information, see the *SA Standard/Advanced Installation Guide*.

Where to Run the Migration Script

Run the migration script on the primary SA core server where the infrastructure component is running. For more information on SA cores and components, see the *SA Standard/Advanced Installation Guide*.

Set Up Your Environment

Before you run the migration script, you must set up your environment. Set the following environment variables on the SA core server where you will run the migration script:

```
export PYTHONPATH=/opt/opsware/spin:/opt/opsware/pylibs2
export LD_LIBRARY_PATH=/opt/opsware/lib/
```

Location of the Log Files

When you run the migration script, it writes log information to the following files:

- `/var/opt/opsware/log/v12n_migration.log` provides more information whenever you run the migration script.
- `/var/log/opsware/twist/v12n_migration_delete.log` provides more information whenever you run the migration script with any of the `--clean` options.

Syntax of the Migration Script

`/opt/opsware/bin/python2 v12n_migrate.py <options>`

Options

Use the following options with the migration script.

table 10 Migration Script Option

Option	Description
`--list` `-l`	List all the VMware vCenter Servers with their managed hypervisors and all the individually managed hypervisors.
`--migrate` `-m`	Migrate all agent-managed VMware vCenter Servers to SA 10.0. You must use the `--username` and `--password` options with this option.
`--username=<name>` `-u=<name>`	An SA user name. This option is required by the `--migrate` option and all of the `--clean` options.
`--password=<pw>` `-p=<pw>`	The password for the user name specified in the `--username` option.
`--clean_vms` `-cv`	Clean up all the old VMware vCenter Server data and related inventory data by permanently deleting the records from the SA database. Use this option only after using the `--migrate` option because the old data is permanently removed. Once you use this option, no further migration can be performed. This option requires the `--username` and `--password` options.

table 10 Migration Script Option

Option	Description
`--clean_hv` `-ch`	Clean up all the old individually managed ESX or ESXi hypervisor data by permanently deleting the records from the SA database. Use this option only after using the `--migrate` option because the old data is permanently removed. Once you use this option, no further migration can be performed. This option requires the `--username` and `--password` options.
`--clean_all` `-ca`	Clean up all the old virtualization data. This option is equivalent to `--clean_vms` and `--clean_hv` options. Use this option only after using the `--migrate` option because the old data is permanently removed. Once you use this option, no further migration can be performed. This option requires the `--username` and `--password` options.
`--help` `-h`	Display help for the migration script.