Server Automation

Software Version: 10.60

Upgrade Guide

Document Release Date: May 24, 2017
Software Release Date: May 24, 2017

Hewlett Packard Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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 Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

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

Support

Visit the HPE Software Support site at: https://softwaresupport.hpe.com.

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE 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 HPE 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 HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HPE Passport login page.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

HPE Software Solutions Now accesses the HPESW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hpe.com/.

Contents

Upgrade

This section describes the requirements and procedures for upgrading to SA 10.60.

Upgrade paths

You can upgrade to SA 10.60 from the following releases:

- SA 10.2x
- SA 10.5x

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

SA core configurations supported for customer upgrade

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

HPE supports customer-performed upgrades to SA 10.x 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 HPE Professional Services. If you are uncertain whether you can upgrade an existing SA Core yourself, contact HPE Technical Support.

These configurations include:

- SA Core with a local SA-supplied Oracle Database
- SA Core with a remote customer-supplied Oracle database
- SA Core with a remote model repository and SA-supplied Oracle database
- SA Core with a remote model repository and SA-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 SA-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

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).

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 Use or by using the `populate-opsware-update-library` script.

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 SA-supplied Oracle database. If you are using a non-SA-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

> 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 11g 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:

Enter the following commands in SQL*Plus:

```
# su - oracle

# sqlplus "/ as sysdba"

# 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 9:00:02	04/04/12 9:00:00	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	GCADMI	04/02/1	04/04/1	SCHEDULE	CHANGELOGPURGE.GC_

	N	2 09:00:02	2 09:00:00	D	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_STATS	OPSWARE _ADMIN	04/02/12 06:00:00	04/03/12 06:00:00	SCHEDULED	gather_opsware_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.

The schema collection jobs of SA (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:

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);
```

SA 10.60 upgrade prerequisites

This section describes the prerequisites for upgrading to SA 10.60.

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) 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 11) but all hosts in each distinct core must be running the same operating system.

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 to add a Secondary Core for a Multimaster Mesh (multiple core SA installation) or to perform an upgrade. The CDF files are saved, by default, in the `/var/opt/opsware/install_opsware/cdf` directory.

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 installation of the Core Components. If a response to a prompt cannot be validated at the time of installation, the installer runs a mini-interview during which you can provide a valid response.

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.

Copy files to the core

If, for security reasons, you have stored your response files in a location other than the default location on the host being upgraded, you should copy the files to the Infrastructure host in the

`/var/opt/opsware/install_opsware/resp` directory for the core to be upgraded.

In addition, copy your CDF file on the same host in the `/var/opt/opsware/install_opsware/cdf` directory.

SA upgrade media

SA is delivered as electronic files that need to be downloaded locally and reassembled as the first prerequisite step in the installation or upgrade. After reassembly, the SA electronic distribution contains several folders, the names of which end with:

- **oracle_sas (Server Automation Database)** - Media used to install the Oracle database
- **primary (Server Automation Product Software)** - Media used to install the SA Core Components
- **upload (Server Automation Agents and Utilities)** - Media used to upload and install SA Core content and tools
- **sat_base (Server Automation Satellite Base)** - Media used to install the SA Satellite components, it does not include the OS Provisioning components
- **sat_osprov (Server Automation Satellite Base including OS Provisioning)** - Media used to install the SA Satellite and the Satellite's OS Provisioning components

The SA Installer requires that the media directory structure be maintained, for example:

`<mountpoint>/<user_defined_prefix>-<media_name>/disk001/opsware_installer/hpsa*.sh`

where `<user_defined_prefix>-<media_name>` is, for example, hpsa-primary. (The hyphen before the media name "-" is mandatory).

The installation media can be made available on the host where the installer will be invoked, either by copying it on the local disk, or through a NFS network share. The installer will auto-mount the media on the other core hosts as needed.

SA upgrade script

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

- To upgrade a core, use:

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

- To upgrade a satellite without OS provisioning components, use:

  ```
  /<mountpoint>/hpsa-sat_base/disk001/opsware_installer/hpsa_upgrade_satellite.sh
  ```

- To upgrade a satellite, use:

  ```
  /<mountpoint>/hpsa-sat_osprov/disk001/opsware_installer/hpsa_upgrade_
  satellite.sh
  ```

Upgrade script command line syntax

The hpsa_upgrade.sh and hpsa_upgrade_satellite.sh scripts accept the arguments listed below:

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).
`--verbose`	Run the upgrade installer in verbose mode which causes more information to be displayed on the console.

SA Core upgrade by root and 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
- user who has permissions to invoke commands with su
- user who has permissions to invoke commands as root with sudo capabilities

When a core has multiple core servers, the installer will need to run commands on hosts other than the one where the installer runs. Therefore, the upgrade process will require user and password credentials for such hosts. The following users are supported when using the SA installer to upgrade SA on remote machines:

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

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

When performing the installation or upgrade of a core as a user other than root, make sure you invoke all the commands using sudo.

For example: `sudo /<media_path>/opsware_installer/hpsa_upgrade.sh`

Settings required for regular users with sudo capabilities

Make the following changes to the `/etc/sudoers` file on every machine where the user installs SA:

```
Defaults lecture=never

Bob ALL=(ALL) ALL

Defaults secure_path = /sbin:/bin:/usr/sbin:/usr/bin
```

> **Note:** For remote users, the home directory must exist on the remote host, otherwise the installer will not be able to validate the credentials.

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

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 the installation, you will be prompted to provide the value for `db.host`. This is the hostname of the Oracle database server 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.

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

SA preserves certain changes you make to SA component configuration files during subsequent upgrades.

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`)
- Software Repository (`word`)
- Command Center (`occ`)
- Deployment Automation (`da`)

- Component of the Global File System (`hub`)
- Command Engine (`way`)
- Model Repository Multimaster component (`vault`)
- Gateways (`opswgw`)

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

During upgrade, the installer may revert the configuration files to the default values. To preserve your customizations, you must save them in the custom configuration files of the components. You can find the list below:

- `/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

During the upgrade, the installer saves a copy of the previous versions of some configuration files in the following location:

`/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

Check prerequisites

In SA, 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 an SA Core Component, you must install the package before performing the upgrade.

For more information about required packages, see the SA Install Guide.

Naming of the SA internal directory

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

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

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

Change the 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.

- "Required Oracle versions" below
- "Required packages for Oracle12c" on the next page
- "Preparing the Oracle environment" on the next page
- "Oracle RAC" on page 21

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 the Oracle database is configured.

Upgrading SA does not affect your existing Oracle installation. Fresh SA 10.60 installations will install Oracle 12c (12.1.0.2) if you choose to install the SA-supplied Oracle database for the Model Repository.

Required packages for Oracle12c

As of SA 10.1, Oracle 12c is shipped as the SA-supplied database. If your SA core is using an Oracle 11g database, you are not required to upgrade it. 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 the SA for a list of these new required packages and instructions on setting up and configuring Oracle 12c.

Preparing the Oracle environment

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

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
```

> 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

As of SA 10.0, the Oracle Export/Import utility is replaced by Oracle's Data Pump Export (`expdp`) 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 10.60, your DBA must grant the following permissions to the user `opsware_admin`.

- `grant create any directory to opsware_admin;`
- `grant drop any directory to opsware_admin;`

Script to fix Oracle parameters

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

`/<distro>/opsware_installer/tools`

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

`/<mountpoint>/hpsa-primary/disk001`

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>
```

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:

1. Make sure that none of the clients are connected to the Oracle RACed database.
2. 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:

1. Make sure that none of the clients are connected to the Oracle RACed database.
2. 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 Oracle RAC support section.

Prepare for SA upgrade

This section provides information on the following topics:

Important: Since SA 10.60 is enabled with HPE AutoPass licensing, ensure that you have enough licenses available for the number of SA Agent managed servers in your business environment. For more information, see **AutoPass licesing** section in the Adminstration Guide.

Preparation for all upgrades to SA 10.60

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

- Recertify the Cores if their certificates have MD5 hashing algorithms.

  Important: You cannot upgrade to version 10.60 if the SA Core's existing certificate is MD5 base.

- Gather the correct values for the parameters shown in "Core parameter values required for upgrade" on page 25.
- 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 10.60, SA users will not see their Remediate Patch Policy jobs in the Job Logs (SA Client) that ran or are scheduled to run. (By default, the data about a job is cleared from the Job Logs (SA Client) after 30 days.)
- Detach the "Python Opsware API Access" Software Policy from the Managed Servers corresponding to the Core hosts and then remediate to uninstall the policy items contained within.

This Software Policy contains the OPSWpytwist ZIP package that should not be installed on Core hosts because the Core hosts already has the contents of this package already installed as an RPM package.

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

Prepare for all multimaster upgrades to SA 10.60

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 10.60, ensure that there are no conflicts in the mesh. To determine any transaction conflicts, follow the procedures described in the SA Administering guide, under the View the state of the Multimaster Mesh section. If there are conflicts, check the Resolve mesh conflicts section.

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

If you need to perform Windows patching, you 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 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.

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.
`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.
`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.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`

Required upgrade parameter values, continued

Parameter	How to find the current value
	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.

`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`

`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.
	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 servicename is `devtruthac03`.

`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

Required upgrade parameter values, continued

Parameter	How to find the current value

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

`truth.twistPwd`	The password for the Oracle `twist` user. To verify that you have the correct value, log in to the Model Repository (truth) as `twist` using this password.
`truth.vaultPwd`	The password for the Oracle `vault` user. To verify that you have the correct value, log in to the Model Repository (truth) as `vault` using this password. This parameter is only relevant to Multimaster Cores.
`twist.integration.passwd`	On the server where the SA 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).
`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, check the value in the file: `/opt/OPSWsamba/etc/smb.conf`
`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.

Required upgrade parameter values, continued

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
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.
db.port	Port on which the database host is being monitored and accepts connections.
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).
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

Required upgrade parameter values, continued

Parameter	How to find the current value
	`# 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 24.
`cgw_admin_port`	On the server hosting the Core Gateway, check the files: `/etc/opt/opsware/opswgw-cgws-<truth.dcNm>/opswgw.properties`
`cgw_address`	On the server hosting the Core Gateway, check the files: `/etc/opt/opsware/opswgw-cgws-<truth.dcNm>/opswgw.properties`
`cgw_proxy_port`	On the server hosting the Core Gateway, check the files: `/etc/opt/opsware/opswgw-cgws-<truth.dcNm>/opswgw.properties`
`agw_proxy_port`	On the server hosting the Core Gateway, check the files: `/etc/opt/opsware/opswgw-agws-<truth.dcNm>/opswgw.properties`
`cgw_slice_tunnel_listener_port`	On the server hosting the Core Gateway, check the files: `/etc/opt/opsware/opswgw-cgws-<truth.dcNm>/opswgw.properties` **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:

Required upgrade parameter values, continued

Parameter	How to find the current value
	`/etc/opt/opsware/opswgw-mgws-<truth.dcNm>/opswgw.properties`
`masterCore.mgw_tunnel_listener_port`	On the server hosting the Management Gateway, check the files: `/etc/opt/opsware/opswgw-mgws-<truth.dcNm>/opswgw.properties`
`word_root`	Does not change from installation.

SA 10.60 upgrade

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 10.60 from 10.2x, 10.5x (includes patch releases and the minor releases).

> - The Oracle database is not upgraded during an SA Core upgrade.
> - 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.), HPE strongly recommends that you contact HPE Professional Services (PSO) for assistance and consider a PSO-supported rolling upgrade procedure which does provide some rollback capabilities.
> - During SA upgrade, the APX HTTP server is updated with the one provided by SA and any customizations made to the APX HTTP server will be lost. If you want to use a different version of APX HTTP, refer "Rebuilding the Apache HTTP server and PHP" in the Develop section.

Supported upgrade paths

You can upgrade to SA 10.60 from the following releases:

- SA 10.2x
- SA 10.5x

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

TLS hardening during upgrade

The upgrade process allows you to select the minimal version of the TLS protocol that will be used by the core components:

- TLSv1 (compatible with previous versions - default)
- TLSv1.1

- TLSv1.2

> **Important:** In a multimaster mesh, you must set all your cores and satellites to the same TLS level.

In case you choose to use the default option, you can harden your cores at a later time. For more information on how to do this, see the SA Administration Guide.

When upgrading a mesh that contains unhardened satellites, choosing to harden the cores during upgrade results in loss of some functionality on the satellites, until the satellites are also upgraded. Therefore in such a case, it is recommended to either:

- Upgrade the satellites immediately after the cores are upgraded
- Choose the default TLS level for the upgrade and harden once all the cores and satellites are upgraded to the new version.

Certification mode change to third-party

To switch SA to **third-party** certificate mode, first upgrade the SA Cores and Agents to 10.60, then run a Core recertification job. You cannot change the certification mode during the upgrade.
See the **Certificate management** section in the Administration guide for details about SA certification modes.

Before the upgrade

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

> **Important:** Read the TLS hardening during upgrade section in "SA 10.60 upgrade " on the previous page before you start the upgrade.

Uninstalling All CORD patches

Before performing the upgrade, CORD patches (for example, 10.21 patch) must be uninstalled from all servers being upgraded.

For a Single Core host (no distributed core components), the SA Installer can automatically remove any CORD patches you have installed. However for a core with distributed components or a Multimaster Mesh with CORD patches installed, you must manually uninstall the patch from all core servers.

In a Multimaster Mesh, the patch must be uninstalled from all cores, before starting the upgrade. Rollback the patch on the secondary cores first, then the primary core, to make sure that the primary core is at a higher version than the secondary cores.

> **Note:** Satellites can be upgraded at a later time, after the cores have been already upgraded to the new version. If the cores were TLS hardened, you must use the upgrade media to rollback the patch on the satellites. After the rollback, the services are not restarted automatically and should not be started manually either (because connections to the cores are not possible due to TLS restrictions). At this point, you may start the upgrade on the satellite.

Checking whether CORD patches are applied

You can check whether patches are applied on your core servers using the following methods:

- On any core server, by checking the **install.inv** file
- On cores with distributed components, by running a Health Check Monitor test

Method 1: Check the install.inv file

On each core server, run the following command:

```
grep -A 2 opsware_patch /var/opt/opsware/install_opsware/inv/install.inv
```

If the command gives no output, then there are no CORD patches installed on the server.

For example, on a Single Host core that has a patch installed, the output would look similar to the one below:

```
%opsware_patch
build_id: opsware_60.0.70014.0
state:  complete
--
%opsware_patch_sql
build_id: opsware_60.0.70014.0
state:  complete
```

Method 2: Run a Health Check Monitor test

For cores with distributed components, you can run the SA Core Health Check Monitor (HCM) to verify that there are no CORD patches applied. To verify that all systems have had the patch removed, run the following command:

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

Usage:

```
# /opt/opsware/oi_util/bin/run_all_probes.sh run check_opsware_version hosts="
[<user*>@]<system>[:<password>] [[<user@>]<system>[:<password>]]..."
[keyfile=<keyfiletype>:<keyfile>[:<passphrase>]]
```

Where:

Health Check Monitor Arguments

Argument	Description
`<system>`	Name/IP of a reachable SA Core server.
`<user*>`	Optional user to access the remote system. The user needs to have sudo permission. Default is "root". **Note:** This option is available only since 10.22.
`<password>`	Optional password on the specified `<system>`.
`<keyfiletype>`	SSH keyfile type (`rsa_key_file` or `dsa_key_file`).
`<keyfile>`	Full path to the SSH keyfile. Specifies the file containing the current server's SSH private key. Passwordless login with keyfile is supported only for the root user.
`<passphrase>`	Optional pass-phrase for `<keyfile>`.

You must 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="192.168.172.5:s3cr3t \ 192.168.172.6: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
```

```
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...

*** 192.168.172.5: opsware_60.0.70014.0

*** 192.168.172.6: opsware_60.0.70014.0

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 section.

Removing CORD patches

If there are patches installed on your core(s), you can follow the procedure below to rollback the patches.

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.
```

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 at the same time as the uninstallation of core server CORD patches.

> **Important:** The patches must be removed in the following order:
>
> 1. Remove any applied CORD patches from the Secondary Core(s) (one core at a time)
> 2. Remove any applied CORD patches from the First (Primary) Core

The CORD patch may be removed by using the CORD patch media or the SA 10.60 media.

- Removing patches using the patch installation media.

  If the CORD installation media is available, it is recommended to rollback the patch using it. For more details, see the Release Notes for the installed patch version.

- Removing patches using the SA 10.60 installation media – **uninstall_patch.sh**

  The following procedure must be applied on **each of the core servers**, starting with the secondary cores and after the rollback completes successfully, continuing with the primary core.

  On a core:

  a. On each server hosting SA components:

     - From the SA 10.60 media, run the uninstall patch script:

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

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

       ```
       /<mountpoint>/hpsa-primary/disk001
       ```

     - 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 the progress of the uninstallation and a success message upon completion. If the CORD patch uninstall is not successful, contact your HPE Support Representative.

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

b. After the **uninstall_patch** script has completed successfully, on the Model Repository node run the following:

```
<distro>/opsware_installer/uninstall_patch_db.sh -r /var/opt/opsware/install_
opsware/resp/resp.<Timestamp> --force_run
```

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

```
/<mountpoint>/hpsa-primary/disk001
```

The response file specified with the `-r` option is created on each core server at install time.

> **Note:** If the core has a remote database, no commands need to be run on them.

- Removing patches using the SA 10.60 installation media – the Management Console

  To rollback patches on a core you can also use the Management Console tool. You need to invoke it **once for each core**, starting with the secondary cores and, after the process completes successfully, on the primary core. The tool will rollback both the component patch (opsware_patch) and the database patch (opsware_patch_db).

  To run this tool, you will need the CDF file of the core. See the "Core Definitions Files" section in the SA Install Guide for details.

  From the installation media, invoke the following command:

```
<distro>/opsware_installer/hpsa_mgmt_console.sh -c <path_to_CDF_file>
```

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

```
/<mountpoint>/hpsa-primary/disk001
```

  Select the **Remove patch** option in the utility menu and follow the instructions.

  For more details, see the "SA Management Console" section in the SA Install Guide.

Removing CORD patches from a satellite

> **Note:** To prevent failures during the component startup (due to incompatible communication protocols between satellites and cores), after the rollback, the services are not restarted automatically and should not be started manually. The upgrade can be started while the components are stopped.

The following procedure must be applied on **each of the satellite servers**, which are running SA components.

- From the SA 10.60 media, run the uninstall patch script:

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

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

  ```
  /<mountpoint>/hpsa-sat_base/disk001 (if the OS Provisioning components are not installed)
  ```

  ```
  /<mountpoint>/hpsa-sat_osprov/disk001
  ```

- 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 HPE Support Representative.

Upgrade a single-host core

If you are upgrading a Multimaster Mesh, use the instructions shown in "Upgrade a multimaster mesh" on page 48.

Ensure that all CORD patches have been uninstalled, see "Uninstalling All CORD patches" on page 32.

To exemplify the steps listed below, a core with the following layout is used:

Server	Core Components installed
192.168.100.1	• SA-installed Oracle database and Model Repository • Core Infrastructure Components • Slice • OS Provisioning Components

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

   ```
   /<distro>/opsware_installer/hpsa_upgrade.sh -c <CDF_full_path>
   ```

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

   ```
   /<mountpoint>/hpsa-primary/disk001
   ```

If for security reasons, you have stored your response files in a location other than the default location on the host being upgraded, you can copy the files to the `/var/opt/opsware/install_opsware/resp` directory on the core to be upgraded. You must also provide the CDF file with the –c option (by default, it is saved in the `/var/opt/opsware/install_opsware/cdf` directory).

2. The SA upgrade script determines the component layout of your core. The **Specify Hosts to Upgrade** screen displays:

```
Specify Hosts to Upgrade

========================

Currently specified hosts:

192.168.100.1

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 same host, enter `c` and Enter to continue.

3. The prompt to select the cryptographic protocol is displayed.

```
Cryptographic Protocol Selection for the Server Automation Components

[WARNING] Please make sure that all the cores and satellites from the mesh are
at the same TLS level.

=============================================================================

1. TLSv1

2. TLSv1.1

3. TLSv1.2

Enter the option number or one of the following directives

(<p>revious, <h>elp, <q>uit)[1]:
```

See the "SA 10.60 upgrade " on page 31section for details.

4. A parameter confirmation interview is displayed:

```
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.

Parameter 1 of 5 (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]:

Parameter 2 of 5 (truth.servicename)

Please enter the service name of the Model Repository instance in the facility
where Opsware Installer is being run [truth.Core1]:

Parameter 3 of 5 (db.sid)

Please enter the SID of the Oracle instance containing the Model Repository
[truth]:

Parameter 4 of 5 (db.port)

Please enter the port on which the database is listening. [1521]:

Parameter 5 of 5 (db.orahome)

Please enter the path of the ORACLE_HOME directory of your Model Repository
(truth) server. [/u01/app/oracle/product/12.1.0.2/db_2]:

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

5. The Host Component Layout screen displays again.

```
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
```

Press `c` to continue.

6. 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.

> **Note:** For a Core upgrade with underlying database as Oracle 11g, if the upgrade fails after performing the Model Repository upgrade, the pre-check will prompt the following errors when you restart the upgrade process:
>
> ```
> FAILURE Oracle optimizer_index_caching = 0 ; required to be = 80
> FAILURE Oracle optimizer_index_cost_adj = 100 ; required to be = 20
> ```
>
> These errors are the result of changes that were performed when you upgrade the Model Repository successfully. You can ignore this error and continue the upgrade process.

7. 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.
8. You should now upgrade the SA Agents installed on managed servers. See "Post-upgrade task" on page 63 for details.

Upgrade a single core with distributed components

If you are upgrading a Multimaster Mesh, use the instructions shown in "Upgrade a multimaster mesh" on page 48.

Ensure that all CORD patches have been uninstalled, see "Uninstalling All CORD patches" on page 32.

To exemplify the steps listed below, a core with the following custom layout is used:

Server	Core Components installed
192.168.100.111	• Oracle database (provided by SA) and Model Repository • Core Infrastructure Components
192.168.100.112	Software Repository Storage
192.168.100.113	Slice
192.168.100.114	OS Provisioning Media Server
192.168.100.115	OS Provisioning Boot Server

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 –c <full_path_to_CDF>
   ```

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

   ```
   /<mountpoint>/hpsa-primary/disk001
   ```

2. If, for security reasons, you have stored your response files in a location other than the default location on the host being upgraded, copy the files to the Infrastructure host in the `/var/opt/opsware/install_opsware/resp` directory for the core to be upgraded. In addition, copy your CDF file on the same host in the `/var/opt/opsware/install_opsware/cdf` directory.
3. The Specify Hosts to Upgrade screen displays. It will look similar to the following:

   ```
   Specify Hosts to Upgrade

   ========================

   Currently specified hosts:
   ```

```
192.168.100.111 (oracle_sas, gateway_master, truth_mm_overlay)

192.168.100.112 (word_store, word_uploads)

192.168.100.113 (slice)

192.168.100.114 (osprov_media)

192.168.100.115 (osprov_boot_slice)

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):
```

In case you have a remote database, the database host is NOT explicitly listed in this step, but only those servers that have SA components installed.

> **Note:** If you do not provide the CDF, all Core servers that are part of the Core being upgraded must be added in this step as shown below.
>
> Enter **1**, to Add/Edit hosts in the Currently Specified Hosts list.
>
> You are prompted to specify the number of server addresses you want to add. Enter the number and press **Enter**.
>
> 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.

4. 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. For each host, the interview will look like:

   ```
   Host Passwords
   ==============
   Parameter 1 of 2
   192.168.100.112 user [user1]:
   Validating user ....
   Parameter 2 of 2
   192.168.100.112 password []: **********
   Validating password ....
   ```

   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.

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

   ```
   Host/Component Layout
   =====================
   Installed Components
   Oracle RDBMS for SA : 192.168.100.111
   Model Repository, First Core : 192.168.100.111
   Multimaster Infrastructure Component : 192.168.100.111
   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) : 192.168.100.112
   Enter one of the following directives
   (<c>ontinue, <p>revious, <h>elp, <q>uit):
   ```

> **Note:** In case you have a remote database, the database host is NOT explicitly listed in this step (that is, the Oracle RDBMS for SAS component), but only those servers that have SA components installed.
>
> **Note:** If you are upgrading a secondary core, the Model Repository component will appear as: "Model Repository, Additional Core" in this screen.

6. The prompt to select the cryptographic protocol is displayed.

```
Cryptographic Protocol Selection for the Server Automation Components

[WARNING] Please make sure that all the cores and satellites from the mesh are
at the same TLS level.

================================================================================

1. TLSv1

2. TLSv1.1

3. TLSv1.2

Enter the option number or one of the following directives

(<p>revious, <h>elp, <q>uit)[1]:
```

   See the SA Upgrade guide for details.

7. The parameter confirmation interview is displayed:

```
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.


Parameter 1 of 5 (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]:


Parameter 2 of 5 (truth.servicename)
```

```
Please enter the service name of the Model Repository instance in the facility
where Opsware Installer is being run [truth.Core1]:


Parameter 3 of 5 (db.sid)

Please enter the SID of the Oracle instance containing the Model Repository
[truth]:


Parameter 4 of 5 (db.port)

Please enter the port on which the database is listening. [1521]:


Parameter 5 of 5 (db.orahome)

Please enter the path of the ORACLE_HOME directory of your Model Repository
(truth) server. [/u01/app/oracle/product/12.1.0/db_1]:

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

End of interview.
```

The Host Component Layout screen displays again.

```
Upgrade components

==================

Components to be Upgraded

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

Model Repository, First Core                          : 192.168.100.111

Multimaster Infrastructure Components                 : 192.168.100.111

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): 192.168.100.112

Up-to-date Components (will not upgrade)

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

Oracle RDBMS for SAS: 192.168.100.111

Enter one of the following directives
```

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

Press `c` to continue.

> **Note:** In case you have a remote database, the database host is NOT explicitly listed in this step (that is, the Oracle RDBMS for SAS component.
>
> **Note:** If you are upgrading a secondary core, the Model Repository component will appear as "Model Repository, Additional Core" in this screen.

8. 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.

> **Note:** For a Core upgrade with underlying database as Oracle 11g, if the upgrade fails after performing the Model Repository upgrade, the pre-check will prompt the following errors when you restart the upgrade process:
>
> ```
> FAILURE Oracle optimizer_index_caching = 0 ; required to be = 80
>
> FAILURE Oracle optimizer_index_cost_adj = 100 ; required to be = 20
> ```
>
> These errors are the result of changes that were performed when you upgrade the Model Repository successfully. You can ignore this error and continue the upgrade process.

9. You should now upgrade the SA Agents installed on managed servers. See "Post-upgrade task" on page 63 for details.

Upgrade a multimaster mesh

When upgrading a multimaster mesh, the following steps must be performed:

1. Make sure that all CORD patches are uninstalled
2. Check the transaction status
3. Shutdown services on the Secondary cores
4. Upgrade the Primary Core
5. Upgrade the Secondary Cores

Check transaction status

Before starting to upgrade a multimaster mesh, make sure that there are no transactions that are not sent or received and that there are no conflicts.To determine any transaction conflicts, follow the procedures described in the SA Administering guide, under the View the state of the Multimaster Mesh section. If there are conflicts, check the Resolve mesh conflicts section.

Shut down the services on the secondary cores

Before starting the upgrade procedure of your cores, you must stop the services on all the secondary cores in the mesh, so as to avoid new running jobs to create conflicts.

Method 1: Shut down using the opsware-sas service

Run the following commands for each secondary core that is part of the mesh:

1. Shut down all Secondary Core services 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 by issuing the following

command:

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

Method 2: Shut down using the Management Console

You can also use the Management Console to stop the services. You need to invoke the following command once on each of the Secondary cores that is part of the mesh. On the Infrastructure host of each core, invoke the Management Console using the installation media:

```
<distro>/opsware_installer/hpsa_mgmt_console.sh –c <path_to_CDF_file>
```

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

```
/<mountpoint>/hpsa-primary/disk001
```

Select the **Shutdown service** option in the utility menu and follow the instructions.

For more details, see the **SA Management console** section in the Install Guide.

Upgrade the Primary Core of a multimaster mesh

Once the steps described above have been performed, you may start to upgrade the Primary Core of the mesh.

The services must be running on the Primary core, but must be stopped on the Secondary cores, as described in the previous step.

The upgrade process is the same as listed in "Upgrade a single-host core" on page 38 or "Upgrade a single core with distributed components" on page 42 sections described above, depending on the core layout. Refer to the corresponding section for the complete procedure.

Upgrade the Secondary Core of a multimaster mesh

Important:

- Start the upgrade process on the secondary cores only after the Primary core upgrade is successfully complete.
- Make sure to copy the cryptographic material from the upgraded Primary Core to the Secondary Cores. Paste the cryptographic material in the same directory:

> `/var/opt/opsware/crypto/cadb/realm/`.
> Otherwise, the Core upgrade fails.

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.

The upgrade process is the same as listed in "Upgrade a single-host core" on page 38 or "Upgrade a single core with distributed components" on page 42 sections described above, depending on the core layout. Refer to the corresponding section for the complete procedure.

Satellite upgrade procedures

Satellites can be upgraded at a later time, after the core upgrades are complete.

> **Important:** See the **TLS hardening during upgrade** section in the **Upgrade** guide before starting the upgrade procedure.

The following sections cover:

- "Single-host Satellite upgrade (OS Provisioning not installed)" below
- "Single-host Satellite with OS Provisioning components" on page 54
- "Satellite with OS Provisioning Components on a separate host upgrade" on page 57

Single-host Satellite upgrade (OS Provisioning not installed)

This procedure upgrades a Satellite installed with all Satellite components on the same host, and without the OS Provisioning components installed.|

> Make sure to copy the cryptographic material from the upgraded Primary Core to the Satellite host. Paste the cryptographic material in the same directory: `/var/opt/opsware/crypto/cadb/realm/`. Otherwise, the Satellite upgrade fails.

Phase 1: Invoking 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 "Uninstalling All CORD patches" on page 32.

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

   ```
   /<distro>/opsware_installer/hpsa_upgrade_satellite.sh -c <full_path_CDF_file>
   ```

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

   ```
   /<mountpoint>/hpsa-sat_base/disk001
   ```

   If for security reasons, you have stored your response files in a location other than the default location on the host being upgraded, you can copy the files to the `/var/opt/opsware/install_opsware/resp` directory on the core to be upgraded. You should also provide the CDF file with the `-c` option. By default, this is saved in the `/var/opt/opsware/install_opsware/cdf` directory.

3. The following menu displays:

   ```
   Specify Host(s) for Satellite Upgrade

   ====================================

   Currently specified hosts:

   <IP_address> (wordcache)

   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
   ```

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

Phase 2: Supplying satellite parameter values

4. The prompt to select the cryptographic protocol is displayed.

   ```
   Cryptographic Protocol Selection for the Server Automation Components

   [WARNING] Please make sure that all the cores and satellites from the mesh are
   at the same TLS level.

   ================================================================================

   1. TLSv1
   ```

```
2. TLSv1.1
3. TLSv1.2
Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit)[1]:
```

For details, see the SA 10.60 upgrade section in the **Upgrade** guide .

5. 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.

6. 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. Change these values only if you have a valid reason to do so. For example, if the values have been changed after the install, but not updated in the files, 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: Upgrading 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 ensures 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 HPE Support.

   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 installed on managed servers. See "Post-upgrade task" on page 63 for details.

Single-host Satellite with OS Provisioning components

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

> Make sure to copy the cryptographic material from the upgraded Primary Core to the Satellite host. Paste the cryptographic material in the same directory: `/var/opt/opsware/crypto/cadb/realm/`. Otherwise, the Satellite upgrade fails.

Phase 1: Invoking 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 CDF file used to install the Satellite.

   ```
   /<distro>/opsware_installer/hpsa_upgrade_satellite.sh -c <full_path_CDF_file>
   ```

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

   ```
   /<mountpoint>/hpsa-sat_osprov/disk001
   ```

   If for security reasons, you have stored your response files in a location other than the default location on the host being upgraded, you can copy the files to the `/var/opt/opsware/install_opsware/resp` directory on the core to be upgraded. You should also provide the CDF file with the `-c` option. By default, this is saved in the `/var/opt/opsware/install_opsware/cdf` directory.

2. The following menu displays:

   ```
   Specify Host(s) for Satellite Upgrade

   ====================================

   Currently specified hosts:

    <IP_address> (wordcache, osprov_media_sat, osprov_boot_sat)

   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
```

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

Phase 2: Supplying satellite parameter values

3. The prompt to select the cryptographic protocol is displayed.

```
Cryptographic Protocol Selection for the Server Automation Components

[WARNING] Please make sure that all the cores and satellites from the mesh are
at the same TLS level.

================================================================================

1. TLSv1

2. TLSv1.1

3. TLSv1.2

Enter the option number or one of the following directives

(<p>revious, <h>elp, <q>uit)[1]:
```

For details, see the **TLS hardening during update** section in the **Upgrade** guide .

4. 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.

5. 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. Change these values only if you have a valid reason to do so. For example, if the values have been changed after the install, but not updated in the files, 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: Upgrading the satellite

6. 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 ensures 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 HPE Support.

   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.

7. 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.
8. You should now upgrade your SA Agents installed on managed servers. See "Post-upgrade task" on page 63 for details.

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.

> Make sure to copy the cryptographic material from the upgraded Primary Core to the Satellite host. Paste the cryptographic material in the same directory: `/var/opt/opsware/crypto/cadb/realm/`. Otherwise, the Satellite upgrade fails.

Phase 1: Invoking 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 CDF file used to install the Satellite.

   ```
   /<distro>/opsware_installer/hpsa_upgrade_satellite.sh -c <full_path_CDF_file>
   ```

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

   ```
   /<mountpoint>/hpsa-sat_osprov/disk001
   ```

   If for security reasons, you have stored your response files in a location other than the default location on the host being upgraded, you can copy the files to the `/var/opt/opsware/install_`

`opsware/resp` directory on the core to be upgraded. You will should also provide the CDF file with the –c option (by default, it is saved to the `/var/opt/opsware/install_opsware/cdf` directory).

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
```

> **Note:** If you do not provide a CDF, you will need to manually add the satellite servers. Since the OS Provisioning components are installed on a separate server from the Satellite components, you must specify the IP address for all the servers that hosts the satellite components.
>
> a. 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
>
> b. 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.

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):
```

3. You are asked to provide the OS credentials for each host:

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

Parameter 1 of 2

192.168.136.36 user [user1]:

Validating user ....

Parameter 2 of 2

192.168.136.36 password []: **********

Validating password ....
```

You are prompted for the credentials 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.

Phase 2: Supplying satellite parameter values

4. The prompt to select the cryptographic protocol is displayed.

```
Cryptographic Protocol Selection for the Server Automation Components

[WARNING] Please make sure that all the cores and satellites from the mesh are
at the same TLS level.

================================================================================

1. TLSv1

2. TLSv1.1

3. TLSv1.2

Enter the option number or one of the following directives

(<p>revious, <h>elp, <q>uit)[1]:
```

For details, see the **TLS hardening during update** section in the **Upgrade** guide .

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.

5. 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. Change these values only if you have a valid reason to do so. For example, if the values have been changed after the install, but not updated in the files, 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: Upgrading the satellite

6. 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 ensures 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 HPE Support.

   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.

7. 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.
8. You should now upgrade your SA Agents installed on managed servers. See "Post-upgrade task" on the next page for details.

Post-upgrade task

This section describes the tasks that may be required after upgrading to SA 10.60.

Upgrade SA Agents

You should now upgrade the SA Agents installed on managed servers as described in the **Agent Upgrade** section of User Guide

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.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Upgrade Guide (Server Automation 10.60)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to hpe_sa_docs@hpe.com.

We appreciate your feedback!