HP Server Automation

Ultimate Edition

Software Version: 10.20

Installation Guide

Support

Visit the HP Software Support Online website at:

https://softwaresupport.hp.com/

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

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

- Search for knowledge documents of interest

- Submit and track support cases and enhancement requests

- Download software patches

- Manage support contracts

- Look up HP support contacts

- Review information about available services

- Enter into discussions with other software customers

- Research and register for software training

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

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

To find more information about access levels, go to:

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

Support Matrices

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

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

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

https://softwaresupport.hp.com/

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

Documentation Updates

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

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

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

How to Find Information Resources

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

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

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

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

To access individual documents:

1 Go to the SA 10.x Documentation Library:

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

2 Log in using your HP Passport credentials.

3 Locate the document title and version that you want, and then click **go**.

1   To download the complete documentation set to a local directory:

   a   Go to the SA Documentation Library:

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

   b   Log in using your HP Passport credentials.

   c   Locate the All Manuals Download title for the SA 10.1 version.

   d   Click the **go** link to download the ZIP file to a local directory.

   e   Unzip the file.

2   To locate a document in the local directory, use the Documentation Catalog (docCatalog.html), which
     provides an indexed portal to the downloaded documents in your local directory.

3   To search for a keyword across all documents in the documentation set:

   a   Open any PDF document in the local directory.

   b   Select **Edit > Advanced Search** (or Shift+Ctrl_F).

   c   Select the All PDF Documents option and browse for the local directory.

   d   Enter your keyword and click Search.

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

Go to the HP Software Documentation Search Portal:

   https://softwaresupport.hp.com/

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

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

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

Product Editions

There are two editions of Server Automation:

• Server Automation (SA) is the Ultimate Edition of Server Automation. For information about Server
  Automation, see the SA Release Notes and the SA User Guide: Server Automation.

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

Document Change Notes

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

Date	Changes
December 2014	Original version of this document for release with SA 10.20.
May 2015	Modified instructions to account for the ability to install as non-root user who has root privileges. Previously, only root user could perform the installation.

Contents

1 SA Installation Overview

This guide provides the requirements and procedures for standard and advanced installations of:

- **Single-Host SA Cores and Multi-Host SA Cores**

  For small facilities, a single-host SA Core has all its core components installed on a single server. An SA Core can also be installed with its core components distributed between multiple host servers for scalability.

- **SA Primary Core with Secondary SA Cores (Multimaster Mesh)**

  For larger facilities, an SA Core, single- or multi-hosted, can act as the Primary Core of a Multimaster Mesh when you install Secondary SA Cores. The Primary and Secondary Cores manage the servers in their respective facilities as well as enable centralized administration of all facilities in the Mesh.

- **SA Satellites**

  A Satellite installation is typically installed for remote sites that do not have a large enough number of potential SA Managed Servers to justify a full SA Core installation. A Satellite installation allows you to install only the minimum necessary Core Components on the Satellite host which then accesses the Primary Core's database and other services through an SA Gateway connection.

- **Multi-Core Configurations (Advanced - requires HP Professional Services)**

  For very large facilities, SA Cores can be configured to communicate with each other across facilities adding scalability and failover capabilities. Such configurations are supported only for HP Professional Services or certified consultant installation. Customer installation is not supported.

This guide also describes all necessary SA Core installation prerequisites and provides useful pre- and post-installation information, tasks and options.

Chapter 2, "SA Core Configurations Supported For Customer Installation" describes the SA Core configurations supported by HP for customer installation. More advanced and complex installation require the services of HP Professional Services or HP-certified consultants.

SA Architecture and Tools

If you are unfamiliar with the data center tasks that SA automates and/or have a need to understand the underlying architecture of an SA Core and its components, see the
SA Overview and Architecture Guide.

2 SA Core Configurations Supported For Customer Installation

This section describes the SA Core configurations that are supported for customer installation. These configurations include:

- 1. SA Core with a Local HP-supplied Oracle Database
- 2. SA Core with a Remote Customer-supplied Oracle Database
- 3. SA Core with a Remote Model Repository and HP-supplied Oracle Database
- 4. SA Core with a Remote Model Repository and HP-supplied Oracle Database and Additional Slice Component Bundle Instances
- 5. SA Core with a Remote Customer-supplied Oracle Database and Additional Slice Component Bundles
- 6. SA Core with a Remote Model Repository and HP-supplied Oracle Database, Additional Slice Component Bundle Instances and Satellites
- 7. SA Core with a Remote Customer-supplied Oracle Database, Additional Slice Component Bundles and Satellites
- 8. 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

> All other SA Core configurations must be installed by HP Professional Services or HP-certified consultants.

Deciding on an SA Core Configuration for your Facility

See Customer Installable SA Core Configurations on page 22 for detailed descriptions of supported SA Core configurations. For performance scalability information, see Chapter 9, SA Performance Scalability, on page 193

The SA Core configuration that is most appropriate for your facility will depend primarily on the number of servers that are to be managed by SA in the facility.

A typical SA Core installation has three main components. The *Model Repository*, the *Infrastructure Component bundle* and one *Slice Component bundle*. SA Provisioning also requires a *Media Server* and *Boot Server*. Since the Media Server and Boot Server do not generate much load and often have environmental dependencies they are not listed in the tables below. If you need more detailed information about SA Core Components, see the *SA Overview and Architecture Guide*.

There is no infallible way to select hardware for an SA Core installation. However, Table 1 and Table 2 show some recommended SA Core Component layouts that should perform well.

As you can see, scaling a core requires adding slices. Each slice adds highly available UI, API, OGFS, Build Manager and Gateway resources. Consider that when you have a small number of core servers, it may be best to begin with two larger servers, then grow the capacity of the core by adding additional slices. In Table 1 and Table 2, the following shorthand is used:

MR Model Repository

INFRA Infrastructure Component bundle

Slice <*x*> Slice Component bundle

OS Prov Operating System Provisioning Component bundle

table 1 **Small-to-Medium SA Deployment (SA 7.80 and later)**

Managed Servers	SA Component Distribution by Server	
	Server 1	Server 2
500	MR, Infra, Slice 0, OS Prov	N/A
1000	MR	Infra, Slice 0, OS Prov

Server Configuration: 4 CPU cores, 16 GB RAM, 1 GB/s network

table 2 **Medium-to-Large SA Deployment (SA 7.80 and later)**

Managed Servers	SA Component Distribution by Server				
	Server 1*	Server 2*	Server 3*	Server 4*	Server 5*
2000	MR	Infra, Slice 0, OS Prov	N/A	N/A	N/A
4000	MR	Infra, Slice 0, OS Prov	Slice 1	N/A	N/A
6000	MR	Infra, Slice 0, OS Prov	Slice 1	Slice 2	N/A
8000	MR	Infra, Slice 0, OS Prov	Slice 1	Slice 2	Slice 3

* Server Configuration: 8 CPU Cores, 16 GB RAM, 1 GB/s network

For more information about performance scalability, see Chapter 9, SA Performance Scalability, on page 193

Deciding on an Oracle Database Configuration

SA requires that you have installed an Oracle database and that it be up and be installed and running before you install the SA Core Components. The database is required for the SA component called the Model Repository which tracks and stores all information about your facility, including:

- An inventory of all servers under SA management.

- An inventory of the hardware associated with these servers, including memory, CPUs, storage capacity, and so on.

- Information about managed server configuration.

- An inventory of the operating systems, system software, and applications installed on managed servers.

- An inventory of SA Provisioning operating system installation media (the media itself is stored in the SA Provisioning Media Server).

- An inventory of software available for installation and the software policies that control how the software is configured and installed. The software installation media itself is stored in the Software Repository.

- Authentication and security information.

HP-Supplied or Customer-Supplied Oracle Database?

Before performing the SA installation, you must decide whether you will use the HP-supplied Oracle database or use an existing database you have installed yourself and you must decide whether that database should be local to the SA Core or installed on a remote database server.

You can easily install the HP-supplied database by running the SA Installer and selecting the option to install the database, either as a local database or on a remote database server by providing the IP address of the remote host.

The primary benefit of using the HP-supplied Oracle database is ease of installation for small or medium sized installations. The HP-supplied database is installed with a configuration that is optimized and tested for use with SA. The HP-supplied database has also been updated with all available patches/PSUs released by Oracle and has been tested to insure compatibility of the database with SA.

Some customers may already have an installed Oracle database or may have larger SA requirements that would benefit from a dedicated Oracle database server. If you have an existing Oracle database you prefer to use or want to install the Oracle database for use by SA yourself, then you can run the SA Installer and choose the option to use an existing Oracle database. Again, this database must be installed and up-and-running and you must have access to the database before you run the SA Installer.

➤ If you plan to use an Oracle database you have installed yourself, you must ensure that the database meets the minimum requirements and configuration documented in Oracle Setup for the Model Repository on page 205.

Local or Remote Oracle Database?

The decision whether to install the Oracle database locally or on a dedicated remote Oracle database server is based on performance. For performance/scalability reasons, HP recommends a remote dedicated Oracle database.

Customer Installable SA Core Configurations

The following are SA Core configurations supported by HP for customer installation.

1. SA Core with a Local HP-supplied Oracle Database

Suitable for small facilities. See Table 1 and Table 2.

See 1. SA Core with a Local HP-supplied Database on page 68

figure 1   **Configuration 1.**
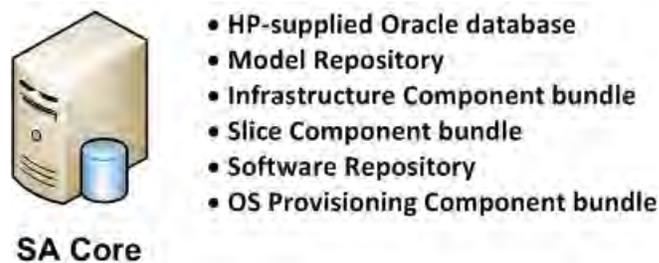
- HP-supplied Oracle database
- Model Repository
- Infrastructure Component bundle
- Slice Component bundle
- Software Repository
- OS Provisioning Component bundle

SA Core

2. SA Core with a Remote Customer-supplied Oracle Database

Suitable for small to medium facilities. See Table 1 and Table 2.

See 2. SA Core with a Remote Customer-supplied Oracle Database on page 74.

figure 2   **Configuration 2**
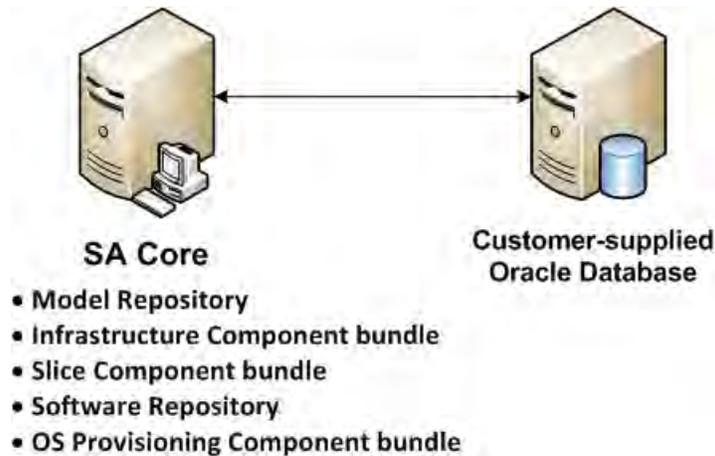
SA Core
- Model Repository
- Infrastructure Component bundle
- Slice Component bundle
- Software Repository
- OS Provisioning Component bundle

Customer-supplied
Oracle Database

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

Suitable for small to medium facilities. See Table 1and Table 2.

See

figure 3   **Configuration 3**
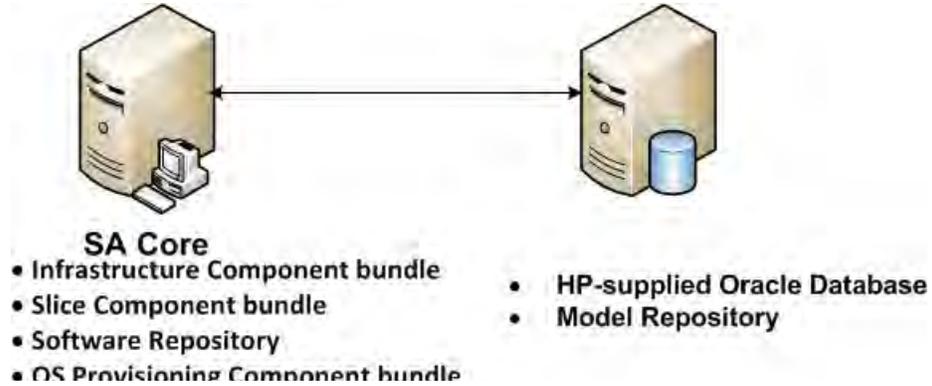
4. SA Core with a Remote Model Repository and HP-supplied Oracle Database and Additional Slice Component Bundle Instances

Suitable for small, medium and some larger facilities depending on the number of Slice Component bundles installed. See Table 1and Table 2.

See

figure 4   **Configuration 4**
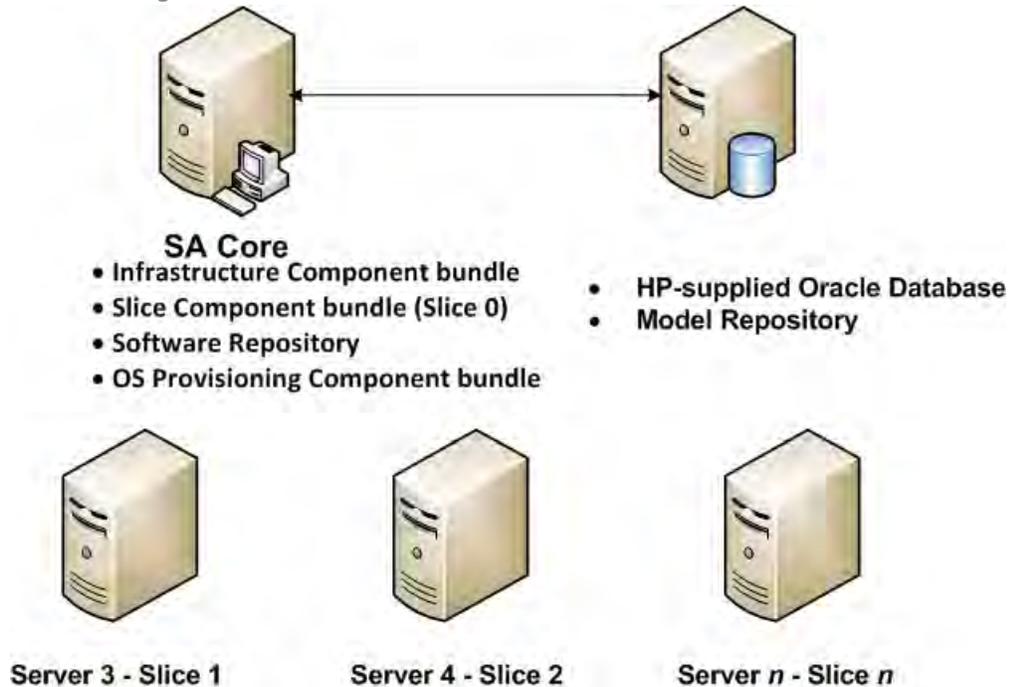
5. SA Core with a Remote Customer-supplied Oracle Database and Additional Slice Component Bundles

Suitable for small, medium and some larger facilities depending on the number of Slice Component bundles installed. See Table 1 and Table 2.

See 5. SA Core with a Remote Customer-supplied Database and Additional Slice Component Bundles on page 95.
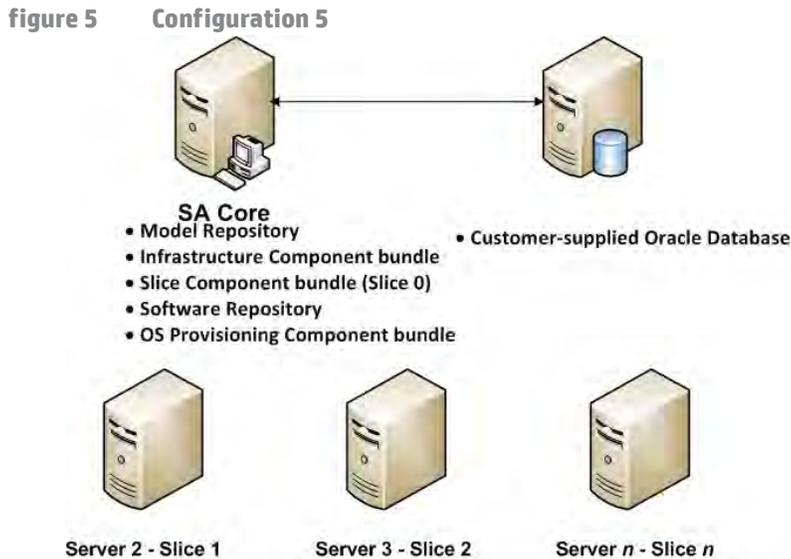
figure 5   Configuration 5

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

Suitable for small, medium and some larger facilities depending on the number of Slice Component bundles installed. See Table 1 and Table 2.

See 6. SA Core with a Remote Model Repository and HP-supplied Oracle Database, Additional Slice Component Bundles and Satellites on page 104.
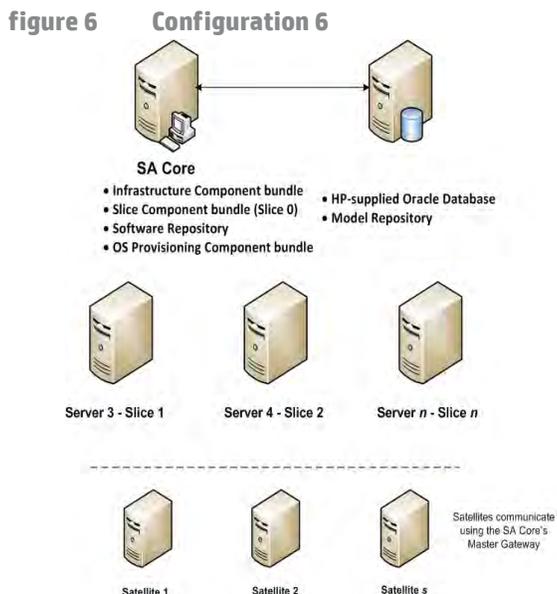
figure 6   Configuration 6

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

Suitable for small, medium and some larger facilities depending on the number of Slice Component bundles installed. See Table 1and Table 2. Satellite installations can handle in facilities in which the number of managed servers is not large enough for a full SA Core.

See 7. SA Core with a Remote Customer-supplied Database, Additional Slice Component Bundles and Satellites on page 113.

figure 7   Configuration 7
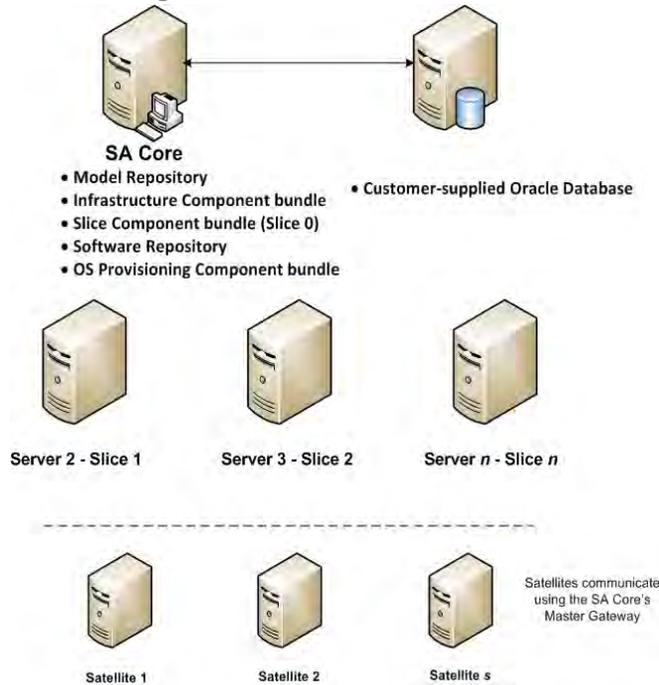
8. First (Primary) Core with a Secondary Core (Multimaster Mesh)

Suitable for medium and larger facilities with a number of servers to be managed large enough to require a second core. See Table 1and Table 2.

See 8. SA First (Primary) Core with a Secondary Core (Multimaster Mesh) on page 121.

figure 8   Configuration 8
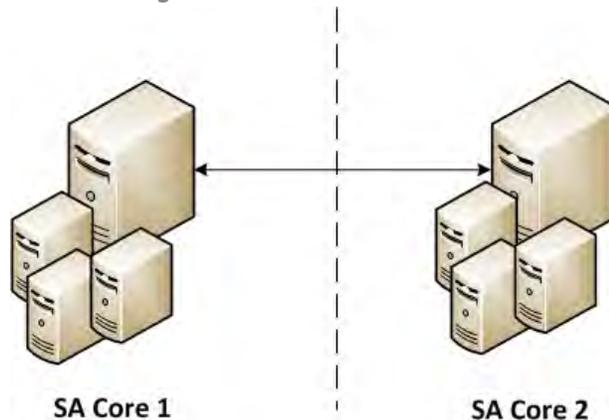
3 Using the SA Installer

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

Invoking the SA Installer

You invoke the SA Installer using one of the following scripts from the *SA Product Software* media or mounted copy. Do not invoke the SA Installer from any other distribution:

- `hpsa_install.sh` — installs the Oracle database and Model Repository, installs the Core Components for a Primary Core, installs the components for Secondary Cores, exports the contents of the Model Repository.

- `hpsa_uninstall.sh` — uninstalls a single Core Component or uninstalls all Core components. For more information about uninstalling an SA Core, see SA Core Uninstallation on page 197.

`hpsa_install.sh` accepts the command line arguments shown in Table 1:

table 1   SA Installer Command Line Arguments

Argument	Description
`-h`	Display the Installer help for the command line options. *To display help during the interview, press `ctrl-I`.*
`-c <cdf_filename>`	Invoke the Installer using the SA installation configuration parameter values in a specified saved Core Definition File (CDF. If you do not specify a CDF, you must provide the values for certain configuration parameters or accept the SA default values. The SA configuration parameter values you provide during the installation interview are used for the current installation and are automatically saved into an initial CDF that is used later during SA Core upgrades and installation of Secondary SA Cores.
`--pwsave`	Specifies that the root passwords for root users for all servers specified during installation are to be encrypted and accessed by a master password that you specify. See Master Passwords on page 29.
`--verbose	--debug`	Run the installer in verbose or debug mode which causes more information to be displayed on the console. See also Installer Logs on page 34.

Best Practice: Using the screen Utility for SA Installation

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 (it is not available by default).

SA Installer Installation Modes

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

Simple Installation Modes

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

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

Advanced Installation Modes

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

Expert Installation Mode

Used by HP Technical Staff

The SA Interview and the Core Definition File (CDF)

During installation, you are required to provide values for certain SA parameters used to configure your SA installation. This process is known as the *SA Interview.* 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 perform an upgrade. See Reusing a Core Definition File (CDF) on page 31. The CDF is saved in:

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

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

Master Passwords

You can specify a master password to be used to access the encrypted passwords of all core hosts specified during the installation of a new SA Core.

To encrypt server root passwords specified during installation, invoke the installation with the `--pwsave` argument. When you begin an installation with the `--pswave` argument specified, the installer encrypts root passwords and saves them in the final CDF on completion of the installation whether a successful or failed install. See Invoking the SA Installer on page 27.

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

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

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

master.password []:


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


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

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

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

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


master.password []:
```

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

SA Core Installation by Root or Non-root Users

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

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

Types of Install Users

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

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

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

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

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

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

Settings Required for Regular Users with sudo Capabilities

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

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

General Settings for User Names

This section describes general rules for user names in SA.

User names should have the following characteristics:

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

Help

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

How and When CDFs are Saved

During installation, the SA Installer saves a temporary CDF whenever you press `c` to continue on an action confirmation screen, for example the `Install Components` screen:

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

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

If you are concerned about security of CDFs, this file should be saved in a secure location or deleted. Before deleting, however, consider you may need to reuse the CDF in future for adding facilities, additional Slice Component bundles, upgrades and patching the SA Core or mesh.

Concluding the Interview

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

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

- if the Infrastructure host is unknown at the point of exit, the CDF is saved as `cdf_tmp.xml` under `/var/tmp` on the server on which the installer was invoked.

Reusing a Core Definition File (CDF)

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

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

Restarting an Interrupted Installation

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

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

    ```
    /<distro>/opsware_installer/hpsa_install.sh -c /var/tmp/cdf_ts_temp.xml
    ```

    where `<distro>` is the full path to the mounted media. Use the latest CDF as determined by the time stamp. See How and When CDFs are Saved on page 31.

2   You see a screen similar to the following:

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


    Currently specified hosts:

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


    Please select one of the following options:

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


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

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

    Press c to continue.

3   You see a screen similar to the following:

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


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

    Enter the password for each host specified as part of the installation.

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

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

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

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

5   You see a screen similar to the following:

    ```
    Host/Component Layout
    ```

```
=====================

Installed Components

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


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


Select a component to assign

1. Slice

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

Press c to continue.

6   You see a screen similar to the following:

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


Navigation keys:
Use <ctrl>P to go to the previous parameter.
Use <ctrl>N to go the next parameter.
Use <tab> to view help on the current parameter.
Use <ctrl>C to abort the interview.




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

1. Re-enter values
2. Continue

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

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

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

```
Install components
==================


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

Up-to-date Components (will not install)
```

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


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

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

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

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

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

Installer Logs

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

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

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

- `<ip_address>-install-infrastructure-<timestamp>.verbose.log`

- `<ip_address>-install-osprov-<timestamp>.verbose.log`

- `<ip_address>-install-slice-<timestamp>.verbose.log`

- `<ip_address>-install-word_uploads-<timestamp>.verbose.log`

Console output is logged to:

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

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

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

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

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

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

SA Parameter Password Security

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

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

• Encrypt the response files and installation logs.

• Purge sensitive information from the Installer response files.

• Store the Installer response files and logs on a secure server.

Table 2 lists cleartext passwords that are automatically obfuscated and passwords that must be manually secured.

table 2   Cleartext Passwords

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

table 2 **Cleartext Passwords (cont'd)**

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

Securing Installer Log and CDFs

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

SA Core Installation Process Flow

The six main phases of the SA core installation process are summarized below. For more detailed information, see the cross references associated with each step.

1   **Planning**: In the planning phase, you must decide which facilities and servers you will manage with SA. You must also choose the type of SA installation that is appropriate for your site(s) and ensure that you have the required hardware and software, including operating systems, and sufficient network connectivity.

See the *SA Overview and Architecture Guide* guide and of this guide for more information.

2   **Pre-installation Requirements:** Before beginning a core installation, whether it is a Single Core or a core in a Multimaster Mesh, you must perform such administrative tasks as ensuring that host names can be resolved, required ports are open and available, and installing any necessary operating system utilities, packages, and/or patches.

See Chapter 4, "Pre-installation System Requirement Checks" on page 39 of this guide for more information.

3   **Prerequisite Information for the HP SA Installer Interview:** Installer Interview Mode requires that you have certain information about your operational environment available because you will be asked to enter it during the interview. The information you provide will be saved into a Core Definition File (*CDF*). You must gather this information and have it at hand as you run the pre-installation interview. Some examples of the information required are the name of the Facility to be managed by the core, the authorization domain, host names and IP addresses, and passwords used for SA users and the Oracle database, and so on.

For a detailed description of the information required during the Installer Interview, see Chapter B, "SA Core Parameter Reference".

4   **SA Core Installation:** During this phase, you will run the Installer, complete the installation interview and install one of the following types of Cores:

— **First or Single Core Installation:** 1. SA Core with a Local HP-supplied Database on page 68.

— **Secondary Core Installations for a Multimaster Mesh:** 8. SA First (Primary) Core with a Secondary Core (Multimaster Mesh) on page 121.

5   **Post-installation Tasks:** Chapter 6, "SA Core Post-Installation Tasks".

6   **Core Configuration:** You will configure SA, performing tasks such as creating SA users and groups. At the end of this phase, SA is ready for operational use by system administrators. See the *SA Administration Guide* for more information.

Figure 1 shows the overall process of an SA core installation.

figure 1   **SA Core Installation Process Flow**
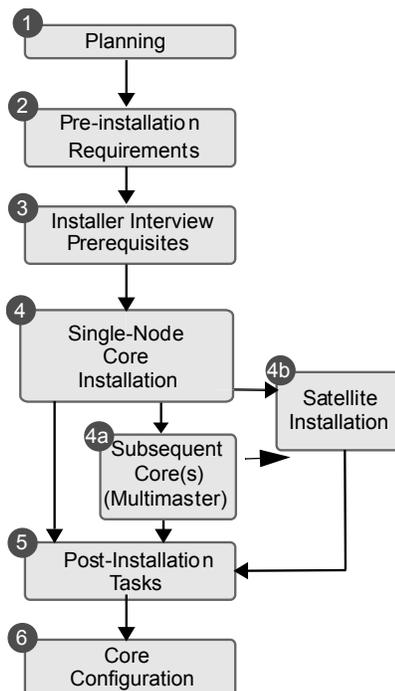
4 Pre-installation System Requirement Checks

This section describes hardware, software and network requirements that you must verify for SA Core host servers, agents, managed Servers and satellites.

Supported operating systems for SA Core hosts and Managed servers are detailed in the *SA Support and Compatibility Matrix*.

You must verify that your SA Core, managed server, and satellite host servers meet the requirements listed in this chapter. If you do not, your installation may fail or core performance may be affected.

There may be additional installation prerequisites.

See the release notes for this SA version.

This section covers the following prerequisites:

table 3   Prerequisite Checklist

Prerequisite Check	Status (Done/Not Done)
1. Transfer the SA Installation Files to a Local Disk	
2. Check that the Operating System for Your SA Core Host, Agents (managed servers), and Satellites is Supported	
3. Check the Oracle Requirements	
4. Check Veritas File System (VxFS) Requirements (optional)	
5. Familiarize Yourself with the SA Installer Prerequisite Checker	
6. Check the NFS Services Configuration	
7. Check the Free Disk Space Requirements	
8. Check the Network Requirements	
9. Download and Install Windows Patch Management Files (optional)	
10. Check the SA Global File System (OGFS) Requirements	
11. Check the Core Host(s) Time and Locale Requirements	
12. Install the Windows Update Service on Windows Server 2003, 2008, 2008 R2 x64 and 2012	
13. Check the User and Group Requirements For Linux	
14. Check SA Cores on VMs Requirements (optional)	

1. Transfer the SA Installation Files to a Local Disk

HP recommends that you copy the SA installation files to a local disk or to a network share and run the Installer from that location. See Download the SA Installation Files on page 66.

2. Check that the Operating System for Your SA Core Host, Agents (managed servers), and Satellites is Supported

For a complete listing of all platforms supported for SA Cores hosts, Agents (managed servers), and Satellites, see the SA Support and Compatibility Matrix document provided with the SA distribution media or available for download at

http://support.openview.hp.com/sc/support_matrices.jsp

➤ In an SA Core, servers that host a core's components must all be running the same operating system. Different update levels are supported on hosts within the same core. In a multiple core mesh, each distinct core can be running under a different operating system but all hosts in each distinct core must be running the same operating system.

3. Check the Oracle Requirements

The Model Repository requires an installed Oracle database. You can use the SA Installer to install the HP-supplied Oracle database. You can also use an Oracle database you have installed yourself, however that database must be up and running before you begin the SA installation. Whatever method you choose, see Oracle Setup for the Model Repository on page 205 for detailed information about required database configuration.

➤ The Oracle database must be installed either on its own host or on a server that has the SA Infrastructure Component bundle installed.

4. Check Veritas File System (VxFS) Requirements (optional)

SA supports the Veritas File System (VxFS) for Red Hat Enterprise Linux 5 and 6 x86_64. VxFS *is not* supported for other operating systems. If you attempt to install SA components on a non-supported operating system running VxFS, the installation will fail and will need to be backed out. The SA Installer Prerequisite Checker validates VxFS for SA Cores and satellites and in cases where prerequisites are not met, the installation will fail before SA is installed. VxFS is not validated for Oracle hosts, therefore, if Oracle is installed on the same host as SA Core Components, the Oracle installation may succeed and the core install subsequently fail. See the *SA Support and Compatibility Matrix* for the latest supported operating systems.

5. Familiarize Yourself with the SA Installer Prerequisite Checker

SA now performs validation of a minimum baseline requirement for an SA Core installation. This validation is performed automatically by the SA Installer during an SA Core installation. You can also run this check as a standalone utility prior to installation to verify the suitability of a server as an SA Core host before attempting an installation.

➤ If the validation finds a requirement that is not met by your server, the installation stops and you must correct the problem before continuing the installation. If a recommended configuration is not met, you will see a warning, but can continue with the installation.

The prerequisites that are validated during the check include:

- **Host Physical Characteristics**
    - — Physical memory
    - — Number of CPUs (cores or physical)
    - — Loopback driver MTU (Linux only)
    - — IDE disk drive optimizations
- **Oracle Database** – disk space, parameter, tablespace requirements (*existing Oracle installations only*)
    - — Supported Oracle version is installed
    - — Required Oracle patches are installed
    - — Supported operating system configuration
    - — Swap space size
    - — Temp space
    - — User `oracle` defined
    - — The port specified by the `db.port` parameter on remote database hosts is being monitored and accepts connections.
- **Required Packages** – packages that must be installed

    During installation, the SA Installer performs a prerequisite check that includes checking for recommended package version levels. You may see warnings during the check if your installation has earlier versions of these packages. HP recommends that you upgrade any packages flagged with a warning in order to ensure SA's full functionality.

    You can continue the SA installation with the earlier packages but may sacrifice the functionality provided by the newer version.

- **Required Patches** – patches that must be installed (SunOS only)
- **Recommended Packages** – packages that should be installed
- **Unsupported Packages** – packages that must not be installed
- **Reserved Ports** – ports that must be open and available
- **Disk Space Requirements** – checks that minimum disk space required for installation available (*fresh installation only*)
- **Operating System Configuration**:
    - — Hostname is a fully qualified domain name (FQDN) and is resolvable

- — File system (links maintained, case sensitive)

- — Ability to create new users and groups

- — Allocated swap space

- — Timezone setting (UTC - sets hwclock to match the system clock on Linux systems) and locale (`en_US.UTF-8` or equivalent)

- — Run level (Linux only)

- — NFS versions

- — No VxFS (SLES only)

- — Sufficient `temp` space is available

- — Translations for localhost are available (Linux only)

- — `/etc/inet/hosts` and `/etc/hosts` are both plain text files (SunOS only)

- — Selinux running (Linux 4 AS and 5 AS server only)

- — Verification that no critical file paths contain symbolic links

- — Red Hat update 5 or later (Linux 4 AS only)

- — gzip installed (SunOS only)

➤ The prerequisite check requires root privileges and validates both required and recommended items. Required items, such as required packages and Oracle settings, must be corrected if the validation fails, however, if you have business requirements that override recommendations, such as number of CPUs, you can still perform an SA Core installation.

Prerequisite Validation of Non-HP-Supplied Oracle Installations

If you intend to use an existing Oracle installation rather than the HP-supplied Oracle database, that database must meet the requirements described in Oracle Setup for the Model Repository on page 205. When you begin an SA Core installation and an existing database installation, the prerequisite checker will validate the Oracle requirements as well as the core server requirements.

SA Core Server Validation

After you have initiated an SA Core installation, the installer performs the prerequisite check before installation of the Oracle database and before installation of the SA Core Components. The validation progress is displayed on screen showing the items being validated and the results of the validation. The display during validation will be similar to this:

```
Processing on Linux/4AS-X86_64 using
/tmp/OPSWprereqs-40.0.0.0.54/Linux_oracle_rqmts.conf
    Checking 'required' packages for Linux/4AS-X86_64
    Checking 'required' patches for LINUX/4AS-X86_64
    Checking 'recommended' packages for LINUX/4AS-X86_64
    Checking 'absent' packages for LINUX/4AS-X86_64
 Testing memory size
Testing for number of CPUs
    Testing hostname for FQDN
    Testing swap space allocated
    Verify timezone is UTC
[...]
```

If the validation indicates that your system does not meet the recommended configuration, you can either stop the installation, take measures to meet the recommendations, and restart the installation or you can choose to continue the installation without changes.

Prerequisites

The SA Prerequisite Check requires the `/bin/sh` Unix shell. If `/bin/sh` is not available, the prerequisite check will not run.

Manual Prerequisite Check

You can run the SA Prerequisite Check manually using the instructions in this section. When run manually before the Oracle RDBMS is installed, the following is validated:

- CPU requirements
- Disk space requirements

When the SA Prerequisite Check is run manually after Oracle RDBMS installation but before SA Core Component installation, the following is validated:

- When the Oracle RDBMS is installed locally, the required RDBMS version and patches.

➤ If the Oracle database is installed remotely, prerequisite testing will extract database access information from the Core Definition File (CDF) of the current core install. If the database is accessible, it will be tested in a remote mode using Oracle's Translation Name Service (TNS). Accessibility depends on the availability of SQL*Plus which is installed as part of the database or as Oracle's InstantClient.

You invoke the prerequisite check from the command line on the server on which you plan to host the SA Core.

Locate the file:

`<distro>/opsware_installer/OPSWprereqs-<version>.zip`

where `<distro>` is the full path to the mounted media. Unzipping this file will create a sub-directory, `OPSWprereqs-<version>` which contains the script `preinstall_requisites.sh`.

Usage

```
.../preinstall_requisites.sh <phase> [--upgrade] [--cdf_file=<path>]
[--resp_file=<path>] [--verbose | --silent]
```

where:

table 4   Prerequisite Check Script Arguments

Argument	Description
`<phase>`	Specifies an Oracle database validation or SA Core host validation **Valid Values**: `Oracle`, `core_inst`, or `satellite`
`<path>`	The fully qualified path to a valid SA Installer Core Definition File (CDF)

table 4   Prerequisite Check Script Arguments (cont'd)

Argument	Description
`--upgrade`	Specifies an upgrade and suppresses the disk space checks. If not specified, fresh install is assumed and disk space checks are run assuming that no SA components are currently installed.
`--cdf_file=<path>`	Specifies the path to a valid CDF for the current installation. When specified, certain values that might be specified during the install process are taken from the CDF, such as Oracle installation values.
`--resp_file=<path>` (**First upgrade of a core to SA 10.0 only**)	For the first upgrade of a 7.8x or 9.x SA Core to 10.0, you can specify the response file for the existing installation. Core parameters are taken from the response file and used as defaults. Subsequent upgrades use the CDF.
`--verbose │ --debug │ --silent`	`verbose` or `-- debug` display additional output, `silent` displays no output.

► You must have root privileges to run the script. There is a test to see if the logged in user can create users and groups. Therefore, the user running the SA Prerequisite Check must be capable of creating users and groups, but the current user must be the same user that will be running the installer.

Interpreting Prerequisite Checker Results

When the prerequisite check completes, you may see messages similar to the following.

```
Prerequisite Checks
===================
Results for <IP_address>:

        FAILURE Insufficient swap space (18 GBytes).
                24 Gbytes is the recommended for Oracle.
        WARNING File system '/' has 29447 MBytes available and 154050 is
                recommended.
        [INFO] Processing on Linux/6Server-X86_64 using /var/tmp/hpsa_media/
                opsware_installer/prereq/Linux_oracle_rqmts.conf
        FAILURE These packages are required but not installed.
                If a version is specified, that version or higher is required.
                PACKAGE ARCH    VERSION
                libaio-devel    x86_64  0.3.107-10.el6

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

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

If your server passes the prerequisite check, you can continue the installation.

Additional Linux Requirements

For Linux systems, you must also adhere to the following requirements:

- You must specify the server's initial run level as level 3 in the `/etc/inittab` file.

- If the server uses Integrated Drive Electronics (IDE) hard disks, you must enable Direct Memory Access (DMA) and some other advanced hard disk features that improve performance by running the following script as a user with root privileges on the server and then reboot the server:

```
# cat > /etc/sysconfig/harddisks << EOF
USE_DMA=1
MULTIPLE_IO=16
EIDE_32BIT=3
LOOKAHEAD=1
EOF
```

- Due to a bug in the Linux kernel, you must configure the loopback interface to use a Maximum Transmission Unit (MTU) size of 16036 bytes or less. To make this change, perform the following tasks:

  a Run the `ifconfig lo mtu 16036` command. This sets the MTU of the running kernel.

► Add the line `MTU=16036` to the end of the `/etc/sysconfig/network-scripts/ifcfg-lo` file. This causes the MTU to be properly set when the system is booted.

6. Check the NFS Services Configuration

NFSv2 and NFSv3 must be enabled and NFSv4 must be disabled to support mounting file systems (`mountd`) and SA recommends configuring how NFS/RPC server ports are assigned.

► NFSv4 is enabled by default for Red Hat Enterprise Linux, SUSE Linux Enterprise Server.

NFS Services Configuration

Perform the following tasks based on your operating system.

Red Hat Enterprise Linux

If NFSv2 and/or NFSv3 are not enabled, you may need to change or modify the following parameters in `/etc/sysconfig/nfs`:

```
MOUNTD_NFS_V2=yes
MOUNTD_NFS_V3=yes
```

Add the following to `/etc/sysconfig/nfs` to disable NFSv4 support for `nfsd`:

```
RPCNFSDARGS="--no-nfs-version 4"
```

SUSE Linux Enterprise Server

Add the following to `/etc/sysconfig/nfs` to disable NFSv4 support for `nfsd`:

```
NFS4_SUPPORT="no"
```

No changes for `mountd` are required unless you have manually modified `/etc/init.d/nfsserver` to disable NFSv2 and NFSv3.

Configuring NFS/RPC Server Ports

For a list of ports used by SA, see Required Open Ports on page 50. Perform the following tasks based on your operating system:

Red Hat Enterprise Linux

Add or enable these parameters in `/etc/sysconfig/nfs`:

```
MOUNTD_PORT=<choose a non-SA port number>
LOCKD_TCPPORT=<choose a non-SA port number>
LOCKD_UDPPORT=<choose a non-SA port number>
STATD_PORT=<choose a non-SA port number>
STATD_OUTGOING_PORT=<choose a non-SA port number>
```

If you have `rquotad` enabled, add or enable this parameter in `/etc/sysconfig/nfs`:

```
RQUOTAD_PORT=<choose a non-SA port number>
```

SUSE Linux Enterprise Server

For `mountd`, modify `/etc/sysconfig/nfs` and modify or add this parameter:

```
MOUNTD_PORT=<choose a non-SA port number>
```

For `lockd`, create or edit `/etc/modprobe.d/lockd` and add:

```
options lockd nlm_udpport=<choose a non-SA port number>
nlm_tcpport=<choose a non-SA port number>
```

For `statd`, if it is installed and running, edit `/etc/init.d/nfsserver`, search for "`startproc /usr/sbin/rpc.statd`" and append the `-p` parameter specifying a non-SA port. For example:

```
startproc /usr/sbin/rpc.statd --no-notify -p<choose a non-SA port number>
```

For `rquotad`, if it is installed and running, edit `/etc/services` and add/edit TCP/UDP ports for `rquotad`, for example:

```
rquotad <choose a non-SA port number>/tcp
rquotad <choose a non-SA port number>/udp
```

Restart the NFS Service

After the required changes are made, restart the NFS server service:

Red Hat Enterprise Linux

```
/sbin/service nfs restart
```

SUSE Linux Enterprise Server

```
/sbin/service nfsserver restart
```

7. Check the Free Disk Space Requirements

This section describes the free disk space (in addition to the operating files system) requirements for any SA Core Server.

Core Server Disk Space Requirements

On each Core Server, the root directory must have at least 72 GB free hard disk space (beyond the file system needs of the operating system). SA components are installed in the `/opt/opsware` directory. Table 5 lists the recommended free disk space requirements for installing and running SA Core Components. These sizes are recommended for primary production data. You must calculate additional storage for backups separately.

table 5   SA Disk Space Requirements

SA Component Directory	Recommended Free Disk Space	Requirement Origin
/etc/opt/opsware	50 MB	Configuration information for all SA Core services. (Fixed disk usage)
/media *	15 GB	**SA Provisioning:** The media directory holds the OS installation media that is shared over NFS or CIFS. The initial size for this directory depends on the total size of all OS installation media sets that you plan on provisioning, such as Windows Server 2003 CD (700mb), Red Hat 3 AS CDs (2GB), and SUSE 9 SP3 (10GB). The network OS install shares do not need to reside on SA core systems and are typically dispersed across multiple servers as the Multimaster Mesh grows. (Bounded disk usage that grows quickly in large increments)
/opt/opsware	25 GB	The base directory for all SA Core services. (Fixed disk usage)
/u01/app/oracle /u02/app/oracle /unn/app/oracle ...	1 - 2 GB 19 - 20 GB 19 - 20 GB	For an SA installed Oracle RDBMS, /u01 contains the Oracle software files. /u02 - /unn contains the Oracle tablespace directory that contains all model and job history information. Known sizes range from 5GB to 50GB of space, depending on the frequency and type of work, the amount of software and servers managed, and the garbage collection frequency settings. (Bounded disk usage that grows slowly in small increments)
/var/log/opsware/word	80 GB	The total log space used by all SA Core Components. (Fixed disk usage)
/var/opt/opsware/	20 GB	The total run space used by all SA Core Components, including instances, pid files, lock files, and so on. (Fixed disk usage)
/var/opt/opsware/word +	80 GB	(*Infrastructure host only*) The total run space used by all SA Core Components, including instances, pid files, lock files, and so on. (Fixed disk usage)
/var/opt/opsware/word * +	80 GB	(*Infrastructure host only*) The total disk space used by software that is imported into SA. Theoretically, this is infinite disk usage depending on how much software you import. Initial size calculation is based on the total size of all packages and patches that you want managed by SA. Known sizes range from 10GB to 250GB.

table 5   SA Disk Space Requirements (cont'd)

SA Component Directory	Recommended Free Disk Space	Requirement Origin
/var/opt/opsware/ ogfs/export/store	20 GB	The home directory for the Global File System (OGFS) enabled SA user accounts.

➤ ***** The entries in Table 5 marked with an asterisk are directory path defaults that you can change during the installation process. The recommended disk space for these directories is based on average-sized directories, which could be smaller or larger, according to usage.

➤ **+** All installed Slices Component bundle hosts will remotely NFS mount these file systems.

➤ For performance reasons, you should install the SA Components on a local disk, not on a network file server. However, for the Software Repository, you can use a variety of storage solutions, including internal storage, Network Attached Storage (NAS), and Storage Area Networks (SANs).

Model Repository (Database) Disk Space Requirements

Additional disk space is required for the Oracle software and the Model Repository data files. Keep in mind that storage requirements for the database grow as the number of managed servers grows.

As a benchmark figure, you should allow an additional 3.1 GB of database storage for every 1,000 servers in the facility that SA manages. When sizing the tablespaces, follow the general guidelines described in Table 6. If you need to determine a more precise tablespace sizing, contact your technical support representative.

table 6   Tablespace Sizes

Tablespace	MB/1000 Servers	Minimum Size
AAA_DATA	256 MB	256 MB
AAA_INDX	256 MB	256 MB
AUDIT_DATA	256 MB	256 MB
AUDIT_INDX	256 MB	256 MB
LCREP_DATA	3,000 MB	1,500 MB
LCREP_INDX	1,600 MB	800 MB
TRUTH_DATA	1,300 MB	700 MB
TRUTH_INDX	400 MB	400 MB
STRG_DATA	1,300 MB	700 MB
STRG_INDX	400 MB	400 MB

Software Repository Disk Space Requirements

The Software Repository contains software packages and other installable files and is part of the *Slice Component bundle.* Typical installations start with approximately 300 GB allocated for the server hosting the Software Repository. However, more space might be required, depending on the number and size of the packages, as well as the frequency and duration of configuration backups.

Media Server Disk Space Requirements

Dependent on your SA Provisioning requirements. This component requires sufficient disk space for the OS media for all the operating system versions you intend to provision.

8. Check the Network Requirements

This section discusses the network requirements within a facility, open ports required for Core Components, and name resolution requirements. These requirements must be met for Primary Core, Secondary Core, and Satellite installations.

Network Requirements Within a Facility

Before running the Installer, your network environment must meet the following requirements:

- It is recommended that all SA Core Servers be on the same Local Area Network (LAN or VLAN). If cores are placed in different subnets, be aware that there may be performance issues.

- There must be full network connectivity between all SA Core Servers and the servers that the SA Core will manage.

- Core Servers expect user accounts to be managed locally and cannot use the Network Information Service (NIS) directory to retrieve password and group information. During installation of the Core Components, the installer checks for the existence of certain target accounts before creating them. If you are using NIS, this check will fail.

- The Software Repository requires a Linux Network File System (NFS) server. See also Additional Linux Requirements on page 45.

- When using network storage for Core Components, such as the Software Repository or SA Provisioning Media Server, you must ensure that the user that runs the install has write access over NFS to the directories where the components will be installed.

- The speed and duplex mode of the Core's and Managed Servers' NIC adapters must match the switch they are connected to. A mismatch will cause poor network performance between the Core and Managed Servers.

- On any given core server, having multiple interfaces which reside on the same subnet is an unsupported configuration. If the slice server has multiple interfaces, the active interfaces MUST reside on separate subnets.

- Firewall/network settings on the SA Core host servers can affect the accessibility of the network ports used for the SAS Web Client, for example, restrictive Linux `iptables` rules. Ensure these operating system/network settings allow required SAS Web Client access.

- The SA gateway only supports tunneling to port 443. You may need to change the gateway configuration to allow tunneling to other ports if you are:

— Using iLO on other ports.

— Integrating with a vCenter server that is on a port other than port 443.

— Integrating with an OpenStack deployment. In this case, you need to allow tunneling to ports 5000, 8774, and 8776, or to the custom ports for your deployment.

For more information, see "Virtualization Service Tasks" in the *SA User Guide: Virtualization Management*.

To identify the gateway host, open the `opswgw.args` file from the iLO or virtualization service server. The `opswgw.args` file is located on the managed server at:

— **UNIX/Linux**: `/etc/opt/opsware/agent`

— **Windows**: `%SystemDrive%\Program Files\Common Files\Opsware\etc\agent`

In this example, your agent gateway name is `opswgw-agws1-TEAL1`:

1   On the gateway host, open the `opswgw.custom` file.

The `opswgw.custom` file is located on the gateway host at:

— **UNIX/Linux**: `/etc/opt/opsware/opswgw-agws1-TEAL1`

— **Windows**: `%SystemDrive%\Program Files\Common Files\Opsware\etc\opt\opsware\ opswgw-agws1-TEAL1`

2   For each port on which you want to allow tunneling (for example, port 5000), add the following new line:

`opswgw.EgressFilter=tcp:*:5000::`

3   Save and close the file.

4   Restart the agent gateway component on the gateway host by running the following command:

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

Required Open Ports

You must configure any firewalls protecting your Core Servers to allow the ports shown in Table to be open. Note that the ports numbers listed in the table are the default values which can be changed during the installation, so ensure you are leaving the correct ports open.

table 7   Open Ports on a Firewall Protecting an SA Core

Source	Destination	Open Port(s)	Notes
Management Desktops	Slice Component bundle hosts	80, 443, 8080	Required
Direct access to Oracle database (reports, troubleshooting, management)	Model repository (`truth`) host	1521	Strongly recommended to allow Oracle management
Management Desktops	Slice Component bundle hosts	1004, 1018, 1032, 2222, 8061	[Optional] Useful for troubleshooting; ports represent `spin`, `way`, `twist`, `tsunami` and `ogsh` (`ssh`).

table 7   Open Ports on a Firewall Protecting an SA Core (cont'd)

Source	Destination	Open Port(s)	Notes
SA Core (Management Gateway)	SA Core (Management Gateway)	2001	Required
SA Core (Management Gateway)	SA Core in a different Multimaster Mesh (management gateway)	22, 2003	[Optional] For scp (default word replication, can be forwarded over 2001 connection), backup for 2001 if it is busy.
Slice Component bundles	SA Agents (in same network)	1002	Required (only for the Agent Gateway managing the Agent).
SA Core (Management Gateway)	Satellite/Gateway	3001	Required
SA Core hosts	Mail server	25	Required for email notifications
SA Core hosts	LDAP server	636	Required for secure LDAP access; port can change if you use unsecure LDAP.
SA Agents	SA Core servers and Satellites managing the agent	3001	Required
SA Satellite/Gateway	SA Core	2001	Required
SA Satellite/Gateway	Managed Agents	1002	Required

* Port 1521 is the default Oracle listener (`listener.ora`) port, but you can specify a different port in your Oracle configuration. In case your installation has been modified to use a port other than 1521, you should verify the port number from the Oracle listener status and ensure that your firewall is configured to allow the correct port to be open for the Oracle listener.

➤ If you have enabled IPTABLES, you must also add exception rules for `mountd` (tcp/udp), `portmapper` (tcp/udp) and port 4040.

➤ SA's data access layers (infrastructure) use connection pooling to the database. The connections between the database and the infrastructure layer must be maintained as long as SA is up and running. Ensure that your firewall is configured so that these connections do not time out and terminate the connections between the database and the infrastructure layers.

Table 8 shows the ports used by the SA Provisioning components that are accessed by servers during the provisioning process. (In SA, Provisioning refers to the installation of an operating system on and configuration of managed servers.)

table 8   **Open Ports for the SA Provisioning Components**

Port	Component	Service
67 (UDP)	Boot Server	DHCP
69 (UDP)	Boot Server	TFTP
111 (UDP, TCP)	Boot Server, Media Server	RPC (`portmapper`), required for NFS
Dynamic/Static*	Boot Server, Media Server	`rpc.mountd`, required for NFS
2049 (UDP, TCP)	Boot Server, Media Server	NFS
8017 (UDP, TCP)	Agent Gateway	Interface to the Build Manager
137 (UDP)	Media Server	SMB NetBIOS Name Service
138 (UDP)	Media Server	SMB NetBIOS Datagram Service
139 (TCP)	Media Server	NetBIOS Session Service
445 (TCP)	Media Server	MS Directory Service

* By default, the `rpc.mountd` process uses a dynamic port, but it can be configured to use a static port. If you are using a dynamic port, the firewall must be an application layer firewall that can understand RPC requests that clients use to locate the port for `mountd`.

➤ The SA Provisioning Boot Server and Media Server run various services (such as `portmapper` and rpc.mountd) that could be susceptible to network attacks. It is recommended that you segregate the SA Provisioning Boot Server and Media Server components onto their own DMZ network. When you segregate these components, the ports listed in Table 8 should be opened to the DMZ network from the installation client network. Additionally, the Boot Server and Media Server should have all vendor-recommended security patches applied.

Table 9 shows the Managed Server port that must be open for SA Core Server connections.

table 9   **Open Ports on Managed Servers**

Port	Component
1002 (TCP)	SA Agent

Required Reserved Ports

The following ports must be reserved for use by SA.

table 10   SA Reserved Ports

Port	Component
3003 (TCP)	Management Gateway proxy
2001 (TCP)	Management Gateway tunnel listener
3002 (TCP)	Core Gateway proxy
2003 (TCP)	Core Gateway slice tunnel listener
8085 (TCP)	Core Gateway admin
5678, 7501 (TCP)	Multimaster component
1003, 1006	Web Services Data Access Engine
1018	Command Engine
1026, 1032	Data Access Engine
7006, 7080	Health Check Monitor
1012, 1017, 8843	SA Provisioning Build Manager
3001, 8017	Agent Gateway proxy
1033	Global File System
8020	Global File System
2222	SSH daemon
1027, 1028, 1029	APX proxy
8081	agentcache component
9009, 9080	Command Center
4433, 80, 81, 82	HTTPS proxy
1002	Agent

Host and Service Name Resolution Requirements

SA must be able to resolve Core Server host names and service names to IP addresses through proper configuration of DNS or the `/etc/hosts` file.

Previous Releases

If you plan to install the Core Components on a server that had a previous SA installation (for example, version 6.x or 7.x), you must verify that the host names and service names resolve correctly for the new installation.

Core Servers and Host/Service Name Resolution

During the installation, the `/etc/hosts` file on machines where the *Slice Component bundle* is installed will be modified to contain entries pointing to the *Secondary Data Access Engine*, the *Command Center*, the *Build Manager*, and the fully qualified domain name of the `localhost`.

All other servers hosting Core Components must be able to resolve their own valid host name and the valid host name of any other SA Core Server (if you will be using a multiple core installation or Multimaster Mesh). A fully qualified name includes the subdomain, for example, `myhost.acct.buzzcorp.com`. Enter the `hostname` command and verify that it displays the fully qualified name found in the local `/etc/hosts` file.

In a *typical* component layout, the Software Repository Store is installed as part of the Infrastructure Component bundle and the Slice Component bundle must able to map the IP of the Infrastructure host to its hostname. In a *custom* component layout, the Software Repository Store may be installed separately on any host, therefore the Slice Component bundle must be able to map the IP of that host to its hostname. It is a common practice, but not a requirement, to host the Software Repository Store and the `OGFS home/audit` directories on the same server.

SA Provisioning: DHCP Proxying

If you plan to install your SA Provisioning components on a separate network from the Core Components, you must set up DHCP proxying to the DHCP server (for example, using Cisco IP Helper). If you use DHCP proxying, the server/router performing the DHCP proxying must also be the network router so that PXE can function correctly.

The SA Provisioning Boot Server component provides a DHCP server, but does not include a DHCP proxy. For DHCP server configuration information, see DHCP Configuration for SA Provisioning on page 161.

9. Download and Install Windows Patch Management Files (optional)

The SA Windows Patch Management feature requires several files from the Microsoft software download repository. These files are 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.

Installing the Required Windows Patch Management Files in an Existing Core

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

See Manually Obtaining the Windows Patching Utilities on page 55 for more information about manually downloading the Windows Patching Utilities.

Supported Windows Versions

- Windows 2000

- Windows XP

- Windows Server 2003 x86 and x64

- Windows Server 2008 x86 and x64

- Windows Server 2008 R2 x64

- Windows Server 2008 x86 Server Core and Windows 2008 x64 Server Core

➤ In order to apply patches to Managed Servers running Windows Server 2000 SP4 and Windows Server 2003 RTM, you must first ensure that the Microsoft update MS04-011 (or a subsequent update) has been applied to those servers.

Requirements

Managed Servers must meet the following Windows patching requirements:

- Windows Installer 3.1 must be installed

- MSXML 3+ must be installed (MSXML is a general requirement for all Windows managed servers regardless of whether the managed server will or will not use the Windows patching feature).

- The Windows Update Agent must be installed

- The Windows (Automatic) Update service must *not* be disabled but must be set to *never* check for updates.

➤ As of Windows Server 2008, the Automatic Update service was renamed the Windows Update service.

Manually Obtaining the Windows Patching Utilities

If you did not install the Windows patch management files during core installation and your SA Core and SA Client do not have internet access, you can perform the following tasks from a machine with internet access to obtain the files and transfer them to the core:

1 Obtain the following files from Microsoft:

➤ The links to these files are provided as a convenience, however, Microsoft Corp. may change the links after the release of this document. Therefore, we cannot guarantee that these links will be valid when you use them and you may need to search the Microsoft Support website to find the correct files.

- **wsusscn2.cab**

    The wsusscn2.cab file contains the Microsoft patch database. Download wsusscn2.cab from:

    http://go.microsoft.com/fwlink/?LinkId=40751

- **WindowsUpdateAgent30-x86.exe**

    The WindowsUpdateAgent30-x86.exe file is required when SA scans x86-based managed servers to determine which Windows patches/hotfixes are installed. Download the package containing WindowsUpdateAgent30-x86.exe from:

    http://go.microsoft.com/fwlink/?LinkID=100334

After downloading, you must rename the file "`WindowsUpdateAgent-x86.exe`".

- **WindowsUpdateAgent30-x64.exe**

  The `WindowsUpdateAgent30-x64.exe` file is required when SA scans x64-based managed servers to determine which Windows patches/hotfixes are installed. Download the package containing `WindowsUpdateAgent30-x64.exe` from:

  http://go.microsoft.com/fwlink/?LinkID=100335

▶ After downloading, you must rename the file "`WindowsUpdateAgent-x64.exe`".

- **WindowsUpdateAgent30-ia64.exe**

  The `WindowsUpdateAgent30-ia64.exe` file is required when SA scans Itanium x64-based managed servers to determine which Windows patches/hotfixes are installed. Download the package containing `WindowsUpdateAgent30-ia64.exe`from:

  http://go.microsoft.com/fwlink/?LinkID=100336

▶ After downloading, you must rename the file "`WindowsUpdateAgent-ia64.exe`".

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

   `/opsw/win_util`

3 Verify that the destination directory contains all these files:

```
WindowsUpdateAgent-x86.exe
WindowsUpdateAgent-x64.exe
WindowsUpdateAgent-ia64.exe
qchain.exe
wsusscn2.cab
```

4 Write down the name of the directory containing the Windows Update Agent files. You will need this location when you run the SA Installer and are prompted to provide the fully qualified directory path to the WUA files. You can also find the WUA file location by checking the SA parameter, `windows_util_loc`.

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

For more information on Windows Patch Management, see the *SA User Guide: Server Patching*.

10. Check the SA Global File System (OGFS) Requirements

This section discusses requirements for SA's Global File System (OGFS). The OGFS represents objects in the platform data model (such as facilities, customers, and device groups) and information available on platform managed devices (such as the configuration setting on a managed network device or the file system of a managed server) as a hierarchical structure of file directories and text files.

OGFS Store and Audit Hosts

When you run the SA Installer interviewer in advanced mode, you can specify values for the `ogfs.store.host.ip` and `ogfs.audit.host.ip` parameters. (See Global File System Prompts on page 94.) If you set either of these parameters to point to a host that does not run the Slice Component bundle (which contains OGFS and the Software repository), then perform the following steps on the host you do specify:

1   With `mkdir`, create the directories that you specified for the `ogfs.store.path` and `ogfs.audit.path` parameters.

2   Modify the export tables.

➤   In these examples, the Slice Component bundle is installed on two separate hosts within the same core.

On a Linux host, modify the `/etc/exports` file, such as:

```
# Begin Opsware ogfs export
/export/ogfs/store 1.2.3.4(rw,no_root_squash,sync) \
1.2.3.5(rw,no_root_squash,sync)
/export/ogfs/audit 1.2.3.4(rw,no_root_squash,sync) \
1.2.3.5(rw,no_root_squash,sync)
# End Opsware ogfs exports
```

where 1.2.3.4 and 1.2.3.5 are example IP addresses of the two Slice Component bundle hosts and where `/export/ogfs/store` and `/export/ogfs/audit` are corresponding paths that exist on the host from where you are exporting the OGFS data.

3   After you add new entries to the export tables, export the directories or restart the Network File System using standard system procedures.

➤   Remember to verify that the NFS Daemon starts when the system reboots. If your security policies require that NFS services be disabled, in order to install the Slice Component bundle on Linux systems you will need to configure the services `nfs`, `nfslock` to start the services and `netfs` to ensure that network (remote) filesystems are mounted after the network is available. Slice Component bundle installation will fail otherwise. The services can be disabled again after installation.

Name Service Caching Daemon (nscd) and OGFS

If the Name Service Caching Daemon (`nscd`) runs on the same server as the Slice Component bundle, then users cannot open a global shell session with a direct `ssh` connection. If `ncsd` is running on the Slice Component bundle server, the Installer turns it off and runs the `chkconfig nscd off` command to prevent it from starting after a reboot. No action is required.

11. Check the Core Host(s) Time and Locale Requirements

This section discusses the time and locale requirements for SA Core Servers.

Core Time Requirements

Core Servers (either Single Core or Multimaster) and Satellite Core Servers must meet the following requirements. These time requirements do not apply to Managed Servers.

•   All SA Core Servers must have their time zone set to Coordinated Universal Time (UTC).

- All SA Core Servers must maintain synchronized system clocks. Typically, you will synchronize the system clocks through an external server that uses NTP (Network Time Protocol) services.

Linux Time Configuration

To configure the time zone on a Linux server, perform the following tasks:

1 Copy or link

   `/usr/share/zoneinfo/UTC`

   to

   `/etc/localtime`.

2 Ensure that the `/etc/sysconfig/clock` file contains the following lines:

```
ZONE="UTC"
UTC=true
```

Locale Requirements

The servers hosting the Model Repository and the Software Repository (part of the Slice Component bundle) must have the `en_US.UTF-8` locale installed.

To display data from Managed Servers using various locales, the server hosting the Global File System (OGFS) must also have all the locales installed.

For information about enabling non-English locales for Windows patching, see the *SA User Guide: Server Patching*.

To verify whether the `en_US.UTF-8` locale is installed on a server, enter the following command:

```
echo $LANG
```

To define or modify the locale, enter the following values in the `/etc/sysconfig/i18n` file:

```
LANG="en_US.UTF-8"
SUPPORTED="en_US.UTF-8:en_US:en"
```

12. Install the Windows Update Service on Windows Server 2003, 2008, 2008 R2 x64 and 2012

Installation of an SA Agent on a managed server requires the Windows Update service to be installed.

- The Windows Update Service Startup Type configuration should be set to *automatic*.

- If the Windows Update Service Startup Type configuration is set to *manual*, the agent must start the service each time it registers software, performs compliance scans, or remediates packages or patches.

- If the Windows Update Service Startup Type configuration is *disabled*, the agent will not start the service and it will be unable to detect installed and needed patches on the managed server, resulting in a *Scan Failed* during Windows patch compliance scans.

  The Windows Event Log may contain an `{E60687F7-01A1-40AA-86AC-DB1CBF673334}` error as described here:

  http://support.microsoft.com/kb/896224

13. Check the User and Group Requirements For Linux

During installation on Linux servers, the SA Installer creates new users and groups (if you are installing OMDB, its installer also adds a user and group).

These users and groups are:

table 11   Users and Groups Created During an SA/Linux Install

userid	group	home directory	shell
twist	users	/var/opt/opsware/twist	/bin/sh
occ	occ	/var/opt/opsware/occ	/bin/sh
opswgw	opswgw	/var/opt/opsware/ opswgw-<gw name>	/sbin/nologin
**oracle	oinstall	/u01/app/oracle	/bin/bash

**SA-supplied Oracle installation only

14. Check SA Cores on VMs Requirements (optional)

SA Cores are certified for VMware VMs running Red Hat Enterprise Linux 5 (update 2 or later) as the guest operating system. The following sections describe the requirements for installing an SA Core on a VMware VM and provide instructions for doing so.

Supported Hypervisor and Guest Operating Systems

See *SA Support and Compatibility Matrix* provided in the documentation directory of the distribution media or available for download from:

http://support.openview.hp.com/sc/support_matrices.jsp

▶ For a list of supported Oracle versions for the Model Repository, see the *SA Support and Compatibility Matrix.*

VM CPU and Memory Requirements

Table 12 shows the minimum number of CPUs and required memory to run SA Cores on VMs:

table 12   VM CPU and Memory Requirements

Number of VMs	Number of CPUs and RAM for each VM		Number of Managed Servers
	4 CPUs 16GB RAM	4 CPUs 16GB RAM	

table 12   VM CPU and Memory Requirements (cont'd)

Number of VMs	Number of CPUs and RAM for each VM		Number of Managed Servers
1	Infrastructure Component bundle SA Provisioning bundle Slice Component bundle		960
2	Infrastructure Component bundle SA Provisioning bundle Slice 0 Component bundle	Slice 1 Component bundle	2250

➤ SA supports core components installed on VMs only when your VM configurations follow VMware best practices for managing resource allocation and overall workload. You must ensure that other VMs sharing the same ESX hypervisor do not significantly impact the resources available to the VM hosting the SA Core. Should you have performance issues, for troubleshooting purposes, HP support may require you to replicate these issues in an environment in which the VM supporting the SA Core is the sole VM active within the ESX hypervisor.

➤ It is essential that you avoid over-commitment of physical resources (CPU and physical memory) to ensure proper functioning of the VMs. Over-commitment of these resources can lead to performance issues as well as time synchronization issues.

SA Satellite Memory Requirements

Table 13 lists provides the minimum number of CPUs and required memory to run SA Satellites on VMs:

table 13   Satellite CPU and Memory Requirements

Number of VMs	Number of CPUs and RAM for each VM	Number of Managed Servers
	2 CPUs 2 GB RAM	
1	Satellite Components	1500

Hardware Performance Issues

The hardware requirements for Hypervisors running SA Core VMs can vary based on these factors:

- The availability of the physical CPUs and memory in the Hypervisor to support the recommended SA Core VM configuration.
- The number of VMs running concurrently on the physical server.
- The number of servers that the SA Core manages.

- The number and complexity of your concurrent operations.

- The number of concurrent users who can access the SA Command Center.

- The number of facilities in which the SA Core operates.

For more information about improving performance see:

http://www.vmware.com/pdf/VI3.5_Performance.pdf

VMware Virtual Center Requirements

Use of the following Virtual Center features with an SA Core installed on a VM has not been validated and could make it difficult for HP support to diagnose possible problems with your installation if required:

- Snapshots

- Distributed Resource Scheduling (DRS)

- VMotion

- Storage VMotion

- Fault Tolerance

- High Availability (HA)

HP is continuing to validate these advanced Virtual Center features and will announce support when available

SA Core Component VMs on SAN or NAS Devices

Running SA Core Components on VMs is supported if the VM images are run from a local disk or SAN. Running SA Core Components on VMs is not supported if the VM images are stored on NAS devices.

VMware VM Timekeeping Issues

You should be familiar with the guidelines about different timekeeping solutions in the VMware, Inc. document, *Timekeeping in VMware Virtual Machines (VMware® ESX 3.5/ESXi 3.5, VMware Workstation 6.5)*. You should also avoid CPU pressure on VMs as described in that white paper.

VMware Tools

VMware Tools can be installed in the VMs that run SA, but the VMware Tools periodic time synchronization option must be disabled.

Conflicts due to Timekeeping Issues

If the time on the SA Cores in a VMware VM-based Multimaster Mesh get out of synchronization due to the time skew described in the VMware white paper described in VMware VM Timekeeping Issues on page 61, conflicts can occur in the Mesh.

If you find conflicts in your Mesh, you should

— Ensure that you have enabled/configured the Timekeeping solution described in the VMware white paper described in the next section.

— Ensure that your VMware Timekeeping implementation is correctly configured.

For more information about resolving conflicts, see "Model Repository Multimaster Component Conflicts" in the *SA Administration Guide*.

Avoiding Conflicts

You can customize your own timekeeping solution based on the VMware, Inc. document, *Timekeeping best practices for Linux* which can be found at:

http://kb.vmware.com/selfservice/microsites/ search.do?language=en_US&cmd=displayKC&externalId=1006427

We attempt to supply valid URLs but, if this URL has been changed or is unavailable, you can search for the paper by title at *http://www.vmware.com*.

Alternatively, you can use the configuration shown below which has been tested and been shown to work in an SA Core/VMware VM environment.

NTP Settings

1   Add the following entries to the `ntp.conf` file:

   a   `tinker panic 0`

   Instructs NTP not to give up if it sees a large jump in time.This entry must be at the top of the `ntp.conf` file.

   b   `restrict 127.0.0.1`

   Do not use the local clock as a time source.

   c   `restrict default kod nomodify notrap`

   d   `server <NTP_server>`

   (for example, `ntp.dev.opsware.com`)

   e   `driftfile /var/lib/ntp/drift`

2   Comment out the following lines:

   ```
   server 127.127.1.0
   fudge 127.127.1.0 stratum 10
   ```

3   Restart the NTP daemon:

4   Ensure that either VMware Tools periodic time synchronization is disabled or VMware VMtools is not installed (you will still need a method of ensuring the time on the VMs is synchronized).

Installation Procedure for SA Cores Under VMware VMs

SA Core pre-installation requirements, disk space requirements, installation, and post-installation requirements under VMware VMs are the same as those for installation on a physical server. You can use the instructions described in this guide to install an SA Core on an existing VMware VM.

5 SA Core Installation

This section describes the installation tasks for SA Cores. The topics covered include:

- SA Core Installation Overview
- Oracle Database Installation Options
- 1. SA Core with a Local HP-supplied Database
- 2. SA Core with a Remote Customer-supplied Oracle Database
- 3. SA Core with a Remote Model Repository and Remote HP-supplied Database
- 4. SA Core with a Remote Model Repository and HP-supplied Oracle Database and Additional Slice Component Bundles
- 5. SA Core with a Remote Customer-supplied Database and Additional Slice Component Bundles
- 6. SA Core with a Remote Model Repository and HP-supplied Oracle Database, Additional Slice Component Bundles and Satellites
- 7. SA Core with a Remote Customer-supplied Database, Additional Slice Component Bundles and Satellites
- 8. SA First (Primary) Core with a Secondary Core (Multimaster Mesh)
- Installing Additional Slice Component Bundles

➤ You must verify that your SA Core, managed server, and satellite host servers meet the requirements listed in Chapter 4, "Pre-installation System Requirement Checks". If you do not, your installation may fail or core performance may be affected.

SA Core Installation Overview

This section describes how to install an SA Core. This core can be:

- A single (standalone) core that manages servers in a single Facility
- The First (Primary) Core of a Multimaster Mesh installation that consists of the First Core and a Secondary Core that manages servers in multiple Facilities
- A single (standalone) core or First Core installation with distributed Core Components.
- Adding additional Slice Component bundles to an existing SA Core.

Whether you are installing a standalone core or the First Core of a Multimaster Mesh, you must perform the tasks described in this section.

There are certain additional post-installation tasks you may need to perform after installing the core, see Chapter 6, "SA Core Post-Installation Tasks".

▶ If you are installing the First (Primary) Core of a Multimaster Mesh, you must complete the tasks described in 8. SA First (Primary) Core with a Secondary Core (Multimaster Mesh) on page 121 to add additional cores to your mesh. If you have a requirement for more than one Secondary Core in a mesh, you must contact HP Professional Services or a certified HP consultant.

A First Core has all the components required to be the primary core of a Multimaster Mesh. You simply need to add a Secondary Core configured to manage servers and communicate with the First Core. In a Multimaster Mesh installation, a First Core's role is not much different than any other core's role in the mesh, however, it does have additional centralized Core Components that oversee communication between the various cores as well as manage conflicts and load balancing.

Installation Phases

A typical SA Core installation has the following phases:

1   *Before Installation*: Ensure that you:

 - have decided on an appropriate Core Configuration, see Deciding on an SA Core Configuration for your Facility on page 19.

 - ensure that all core host installation prerequisites have been met

 - have the information needed to complete the HPSA Installer interview

 - have all necessary permissions to complete the installation

 - have the SA installation media.

 - invoke the SA Installer only from the *SA Product Software* media or mounted copy

 For more information, see Chapter 4, "Pre-installation System Requirement Checks".

2   *Database Installation*: The Model Repository requires that an Oracle database is installed and available *before* the HPSA Installer is run. You can:

 - Install the *HP-supplied Oracle database* that is provided with the SA product software and installed with the SA Core.

 - Use an *sel-installed Oracle database installation* that you have configured for use with SA. This database must be installed and running before you begin the SA Core installation and reserved for use only by SA.

 - Install a database using the *Oracle Universal Installer* before beginning the SA installation and configure it for use with SA. This database must be only used by SA.

 If you plan to use an existing non-HP-supplied Oracle database installation it must be configured for SA, see Oracle Setup for the Model Repository on page 205).

3   *SA Installation Interview*: When you install an SA Core, you are required to complete the SA Interview during which you are asked to provide the values for certain SA configuration parameters. At the end of the interview, SA automatically saves the configuration information to a *Core Configuration file (CDF)*. This CDF may also be used later during Secondary Core (multimaster Mesh), and Satellite installation and during SA Core upgrades.

4   SA *Core Component Installation*: After you complete the SA Interview, the SA Installer installs the SA Core Components on your host server(s).

5   *After Installation*: You must complete the post-installation tasks. For more information, Chapter 6, "SA Core Post-Installation Tasks".

▶ Should the SA Installer encounter a correctable error, the installation stops. Correct the error and retry the installation. For information about , see Restarting an Interrupted Installation on page 32.

Oracle Database Installation Options

A functioning, properly configured Oracle 12c database must be available *before* you begin the SA installation process. You can choose to:

- See the *SA Support and Compatibility Matrix* for supported Oracle versions.

- Use the SA-supplied Oracle 12c database and allow the SA Installer to install and pre-configure the database. If you choose to install the SA-supplied Oracle database, the SA Installer guides you through the process as described in this chapter.

  The SA-supplied Oracle database requires that certain system and Oracle environment variables be specified for use with SA. See SA-Supplied Oracle RDBMS Software and Database Setup on page 225.

- Use the Oracle Universal Installer to install a non-SA-supplied Oracle 12c database. However, you must manually configure this database for use with SA. For required Oracle configuration information, see Non-SA-Supplied Oracle Software and Database Setup on page 217. If you choose to use the Oracle Universal Installer to install Oracle, you must install the database before running the SA Installer, and have all database-related information required by the Installer Interview, such as passwords, the path to ORACLE_HOME, and so on.

- Use an existing Oracle 12c installation. This database must be for the exclusive use of SA. You must manually configure this database for use with the SA Model Repository. For more information about the required configuration, see Non-SA-Supplied Oracle Software and Database Setup on page 217. You may need to contact your local Oracle DBA for assistance in integrating SA with your pre-existing Oracle database.

- If you are not using a remote Oracle database, the Model Repository component must be installed on the same server as the Oracle database for both First and Secondary Cores.

> The Oracle database must be installed either on its own host or on a server that has the SA Infrastructure Component bundle installed.

FIPS Compliance Options

HP Server Automation (SA) complies with the Federal Information Processing Standards publication 140-2, a security standard that enables government entities to procure equipment that uses validated cryptographic modules. During installation you can choose to enable FIPS by setting the fips.mode parameter to enabled.

When FIPS is enabled, you will be restricted to SHA1 as the hash algorithm. You will be prompted during the installation to specify whether FIPS should be enabled or not.

Under normal security conditions, HP recommends using SHA1with a key length of 2048. Higher security requirements could require FIPS with a key length of 4096 or SHA256. Note that use of FIPS or SHA256 can impact core performance. Contact your Security Administrator for more information.

See Appendix F, "HP SA FIPS 140-2 Compliance Statement".

Enabling IPv6 Networking

To enable IPv6 networking, run the `enable_ipv6.sh` script as a post-installation or upgrade step. This enables IPv6 on HPSA core and satellite gateways and OS provisioning components on SA 10.2 or later releases. The script is available on all infrastructure, slices, boot servers, and satellite systems.

There are two new optional parameters for the enable_ipv6.sh script:

- -i <IPV6 address>: use specified IPV6 address instead of autodiscovered based on hostname DNS AAAA resolution.

- -n : do not start/restart SA components when making configuration file changes.

For more information, see Enabling IPv6 Networking Post-Installation.

For further information about IPv6 and the `enable_ipv6.sh` script, see "SA Remote Communications Administration" in the *SA Administration Guide*.

For information about running the `enable_ipv6.sh` script post-installation, see Enabling IPv6 Networking Post-Installation.

Cryptographic Material Options

SA cryptographic material enables encrypted communications between SA Core Components. SA installs its own cryptographic material. Simply allow SA to generate its own material when prompted during installation.

As of this release, if you want to use cryptographic material from a previous SA installation (SA 10.0 or earlier), you can no longer simply copy the existing crypto file due to enhancements to the way SA handles encryption.

You can, however, copy the crypto file from an existing SA 10.1 or later SA Core. You can do so by copying the crypto file `/var/opt/opsware/crypto/cadb/realm/opsware-crypto.db.e` and the `/etc/opt/opsware/crypto/security.conf` file to the same locations on the server that will host the SA Core or First Core (Multimaster Mesh) before beginning the installation. During installation, do not have the installer generate cryptographic material and when you are prompted, provide the password for this cryptographic material.

Download the SA Installation Files

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

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

Electronic Download Files

(~26.6 GB total size to download)

1   Software_SA_Product_Software_10.20_Part_1_T8900-15063-01.setup

2   Software_SA_Product_Software_10.20_Part_2_T8900-15063-02.tar.gz

3	Software_SA_Product_Software_10.20_Part_3_T8900-15063-03.tar.gz
4	Software_SA_Product_Software_10.20_Part_4_T8900-15063-04.tar.gz
5	Software_SA_Product_Software_10.20_Part_5_T8900-15063-05.tar.gz
6	Software_SA_Product_Software_10.20_Part_6_T8900-15063-06.tar.gz
7	Software_SA_Product_Software_10.20_Part_7_T8900-15063-07.tar.gz
8	Software_SA_Product_Software_10.20_Part_8_T8900-15063-08.tar.gz

Download Verification and Reassembly

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

2   Run the setup script

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

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

— Check the downloaded file integrity

— Assemble the split files

— Extract Server Automation 10.2 bits into a directory called T8900-15063 (~30GB extracted).

— Provide needed information for Server Automation 10.2 Installation and/or Upgrade

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

Server Automation Distribution Contents

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

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

Server Automation Distribution Handling

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

For example:

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

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

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

where:

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

(Optional) Directly Extract SA Distribution via Script

As an alternative to the default SA distribution handling described under Server Automation Distribution Handling on page 67, you can export the Server Automation distribution directory extracted by the setup script and mount at a remote Linux location for remote access (NFS export)

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

For example:

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

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

1. SA Core with a Local HP-supplied Database

This section describes installing all SA components and the HP-supplied Oracle database on the same server. This is the simplest and easiest installation method. You can use the right-hand column to indicate that a phase is completed:

table 14   Core Installation Phases

Phase	Complete
Phase 1: Preparing to Install the SA Core	
Phase 2: Run the SA Installer	
Phase 3: Specify the Core Components Host/Select Installation Type	
Phase 4: Select the Interview Type and Provide SA Parameter Values	
Phase 5: Install the SA Components	

Phase 1: Preparing to Install the SA Core

1   You will need the *SA Product Software* media, the *Agent and Utilities* media and the *Oracle_SA* installation media.

2   The server on which the SA components and the Oracle database are to be installed must be running a supported Red Hat Enterprise Linux or SUSE Enterprise Server Linux operating system. See the *SA Support and Compatibility Matrix*.

3   On the server where you will install SA, mount the *Product Software* media, the *Agent and Utilities* media and the *Oracle_SA* installation media, or NFS-mount a directory that contains a copy of the media contents:

   a   Open a terminal window and log in as auser with root privileges.

   b   Change to the root directory:

      `cd /`

The SA Installer must have *read/write root privileges* to the directories in which the SA components, including NFS-mounted network appliances, are to be installed.

Phase 2: Run the SA Installer

On the server on which you plan to install SA and the Oracle database, run the install script:

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

where `<distro>` is the full path to the mounted media.

You see messages displayed on screen as the SA Installer loads the required files.

Logs for the installation are automatically stored. See Installer Logs on page 34.

Phase 3: Specify the Core Components Host/Select Installation Type

Before SA begins the installation, it performs a prerequisite check that validates that the host on which you are installing SA meets the minimum requirements (see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation can fail or core performance may be negatively effected. If your host fails the prerequisite check or displays warnings, correct the problem(s) or contact your support representative.

1   The following menu displays:

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

Currently specified hosts:
```

`192.168.136.36` (this is the IP address of the host on which the installer is invoked)

```
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 example installation uses the host the installer is invoked on for all Core Components, type `c` and press Enter to continue. You can invoke the installation from a remote machine by selecting `2` to delete the localhost IP address followed by `1` to add the remote host IP address.

2   A screen similar to the following displays:

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

Currently specified hosts:

        192.168.136.36

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):
```

When you are satisfied with the entries, press C to continue.

The SA Installer attempts to set up NFS mounts to the installation media and prepares the server for the installation.

After the host preparation completes, the following menu displays:

3   The following menu displays:

```
Install Type
============

1. Typical Primary Core
2. Custom Primary Core
3. Typical Secondary Core
4. Custom Secondary Core

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

Enter 1 (Typical Primary Core) and Enter to continue.

4   The following menu displays:

```
Oracle Installation
===================

1. Install Oracle with SA
2. Use Existing Oracle Database

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

Enter 1 (Install Oracle with SA) and press Enter to continue.

Phase 4: Select the Interview Type and Provide SA Parameter Values

1 The following menu displays:

```
Interview Type
==============

1. Simple Interview
2. Advanced Interview
3. Expert Interview

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

Enter `1` (Simple Interview) and Enter to continue.

2 You are prompted to supply values for the following SA parameters:

- `opsware_admin user` (`truth.oaPwd`): an SA administrator password (the default username is `admin`).

➤ The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.

- `decrypt_passwd`: A password for the SA cryptographic material.

➤ You will see this prompt only if you are using your own crypto file and not allowing SA to automatically generate the crypto file.

- `truth.dcNm`: A name for your SA facility.

- `crypto.hash_algorithm`: The hashing algorithm [SHA1 or SHA256] for SA cryptographic module

- `crypto.key_length`: the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module.

- `windows_util_loc`: The location for the Microsoft Patching utilities.

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

- `word.store.host`: The IP address of the NFS server for the Software Repository.

- `word.store.path`: The absolute path on the NFS server for Software Repository (`/var/opt/opsware/word`)

For more information about these parameters, see the Appendix B, "SA Core Parameter Reference".

You see these prompts (the prompts display one at a time; after you provide a value and press enter you see a message, `Validating...`, and if the value is acceptable, the next prompt displays:

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

Navigation Keys:
Use <Ctrl>P to go to the previous parameter.
Use <Ctrl>N to go to the next parameter.
Use >Tab> to view help on the current parameter.
Use <Ctrl>C to interrupt the interview.

Parameter 1 of 8 (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password
used to connect to the Oracle database.: []

Parameter 2 of 8 (fips.mode)
Do you want SA to be in FIPS mode? (y/n) [n]: n

Parameter 3 of 8: (crypto.hash_algorithm)
Please enter the hashing algorithm [SHA1 or SHA256] for SA cryptographic
module. [SHA1]:
```

➤ If you enable FIPS mode in Parameter 2 (`Do you want SA to be in FIPS mode? (y/n) [n]: y`), SA automatically sets the value of Parameter 3 to SHA1. If FIPS is not enabled, you can choose between SHA1 or 256.

```
Parameter 4 of 8: (crypto.key_length)
Please enter the key length [2048 or 4096] used for hashing algorithm of SA
cryptographic module. [2048]:

Parameter 5 of 8 (truth.dcNm)
Please enter the short name of the facility where the Opsware Installer is
being run (no spaces).: []

Parameter 6 of 8 (windows_util_loc)
Please enter the directory path containing the Microsoft patching
utilities. Press Ctrl-I for a list of required files or enter "none" if you
do not wish to upload the utilities at this time (none).: []

Parameter 7 of 8 (word.store.host)
Please enter the IP address of the NFS server for the Software Repository.
For satellite installs, please enter the IP address of the Software
Repository Cache. [192.168.136.39]:

Parameter 8 of 8 (word.store.path)
Please enter the absolute path on the NFS server for Software Repository
[/var/opt/opsware/word]:
```

You are asked to re-enter any required passwords for confirmation.

➤ Uploading the Microsoft patching utilities is optional, however, if you expect to have Windows-based managed servers, you should follow the instructions for obtaining these files as described in Chapter 4, "Pre-installation System Requirement Checks".

When you have supplied values for all parameters, the following message displays:

```
All parameters have values.  Do you wish to finish the interview? (y/n):
```

Enter `y` and press Enter to continue. If you enter `n`, you are presented with each parameter again with the value you entered as the default. You can then change the value or accept the default. If you need to exit the installation, press Ctrl-C.

3   You now install the database and SA Components.

Phase 5: Install the SA Components

1   The following screen displays:

```
Install Components
==================

Oracle RDBMS for SA
Model Repository, First Core
Core Infrastructure Components
Slice
OS Provisioning Components
Software Repository - Content (install once per mesh)

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

Enter c and press Enter to begin the prerequisite checks.

➤   Before SA begins the installation, it performs a prerequisite check that validates that the host on which you are installing SA meets the minimum requirements (see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation can fail or core performance may be negatively effected. If your host fails the prerequisite check or displays warnings, correct the problem(s) or contact HP support services.

2   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.

        WARNING Nothing listening at db.host:db.port (ip_address).
                Note: Can be ignored if core install will be performed
                using hpsa_install script.

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 installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core 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 installation.

You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, the Core Description File (CDF) is automatically saved.

Post-Installation Tasks

You must now complete the tasks described in Chapter 6, "SA Core Post-Installation Tasks."

2. SA Core with a Remote Customer-supplied Oracle Database

This section describes installing all SA components on the same host with an existing remote non-HP-supplied Oracle database.

➤ Since this layout uses a customer supplied database, the remote Oracle database must have been installed and configured as described in Non-SA-Supplied Oracle Software and Database Setup on page 217 before you begin the SA Core installation.

You can use the right-hand column to indicate that a phase is completed:

table 15   Core Installation Phases

Phase	Complete
Phase 1: Preparing to Install the SA Core	
Phase 2: Run the SA Installer	
Phase 3: Specify Core Components Host/Select Installation Type	
Phase 4: Select the Interview Type and Provide SA Parameter Values	
Phase 5: Install the SA Components	

Phase 1: Preparing to Install the SA Core

1   You will need the *SA Product Software* media and the *Agent and Utilities* media.

2   The server on which the SA Core Components are to be installed must be running a supported Red Hat Enterprise Linux or SUSE Enterprise Server Linux operating system. See the *SA Support and Compatibility Matrix*.

3   On the server where you will install SA, mount the *Product Software* media and *Agent and Utilities* media or NFS-mount a directory that contains a copy of the media contents:

   a   Open a terminal window and log in asa user with root privileges.

   b   Change to the root directory:

   ```
   cd /
   ```

➤ The SA Installer must have *read/write root privileges*to the directories in which the SA components, including NFS-mounted network appliances are to be installed.

Phase 2: Run the SA Installer

On the server on which you plan to install SA and the Oracle database, run the install script:

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

where `<distro>` is the full path to the mounted media.

You see messages displayed on screen as the SA Installer loads the required files.

Logs for the installation are automatically stored. See Installer Logs on page 34.

Phase 3: Specify Core Components Host/Select Installation Type

➤ Before SA begins the installation, it performs a prerequisite check that validates that the host on which you are installing SA meets the minimum requirements (see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation can fail or core performance may be negatively effected. If your host fails the prerequisite check or displays warnings, correct the problem(s) or contact HP support services.

1 The following menu displays:

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

Currently specified hosts:

192.168.136.36 (this is the IP address of the host on which the installer is invoked)

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 all SA Core Components are to be installed on the current host, if the host you plan to install the core on isn't already listed, enter 1 to add the server's IP address and press Enter.

When you are satisfied with the entries, press C to continue.

At this point, the SA Installer attempts to set up NFS mounts to the installation media and prepare the server for installation.

2 The following menu displays:

```
Install Type
============

1. Typical Primary Core
2. Custom Primary Core
3. Typical Secondary Core
4. Custom Secondary Core

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

Enter 1 (Typical Primary Core) and Enter to continue.

3 The following menu displays:

```
Oracle Installation
===================

1. Install Oracle with SA
2. Use Existing Oracle Database
```

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

Enter 2 (Use Existing Oracle Database) and press Enter to continue.

Phase 4: Select the Interview Type and Provide SA Parameter Values

1   The following menu displays:

```
Interview Type
==============

1. Simple Interview
2. Advanced Interview
3. Expert Interview

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

Enter 1 (Simple Interview) and Enter to continue.

2   You are prompted to supply values for the following SA parameters:

- opsware_admin user (truth.oaPwd): an SA administrator password (the default username is admin).

- crypto.hash_algorithm: The hashing algorithm [SHA1 or SHA256] for SA cryptographic module

- crypto.key_length: the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module.

▶   The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.

- decrypt_passwd: A password for the SA cryptographic material.

▶   You will see this prompt only if you are using your own crypto file and not allowing SA to automatically generate the crypto file.

- truth.dcNm: A name for your SA facility.

- windows_util_loc: The location for the Microsoft Patching utilities.

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

- db.host: the IP address of the remote database server.

- word.store.host: The IP address of the NFS server for the Software Repository.

- word.store.path: The absolute path on the NFS server for Software Repository (/var/opt/opsware/word)

For more information about these parameters, see the Appendix B, "SA Core Parameter Reference".

You see these prompts (the prompts display one at a time; after you provide a value and press enter you see a message, Validating..., and if the value is acceptable, the next prompt displays:

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

Navigation Keys:
Use <Ctrl>P to go to the previous parameter.
Use <Ctrl>N to go to the next parameter.
Use >Tab> to view help on the current parameter.
Use <Ctrl>C to interrupt the interview.

Parameter 1 of 10 (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password
used to connect to the Oracle database.: []

Parameter 2 of 11(fips.mode)
Do you want SA to be in FIPS mode? (y/n) [n]: n

Parameter 3 of 11: (crypto.hash_algorithm)
Please enter the hashing algorithm [SHA1 or SHA256] for SA cryptographic
module. [SHA1]:
```

▶ If you enable FIPS mode in Parameter 2 (Do you want SA to be in FIPS mode? (y/n) [n]: y), SA automatically sets the value of Parameter 3 to SHA1. If FIPS is not enabled, you can choose between SHA1 or 256.

```
Parameter 4 of 11: (crypto.key_length)
Please enter the key length [2048 or 4096] used for hashing algorithm of SA
cryptographic module. [2048]:

Parameter 5 of 11 (decrypt_passwd)
Please enter the password for the cryptographic material.: []

Parameter 6 of 11 (truth.dcNm)
Please enter the short name of the facility where the Opsware Installer is
being run (no spaces).: []

Parameter 7 of 11 (windows_util_loc)
Please enter the directory path containing the Microsoft patching
utilities. Press Ctrl-I for a list of required files or enter "none" if you
do not wish to upload the utilities at this time (none).: []
```

▶ Uploading the Microsoft patching utilities is optional, however, if you expect to have Windows-based managed servers, you should follow the instructions for obtaining these files as described in Chapter 4, "Pre-installation System Requirement Checks".

```
Parameter 8 of 11 (db.host)
Please enter the IP address of the database host: []
```

▶ You see this prompt only when you are using the non-SA supplied Oracle database.

```
Parameter 9 of 11 (truth.servicename)
Please enter the service name of the Model Repository instance in the
facility where Opsware Installer is being run [192.168.136.39]:

Parameter 10 of 11 (word.store.host)
Please enter the IP address of the NFS server for the Software Repository.
For satellite installs, please enter the IP address of the Software
Repository Cache. [192.168.136.39]:

Parameter 11 of 11 (word.store.path)
Please enter the absolute path on the NFS server for Software Repository
[/var/opt/opsware/word]:
```

```
Please enter the service name of the Model Repository instance in the
facility where Opsware Installer is being run [truth.rose2]:
```

You are asked to re-enter any required passwords for confirmation.

When you have supplied values for all parameters, the following message displays:

```
All parameters have values.  Do you wish to finish the interview? (y/n):
```

Enter y and press Enter to continue. If you enter n, you are presented with each parameter again with the value you entered as the default. You can then change the value or accept the default. If you need to exit the installation, press Ctrl-C.

3   You now install the SA Components.

Phase 5: Install the SA Components

1   The following screen displays:

```
Install Components
==============
Model Repository, First Core
Core Infrastructure Components
Slice
OS Provisioning Components
Software Repository - Content (install once per mesh)

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

Enter c and press Enter to begin the prerequisite checks.

➤   Before SA begins the SA component installation, it performs prerequisite checks that validate that the host on which you are installing SA meets the minimum requirements for the installation. The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on. If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem and retry the installation or, if you are unable to resolve the problem, contact HP support services.

2   If the prerequisite check completes successfully, you may still see some 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.

        WARNING Nothing listening at db.host:db.port (ip_address).
                Note: Can be ignored if core install will be performed
                using hpsa_install script.

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 installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core 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 installation.

You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, you the Core Description File (CDF) is automatically saved.

Post-Installation Tasks

You must now complete the tasks described in Chapter 6, "SA Core Post-Installation Tasks."

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

This section describes installing SA components on one host and the Model Repository and an HP-supplied Oracle database on a second host. You can use the right-hand column to indicate that a phase is completed:

table 16　　Core Installation Phases

Phase	Complete
Phase 1: Preparing to Install the SA Core	
Phase 2: Run the SA Installer	
Phase 3: Specify the Core Component Hosts	
Phase 4: Select the Installation Type	
Phase 5: Select the Interview Type and Provide SA Parameter Values	
Phase 6: Install the SA Components	

➤ The remote Oracle database must have been configured as described in SA-Supplied Oracle RDBMS Software and Database Setup on page 225 before you begin the SA Core installation.

Phase 1: Preparing to Install the SA Core

1　You will need the *SA Product Software* media, *Agent and Utilities* media and the *Oracle_SA* installation media.

2　The servers on which the SA Core Components and the Oracle Database are to be installed must be running a supported Red Hat Enterprise Linux or SUSE Enterprise Server Linux operating system. See the *SA Support and Compatibility Matrix*.

3　On the server where you will install the SA, mount the *Product Software* media, *Agent and Utilities* media and the *Oracle_SA* media, or NFS-mount a directory that contains a copy of the media contents:

　　a　Open a terminal window and log in as a user with root privileges.

   b   Change to the root directory:

```
cd /
```

➤   The SA Installer must have *read/write root privileges* to the directories in which the SA components, including NFS-mounted network appliances are to be installed.

Phase 2: Run the SA Installer

On the server on which you plan to install SA and the Oracle database, run the install script:

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

where `<distro>` is the full path to the mounted media.

You see messages displayed on screen as the SA Installer loads the required files.

Logs for the installation are automatically stored. See

Phase 3: Specify the Core Component Hosts

➤   Before SA begins the installation, it performs a prerequisite check that validates that the host on which you are installing SA meets the minimum requirements (see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation can fail or core performance may be negatively effected. If your host fails the prerequisite check or displays warnings, correct the problem(s) or contact HP support services.

For this example installation, we'll use two servers for the core component installation. You will, of course, modify this value for your particular system requirements. Components will be installed as follows:

table 17   **Core Component Layout**

Server	Core Component to be Installed
192.168.136.36	Oracle database and Model Repository
192.168.136.39	Multimaster Infrastructure Components
	Software Repository Storage and Content
	SA Provisioning Media Server
	SA Provisioning Boot Server, Slice version

1   You see this screen:

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

Currently specified hosts:
```

`192.168.136.36` (this is the IP address of the host on which the installer is invoked)

```
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): 1

Enter number of hosts to add:
```

At this point, the host on which the install script was invoked should be listed by default.

2   You are asked to specify the number of hosts that will be involved in the installation:

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

Enter the appropriate number. For this example, we use two hosts, the default host and one we add:

```
Enter number of hosts to add: 1
```

3   The following screen displays:

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

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

Enter the hostname or IP address of the server that will host the Model Repository and Oracle database and press Enter.

You see this message:

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

Enter Y to continue.

For this example, we add the host:

•   192.168.136.39

4   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):
```

Note that 192.168.136.39 is now listed.

5   At this point you can press 2 to delete a host or 1 to add/edit a hostname/IP address. When you choose 1 for an existing list of hosts, you see this prompt:

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

When you are satisfied with the entries, press C to continue.

6 You are asked to provide the passwords for each added host:

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

Parameter 1 of 1

192.168.136.39 password []:
```

Type the password (which is obfuscated) and press Enter. SA validates the password. After you provide all required passwords, you see the message:

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

Enter Y and press Enter to continue.

After you provide all required passwords, the SA Installer attempts to set up NFS mounts to the installation media and prepares each specified server for the installation.

Phase 4: Select the Installation Type

1 After the SA Installation media is mounted for all servers, the following menu displays:

```
Install Type
============
1. Typical Primary Core
2. Custom Primary Core
3. Typical Secondary Core
4. Custom Secondary Core

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

Enter 2 (Custom Primary Core) and Enter to continue.

2 The following menu displays:

```
Oracle Installation
===================

1. Install Oracle with SA
2. Use Existing Oracle Database

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

Enter 1 (Install Oracle with SA) and Enter to continue.

3 The following is displayed:

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

1. Oracle Database and Model Repository, First Core
2. Multimaster Infrastructure Components
3. Software Repository Storage and Content
4. Slice
5. OS Provisioning Media Server
6. OS Provisioning Boot Server, Slice version

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

Note that no host (IP address) is associated with the components.

You now must associate the core components with the servers (IP addresses) they are to be installed on. To do so, you enter the component's number at the prompt. For example, enter 1 to add the host for the Model Repository, enter 2 for the Multimaster Infrastructure Components, and so on.

4   Screens similar to the following display as you assign component hosts:

```
Host Assignment for Model Repository, First Core
=========================================================

1. 192.168.136.36
2. 192.168.136.39

Enter the number of the host or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): 1
```

Enter 1 to specify 192.168.136.36 for the Model Repository and database. You are returned to the Host Component Layout screen and can select the next component and assign its host. Do the same for all remaining components.

When you have assigned hosts for all components, you see a screen similar to this:

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

1. Oracle Database and Model Repository [192.168.136.36]
2. Multimaster Infrastructure Components [192.168.136.39]
3. Software Repository Storage and Content [192.168.136.39]
4. Slice [192.168.136.39]
5. OS Provisioning Media Server [192.168.136.39]
6. OS Provisioning Boot Server, Slice version [192.168.136.39]

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

Note that the Slice Component bundle (option 4) can have multiple host IP addresses as the Slice components can have multiple instances to improve performance.

Enter c and press Enter to continue.

Phase 5: Select the Interview Type and Provide SA Parameter Values

1   The following menu displays:

```
Interview Type
==============

1. Simple Interview
2. Advanced Interview
3. Expert Interview

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

Enter 1 (Simple Interview) and Enter to continue.

2   You are prompted to supply values for the following SA parameters:

- opsware_admin user (truth.oaPwd): an SA administrator password (the default username is admin).

- crypto.hash_algorithm: The hashing algorithm [SHA1 or SHA256] for SA cryptographic module

- `crypto.key_length`: the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module.

The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.

- `decrypt_passwd`: A password for the SA cryptographic material.

▶ You will see this prompt only if you are using your own crypto file and not allowing SA to automatically generate the crypto file.

- `truth.dcNm`: A name for your SA facility.

- `word.store.host`: The IP address of the NFS server for the Software Repository.

- `word.store.path`: The absolute path on the NFS server for Software Repository (`/var/opt/opsware/word`)

For more information about these parameters, see the Appendix B, "SA Core Parameter Reference".

You see these prompts (the prompts display one at a time; after you provide a value and press enter you see a message, `Validating...`, and if the value is acceptable, the next prompt displays:

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

Navigation Keys:
Use <Ctrl>P to go to the previous parameter.
Use <Ctrl>N to go to the next parameter.
Use >Tab> to view help on the current parameter.
Use <Ctrl>C to interrupt the interview.

Parameter 1 of 9 (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password
used to connect to the Oracle database.: []

Parameter 2 of 9 (fips.mode)
Do you want SA to be in FIPS mode? (y/n) [n]: n

Parameter 3 of 9: (crypto.hash_algorithm)
Please enter the hashing algorithm [SHA1 or SHA256] for SA cryptographic
module. [SHA1]:
```

▶ If you enable FIPS mode in Parameter 2 (`Do you want SA to be in FIPS mode? (y/n) [n]: y`), SA automatically sets the value of Parameter 3 to SHA1. If FIPS is not enabled, you can choose between SHA1 or 256.

```
Parameter 4 of 9: (crypto.key_length)
Please enter the key length [2048 or 4096] used for hashing algorithm of SA
cryptographic module. [2048]:

Parameter 5 of 9 (decrypt_passwd)
Please enter the password for the cryptographic material.: []
```

▶ You will see this prompt only if you are using your own crypto file and not allowing SA to automatically generate the crypto file.

```
Parameter 6 of 9 (truth.dcNm)
Please enter the short name of the facility where the Opsware Installer is
being run (no spaces).: []
```

```
Parameter 7 of 9 (windows_util_loc)
Please enter the directory path containing the Microsoft patching
utilities. Press Ctrl-I for a list of required files or enter "none" if you
do not wish to upload the utilities at this time (none).: []

Parameter 8 of 9 (word.store.host)
Please enter the IP address of the NFS server for the Software Repository.
For satellite installs, please enter the IP address of the Software
Repository Cache. [192.168.136.39]:

Parameter 9 of 9 (word.store.path)
Please enter the absolute path on the NFS server for Software Repository
[/var/opt/opsware/word]:
```

You are asked to re-enter any required passwords for confirmation.

► Uploading the Microsoft patching utilities is optional, however, if you expect to have Windows-based managed servers, you should follow the instructions for obtaining these files as described in Chapter 4, "Pre-installation System Requirement Checks".

When you have supplied values for all parameters, the following message displays:

```
All parameters have values.  Do you wish to finish the interview? (y/n):
```

Enter y and press Enter to continue. If you enter n, you are presented with each parameter again with the value you entered as the default. You can then change the value or accept the default. If you need to exit the installation, press Ctrl-C.

3 You are now ready to begin the database and SA Component installation.

Phase 6: Install the SA Components

1 A screen similar to the following displays:

```
Install components
==================
Oracle RDBMS for SA                                 : 192.168.136.36
Model Repository, First Core                        : 192.168.136.36
Core Infrastructure Components          : 192.168.136.39
Slice                                               : 192.168.136.39
OS Provisioning Components                          : 192.168.136.39
Software Repository - Content (install once per mesh): 192.168.136.39

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

Enter c and press Enter to begin the prerequisite checks.

► If the server that will host your Slice Component bundle has more than one network interface installed, SA will detect the presence of two NICs and display a screen similar to the following:

```
Slice Network Interface Configuration
=====================================


Parameter 1 of 2 (Slice: 192.168.136.38)


Please select the interface to use for 192.168.136.38


1) eth2      -- 192.168.136.55
2) eth1      -- 192.168.136.77
3) eth0      -- 192.168.136.38  (default)
```

```
 [3]:

Parameter 2 of 2 (Slice: 192.168.136.41)

Please select the interface to use for 192.168.136.41

1) eth0      -- 192.168.136.41  (default)
2) eth2      -- 192.168.136.54
3) eth1      -- 192.168.136.76
 [1]:
```

Select the appropriate network interface for each host by entering the associated number from the list.

When you have configured all interfaces, you see the message:

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

Enter y and press Enter to continue. You can edit the list again by pressing n and Enter.

2   The prerequisite check begins.

➤   Before SA begins the SA component installation, it performs prerequisite checks that validate that the host on which you are installing SA meets the minimum requirements for the installation. The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on. If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem and retry the installation or, if you are unable to resolve the problem, contact HP support services.

3   If the prerequisite check completes successfully, you may still see some 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.

        WARNING Nothing listening at db.host:db.port (ip_address).
               Note: Can be ignored if core install will be performed
               using hpsa_install script.

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 installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core 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 installation.

4   You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, you the Core Description File (CDF) is automatically saved.

Upon completion, a message displays indicating successful installation.

Post-Installation Tasks

You must now complete the tasks described in

4. SA Core with a Remote Model Repository and HP-supplied Oracle Database and Additional Slice Component Bundles

This section describes installing SA Core Components on one host, and installing the Model Repository and an HP-supplied Oracle database on a second host. You can use the right-hand column to indicate that a phase is completed:

table 18   Core Installation Phases

Phase	Complete
Phase 1: Preparing to Install the SA Core	
Phase 2: Run the SA Installer	
Phase 3: Specify the Core Component Hosts	
Phase 4: Select the Installation Type	
Phase 5: Select the Interview Type and Provide SA Parameter Values	
Phase 6: Install the SA Components	

➤   The remote Oracle database must have been configured as described in SA-Supplied Oracle RDBMS Software and Database Setup on page 225 before you begin the SA Core installation.

Phase 1: Preparing to Install the SA Core

1   You will need the *SA Product Software* media, the *Agent and Utilities* media and the *Oracle_SA* installation media.

2   The servers on which the SA Core Components and the Oracle database are to be installed must be running a supported Red Hat Enterprise Linux or SUSE Enterprise Server Linux operating system. See the *SA Support and Compatibility Matrix*.

3   On the server where you will install SA, mount the *Product Software* media and the *Agent and Utilities* media, or NFS-mount a directory that contains a copy of the media contents.

4   Open a terminal window and log in asa user with root privileges.

5   Change to the root directory:

```
cd /
```

> The SA Installer must have *read/write root privileges* to the directories in which the SA components, including NFS-mounted network appliances are to be installed.

Phase 2: Run the SA Installer

On a server on which you plan to install SA components, run the install script:

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

where `<distro>` is the full path to the mounted media.

You see messages displayed on screen as the SA Installer loads the required files.

Logs for the installation are automatically stored. See Installer Logs on page 34.

Phase 3: Specify the Core Component Hosts

> Before SA begins the installation, it performs a prerequisite check that validates that the host on which you are installing SA meets the minimum requirements (see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation can fail or core performance may be negatively effected. If your host fails the prerequisite check or displays warnings, correct the problem(s) or contact HP support services.

For this example installation, we'll use six remote servers for the core component installation. You will, of course, modify this for your particular system requirements. Components will be installed as follows:

table 19   Core Component Layout

Server	Core Component to be Installed
192.168.136.36	Oracle database and Model Repository
192.168.136.39	Multimaster Infrastructure Components Software Repository Storage and Content SA Provisioning Media Server SA Provisioning Boot Server, Slice version
192.168.136.40	Slice 0
192.168.136.41	Slice 1
192.168.136.42	Slice 2

1 After running the install script you see this screen:

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

Currently specified hosts:

192.168.136.36 (this is the IP address of the host on which the installer is invoked)

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): 1

Enter number of hosts to add:
```

At this point, the host on which the install script was invoked should be listed by default. Enter 1 to add the IP addresses for the other hosts to be used in this installation and press Enter.

2 You are asked to specify the number of hosts that will be involved in the installation:

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

Enter the appropriate number. For this example, we add four additional hosts:

```
Enter number of hosts to add: 4
```

3 The following screen displays:

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

Parameter 1 of 4
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 all remaining servers. You see this message:

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

Enter Y to continue.

For this example, we add the hosts:

- **192.168.136.39**

- **192.168.136.40**

- **192.168.136.41**

- **192.168.136.42**

4 A screen similar to the following displays:

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

Currently specified hosts:

        192.168.136.36
        192.168.136.39
        192.168.136.40
        192.168.136.41
        192.168.136.42
```

```
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):
```

5   At this point you can press 2 to delete a host or 1 to add/edit a hostname/IP address. When you choose 1 for an existing list of hosts, you see this prompt:

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

When you are satisfied with the entries, press C to continue.

6   You are asked to provide the passwords for the added hosts:

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

Parameter 1 of 4

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

Type the password (which is obfuscated) and press Enter. SA validates the password. 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.

After you provide all required passwords, the SA Installer attempts to set up NFS mounts to the installation media and prepares each specified server for the installation.

Phase 4: Select the Installation Type

1   The following menu displays:

```
Install Type
============

1. Typical Primary Core
2. Custom Primary Core
3. Typical Secondary Core
4. Custom Secondary Core

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

Enter 1 (Typical Primary Core) and Enter to continue.

2   The following menu displays:

```
Oracle Installation
===================

1. Install Oracle with SA
2. Use Existing Oracle Database

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

Enter 2 (Use Existing Oracle Database) and Enter to continue.

3   The following is displayed:

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

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

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

Note that no host (IP address) is associated with the components.

4   You now must associate the core components with the servers (IP addresses) they are to be installed on. To do so, you enter the component's number at the prompt. For example, enter 1 to add the host for the Model Repository, enter 2 for the Multimaster Infrastructure Components, and so on.

5   Screens similar to the following display as you assign component hosts:

```
Host Assignment for Model Repository, First Core
================================================================

1. 192.168.136.36
2. 192.168.136.39
3. 192.168.136.40
4. 192.168.136.41
5. 192.168.136.42

Enter the number of the host or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): 1
```

Enter 1 to select 192.168.136.36 for the Model Repository. You are returned to the Host Component Layout screen and can select the next component and assign its host. Do the same for all remaining components.

When you have assigned hosts for all components, you see a screen similar to this:

```
Install Components
==================
1. Model Repository, First Core                  :192.168.136.36
2. Multimaster Infrastructure Components         :192.168.136.39
3. Software Repository Storage and Content       :192.168.136.39
4. Slice                                         :192.168.136.40,
                                                  192.168.136.41,
                                                  192.168.136.42
5. OS Provisioning Media Server                  :192.168.136.39
6. OS Provisioning Boot Server, Slice version    :192.168.136.39

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

Note that the Slice Component bundle (option 4) has multiple host IP addresses listed as the Slice components can have multiple instances to improve performance.

Enter c and press Enter to continue.

Phase 5: Select the Interview Type and Provide SA Parameter Values

1   The following menu displays:

```
Interview Type
==============

1. Simple Interview
2. Advanced Interview
3. Expert Interview

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

Enter 1 (Simple Interview) and Enter to continue.

2   You are prompted to supply values for the following SA parameters:

- opsware_admin user (truth.oaPwd): an SA administrator password (the default username is admin).

- crypto.hash_algorithm: The hashing algorithm [SHA1 or SHA256] for SA cryptographic module

- crypto.key_length: the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module.

The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.

- decrypt_passwd: A password for the SA cryptographic material.

➤ You will see this prompt only if you are using your own crypto file and not allowing SA to automatically generate the crypto file.

- truth.dcNm: A name for your SA facility.

- word.store.host: The IP address of the NFS server for the Software Repository.

- word.store.path: The absolute path on the NFS server for Software Repository (/var/opt/opsware/word)

- db.host: the IP address of the database server.

For more information about these parameters, see the Appendix B, "SA Core Parameter Reference".

You see these prompts (the prompts display one at a time; after you provide a value and press enter you see a message, Validating..., and if the value is acceptable, the next prompt displays:

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

Navigation Keys:
Use <Ctrl>P to go to the previous parameter.
Use <Ctrl>N to go to the next parameter.
Use >Tab> to view help on the current parameter.
Use <Ctrl>C to interrupt the interview.

Parameter 1 of 11 (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password
used to connect to the Oracle database.: []

Parameter 2 of 11 (fips.mode)
Do you want SA to be in FIPS mode? (y/n) [n]: n
```

```
Parameter 3 of 11: (crypto.hash_algorithm)
Please enter the hashing algorithm [SHA1 or SHA256] for SA cryptographic
module. [SHA1]:
```

➤ **If you enable FIPS mode in Parameter 2 (**`Do you want SA to be in FIPS mode? (y/n) [n]: y`), SA automatically sets the value of Parameter 3 to SHA1. If FIPS is not enabled, you can choose between SHA1 or 256.

```
Parameter 4 of 11: (crypto.key_length)
Please enter the key length [2048 or 4096] used for hashing algorithm of SA
cryptographic module. [2048]:

Parameter 5 of 11 (decrypt_passwd)
Please enter the password for the cryptographic material.: []

Parameter 6 of 11 (truth.dcNm)
Please enter the short name of the facility where the Opsware Installer is
being run (no spaces).: []

Parameter 7 of 11 (windows_util_loc)
Please enter the directory path containing the Microsoft patching
utilities. Press Ctrl-I for a list of required files or enter "none" if you
do not wish to upload the utilities at this time (none).: []

Parameter 8 of 11 (word.store.host)
Please enter the IP address of the NFS server for the Software Repository.
For satellite installs, please enter the IP address of the Software
Repository Cache. [192.168.136.39]:

Parameter 9 of 11 (word.store.path)
Please enter the absolute path on the NFS server for Software Repository [/
var/opt/opsware/word]:

Parameter 10 of 11 (db.host)
Please enter the IP address of the database server.

Parameter 11 of 11 (truth.servicename)
Please enter the service name of the Model Repository instance in the
facility where Opsware Installer is being run [192.168.136.36]:
```

You are asked to re-enter any required passwords for confirmation.

➤ Uploading the Microsoft patching utilities is optional, however, if you expect to have Windows-based managed servers, you should follow the instructions for obtaining these files as described in Chapter 4, "Pre-installation System Requirement Checks".

When you have supplied values for all parameters, the following message displays:

```
All parameters have values.  Do you wish to finish the interview? (y/n):
```

Enter `y` and press Enter to continue. If you enter `n`, you are presented with each parameter again with the value you entered as the default. You can then change the value or accept the default. If you need to exit the installation, press Ctrl-C.

3 You are now ready to begin the database and SA Component installation.

Phase 6: Install the SA Components

1 A screen similar to the following displays:

```
Install components
==================
Model Repository, First Core                   : 192.168.136.36
Multimaster Infrastructure Components          : 192.168.136.39
Software Repository Storage                     : 192.168.136.39
Slice                                          : 192.168.136.40, 192.168.136.41, 192.168.136.42
OS Provisioning Media Server                   : 192.168.136.39
OS Provisioning Boot Server, Slice version     : 192.168.136.39
Software Repository - Content (install once per mesh): 192.168.136.39

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

Enter c and press Enter to begin the prerequisite checks.

➤ If the server that will host your Slice Component bundle has more than one network interface installed, SA will detect the presence of two NICs and display a screen similar to the following:

```
Slice Network Interface Configuration
=====================================

Parameter 1 of 2 (Slice: 192.168.136.38)

Please select the interface to use for 192.168.136.38

1) eth2      -- 192.168.136.55
2) eth1      -- 192.168.136.77
3) eth0      -- 192.168.136.38  (default)
 [3]:

Parameter 2 of 2 (Slice: 192.168.136.41)

Please select the interface to use for 192.168.136.41

1) eth0      -- 192.168.136.41  (default)
2) eth2      -- 192.168.136.54
3) eth1      -- 192.168.136.76
 [1]:
```

Select the appropriate network interface for each host by entering the associated number from the list.

When you have configured all interfaces, you see the message:

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

Enter y and press Enter to continue. You can edit the list again by pressing n and Enter.

2 The prerequisite check begins.

➤ Before SA begins the SA component installation, it performs prerequisite checks that validate that the host on which you are installing SA meets the minimum requirements for the installation. The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on. If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem and retry the installation or, if you are unable to resolve the problem, contact HP support services.

3 If the prerequisite check completes successfully, you may still see some 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.

        WARNING Nothing listening at db.host:db.port (ip_address).
               Note: Can be ignored if core install will be performed
               using hpsa_install script.

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 installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core 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 installation.

4 You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, you the Core Description File (CDF) is automatically saved.

Upon completion, a message displays indicating successful installation.

Post-Installation Tasks

You must now complete the tasks described in Chapter 6, "SA Core Post-Installation Tasks."

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

This section describes installing all SA components on one host with an existing remote customer-supplied Oracle database that you have installed yourself and additional Slice Component bundle instances. You can use the right-hand column to indicate that a phase is completed:

table 20   Core Installation Phases

Phase	Complete
Phase 1: Prepare to Install the SA Core	
Phase 2: Run the SA Installer	
Phase 3: Specify the Core Component Hosts	

table 20   Core Installation Phases

Phase	Complete
Phase 4: Select the Installation Type	
Phase 5: Select the Interview Type and Provide SA Parameter Values	
Phase 6: Install the SA Components and the Oracle Database	

➤ The remote Oracle database must have been configured as described in Non-SA-Supplied Oracle Software and Database Setup on page 217 before you begin the SA Core installation.

Phase 1: Prepare to Install the SA Core

1 You will need the *SA Product Software* media and the *Agent and Utilities* media.

2 The servers on which the SA Core Components are to be installed must be running a supported Red Hat Enterprise Linux or SUSE Enterprise Server Linux operating system.

3 On the server where you will install the SA Core, mount the *Product Software* media and the *Agent and Utilities* media, or NFS-mount a directory that contains a copy of the media contents:

   a Open a terminal window and log in asa user with root privileges.

   b Change to the root directory:

   ```
   cd /
   ```

➤ The SA Installer must have *read/write root privileges* to the directories in which the SA components, including NFS-mounted network appliances are to be installed.

Phase 2: Run the SA Installer

On a server on which you plan to install SA components, run the install script:

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

where `<distro>` is the full path to the mounted media.

You see messages displayed on screen as the SA Installer loads the required files. Logs for the installation are automatically stored. See Installer Logs on page 34.

Phase 3: Specify the Core Component Hosts

➤ Before SA begins the installation, it performs a prerequisite check that validates that the host on which you are installing SA meets the minimum requirements (see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation can fail or core performance may be negatively effected. If your host fails the prerequisite check or displays warnings, correct the problem(s) or contact HP support services.

For this example installation, we'll use four hosts for the core component installation. You will, of course, modify this for your particular system requirements. Components will be installed as follows:

table 21   Core Component Layout

Server	Core Component to be Installed
192.168.136.39	Model Repository
192.168.136.39	Multimaster Infrastructure Components
192.168.136.39	Software Repository Storage and Content
192.168.136.40, 192.168.136.41, 192.168.136.42	Slice
192.168.136.39	SA Provisioning Media Server
192.168.136.39	SA Provisioning Boot Server, Slice version

1   You see this screen:

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

`192.168.136.39` (this is the IP address of the host on which the installer is invoked)

```
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): 1

Enter number of hosts to add:
```

2   You are asked to specify the number of hosts that will be involved in the installation:

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

Enter the appropriate number. For this example, we add three hosts in addition to the default host:

```
Enter number of hosts to add: 3
```

3   The following screen displays:

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

Parameter 1 of 3
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 all remaining servers. You see this message:

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

Enter Y to continue.

For this example, we add the hosts:

- 192.168.136.40
- 192.168.136.41
- 192.168.136.42

4 A screen similar to the following displays:

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

Currently specified hosts:

        192.168.136.39
        192.168.136.40
        192.168.136.41
        192.168.136.42

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):
```

5 At this point you can press 2 to delete a host or 1 to add/edit a hostname/IP address. When you choose 1 for an existing list of hosts, you see this prompt:

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

When you are satisfied with the entries, press C to continue.

6 You are asked to provide the passwords for each host in the list shown in Step 4:

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

Parameter 1 of 3

192.168.136.40 password []:*****
```

You are prompted for the password for each specified host. 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.

After you provide all required passwords, the SA Installer attempts to set up NFS mounts to the installation media and prepares each specified server for the installation.

Phase 4: Select the Installation Type

1 After the SA Installation media is mounted for all servers, the following menu displays:

```
Install Type
============

1. Typical Primary Core
2. Custom Primary Core
3. Typical Secondary Core
4. Custom Secondary Core

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

Enter 1 (Typical Primary Core) and Enter to continue.

2   The following menu displays:

```
Oracle Installation
===================

1. Install Oracle with SA
2. Use Existing Oracle Database

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

Enter 2 (Use Existing Oracle Database) and Enter to continue.

3   The following is displayed:

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

1. Model Repository, First Core
2. Infrastructure and Software Repository Content
3. Slice
4. OS Provisioning Components

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

Note that no host (IP address) is associated with the components.

4   You now must associate the core components with the servers (IP addresses) they are to be installed on. To do so, you enter the component's number at the prompt. For example, enter 1 to add the host for the Oracle database and the Model Repository, enter 2 for the Multimaster Infrastructure Components, and so on.

5   Screens similar to the following display as you assign component hosts:

```
Host Assignment for Model Repository, First Core
============================================================

1. 192.168.136.39
2. 192.168.136.40
3. 192.168.136.41
4. 192.168.136.42

Enter the number of the host or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): 1
```

Enter 1 to select 192.168.136.39 for the Model Repository. You are returned to the Host Component Layout screen and can select the next component and assign its host. Do the same for all remaining components.

When you have assigned hosts for all components, you see a screen similar to this:

```
Install Components
==================
1. Model Repository, First Core                :192.168.136.39
2. Multimaster Infrastructure Components:       :192.168.136.39
3. Software Repository Storage and Content      :192.168.136.39
4. Slice                                        :192.168.136.40,
                                                 192.168.136.41,
                                                 192.168.136.42
5. OS Provisioning Media Server:                :192.168.136.39
6. OS Provisioning Boot Server, Slice version:  :192.168.136.39


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

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

Note that the Slice Component bundle (option 4) has multiple host IP addresses listed as the Slice components can have multiple instances to improve performance.

Enter `c` and press Enter to continue.

Phase 5: Select the Interview Type and Provide SA Parameter Values

1   The following menu displays:

```
Interview Type
==============

1. Simple Interview
2. Advanced Interview
3. Expert Interview

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

Enter `1` (Simple Interview) and Enter to continue.

2   You are prompted to supply values for the following SA parameters:

- `opsware_admin user` (`truth.oaPwd`): an SA administrator password (the default username is `admin`).

- `crypto.hash_algorithm`: The hashing algorithm [SHA1 or SHA256] for SA cryptographic module

- `crypto.key_length`: the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module.

➤ The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.

- `decrypt_passwd`: A password for the SA cryptographic material.

➤ You will see this prompt only if you are using your own crypto file and not allowing SA to automatically generate the crypto file.

- `truth.dcNm`: A name for your SA facility.

- `word.store.host`: The IP address of the NFS server for the Software Repository.

- `word.store.path`: The absolute path on the NFS server for Software Repository (`/var/opt/opsware/word`)

- `db.host`: the IP address of the database server.

For more information about these parameters, see the Appendix B, "SA Core Parameter Reference".

You see these prompts (the prompts display one at a time; after you provide a value and press enter you see a message, `Validating...`, and if the value is acceptable, the next prompt displays:

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

```
Navigation Keys:
Use <Ctrl>P to go to the previous parameter.
Use <Ctrl>N to go to the next parameter.
Use >Tab> to view help on the current parameter.
Use <Ctrl>C to interrupt the interview.

Parameter 1 of 12 (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password
used to connect to the Oracle database.: []

Parameter 2 of 12 (fips.mode)
Do you want SA to be in FIPS mode? (y/n) [n]: n

Parameter 3 of 12: (crypto.hash_algorithm)
Please enter the hashing algorithm [SHA1 or SHA256] for SA cryptographic
module. [SHA1]:
```

➤ If you enable FIPS mode in Parameter 2 (Do you want SA to be in FIPS mode? (y/n) [n]: y),
SA automatically sets the value of Parameter 3 to SHA1. If FIPS is not enabled, you can choose between
SHA1 or 256.

```
Parameter 4 of 12: (crypto.key_length)
Please enter the key length [2048 or 4096] used for hashing algorithm of SA
cryptographic module. [2048]:

Parameter 5 of 12 (decrypt_passwd)
Please enter the password for the cryptographic material.: []

Parameter 6 of 12 (truth.dcNm)
Please enter the short name of the facility where the Opsware Installer is
being run (no spaces).: []

Parameter 7 of 12 (windows_util_loc)
Please enter the directory path containing the Microsoft patching
utilities. Press Ctrl-I for a list of required files or enter "none" if you
do not wish to upload the utilities at this time (none).: []

Parameter 8 of 12 (db.host)
Please enter the IP address of the database server: []
```

➤ You see this prompt only when you are using a remote, customer installed Oracle database.

```
Parameter 9 of 12 (truth.servicename)
Please enter the service name of the Model Repository instance in the
facility where Opsware Installer is being run [truth.rose2]:

Parameter 10 of 12 (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]: /u01/app/oracle/
product/12.1.0/client_1/

Parameter 11 of 12 (word.store.host)
Please enter the IP address of the NFS server for the Software Repository.
For satellite installs, please enter the IP address of the Software
Repository Cache. [192.168.136.39]:

Parameter 12 of 12 (word.store.path)
Please enter the absolute path on the NFS server for Software Repository [/
var/opt/opsware/word]:
```

You are asked to re-enter any required passwords for confirmation.

> Uploading the Microsoft patching utilities is optional, however, if you expect to have Windows-based managed servers, you should follow the instructions for obtaining these files as described in Chapter 4, "Pre-installation System Requirement Checks"

When you have supplied values for all parameters, the following message displays:

```
All parameters have values.  Do you wish to finish the interview? (y/n):
```

Enter y and press Enter to continue. If you enter n, you are presented with each parameter again with the value you entered as the default. You can then change the value or accept the default. If you need to exit the installation, press Ctrl-C.

3   You are now ready to begin the SA Component installation.

Phase 6: Install the SA Components and the Oracle Database

1   A screen similar to the following displays:

```
Install components

==================
Model Repository, First Core                     : 192.168.136.39
Multimaster Infrastructure Components            : 192.168.136.39
Software Repository Storage                      : 192.168.136.39
Slice                                            : 192.168.136.40, 192.168.136.41, 192.168.136.42
OS Provisioning Media Server                     : 192.168.136.39
OS Provisioning Boot Server, Slice version       : 192.168.136.39
Software Repository - Content (install once per mesh): 192.168.136.39

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

Enter c and press Enter to begin the prerequisite checks.

> If the server that will host your Slice Component bundle has more than one network interface installed, SA will detect the presence of two NICs and display a screen similar to the following:

```
Slice Network Interface Configuration
=====================================


Parameter 1 of 2 (Slice: 192.168.136.38)


Please select the interface to use for 192.168.136.38


1) eth2      -- 192.168.136.55
2) eth1      -- 192.168.136.77
3) eth0      -- 192.168.136.38  (default)
 [3]:


Parameter 2 of 2 (Slice: 192.168.136.41)


Please select the interface to use for 192.168.136.41


1) eth0      -- 192.168.136.41  (default)
2) eth2      -- 192.168.136.54
3) eth1      -- 192.168.136.76
 [1]:
```

Select the appropriate network interface for each host by entering the associated number from the list.

When you have configured all interfaces, you see the message:

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

Enter `y` and press Enter to continue. You can edit the list again by pressing `n` and Enter.

2 The prerequisite check begins.

➤ Before SA begins the installation, it performs prerequisite checks that validate that the host on which you are installing SA meets the minimum requirements for the installation (see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem and retry the installation or, if you are unable to resolve the problem, contact HP support services.

3 If the prerequisite check completes successfully, you may still see some 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.

        WARNING Nothing listening at db.host:db.port (ip_address).
                Note: Can be ignored if core install will be performed
                using hpsa_install script.

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 installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core 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 installation.

4 You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, you the Core Description File (CDF) is automatically saved.

Upon completion, a message displays indicating successful installation.

Post-Installation Tasks

You must now complete the tasks described in Chapter 6, "SA Core Post-Installation Tasks."

6. SA Core with a Remote Model Repository and HP-supplied Oracle Database, Additional Slice Component Bundles and Satellites

This section describes installation of an SA Core with a Model Repository and HP-supplied Database installed on the same remote host, additional Slice Component bundles and multiple Satellite installations.

➤ The remote Oracle database must have been configured as described in SA-Supplied Oracle RDBMS Software and Database Setup on page 225 before you begin the SA Core installation.

You can use the right-hand column to indicate that a phase is completed:

table 22   Core Installation Phases

Phase	Complete
Phase 1: Preparing to Install the SA Core	
Phase 2: Run the SA Installer	
Phase 3: Specify the Core Component Hosts	
Phase 4: Select the Installation Type	
Phase 5: Select the Interview Type and Provide SA Parameter Values	
Phase 6: Install the SA Components and the Oracle Database	

Phase 1: Preparing to Install the SA Core

1   You will need the *SA Product Software* media, *Agent and Utilities* media and the *Oracle_SA* installation media.

2   The servers on which SA Core Components and the Oracle Database are to be installed must be running a supported Red Hat Enterprise Linux or SUSE Enterprise Server Linux operating system.

3   On the server where you will install the SA components, mount the *Product Software* media, *Agent and Utilities* media and the *Oracle_SA* media, or NFS-mount a directory that contains a copy of the media contents.

4   Open a terminal window and log in asa user with root privileges.

5   Change to the root directory:

```
cd /
```

➤ The SA Installer must have *read/write root privileges* to the directories in which the SA components, including NFS-mounted network appliances are to be installed.

Phase 2: Run the SA Installer

On the server on which you plan to install SA and the Oracle database, run the install script:

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

where `<distro>` is the full path to the mounted media.

You see messages displayed on screen as the SA Installer loads the required files.

Logs for the installation are automatically stored. See Installer Logs on page 34.

Phase 3: Specify the Core Component Hosts

Before SA begins the installation, it performs a prerequisite check that validates that the host on which you are installing SA meets the minimum requirements (see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation can fail or core performance may be negatively effected. If your host fails the prerequisite check or displays warnings, correct the problem(s) or contact HP support services.

For this example installation, we'll use four remote servers for the core component installation. You will, of course, modify this for your particular system requirements. Components will be installed as follows:

table 23   Core Component Layout

Server	Core Component to be Installed
192.168.136.39	Oracle database and Model Repository
192.168.136.39	Multimaster Infrastructure Components
192.168.136.39	Software Repository Storage and Content
192.168.136.40, 192.168.136.41, 192.168.136.42	Slice 0, Slice 1, Slice 2
192.168.136.39	SA Provisioning Media Server
192.168.136.39	SA Provisioning Boot Server, Slice version

1   You see this screen:

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

192.168.136.39 (this is the IP address of the host on which the installer is invoked)


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): 1

Enter number of hosts to add:
```

2   You are asked to specify the number of hosts that will be involved in the installation:

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

Enter the appropriate number. For this example, we add three hosts in addition to the server on which the install script is invoked:

```
Enter number of hosts to add: 3
```

3   The following screen displays:

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

Parameter 1 of 3
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 all remaining servers. You see this message:

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

Enter Y to continue.

For this example, we add the hosts:

- **192.168.136.40**

- **192.168.136.41**

- **192.168.136.42**

4   A screen similar to the following displays:

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

Currently specified hosts:

        192.168.136.39
        192.168.136.40
        192.168.136.41
        192.168.136.42

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):
```

5   At this point you can press 2 to delete a host or 1 to add/edit a hostname/IP address. When you choose 1 for an existing list of hosts, you see this prompt:

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

When you are satisfied with the entries, press C to continue.

6   You are asked to provide the passwords for each host in the list shown in Step 4:

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

Parameter 1 of 5

192.168.136.40 password []:*****
```

You are prompted for the password for each specified host. 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.

After you provide all required passwords, the SA Installer attempts to set up NFS mounts to the installation media and prepares each specified server for the installation.

Phase 4: Select the Installation Type

1   After the SA Installation media is mounted for all servers, the following menu displays:

```
Install Type
============

1. Typical Primary Core
2. Custom Primary Core
3. Typical Secondary Core
4. Custom Secondary Core

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

Enter 1 (Typical Primary Core) and Enter to continue.

2   The following menu displays:

```
Oracle Installation
===================

1. Install Oracle with SA
2. Use Existing Oracle Database

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

Enter 1 (Install Oracle with SA) and Enter to continue.

3   The following is displayed:

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

1. Oracle database and Model Repository, First Core
2. Multimaster Infrastructure Components
3. Software Repository Storage and Content
4. Slice
5. OS Provisioning Media Server
6. OS Provisioning Boot Server, Slice version

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

Note that no host (IP address) is associated with the components.

4   You now must associate the core components with the servers (IP addresses) they are to be installed on. To do so, you enter the component's number at the prompt. For example, enter 1 to add the host for the Oracle database and the Model Repository, enter 2 for the Multimaster Infrastructure Components, and so on.

5 Screens similar to the following display as you assign component hosts:

```
Host Assignment for Model Repository, First Core
===========================================================

1. 192.168.136.39
2. 192.168.136.40
3. 192.168.136.41
4. 192.168.136.42

Enter the number of the host or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): 1
```

Enter 1 to select 192.168.136.39 for the Model Repository. You are returned to the Host Component Layout screen and can select the next component and assign its host. Do the same for all remaining components.

When you have assigned hosts for all components, you see a screen similar to this:

```
Install Components
====================

1. Oracle RDBMS for SA and Model Repository, First Core :192.168.136.39
2. Multimaster Infrastructure Components                :192.168.136.39
3. Software Repository Storage and Content              :192.168.136.39
4. Slice                                                :192.168.136.40,
                                                         192.168.136.41,
                                                         192.168.136.42
5. OS Provisioning Media Server                         :192.168.136.39
6. OS Provisioning Boot Server, Slice version           :192.168.136.39

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

Note that the Slice Component bundle (option 4) has multiple host IP addresses listed as the Slice components can have multiple instances to improve performance.

Enter c and press Enter to continue.

Phase 5: Select the Interview Type and Provide SA Parameter Values

1 The following menu displays:

```
Interview Type
==============

1. Simple Interview
2. Advanced Interview
3. Expert Interview

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

Enter 1 (Simple Interview) and Enter to continue.

2 You are prompted to supply values for the following SA parameters:

- opsware_admin user (truth.oaPwd): an SA administrator password (the default username is admin).

The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.

- `crypto.hash_algorithm`: The hashing algorithm [SHA1 or SHA256] for SA cryptographic module
- `crypto.key_length`: the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module.
- `decrypt_passwd`: A password for the SA cryptographic material.

▶ You will see this prompt only if you are using your own crypto file and not allowing SA to automatically generate the crypto file.

- `truth.dcNm`: A name for your SA facility.
- `word.store.host`: The IP address of the NFS server for the Software Repository.
- `word.store.path`: The absolute path on the NFS server for Software Repository (`/var/opt/opsware/word`)

For more information about these parameters, see the Appendix B, "SA Core Parameter Reference".

You see these prompts (the prompts display one at a time; after you provide a value and press enter you see a message, `Validating...`, and if the value is acceptable, the next prompt displays:

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

Navigation Keys:
Use <Ctrl>P to go to the previous parameter.
Use <Ctrl>N to go to the next parameter.
Use >Tab> to view help on the current parameter.
Use <Ctrl>C to interrupt the interview.

Parameter 1 of 10 (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password
used to connect to the Oracle database.: []

Parameter 2 of 10 (fips.mode)
Do you want SA to be in FIPS mode? (y/n) [n]: n

Parameter 3 of 10: (crypto.hash_algorithm)
Please enter the hashing algorithm [SHA1 or SHA256] for SA cryptographic
module. [SHA1]:
```

▶ If you enable FIPS mode in Parameter 2 (`Do you want SA to be in FIPS mode? (y/n) [n]: y`), SA automatically sets the value of Parameter 3 to SHA1. If FIPS is not enabled, you can choose between SHA1 or 256.

```
Parameter 4 of 10: (crypto.key_length)
Please enter the key length [2048 or 4096] used for hashing algorithm of SA
cryptographic module. [2048]:

Parameter 5 of 10 (decrypt_passwd)
Please enter the password for the cryptographic material.: []

Parameter 6 of 10 (truth.dcNm)
Please enter the short name of the facility where the Opsware Installer is
being run (no spaces).: []

Parameter 7 of 10 (windows_util_loc)
Please enter the directory path containing the Microsoft patching
utilities. Press Ctrl-I for a list of required files or enter "none" if you
do not wish to upload the utilities at this time (none).: []
```

```
Parameter 8 of 10 (truth.servicename)Please enter the service name of the
Model Repository instance in the facility where Opsware Installer is being
run [192.168.136.39]:

Parameter 9 of 10 (word.store.host)
Please enter the IP address of the NFS server for the Software Repository.
For satellite installs, please enter the IP address of the Software
Repository Cache. [192.168.136.39]:

Parameter 10 of 10 (word.store.path)
Please enter the absolute path on the NFS server for Software Repository [/
var/opt/opsware/word]:
```

You are asked to re-enter any required passwords for confirmation.

▶ Uploading the Microsoft patching utilities is optional, however, if you expect to have Windows-based managed servers, you should follow the instructions for obtaining these files as described in Chapter 4, "Pre-installation System Requirement Checks"

When you have supplied values for all parameters, the following message displays:

```
All parameters have values.  Do you wish to finish the interview? (y/n):
```

Enter y and press Enter to continue. If you enter n, you are presented with each parameter again with the value you entered as the default. You can then change the value or accept the default. If you need to exit the installation, press Ctrl-C.

3   You are now ready to begin the database and SA Component installation.

Phase 6: Install the SA Components and the Oracle Database

1   A screen similar to the following displays:

```
Install components
==================
Oracle RDBMS for SA and Model Repository, First Core : 192.168.136.39
Multimaster Infrastructure Components              : 192.168.136.39
Software Repository Storage                        : 192.168.136.39
Slice                                              : 192.168.136.40, 192.168.136.41, 192.168.136.42
OS Provisioning Media Server                       : 192.168.136.39
OS Provisioning Boot Server, Slice version         : 192.168.136.39
Software Repository - Content (install once per mesh): 192.168.136.39

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

Enter c and press Enter to begin the prerequisite checks.

If the server that will host your Slice Component bundle has more than one network interface installed, SA will detect the presence of two NICs and display a screen similar to the following:

```
Slice Network Interface Configuration
=====================================

Parameter 1 of 2 (Slice: 192.168.136.38)

Please select the interface to use for 192.168.136.38

1) eth2      -- 192.168.136.55
2) eth1      -- 192.168.136.77

3) eth0      -- 192.168.136.38  (default)
 [3]:

Parameter 2 of 2 (Slice: 192.168.136.41)

Please select the interface to use for 192.168.136.41

1) eth0      -- 192.168.136.41  (default)
2) eth2      -- 192.168.136.54
3) eth1      -- 192.168.136.76
 [1]:
```

Select the appropriate network interface for each host by entering the associated number from the list.

When you have configured all interfaces, you see the message:

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

Enter `y` and press Enter to continue. You can edit the list again by pressing `n` and Enter.

2   The prerequisite check begins.

Before SA begins the installation, it performs prerequisite checks that validate that the host on which you are installing SA meets the minimum requirements for the installation (see). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem and retry the installation or, if you are unable to resolve the problem, contact HP support services.

3 If the prerequisite check completes successfully, you may still see some 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.

    WARNING Nothing listening at db.host:db.port (ip_address).
            Note: Can be ignored if core install will be performed
            using hpsa_install script.

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 installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core 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 installation.

4 You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, you the Core Description File (CDF) is automatically saved.

Upon completion, a message displays indicating successful installation.

Post-Installation Tasks

You must now complete the tasks described in Chapter 6, "SA Core Post-Installation Tasks."

Adding Satellites

See the Satellite installation procedure described in Chapter 7, "Satellite Installation".

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

This section describes installing all SA Core Components on the same host using a remote customer-supplied Oracle Database, additional Slice Component bundles and multiple Satellite installations You can use the right-hand column to indicate that a phase is completed:

table 24   Core Installation Phases

Phase	Complete
Phase 1: Preparing to Install the SA Core	
Phase 2: Run the SA Installer	
Phase 3: Specify the Core Component Hosts	
Phase 4: Select the Installation Type	
Phase 5: Select the Interview Type and Provide SA Parameter Values	
Phase 6: Install the SA Components	

▶ The remote Oracle database must have been configured as described in Non-SA-Supplied Oracle Software and Database Setup on page 217 before you begin the SA Core installation.

Phase 1: Preparing to Install the SA Core

1 You will need the *SA Product Software* media and the *Agent and Utilities* media.

2 The server on which the SA Core Components are to be installed must be running a supported Red Hat Enterprise Linux or SUSE Enterprise Server Linux operating system.

3 On the server where you will install the SA, mount the *Product Software* media and the *Agent and Utilities* media or NFS-mount a directory that contains a copy of the media contents:

    a Open a terminal window and log in as a user with root privileges.

    b Change to the root directory:

```
cd /
```

▶ The SA Installer must have *read/write root privileges* to the directories in which the SA components, including NFS-mounted network appliances are to be installed.

Phase 2: Run the SA Installer

On the server on which you plan to install SA and the Oracle database, run the install script:

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

where `<distro>` is the full path to the mounted media.

You see messages displayed on screen as the SA Installer loads the required files.

Logs for the installation are automatically stored. See Installer Logs on page 34.

Phase 3: Specify the Core Component Hosts

Before SA begins the installation, it performs a prerequisite check that validates that the host on which you are installing SA meets the minimum requirements (see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation can fail or core performance may be negatively effected. If your host fails the prerequisite check or displays warnings, correct the problem(s) or contact HP support services.

For this example installation, we'll use four remote servers for the core component installation. You will, of course, modify this for your particular system requirements. Components will be installed as follows:

table 25   Core Component Layout

Server	Core Component to be Installed
192.168.136.36	Model Repository
192.168.136.39	Multimaster Infrastructure Components
192.168.136.39	Software Repository Storage and Content
192.168.136.40, 192.168.136.41, 192.168.136.42	Slice 0, Slice 1, Slice 2
192.168.136.39	SA Provisioning Media Server
192.168.136.39	SA Provisioning Boot Server, Slice version

1   You see this screen:

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

192.168.136.36 (this is the IP address of the host on which the installer is invoked)


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): 1

Enter number of hosts to add:
```

2   You are asked to specify the number of hosts that will be involved in the installation:

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

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

```
Enter number of hosts to add: 4
```

3   The following screen displays:

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

Parameter 1 of 4
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 all remaining servers. You see this message:

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

Enter Y to continue.

For this example, we add the hosts:

- 192.168.136.36
- 192.168.136.39
- 192.168.136.40
- 192.168.136.41
- 192.168.136.42

4   A screen similar to the following displays:

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

Currently specified hosts:

        192.168.136.36
        192.168.136.39
        192.168.136.40
        192.168.136.41
        192.168.136.42

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):
```

5   At this point you can press 2 to delete a host or 1 to add/edit a hostname/IP address. When you choose 1 for an existing list of hosts, you see this prompt:

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

When you are satisfied with the entries, press C to continue.

6   You are asked to provide the passwords for each host in the list shown in Step 4:

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

Parameter 1 of 4

192.168.136.39 password []:*****
```

You are prompted for the password for each specified host. 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.

After you provide all required passwords, the SA Installer attempts to set up NFS mounts to the installation media and prepares each specified server for the installation.

Phase 4: Select the Installation Type

1   After the SA Installation media is mounted for all servers, the following menu displays:

```
Install Type
============

1. Typical Primary Core
2. Custom Primary Core
3. Typical Secondary Core
4. Custom Secondary Core

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

Enter 21 (Typical Primary Core) and Enter to continue.

2   The following menu displays:

```
Oracle Installation
===================

1. Install Oracle with SA
2. Use Existing Oracle Database

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

Enter 2 (Use Existing Oracle Database) and Enter to continue.

3   The following is displayed:

```
Host/Component Layout
=====================
```
```
1. Model Repository, First Core
2. Multimaster Infrastructure Components
3. Software Repository Storage and Content
4. Slice
5. OS Provisioning Media Server
6. OS Provisioning Boot Server, Slice version
```
```
Enter the number of the component or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

Note that no host (IP address) is associated with the components.

4   You now must associate the core components with the servers (IP addresses) they are to be installed on. To do so, you enter the component's number at the prompt. For example, enter 1 to add the host for the Oracle database and the Model Repository, enter 2 for the Multimaster Infrastructure Components, and so on.

5   Screens similar to the following display as you assign component hosts:

```
Host Assignment for Model Repository, First Core
================================================================

1. 192.168.136.36
2. 192.168.136.39
3. 192.168.136.40
4. 192.168.136.41
5. 192.168.136.42
```

```
Enter the number of the host or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): 1
```

Enter 1 to select 192.168.136.36 for the Model Repository. You are returned to the Host Component Layout screen and can select the next component and assign its host. Do the same for all remaining components.

When you have assigned hosts for all components, you see a screen similar to this:

```
Install Components
=====================

1. Model Repository, First Core                    :192.168.136.36
2. Multimaster Infrastructure Components           :192.168.136.39
3. Software Repository Storage and Content         :192.168.136.39
4. Slice                                           :192.168.136.40,
                                                   :192.168.136.41,
                                                   :192.168.136.42
5. OS Provisioning Media Server                    :192.168.136.39
6. OS Provisioning Boot Server, Slice version      :192.168.136.39


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

Note that the Slice Component bundle (option 4) has multiple host IP addresses listed as the Slice components can have multiple instances to improve performance.

Enter c and press Enter to continue.

Phase 5: Select the Interview Type and Provide SA Parameter Values

1   The following menu displays:

```
Interview Type
==============

1. Simple Interview
2. Advanced Interview
3. Expert Interview

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

Enter 1 (Simple Interview) and Enter to continue.

2   You are prompted to supply values for the following SA parameters:

- opsware_admin user (truth.oaPwd): an SA administrator password (the default username is admin).

➤   The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.

- crypto.hash_algorithm: The hashing algorithm [SHA1 or SHA256] for SA cryptographic module

- crypto.key_length: the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module.

- decrypt_passwd: A password for the SA cryptographic material.

➤ You will see this prompt only if you are using your own crypto file and not allowing SA to automatically generate the crypto file.

- • `truth.dcNm`: A name for your SA facility.

- • `word.store.host`: The IP address of the NFS server for the Software Repository.

- • `word.store.path`: The absolute path on the NFS server for Software Repository (`/var/opt/opsware/word`)

- • `db.host`: the IP address of the database server.

For more information about these parameters, see the Appendix B, "SA Core Parameter Reference".

You see these prompts (the prompts display one at a time; after you provide a value and press enter you see a message, `Validating...`, and if the value is acceptable, the next prompt displays:

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

Navigation Keys:
Use <Ctrl>P to go to the previous parameter.
Use <Ctrl>N to go to the next parameter.
Use >Tab> to view help on the current parameter.
Use <Ctrl>C to interrupt the interview.

Parameter 1 of 11 (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password
used to connect to the Oracle database.: []

Parameter 2 of 11 (fips.mode)
Do you want SA to be in FIPS mode? (y/n) [n]: n

Parameter 3 of 11: (crypto.hash_algorithm)
Please enter the hashing algorithm [SHA1 or SHA256] for SA cryptographic
module. [SHA1]:
```

➤ If you enable FIPS mode in Parameter 2 (`Do you want SA to be in FIPS mode? (y/n) [n]: y`), SA automatically sets the value of Parameter 3 to SHA1. If FIPS is not enabled, you can choose between SHA1 or 256.

```
Parameter 4 of 11: (crypto.key_length)
Please enter the key length [2048 or 4096] used for hashing algorithm of SA
cryptographic module. [2048]:

Parameter 5 of 11 (decrypt_passwd)
Please enter the password for the cryptographic material.: []

Parameter 6 of 11 (truth.dcNm)
Please enter the short name of the facility where the Opsware Installer is
being run (no spaces).: []

Parameter 7 of 11 (windows_util_loc)
Please enter the directory path containing the Microsoft patching
utilities. Press Ctrl-I for a list of required files or enter "none" if you
do not wish to upload the utilities at this time (none).: []

Parameter 8 of 11 (word.store.host)
Please enter the IP address of the NFS server for the Software Repository.
For satellite installs, please enter the IP address of the Software
Repository Cache. [192.168.136.39]:
```

```
Parameter 9 of 11 (word.store.path)
Please enter the absolute path on the NFS server for Software Repository
[/var/opt/opsware/word]:

Parameter 10 of 11 (db.host)
Please enter the IP address of the database server: []

Parameter 11 of 11 (truth.servicename)
Please enter the service name of the Model Repository instance in the
facility where Opsware Installer is being run [truth.rose2]:
```

➤ You see this prompt only when you are using the non-SA supplied Oracle database.

   You are asked to re-enter any required passwords for confirmation.

➤ Uploading the Microsoft patching utilities is optional, however, if you expect to have Windows-based managed servers, you should follow the instructions for obtaining these files as described in Chapter 4, "Pre-installation System Requirement Checks"

   When you have supplied values for all parameters, the following message displays:

   ```
   All parameters have values.  Do you wish to finish the interview? (y/n):
   ```

   Enter y and press Enter to continue. If you enter n, you are presented with each parameter again with the value you entered as the default. You can then change the value or accept the default. If you need to exit the installation, press Ctrl-C.

3 You are now ready to begin the database and SA Component installation.

Phase 6: Install the SA Components

1 A screen similar to the following displays:

```
Install components
==================
Model Repository, First Core                    : 192.168.136.36
Multimaster Infrastructure Components           : 192.168.136.39
Software Repository Storage                     : 192.168.136.39
Slice                                           : 192.168.136.40, 192.168.136.41, 192.168.136.42
OS Provisioning Media Server                    : 192.168.136.39
OS Provisioning Boot Server, Slice version      : 192.168.136.39
Software Repository - Content (install once per mesh): 192.168.136.39

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

Enter c and press Enter to begin the prerequisite checks.

➤ If the server that will host your Slice Component bundle has more than one network interface installed, SA will detect the presence of two NICs and display a screen similar to the following:

```
Slice Network Interface Configuration
=====================================


Parameter 1 of 2 (Slice: 192.168.136.38)


Please select the interface to use for 192.168.136.38


1) eth2      -- 192.168.136.55
2) eth1      -- 192.168.136.77
3) eth0      -- 192.168.136.38  (default)
 [3]:
```

```
Parameter 2 of 2 (Slice: 192.168.136.41)

Please select the interface to use for 192.168.136.41

1) eth0       -- 192.168.136.41  (default)
2) eth2       -- 192.168.136.54
3) eth1       -- 192.168.136.76
 [1]:
```

Select the appropriate network interface for each host by entering the associated number from the list.

When you have configured all interfaces, you see the message:

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

Enter y and press Enter to continue. You can edit the list again by pressing n and Enter.

2   The prerequisite check begins.

➤   Before SA begins the installation, it performs prerequisite checks that validate that the host on which you are installing SA meets the minimum requirements for the installation (see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem and retry the installation or, if you are unable to resolve the problem, contact HP support services.

3   If the prerequisite check completes successfully, you may still see some 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.

     WARNING Nothing listening at db.host:db.port (ip_address).
             Note: Can be ignored if core install will be performed
             using hpsa_install script.

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 installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core 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 installation.

4   You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, you the Core Description File (CDF) is automatically saved.

Upon completion, a message displays indicating successful installation.

Post-Installation Tasks

You must now complete the tasks described in Chapter 6, "SA Core Post-Installation Tasks."

Adding Satellites

See the Satellite installation procedure described in Chapter 7, "Satellite Installation".

8. SA First (Primary) Core with a Secondary Core (Multimaster Mesh)

This section provides an installation summary for a Single Host SA First (Primary) Core with a Secondary Core (Multimaster Mesh). The cores in a mesh can be installed with any of the configurations described in configurations 1 - 7 above.

Phase 1: Install the SA First (Primary) Core

Decide the configuration you will use and follow the instructions in configurations 1 - 7 above.

After the First (Primary) Core installation is completed, you can install Secondary Cores for your Multimaster Mesh.

Overview of the Secondary Core Installation Process

The following are the typical phases of installing a Secondary Core:

1   *Prepare for Installation*: Ensure that all installation prerequisites have been met, that you have the information needed to complete the Installer interview, that you have all necessary permissions to complete the installation, and that you have the SA installation media. For more information, see Chapter 4, "Pre-installation System Requirement Checks".

On the First Core Infrastructure Host

2   *Define a New Facility and Export First Core Model Repository Content*: During this phase you define the facility in which the new Secondary Core is to be installed, export the First Core's Model Repository content, and copy the resulting export files to the new Secondary Core host.

➤   When adding a new facility to an existing core that was previously patched, the new core will have the core's base version installed (not the patch version, for example 10.0, not 10.0x or 10.10, not 10.1x). After the Secondary Core is created, you must apply the desired patch.

On the Server that will Host the New Secondary Core

3   *Install the Oracle Database and install the Secondary Core Components:* During this phase you can install the HP-supplied Oracle database for the Secondary Core(s) Model Repository. This database is automatically configured to work with the SA Model Repository. See Oracle Setup for the Model Repository *on page 205* for information about the SA Oracle database configuration differs from a default Oracle configuration.

Alternatively, you can install a database using the Oracle Universal Installer or use an existing Oracle 12c database installation (Oracle10 and 9*i* are not supported) and select to use an existing database during installation. However, there are database configuration requirements that must be met in order for such databases to be compatible with the SA Model Repository.

See

You will also install the Secondary Core's components and import the Model Repository content that was exported from the First Core into the database.

4 *Post Installation Tasks*: During this phase you must perform various post-installation tasks to complete the configuration of the new Secondary Core.

➤ Before proceeding with the installation, confirm that you have addressed the issues in

Phase 2: Prepare to Add the Secondary Core

This section describes adding Secondary Cores that, with an existing First Core, create a Multimaster Mesh of SA Cores that can coordinate server management. The cores in a mesh can be installed with any of the configurations described in configurations 1 - 7 above.

➤ If you will be defining and installing multiple Facilities and Secondary Cores, you must install only one Secondary Core at a time. In other words, you must define each Secondary Core's Facility then completely install its core components and content before defining another Facility and installing another Secondary Core. Simultaneous definition/installation of Facilities/cores is not supported.

To prepare to add a Secondary Core, perform the following tasks:

1 Locate the *SA Product Software* media and, if you will install the HP-supplied Oracle database used by the SA Model Repository, the *Oracle_SA* media.

2 On the First Core's Infrastructure Component server and on the server that will host the new Secondary Cores Model Repository, mount the SA *Product Software* and *Oracle_SA* media or NFS-mount the directory that contains a copy of the media contents.

3 Create a directory on the Secondary Core's database server in which, during Phase 3, you will create the TAR.GZ file that contains files from the First Core (CDF, Model Repository content, cryptographic material) that must be copied to and extracted on the new Secondary Core host.

```
#mkdir /tmp/DB_export
```

Prepare the Environment

1 Before starting the primary database export, ensure that the COMPATIBLE parameters in the primary and secondary database `init.ora` file are set correctly. SA recommends setting the COMPATIBLE parameter to the Oracle RDBMS software version. Refer to the Oracle Doc ID: 553337.1 for information on how the COMPATIBLE parameter affects the Data Pump Export-Import process.

2 The Oracle Data Pump Export-Import process also depends on the Oracle Client version (`expdp` and `impdp`). For remote database installations, SA strongly recommends the Oracle Full Client be the same version as the Oracle RDBMS software. Refer to Oracle Doc ID: 553337.1 for information about how the Oracle Client version affects the Data Pump Export-Import process.

➤ The Installer must have *read/write root* privileges to the directories where it installs SA components, even on NFS-mounted network appliances.

Phase 3: Export First Core Files to a TAR.GZ File and Copy to New Secondary Core Host

In this phase, you export First Core files (CDF, Model Repository content, cryptographic material) into a TAR.GZ file that must be copied to the new Secondary Core.

1   On the First Core host, create a directory in which the TAR.GZ file will be saved. You can specify a custom location or accept the default:

    `/var/opt/opsware/truth`

2   `cd /`

3   On the server that hosts the First Core's *Infrastructure Component* host, invoke the Add Datacenter to Mesh script (`hpsa_add_dc_to_mesh.sh`).

    You must specify the full path to the Facility definition script.

    For example:

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

    where `<distro>` is the full path to the mounted media.

4   A screen similar to the following displays:

    ```
    ---------------------------------------
    add_dc_to_mesh will be performed on the following identified core host(s).
    If there is any inconsistency then try again with the correct CDF.

    16.77.42.65   (oracle_sas, truth_mm_overlay)
    16.77.41.24   (infrastructure, word_uploads)
    16.77.43.252  (slice, osprov)


    ---------------------------------------
    Do you want to continue (Y/N) [Y]:
    ```

    Type `Y` and press Enter to continue.

5   You are asked to provide the passwords for each host in the list shown in Step 4:

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

    Parameter 1 of 2

    <ip_address> password []:******
    ```

    You are prompted for the password for each specified host. SA validates each password as it is entered. 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.

    After you provide all required passwords, the SA Installer attempts to set up NFS mounts to the installation media and prepares each specified server for the installation.

▶   For the next step, the Secondary Core will use the FIPS compliance settings you specified during the installation of the Primary Core. You will not be prompted for FIPS enablement during the Secondary Core installation.

6   A screen similar to the following 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.

Parameter 1 of 8 (truth.dest)
Please enter the full path to the directory where the export file will be
saved [/var/opt/opsware/truth/]:

Parameter 2 of 8 (newCore.dcNm)
Please enter the short name of the new facility you would like to define
(no spaces) []: rose1

Parameter 3 of 8 (newCore.dcDispNm)
Please enter the long name for the facility that you are adding to the
mesh. [rose1]:

Parameter 4 of 8 (newCore.dbHost)
Please enter the hostname/IPaddress of the server where you are planning to
install the Oracle database in the new facility. []: 16.77.1.191

Parameter 5 of 8 (newCore.mgwIP)
Please enter the IP address of the server where you are planning to install
the Infrastructure component in the new facility (or where the management
gateway will be installed). []: 16.77.1.192

Parameter 6 of 8 (newCore.dcSubDom)
Please enter the subdomain for the facility you are about to create
(lowercase,no spaces) [rose1.com]:

Parameter 7 of 8 (newCore.servicename)
Please enter the tnsname of the Model Repository instance that you will be
installing in the new facility [truth.rose1]:

Parameter 8 of 8 (db.orahome)
Please enter the path of the ORACLE_HOME directory of your Model Repository
(truth) server. [/u01/app/oracle/product/12.1.0/client_1]:
```

➤   This must be the ORACLE_HOME directory for the *Primary Core* Model Repository.

You are asked to re-enter any required passwords for confirmation.

After you have entered or accepted all required values, you see this prompt:

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

Type Y to continue. If you need to re-enter a value, type N.

7   The following screen displays:

```
Ready to perform add DC to mesh
==============================

Actions that will be performed:
------------------------
  Define New Facility, Update Gateway Config
  Export Model Repository (truth)

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

Type c and press Enter to continue.

8   The following prompt displays only if you are using a remote database:

```
Database is on <dbserver_ip_address>. Password is needed.
============================================================


<dbserver_ip_address> password []:*****
Re-enter the password to confirm:
```

Enter the password for your database server. Re-enter the password for confirmation.

9   A number of informational messages are displayed as the process continues.

```
[INFO] ****************************************************************

[INFO] Database export files *.dmp and *.log will be available on database
server

[INFO] under directory: /u01/app/oracle/admin/truth/dpdump/

[INFO] File source_db_charset.txt is now available on this server in:

[INFO] /var/opt/opsware/truth/

[INFO] The Database export *.dmp files

[INFO] (truth*_exp.dmp, aaa*_exp.dmp, gcadmin*_exp.dmp,
lcrep*_exp.dmp,lcrep_tables*_exp.dmp)

[INFO] and *.log files are now available on the Primary database server.

[INFO] ****************************************************************
```

A completion message displays when the script completes.

10 When the script completes, in the directory, /var/opt/opsware/truth (or the custom location
you specified for the export file path (truth.dest), you will find a truth.newCore4.tar.gz file.
Copy this file to your new Secondary Core host's database server.

11 Continue to Phase 4.

Phase 4: Extract First Core Model Repository CDF on the Secondary Core

The steps in the following phases assume you have already mounted the SA primary distribution for the Secondary Core.

You perform the steps in this phase on the new *Secondary Core host*.

1   Log in to the server that will be the Secondary Core host's database server as the user that performs the installation.

CD /.

➤ The database server will be installed in phase 5a or 5b if the database does not exist yet.

2   Run the following command to extract the CDF from the TAR.GZ file you created in Phase 3.

```
<distro>/opsware_installer/tools/get_cdf_from_pkg.sh /<export_file_path>/
truth.newCore4.tar.gz
```

where `<distro>` is the full path to the mounted media. The CDF required to begin Secondary Core installation is extracted to `/var/tmp`.

Make note of the location of the extracted CDF. You will need this in the next phase.

➤ If you plan to initiate the Secondary Core installation from a remote server, you must copy this CDF to the the remote server and proceed to phase 5.

➤ `truth.newCore4.tar.gz` can be quite large. You may want to remove the file after installation is complete.

Phase 5 can be performed using any one of three Secondary Core configurations:

- Phase 5a: Install All Secondary Core Components on a Single Host

  All Secondary Core Components and SA-supplied Oracle database on the same host

- Phase 5b: Install the Secondary Core Components on Multiple Hosts, SA-Supplied Oracle Database on Model Repository Host

  Secondary Core Components distributed to different hosts, SA-supplied Oracle database on the Model Repository host

- Phase 5c: Install the Secondary Core Components on Multiple Hosts, Remote Non SA-Supplied Database on Remote Database Server

  Secondary Core Components distributed to different hosts, non-SA-supplied database on a remote database Host

Phase 5a: Install All Secondary Core Components on a Single Host

This section describes installing all SA Core Components and the SA-supplied Oracle database on a single host. If you plan to install components on different hosts, see Phase 5b: Install the Secondary Core Components on Multiple Hosts, SA-Supplied Oracle Database on Model Repository Host on page 130.

During this phase, the First Core Model Repository content exported during Step 4 is imported into the Secondary Core's Model Repository, the cryptographic material is extracted to the appropriate location on the host and the SA Secondary Core Components installed.

> If you plan to use a remote Oracle database, there are specific configuration tasks you must perform on the database before installing the Secondary Core. See *Appendix A: Oracle Setup for the Model Repository* and the installation procedure described in

1   Invoke the SA Installer and specify (-c argument) the CDF extracted in Phase 4:

```
<distro>/opsware_installer/hpsa_install.sh -c /var/tmp/cdf.newCore4.xml
```

where `<distro>` is the full path to the mounted media.

2   After a few informational messages display, a screen similar to the following displays:

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


Currently specified hosts:


<newCore4_IP_Address>


Please select one of the following options:


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


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

3   Press `c` to continue. A screen similar to the following displays:

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


<newCore4_IP_Address> password []:*****
```

Enter the password for the new Secondary Core host and press Enter. The password is validated and a number of informational messages display as the script continues.

4   A screen similar to the following displays:

```
Install Type
============


1. Typical Secondary Core
2. Custom Secondary Core


Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit): 2
```

Select option 2, Custom Secondary Core, and press Enter.

5   A screen similar to the following displays:

```
Oracle Installation
===================


1. Install Oracle with SA
2. Use existing Oracle database


Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit): 1
```

Select option `1`, Install Oracle with SA, and press Enter.

6   A screen similar to the following displays:

```
Interview Type
==============

1. Simple Interview
2. Advanced Interview
3. Expert Interview

Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit): 1
```

Type `1` to select the Simple Interview and press `c` to continue.

7   A screen similar to the following 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.


Parameter 1 of 9 (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password
used to connect to the Oracle database. []: *************

Parameter 2 of 9 (decrypt_passwd)
Please enter the password for the cryptographic material [*******]:

Parameter 3 of 9 (truth.dcNm)
Please enter the short name of the facility where Opsware Installer is
being run (no spaces) [rose2]:

Parameter 4 of 9 (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 5 of 9 (db.host)
Please enter the hostname/IPaddress of the Oracle database server.
[16.77.1.191]:

Parameter 6 of 9 (truth.servicename)
Please enter the service name of the Model Repository instance in the
facility where Opsware Installer is being run [truth.rose2]:
```

You see this prompt only when you are using the non-SA supplied Oracle database.

```
Parameter 7 of 9 (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]: /u01/app/oracle/
product/12.1.0/client_1

Parameter 8 of 9 (word.store.host)
Please enter the IP address of the NFS server for the Software Repository.
For satellite installs, please enter the IP address of the Software
Repository Cache. [newCore4_IP_Address]:

Parameter 9 of 9 (word.store.path)
Please enter the absolute path on the NFS server for Software Repository
[/var/opt/opsware/word]:

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

Since you specified the CDF file from the First Core Model Repository export, you can except the defaults, enter 2 and press c to continue.

You are asked to re-enter any required passwords for confirmation.

8   A screen similar to the following displays:

```
Install components
==================

Oracle RDBMS for SA
Model Repository, Additional Core
Core Infrastructure Components
Slice
OS Provisioning Components

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

Press c to continue.

9   The prerequisite check begins.

10   If the prerequisite check completes successfully, you may still see some 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.

    WARNING Nothing listening at db.host:db.port (ip_address).
            Note: Can be ignored if core install will be performed
            using hpsa_install script.

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 installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core performance may be negatively affected if you continue without resolving them.

If your server passes the prerequisite check, enter `c` and press Enter.

11 A screen similar to the following displays:

```
Package file pathname
=====================


package file path [/var/tmp/truth.newCore4.tar.gz]:
```

Enter the file name and path for the TAR.GZ file you extracted to the Secondary Core's database server in Phase 4 and press Enter. The Model Repository content and cryptographic material is extracted to the appropriate directories on the host. The SA installer also performs certain post-Oracle installation tasks and sets required file permissions. When the installation completes, you the Core Description File (CDF) is automatically saved.

12 The script displays process messages and a completion message. During this process, the Installer registers the new Secondary Core's Facility with the First Core's Model Repository, automatically generating a unique ID for the Facility.

Phase 5b: Install the Secondary Core Components on Multiple Hosts, SA-Supplied Oracle Database on Model Repository Host

Use the following procedure to install SA Secondary Core Components on different host servers, for example, Slice Component bundle and/or Model Repository on different servers than the Infrastructure components. The Oracle database and the Model Repository are installed on the same host.

During this phase, the First Core Model Repository content exported during Step 4 is imported into the Secondary Core's Model Repository, the cryptographic material is extracted to the appropriate location on the host and the SA Secondary Core Components installed.

1 Invoke the HPSA Installer specifying (`-c` argument) the CDF extracted in Phase 4:

`<distro>/opsware_installer/hpsa_install.sh -c /var/tmp/cdf.newCore4.xml`

where `<distro>` is the full path to the mounted media.

You see messages displayed on screen as the SA Installer loads the required files.

For this example installation, we'll use six remote servers for the core component installation. You will, of course, modify this for your particular system requirements. Components will be installed as follows:

table 26   Core Component Layout

Server	Core Component to be Installed
192.168.136.36	Oracle and Model Repository
192.168.136.39	Multimaster Infrastructure Components
192.168.136.39	Software Repository Storage and Content

table 26   Core Component Layout (cont'd)

Server	Core Component to be Installed
192.168.136.38, 192.168.136.41, 192.168.136.42	Slice (installs multiple Slice instances)
192.168.136.40	SA Provisioning Media Server
192.168.136.40	SA Provisioning Boot Server, Slice version

2   After a few informational messages display, a screen similar to the following displays:

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

Currently specified hosts:

<newCore4_IP_Address>

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): 1
```

Enter 1 to Add/Edit host(s) and press Enter to continue.

3   You are asked to specify the number of hosts that will be involved in the installation:

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

Enter the appropriate number. For this example, we use five hosts in addition to the host on which the install script was invoked:

```
Enter number of hosts to add: 5
```

4   The following screen displays:

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

Parameter 1 of 5
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 all remaining servers. You see this message:

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

Enter Y to continue.

For this example, we add the hosts:

• 192.168.136.38

• 192.168.136.39

• 192.168.136.40

• 192.168.136.41

- **192.168.136.42**

5 A screen similar to the following displays:

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

Currently specified hosts:

        192.168.136.36
        192.168.136.38
        192.168.136.39
        192.168.136.40
        192.168.136.41
        192.168.136.42

Please select one of the following options:

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

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

6 At this point you can press 2 to delete a host or 1 to add/edit a hostname/IP address. When you choose 1 for an existing list of hosts, you see this prompt:

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

When you are satisfied with the entries, press C to continue.

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

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

Parameter 1 of 3

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

You are prompted for the password for each specified host. 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.

After you provide all required passwords, the SA Installer attempts to set up NFS mounts to the installation media and prepares each specified server for the installation.

8 After the SA Installation media is mounted for all servers, the following menu displays:

```
Install Type
============

1. Typical Secondary Core
2. Custom Secondary Core

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

Select Option 2, Custom Secondary Core and press c to continue.

9   The following screen displays:

```
Oracle Installation
===================

1. Install Oracle with SA
2. Use existing Oracle database

Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit): 1
```

Select 1, `Install Oracle with SA` then press c to continue.

10   The following screen displays:

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

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

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

You use this menu to assign the host on which the SA Core Components are to be installed.

Press the associated number for the component (for example, 1 for the Model Repository). You will see a menu that lists the available hosts and the name of the component to be assigned. It will look similar to this:

```
Host Assignment for Model Repository, Additional Core
=====================================================

1. 192.168.136.36
2. 192.168.136.38
3. 192.168.136.39
4. 192.168.136.40
5. 192.168.136.41
6. 192.168.136.42

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

11   Type the number associated with the hostname/IP address of the server you want to host the current SA Core Component and press enter.

```
Enter the number of the host or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): 1
```

Selecting 1 assigns the Model Repository to the IP address, 192.168.136.36. You will be returned to the Host Component Layout menu. Note that the Model Repository displays the hostname/IP address it was assigned to:

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

1. Model Repository, Additional Core        :192.168.136.36
2. Multimaster Infrastructure Components     :192.168.136.39
3. Software Repository Storage               :192.168.136.36
4. Slice                                     :192.168.136.38,
                                             :192.168.136.41,
                                             :192.168.136.42
5. OS Provisioning Media Server              :192.168.136.40
6. OS Provisioning Boot Server, Slice version :192.168.136.40


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

Repeat this step for each component listed on the Host Component Layout menu.

You can assign multiple Slice Component bundles to the same host or to different hosts (you must assign at least one) :

```
Host Assignment for Slice
=========================

1 ( ) 192.168.136.36
2 ( ) 192.168.136.39


Enter the number of the host or one of the following directives
(<c>ontinue, <p>revious, <a>ll, <u>nselect all, <h>elp, <q>uit):
```

After you have assigned a Slice Component bundle to a host, an asterisk is displayed next to the hostname/IP address:

```
2 (*) 192.168.136.39
```

After you have assigned a hostname/IP address for all components, enter c at the prompt and press Enter to continue.

12 The following Menu displays:

```
Interview Type
==============

1. Simple Interview
2. Advanced Interview
3. Expert Interview


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

Type 1 for the Simple Interview and press Enter to continue.

13 The following screen 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.


Parameter 1 of 9 (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password
used to connect to the Oracle database. []: *************

Parameter 2 of 9 (decrypt_passwd)
Please enter the password for the cryptographic material [*******]:

Parameter 3 of 9 (truth.dcNm)
Please enter the short name of the facility where Opsware Installer is
being run (no spaces) [rose2]:

Parameter 4 of 9 (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 5 of 9 (db.host)
Please enter the hostname/IPaddress of the Oracle database server.
[192.168.136.39]:

Parameter 6 of 9 (truth.servicename)
Please enter the service name of the Model Repository instance in the
facility where Opsware Installer is being run [truth.rose2]:

Parameter 7 of 9 (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]: /u01/app/oracle/
product/12.1.0/client_1

Parameter 8 of 9 (word.store.host)
Please enter the IP address of the NFS server for the Software Repository.
For satellite installs, please enter the IP address of the Software
Repository Cache. [192.168.136.39]:

Parameter 9 of 9 (word.store.path)
Please enter the absolute path on the NFS server for Software Repository [/
var/opt/opsware/word]:

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

Since you specified the CDF file from the First Core Model Repository export, you can except the defaults and press c to continue.

You are asked to re-enter any required passwords for confirmation.

When you have supplied values for all parameters, the following message displays:

```
All parameters have values.  Do you wish to finish the interview? (y/n):
```

Enter y and press Enter to continue. If you enter n, you are presented with each parameter again with the value you entered as the default. You can then change the value or accept the default. If you need to exit the installation, press Ctrl-C.

14 A screen similar to the following displays:

```
Install components

===================
Oracle Database, Model Repository, First Core        : 192.168.136.36
Multimaster Infrastructure Components                 : 192.168.136.39
Software Repository Storage                           : 192.168.136.39
Slice                                                 : 192.168.136.38, 192.168.136.41, 192.168.136.42
OS Provisioning Media Server                          : 192.168.136.40
OS Provisioning Boot Server, Slice version            : 192.168.136.40
Software Repository - Content (install once per mesh): 192.168.136.39

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

Enter c and press Enter to begin the prerequisite checks.

If the server that will host your Slice Component bundle has more than one network interface installed, SA will detect the presence of two NICs and display a screen similar to the following:

```
Slice Network Interface Configuration
=====================================

Parameter 1 of 2 (Slice: 192.168.136.38)

Please select the interface to use for 192.168.136.38

1) eth2      -- 192.168.136.55
2) eth1      -- 192.168.136.77
3) eth0      -- 192.168.136.38  (default)
 [3]:

Parameter 2 of 2 (Slice: 192.168.136.41)


Please select the interface to use for 192.168.136.41

1) eth0      -- 192.168.136.41  (default)
2) eth2      -- 192.168.136.54
3) eth1      -- 192.168.136.76
 [1]:
```

Select the appropriate network interface for each host by entering the associated number from the list.

When you have configured all interfaces, you see the message:

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

Enter y and press Enter to continue. You can edit the list again by pressing n and Enter.

15 The prerequisite check begins.

➤ Before SA begins the installation, it performs prerequisite checks that validate that the host on which you are installing SA meets the minimum requirements for the installation (see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem and retry the installation or, if you are unable to resolve the problem, contact HP support services.

16 If the prerequisite check completes successfully, you may still see some 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.

    WARNING Nothing listening at db.host:db.port (ip_address).
            Note: Can be ignored if core install will be performed
            using hpsa_install script.

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 installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core 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 installation.

17 A screen similar to the following displays:

```
Package file pathname
====================

package file path [/var/tmp/truth.newCore4.tar.gz]:
```

Enter the file name and path for the TAR.GZ file you extracted to the Secondary Core's database server in Phase 4 and press Enter. The Model Repository content and cryptographic material is extracted to the appropriate directories on the host. The SA installer also performs certain post-Oracle installation tasks and sets required file permissions. After the extraction complete, the SA Installer begins the Secondary Core installation.

18 You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, you the Core Description File (CDF) is automatically saved.

Upon completion, a message displays indicating successful installation.

Phase 5c: Install the Secondary Core Components on Multiple Hosts, Remote Non SA-Supplied Database on Remote Database Server

Use the following procedure to install all SA Core Components on different host servers, for example, Slice Component bundle and/or Model Repository on different servers than the infrastructure components. It also uses an existing remote non-SA-supplied Oracle database. For information about configuring a non-SA-supplied Oracle database for use with SA, see Oracle Setup for the Model Repository on page 205.

During this phase, the First Core Model Repository content exported during Step 4 is imported into the Secondary Core's Model Repository, the cryptographic material is extracted to the appropriate location on the host and the SA Secondary Core Components installed.

1   Invoke the HPSA Installer specifying the CDF (-c argument) extracted in Phase 4:

`<distro>/opsware_installer/hpsa_install.sh -c /var/tmp/cdf.newCore4.xml`

where `<distro>` is the full path to the mounted media.

You see messages displayed on screen as the SA Installer loads the required files.

For this example installation, we'll use six remote servers for the core component installation. You will, of course, modify this for your particular system requirements. Components will be installed as follows:

table 27   Core Component Layout

Server	Core Component to be Installed
192.168.136.36	Model Repository
192.168.136.39	Multimaster Infrastructure Components
192.168.136.39	Software Repository Storage and Content
192.168.136.38, 192.168.136.41, 192.168.136.42	Slice
192.168.136.40	SA Provisioning Media Server
192.168.136.40	SA Provisioning Boot Server, Slice version

2   After a few informational messages display, a screen similar to the following displays:

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

Currently specified hosts:

<newCore4_IP_Address>

Please select one of the following options:

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

Enter the option number or one of the following directives

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

Enter 1 and press Enter to continue.

3   You are asked to specify the number of hosts that will be involved in the installation:

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

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

```
Enter number of hosts to add: 6
```

4   The following screen displays:

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

Parameter 1 of 6
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 all remaining servers. You see this message:

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

Enter Y to continue.

For this example, we add the hosts:

- 192.168.136.36

- 192.168.136.38

- 192.168.136.39

- 192.168.136.40

- 192.168.136.41

- 192.168.136.42

5   A screen similar to the following displays:

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

Currently specified hosts:

        192.168.136.36
        192.168.136.38
        192.168.136.39
        192.168.136.40
        192.168.136.41
        192.168.136.42

Please select one of the following options:

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

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

6   At this point you can press 2 to delete a host or 1 to add/edit a hostname/IP address. When you choose 1 for an existing list of hosts, you see this prompt:

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

When you are satisfied with the entries, type C and press Enter to continue.

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

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

192.168.136.36 password []:
```

You are prompted for the password for each specified host. Type the password (which will be obfuscated) and press Enter. After you provide all required passwords, the SA Installer attempts to set up NFS mounts to the installation media and prepares each specified server for the installation.

8 After the host preparation completes, the following menu displays:

```
Install Type
============

1. Typical Secondary Core
2. Custom Secondary Core

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

Select Option 1, `Typical Secondary Core` and press Enter to continue.

9 The following screen displays:

```
Oracle Installation
===================

1. Install Oracle with SA
2. Use existing Oracle database

Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit): 2
```

Select 2, `Use existing Oracle database` then press Enter to continue.

10 The following screen displays:

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

1. Model Repository, Additional Core
2. Core Infrastructure Components
3. Slice
4. OS Provisioning Components

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

You use this menu to assign the host on which the SA Core Components are to be installed.

Press the associated number for the component (for example, `1` for the Model Repository). You will see a menu that lists the available hosts and the name of the component to be assigned. It will look similar to this:

```
Host Assignment for Model Repository, Additional Core
=====================================================

1. 192.168.136.36
2. 192.168.136.38
3. 192.168.136.39
```

```
4. 192.168.136.40
5. 192.168.136.41
6. 192.168.136.42

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

11 Type the number associated with the hostname/IP address of the server you want to host the current SA Core Component and press enter.

Selecting 1 assigns the Model Repository to the IP address, 192.168.136.36. You will be returned to the Host Component Layout menu. Note that the Model Repository displays the hostname/IP address it was assigned to:

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

1. Model Repository, Additional Core   :192.168.136.36
2. Core Infrastructure Components       :192.168.136.39
3. Slice                                :192.168.136.38, 192.168.136.41,
                                        :192.168.136.42
4. OS Provisioning Components           :192.168.136.40

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

Repeat this step for each component listed on the Host Component Layout menu.

You can assign multiple Slice Component bundles to the same host or to different hosts (you mus assign at least one):

```
Host Assignment for Slice
=========================

1 ( ) 192.168.136.36
2 ( ) 192.168.136.39


Enter the number of the host or one of the following directives
(<c>ontinue, <p>revious, <a>ll, <u>nselect all, <h>elp, <q>uit):
```

After you have assigned a Slice Component bundle to a host, an asterisk is displayed next to the hostname/IP address:

```
2 (*) 192.168.136.39
```

After you have assigned a hostname/IP address for all components, enter c at the prompt and press Enter to continue.

12 The following Menu displays:

```
Interview Type
==============

1. Simple Interview
2. Advanced Interview
3. Expert Interview

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

Type 1 for the Simple Interview and press Enter to continue.

13 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.



Parameter 1 of 9 (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password
used to connect to the Oracle database. []: *************

Parameter 2 of 9 (decrypt_passwd)
Please enter the password for the cryptographic material [*******]:

Parameter 3 of 9 (truth.dcNm)
Please enter the short name of the facility where Opsware Installer is
being run (no spaces) [rose2]:

Parameter 4 of 9 (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 5 of 9 (db.host)
Please enter the hostname/IPaddress of the Oracle database server.
[192.168.136.39]:

Parameter 6 of 9 (truth.servicename)
Please enter the service name of the Model Repository instance in the
facility where Opsware Installer is being run [truth.rose2]:

Parameter 7 of 9 (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]: /u01/app/oracle/
product/12.1.0/client_1

Parameter 8 of 9 (word.store.host)
Please enter the IP address of the NFS server for the Software Repository.
For satellite installs, please enter the IP address of the Software
Repository Cache. [192.168.136.39]:

Parameter 9 of 9 (word.store.path)
Please enter the absolute path on the NFS server for Software Repository
[/var/opt/opsware/word]:

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

You are asked to re-enter any required passwords for confirmation.

Since you provided the CDF you created when you installed the Primary SA Core, SA uses many of the default core configuration parameter values from that CDF as the default for this interview.

When you have supplied all required values, you see this prompt:

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

Enter Y and press Enter to continue.

14 A screen similar to the following displays:

```
Install components

==================
Model Repository, First Core                 : 192.168.136.36
Multimaster Infrastructure Components         : 192.168.136.39
Software Repository Storage                   : 192.168.136.39
Slice                                         : 192.168.136.38, 192.168.136.41, 192.168.136.42
OS Provisioning Media Server                  : 192.168.136.40
OS Provisioning Boot Server, Slice version    : 192.168.136.40
Software Repository - Content (install once per mesh): 192.168.136.39

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

Type c and press Enter to begin the prerequisite checks.

➤ If the server that will host your Slice Component bundle has more than one network interface installed, SA will detect the presence of two NICs and display a screen similar to the following:

```
Slice Network Interface Configuration
=====================================

Parameter 1 of 2 (Slice: 192.168.136.38)

Please select the interface to use for 192.168.136.38

1) eth2       -- 192.168.136.55
2) eth1       -- 192.168.136.77
3) eth0       -- 192.168.136.38  (default)
 [3]:

Parameter 2 of 2 (Slice: 192.168.136.41)

Please select the interface to use for 192.168.136.41

1) eth0       -- 192.168.136.41  (default)
2) eth2       -- 192.168.136.54
3) eth1       -- 192.168.136.76
 [1]:
```

Select the appropriate network interface for each host by entering the associated number from the list.

When you have configured all interfaces, you see the message:

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

Enter y and press Enter to continue. You can edit the list again by pressing n and Enter.

15 The prerequisite check begins.

➤ Before SA begins the installation, it performs prerequisite checks that validate that the host on which you are installing SA meets the minimum requirements for the installation (see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41). The check insures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem and retry the installation or, if you are unable to resolve the problem, contact HP support services.

16 If the prerequisite check completes successfully, you may still see some 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.

     WARNING Nothing listening at db.host:db.port (ip_address).
             Note: Can be ignored if core install will be performed
             using hpsa_install script.

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 installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core 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 installation.

17 The following prompt displays because you are using a remote existing database:

```
Database is on <dbserver_ip_address>.  Password is needed.
===========================================================


<dbserver_ip_address> password []:
Re-enter the password to confirm:
```

Enter the password for your database server. You are asked to re-enter the password for confirmation.

18 A screen similar to the following displays:

```
Package file pathname
====================


Specify full path to the compressed package.


package file path [/var/tmp/<filename>.tar.gz]:
```

Enter the file name and path for the TAR.GZ file you extracted to the Secondary Core's database server in Phase 4 and press Enter. The Model Repository content and cryptographic material is extracted to the appropriate directories on the host. The SA installer also performs certain post-Oracle installation tasks and sets required file permissions. After the extraction complete, the SA Installer begins the Secondary Core installation.

19 You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, you the Core Description File (CDF) is automatically saved.

Upon completion, a message displays indicating successful installation.

Secondary Core Post-Installation Tasks

After you have added a new core to a Multimaster Mesh, you must perform the tasks described in this section.

Associate Customers with the New Facility

Associate the appropriate customers with each new Facility so that servers managed at that Facility are associated with the correct customers accounts. For more information, see the Customer Account Administration section of the *SA Administration Guide*.

Update Permissions for the New Facility

After you have added a new Facility to your Multimaster Mesh, your SA users will not yet have the required permissions to access the new Facility. You must assign the required permissions to the user groups. For more information, see the User Group and Setup section of the *SA Administration Guide*.

Verify Multimaster Transaction Traffic

To verify Multimaster transaction traffic with the target Facility, perform the following tasks:

1 Log in to the SAS Web Client as any user who belongs to the `Opsware System Administrators` group.

2 From the Navigation panel, click Multimaster Tools under Administration. The View window appears.

3 In the State View Window, note the color of the status box beside each transaction.

A *transaction* is a unit of change to a Model Repository database that consists of one or more updates to rows and has a globally unique transaction ID. If the transactions within the Secondary Core's Facility are green, the new SA Core is integrated into the Multimaster Mesh.

➤ It is normal for some transactions to display an orange status (not sent) for a short period.

4 Click **Refresh** to refresh the cached data until all transactions display green.

For more information, see the Multimaster Mesh Administration section in the *SA Administration Guide*.

Installing Additional Slice Component Bundles

You can install additional Slice Component bundles on an existing SA Core in order to improve the scalability. To install an addition Slice Component bundle to an installed SA core, perform the following tasks.

1 On any core server in the SA Core in which you plan to install the additional Slice Component bundle, run the install script, specifying the Core Description File (CDF) you generated when you installed the core by using the `-c` argument and the full path to the file:

```
/<distro>/opsware_installer/hpsa_install.sh -c /usr/tmp/hpsa_cdf.xml
```

where `<distro>` is the full path to the mounted media. You see messages displayed on screen as the SA Installer loads the required files.

Logs for the installation are automatically stored. See

2 You see a screen similar to the following:

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

Currently specified hosts:

        192.168.136.36 (oracle_sas)
        192.168.136.38 (slice)
        192.168.136.39 (infrastructure)
        192.168.136.40 (osprov)


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): 1
Enter number of hosts to add (or enter "0" to edit the list): 1
```

Enter 1 to add the IP address of the server that will host the additional Slice Component bundle.

For example:

```
Adding hosts
============

Parameter 5 of 5
Hostname / IP []: 192.168.136.43

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

3 After you have specified the host server's IP address, the Specify Hosts to Install screen looks similar to this:

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

Currently specified hosts:

        192.168.136.36 (oracle_sas)
        192.168.136.38 (slice)
```

```
            192.168.136.39 (infrastructure)
            192.168.136.40 (osprov)
            192.168.136.43


    Please select one of the following options:

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


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

Note that the last IP address in the list is the IP address you just entered however, no component is assigned to that IP address for installation.

To assign the Slice Component bundle to the IP address you just specified, enter c and press Enter to continue.

You are prompted to provide the host password for each host in the list.

The installer validates each password, then you see messages displayed as the installer prepares the server for installation.

4   When the set up completes, you see a screen similar to the following:

```
    Install Type
    ============


    1. Typical Primary Core


    Enter the option number or one of the following directives
    (<p>revious, <h>elp, <q>uit): 1
```

Accept the default.

➤   The Install Type is stored in the Core Definition File (CDF) when you install the SA First Core and is the default for subsequent installations and upgrades. You cannot use a Typical Installation type for the SA Core and a Custom Installation type for subsequent installations. Both installs must be of the same Installation type.

5   You see a screen similar to the following:

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


    Installed Components

    Oracle RDBMS for SAS                              : 192.168.136.36
    Model Repository, First Core                      : 192.168.136.36
    Core Infrastructure Components                    : 192.168.136.39
    Slice                                             : 192.168.136.38
    OS Provisioning Components                        : 192.168.136.40
    Software Repository - Content (install once per mesh): 192.168.136.39


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


    Select a component to assign


    1. Slice
```

```
Enter the number of the component or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): 1
```

In this case, since all other components have already been installed and only the Slice Component bundle can have multiple instances, only the Slice option is displayed. Select `1` and press Enter,

6   You see a screen similar to the following:

```
Host Assignment for Slice
=========================

1 ( ) 192.168.136.36
2 ( ) 192.168.136.39
3 ( ) 192.168.136.40
4 ( ) 192.168.136.43

Enter the number of the host or one of the following directives
(<c>ontinue, <a>ll, <u>nselect all, <p>revious, <h>elp, <q>uit): 4
```

Enter the line number associated with the IP address you specified above. An asterisk appears next to your selection.

```
Host Assignment for Slice
=========================

1 ( ) 192.168.136.36
2 ( ) 192.168.136.39
3 ( ) 192.168.136.40
4 (*) 192.168.136.43

Enter the number of the host or one of the following directives
(<c>ontinue, <a>ll, <u>nselect all, <p>revious, <h>elp, <q>uit): c
```

Enter `c` then press Enter to continue.

7   You see a screen similar to the following:

```
Host Assignment for Slice
=========================

1 ( ) 192.168.136.36
2 ( ) 192.168.136.39
3 ( ) 192.168.136.40
4 (*) 192.168.136.43


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

Installed Components

Oracle RDBMS for SAS                            : 192.168.136.36
Model Repository, First Core                    : 192.168.136.36
Core Infrastructure Components                  : 192.168.136.39
Slice                                           : 192.168.136.38
OS Provisioning Components                      : 192.168.136.40
Software Repository - Content (install once per mesh): 192.168.136.39

-----------------------------------------
```

```
Select a component to assign

1. Slice [192.168.136.43]

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

Enter c then press Enter to continue.

8　You see a screen similar to the following where you can modify installation parameters if necessary:

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

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

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

1. Re-enter values
2. Continue

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

Enter c then press Enter to continue.

After a prerequisite check, the Slice Component bundle is installed on the host you specified. You see some messages displayed as the installation proceeds and a completion message when the installation is finished.

6 SA Core Post-Installation Tasks

This section describes system administration tasks that you must perform after installing an SA Core.

Run the Health Check Monitor

The Health Check Monitor (HCM) includes a suite of tests to check the status of an SA Core. For a full description of the monitor and its tests, see the *SA Administration Guide*.

Run the following command:

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

Usage:

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

Where:

table 28   Health Check Monitor Arguments

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

For `<probe>` specify `check_opsware_version`.

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

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

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

The SA Client

The SA Client is a powerful Java client for the Server Automation System. It provides the look-and-feel of a Microsoft Windows desktop application with the cross-platform flexibility of Java. If you installed your core on multiple servers, you can access the SA Client from any Core Server hosting a Component Slice bundle.

To access the SA Client for the first time, you must invoke the SA Client Launcher from the SAS Web Client Main Page. Clicking on this link will install the SA Client and the required Java Runtime Environment (JRE) on your local machine. Once installed, you can invoke the SA Client from the local machine rather than from the SAS Web Client.

➤ The SA Client is installed with the Java 2 Runtime Environment, Standard Edition 1.4.2._15. The SA Client is a Java application that installs and runs with its own Java Runtime Environment (JRE). The SA Client will not interfere with any other versions of JRE you may have installed on your system. The JDK will not be used (and is not usable) by any other Java application on the target computer, and it will not set itself as the default JDK on the target computer.

Note that the SA Client adds certain functionality not in the SAS Web Client. Instructions in this documentation set will explicitly identify either the SAS Web Client or the SA Client as required to complete a task.

See the *SA User Guide: Server Automation* and *SA Getting Started* for more information about both clients.

Installing the SA-Required Flash Player

SA requires that you install Adobe Flash Player. You can download it here:

http://get.adobe.com/flashplayer/otherversions

1 Select Windows.

2 Select Flash Player for Internet Explorer.

3 Follow the onscreen instructions to install.

Enable Oracle Automatic Optimizer Statistics Collection

SA relies on Oracle's Automatic Optimizer statistics collection to collect schema statistics used to avoid database performance degradation. By default, Oracle's Automatic optimizer statistics collection should be enabled.

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

1 Enter 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
```

2 If the status is not `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 Server Discovery and Agent Installation

SA Client Server discovery and Agent installation identifies servers on your network that do not have Server Agents installed and installs (deploys) Agents onto those servers.

Enabling Server Discovery and Agent Installation for UNIX and Windows Servers

During SA Core installation, the SA Installer automatically installs all required software to perform server discovery and Agent installation from UNIX and Windows hosts . No other configuration is required.

Launch the SAS Web Client

To launch the SAS Web Client:

1 In a supported web browser, enter the following URL:

```
http://<SA_hostname>
```

where `<SA_hostname>` is the host name or IP address of the server on which you installed SA.

2 The browser displays instructions for installing the required SA security certificate.

3 The SAS Web Client Logon screen displays and prompts you for a user name and password.

Enter the SA Administrator username and password. The default is `admin` and the password you specified in Phase 1.

4   After you are logged in, you see the SAS Web Client home page.

figure 2   The SAS Web Client Home Page]
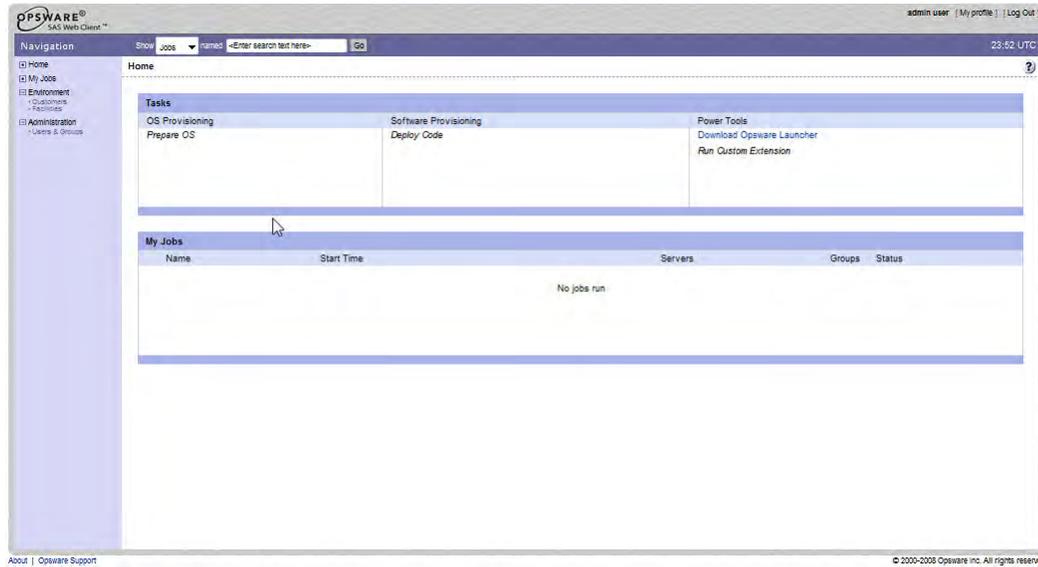
Download and Install the SA Client Launcher Installation Package

The SA Client requires a Microsoft Windows-based system that is connected to the network on which SA is installed. The SA Client also requires that the Adobe Flash Player be installed for certain functions. See the *SA Planning and Installation Guide*, "First Core Post-installation Tasks", for more information about installing the Flash Player for use with SA.

You must download and install the SA Client, which is required for most SA features.

1   You must be logged on to the SAS Web Client as the SA Administrator user.

1   From the SAS Web Client home page, click on launcher download link in the Tasks panel.

2   Save the file to a directory on your local hard drive.

3   Double click the file to begin the installation and follow the on screen instructions.

Create a User Account with Administrator Privileges

Using the SA Client, you must create a new System Administrator user and assign the appropriate SA privileges.

See the *SA Administration Guide*: *User and User Group Setup and Security* for instuctions about creating new users.

Create an SA User as a Member of the Software Policy Setters and Software Deployers User Groups

This user has the privileges to scan your facility's network for servers not yet managed by SA.

See the *SA Administration Guide*: *User and User Group Setup and Security* for instuctions about creating new users and adding users to user groups.

Chapter 6

Grant the Software Policy Setters and Software Deployers User Groups the Required Facility Privileges

See the *SA Administration Guide*: *User and User Group Setup and Security* for instuctions about granting privileges to user groups.

Scan for Unmanaged Servers on your Network

In this phase, SA scans your network to discover any servers not managed by SA. After SA discovers your unmanaged servers, you are given the choice to bring each server into the SA Managed Server Pool.

You can scan for unmanaged servers in several ways:

- By specified IP addresses
- By IP address ranges
- Using pre-prepared lists of IP addresses

This section does not attempt to describe all methods, rather it uses a single method for simplicity. For more information about scanning for unmanaged servers (using SA server discovery and Agent installation), see the *SA User Guide: Server Automation*.

Perform the following tasks to scan for an unmanaged server on your network:

1 Log on to the SA Client as the SA Superuser you created above by double clicking on the SA Client program file or shortcut.

2 On the SA Client main screen, select the Devices tab and then select Unmanaged Servers in the navigation pane.

figure 3   **Select Unmanaged Servers**

3   Select *Explicit IPs/Hostnames* from the drop down list to specify a list of specific IP addresses to scan, separated by spaces (commas not supported). For convenience, you can click the ellipsis（...） button to display a simple text editor that allows you to more easily enter multiple IP addresses. You can also save the file for future use. Clicking OK will cause the IP addresses you entered to populate the *IP Address or Hostnames* field.

figure 4   **Specifying Specific IP Addresses or Hostnames**

4   Click **Scan** to begin the scan for unmanaged servers.

When the scan is complete, a list of discovered unmanaged servers is shown. SA displays each server's:

- status

- IP address

- host name

- detected operating system

- any open ports that can be used to connect to the server.

figure 5   **Sample Unmanaged Server Scan Results**

Bringing a server Under SA Management

1   Select server(s) you want to manage with SA. The SA Client supports hot keys to make multiple selections.

2 From the **Actions** menu, select **Manage Server**. The Manage Servers dialog box appears as shown in Figure 6.

figure 6   Manage Servers Dialog

3 Select a network protocol to use for connecting to the server from the drop-down list.

In most cases, choosing *Select Automatically* to allow SA to select an appropriate protocol for each server is recommended.

For VMware ESXi servers where the Linux-based service console (COS) has been removed, you must choose VMware ESX Web Services. For more information on managing virtual servers, see the *SA User Guide: Server Automation*.

4 Enter a username and password to use for logging into the managed server.

Windows-based systems: log in using the Windows administrator username/password.

UNIX-based systems: log in as root. If logging in as root is not permitted, select the *Become root (UNIX)* checkbox. Select *Supply root password* and enter the password or select *Use sudo* if sudo access is enabled for that account.

If you log in using sudo, the sudo user's configuration file (typically /etc/sudoers) must allow the account to run any command with root privileges. This is typically accomplished by using the "ALL" alias in the sudoers file.

▶ If you are unable to bring the server under SA management by logging in as root, see the *SA User Guide: Server Automation* for more details about logging in as a non-root user for agent deployment.

5 Select V*erify prerequisites, copy installer, and install agent*.

See "Server Discovery and Agent Installation" in the *SA User Guide: Server Automation* for more information.

6 Accept the default Installer options.

7 Click **OK**. SA performs the required actions on the selected unmanaged servers to bring them into the Managed Server Pool.

8 The SA Client displays the results and updates the status icons for the new managed servers.

You can now use SA to manage these servers.

▶ At this point it would be a good idea to perform the tutorials in the *SA Getting Started* guide and become familiar with the SA interfaces and features. The *SA Getting Started* guide also provides interactive tutorials.

Adding or Changing an SA Client Launcher Proxy Server

By default, the SA Client uses the proxy server settings configured for the default browser on your local system. For example, if your default browser has no proxy server settings configured, neither will the SA Client.

You can configure SA Client to use a proxy server by editing the Java Web Start `deployment.properties` file.

For details on how to do that, see the *SA User Guide: Server Automation*.

Configuring Contact Information in SA Help

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

1   In the SA Core, log on asa user with root provileges to the server running the Command Center (Slice Component bundle).

2   Change to the following directory:

    /etc/opt/opsware/occ

3   Open the `psrvr.properties` file in a text editor.

4   Modify the values in the following fields to change the contact information in the SAS Web Client Help:

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

5   Save the file and exit.

6   Restart the Command Center component by entering the following command:

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

Pre-Defined User Groups Permissions

SA provides an extended set of role-based, pre-defined user groups. If you plan to use these groups, you must grant read and/or write permissions to the first Facility and any other appropriate permissions to the groups. For more information about predefined user groups and permissions, see the section "Pre-Defined User Groups" and Appendix A: "Permissions Reference" in the *SA Administration Guide*.

Installing Application Configuration (AppConfig) Content

In order to get the baseline set of Application Configurations (AppConfigs) into your core, you must perform the post-installation tasks described in this section using the DCML Exchange Tool (DET).

The AppConfig content archive is located on the Agent & Utilities media in the `<distro>/packages/` directory with the file name:

OPSWContent-AppConfig-<current_version>.tgz.

Complete the following steps:

1   The AppConfig content archive is in `tar/gz` format, so you must uncompress it with `gunzip` and extract it using tar. You can also use GNU tar with the `xvzf` flags to simultaneously uncompress and extract the file, for example:

    ```
    tar xvzf OPSWContent-AppConfig-<current_version>.tgz
    ```

    This command creates a directory named `AppConfig`.

2   Install the Content Baseline Tool (`cbt`) (for example, `cbt-34_1_0_27.zip`) from the primary Product Software media. The tool is located in the directory `<distro>/packages/<core OS>`. Install the tool under `/usr/local` or any known path and add the location to your path, for example:

    ```
    export PATH=$PATH:/usr/local/cbt/bin
    ```

3   Set the JAVA_HOME environment variable to use Opsware's JRE:

    ```
    export JAVA_HOME=/opt/opsware/jdk1.6/
    ```

4   Verify that `cbt` is working properly by invoking it using `cbt  -v`. This command should return a version, if not, check your installation, PATH and/or JAVA_HOME settings.

5   Import the content using a `cbt` config file or by manually entering the user names and passwords for the DCML Exchange Tool and Web Services Data Access Engine users (for example, `admin` and `detuser`):

    ```
    cbt -i AppConfig -cf core.cfg
    ```

    Shown below is a sample `cbt` config file. Change the `*.host` entries and/or passwords as necessary:

    ```
    cbt.numthreads: 5
    mail.from: joeuser@opsware.com
    spike.host: USE YOUR IP ADDRESS FOR YOUR SA CORE OR COMPONENT
    way.host: USE YOUR IP ADDRESS FOR YOUR SA CORE
    word.host: USE YOUR IP ADDRESS FOR YOUR SA CORE
    spin.host: USE YOUR IP ADDRESS FOR YOUR SA CORE
    twist.host: USE YOUR IP ADDRESS FOR YOUR SA CORE
    spike.username: admin
    spike.password=admin
    twist.username: detuser
    twist.password=detuser
    ssl.keyPairs: /var/opt/opsware/crypto/twist/spog.pkcs8
    ssl.trustCerts: /var/opt/opsware/crypto/twist/opsware-ca.crt
    twist.certPaths: /var/opt/opsware/crypto/twist/opsware-ca.crt
    ```

6   Launch the SA Client and select **Tools ➤ Options** and **Reload cache now**, or wait a few minutes, then verify that your new Content is available.

7   AppConfig content appears in two locations in the SA Client, in the Application Configuration and in the Audit and Remediation feature. To view the AppConfig content in the SA Client, select:

    Navigation pane ➤ Library ➤ By Type ➤ Application Configuration

    or, when viewing an Audit or Snapshot Specification rule:

    Navigation pane ➤ Library ➤ By Type ➤ Audit and Remediation

If you have any questions on any Content, please contact technical support.

Agent Deployment Tool (ADT) Requirements

If you plan to use the Agent Deployment Tool (ADT) to deploy Server Agents, you must have the following in the root user's path on each server hosting the Slice Component bundle(s) (includes the Gateway) and each Satellite server:

- OpenSSH client

- telnet client (standard client that ships with Linux)

- rlogin (standard rlogin that ships with Linux)

Storage Visibility and Automation

If you plan to use Storage Visibility and Automation, see the *Storage Visibility and Automation Installation & Administration Guide.*

➤ Storage Essentials (SE) version 6.1.1 or later is required to view, report, or perform any Service Automation Visualizer (SAV) and Service Automation Reporter (SAR) operation on SAN objects, such as arrays, switches, volumes, and so on. SAN objects are discovered in Storage Essentials. To enable discovered SAN objects in the SA, SAV, and SAR products, the Server Automation SE Connector component must be installed and configured.

BSA Essentials Reporting

If you plan to use reports, see the "Reports" section of the *HP Automation Insight User Guide*, and the solution pack user guides that are provided with each solution pack available for download on HPLN.

NA/SA Integration

For information about integrating SA with Network Automation (NA), see the *SA Integration Guide* and your NA documentation.

Operations Orchestrator/SA Integration

For information about integrating SA with Operations Orchestration (OO), see the *SA Integration Guide* and the OO documentation.

DHCP Configuration for SA Provisioning

The Dynamic Host Configuration Protocol (DHCP) specifies how to assign dynamic IPv4 and IPv6 addresses to servers on a network. SA Provisioning uses DHCP to allow network booting and configuration of unprovisioned servers in the Server Pool. DHCP is also used to configure networking on newly provisioned servers that have not been assigned a static network configuration.

For information for setting up DHCP for SA Provisioning, see the *SA User Guide: OS Provisioning*.

SA also supports Windows and Linux network booting in DHCPless environments (static IP). See the *SA User Guide: OS Provisioning*.

Enabling IPv6 Networking Post-Installation

This section describes scenarios to enable IPv6 networking after installation. For details about the `enable_ipv6.sh` script, see the "Enable_ipv6.sh Script" section in the *SA Administration Guide*.

For the purpose of enabling IPv6 on HPSA, the following entities are considered to be a single unit:

- A single core with all its slices (excluding the satellites and managed servers behind those satellites)
- A satellite with its associated gateways and OS provisioning components
- Multiple satellite instances in the same realm with their associated gateways and OS provisioning components
- The cores in a multimaster mesh (excluding the satellites and managed servers behind those satellites)

➤ In all of these scenarios, the phrase "run `enable_ipv6.sh`" means that the script can be run in interactive mode (default) or non-interactive mode (with the `-f` option).

Single Core With Single Slice
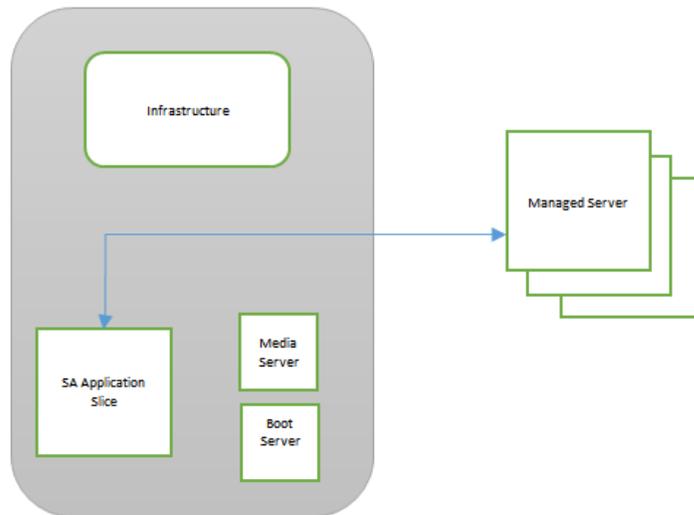
The simplest setup is a single core with all HPSA components installed in the same host. In this case, run the `enable_ipv6.sh` script from the core host. This will enable IPv6 for the gateways (core, agent, and management gateways) and OS provisioning components.

```
# /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f
```

Single Core With Multiple Slices - Boot Server and Slice Running on Same Host
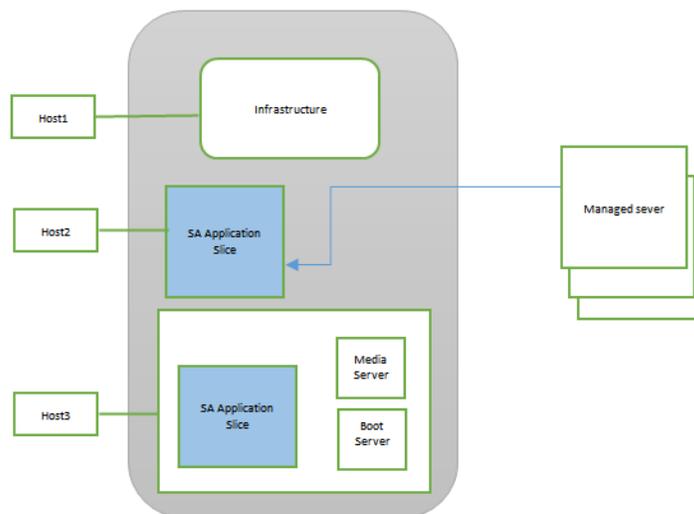
Run `enable_ipv6.sh` on all infrastructure and slice hosts (Host1, Host2, and Host3 in the previous figure). Note that Host3 is running slice and has Boot and Media Server as well.

```
# /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh -f
```

Single Core Multiple Slices - Boot Server Running On a Separate Host
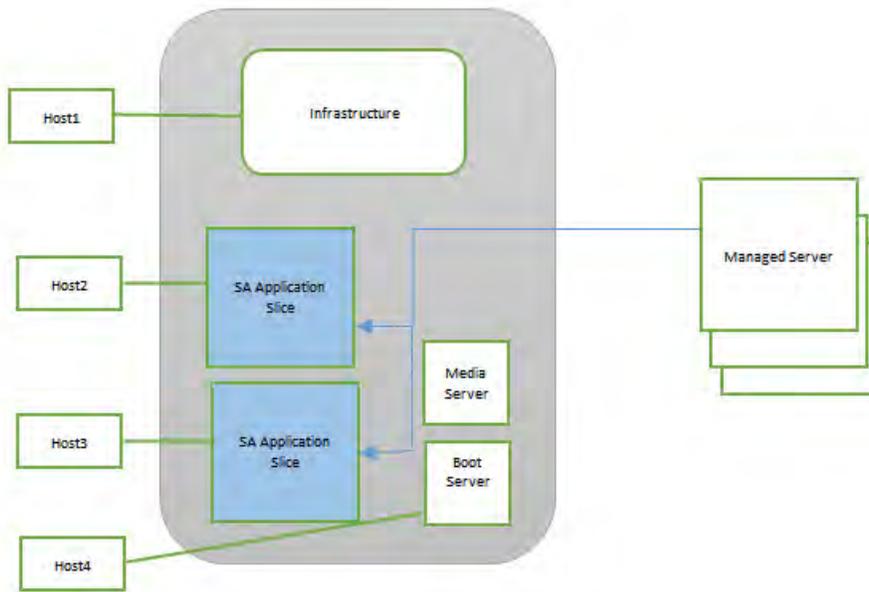
The previous figure shows that Host1 runs the infrastructure, and Host2 and Host3 run slices. Run the `enable_ipv6.sh` script in these hosts as:

```
# /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh -f
```

Host4 runs the Boot Server and the Media Server. Host4 does not run any gateway. In this case, the OS provisioning component (Boot Server) is running in a system different from the one in which the gateway is running. Run the `enable_ipv6.sh` script with the `-g` option, where the user has to pass the IPv6 address of the slice running agent gateway.

In the following example, Boot Server (Host4) can be associated with Host2 or Host3 (which run the agent gateway):

```
# /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh -f -g<IPv6 address of
Host2 or Host3>
```

Single Core With Two Satellites and OS Provisioning Boot Server Behind the Satellite
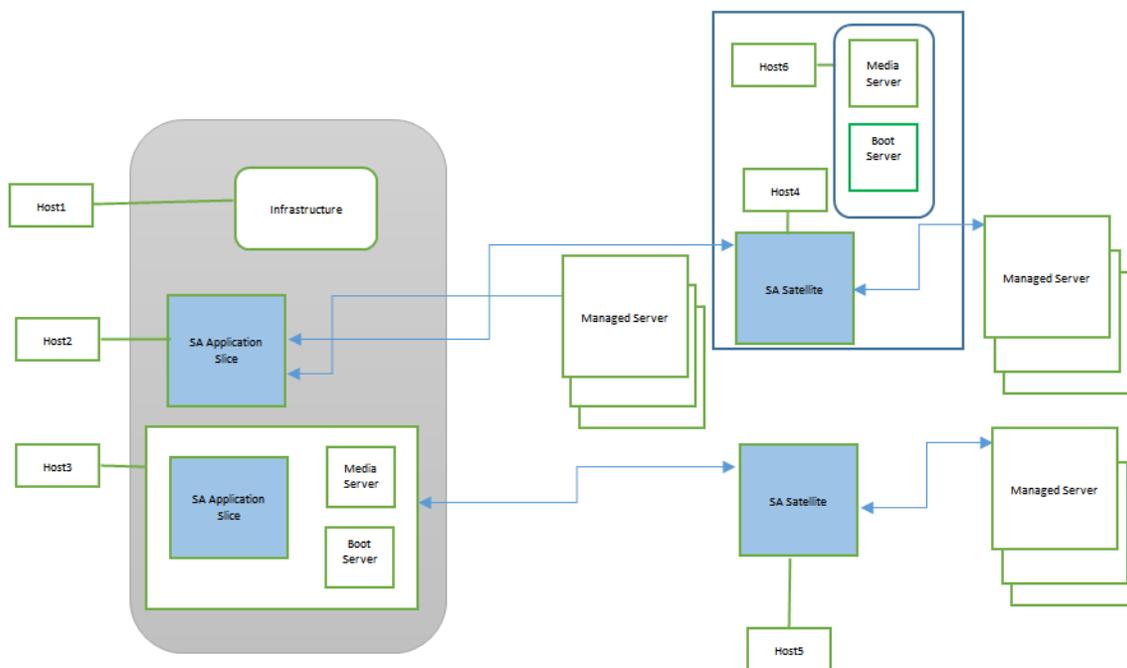
Host1, Host2, and Host3 run the core components and can be considered as one unit.

Host4 and Host5 run the satellites and can be considered as one unit.

Host6 is running OS provisioning boot server and is associated with the satellite running Host4.

The user can choose to:

•   Enable IPv6 on core and satellites:

In this case, run `enable_ipv6.sh` on all hosts (Host1 through Host6).

On Host1 to Host5, run:

```
# /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh -f
```

On Host6, run:

```
# /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f –g <IPv6 Address of
Satellite>
```

- Keep the core as IPv4, and enable IPv6 in satellites:

  In this case, enable IPv6 on host4, host5, and host6.

  On Host4 and Host5, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f
  ```

  On Host6, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f –g <IPv6 Address of
  Satellite>
  ```

- Enable IPv6 on the core, and keep the satellites as IPv4:

  On Host1, Host2, and Host3, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f
  ```

Multiple Cores With Single and Multiple Instances of Satellites and the OS Provisioning Boot Server Behind a Satellite
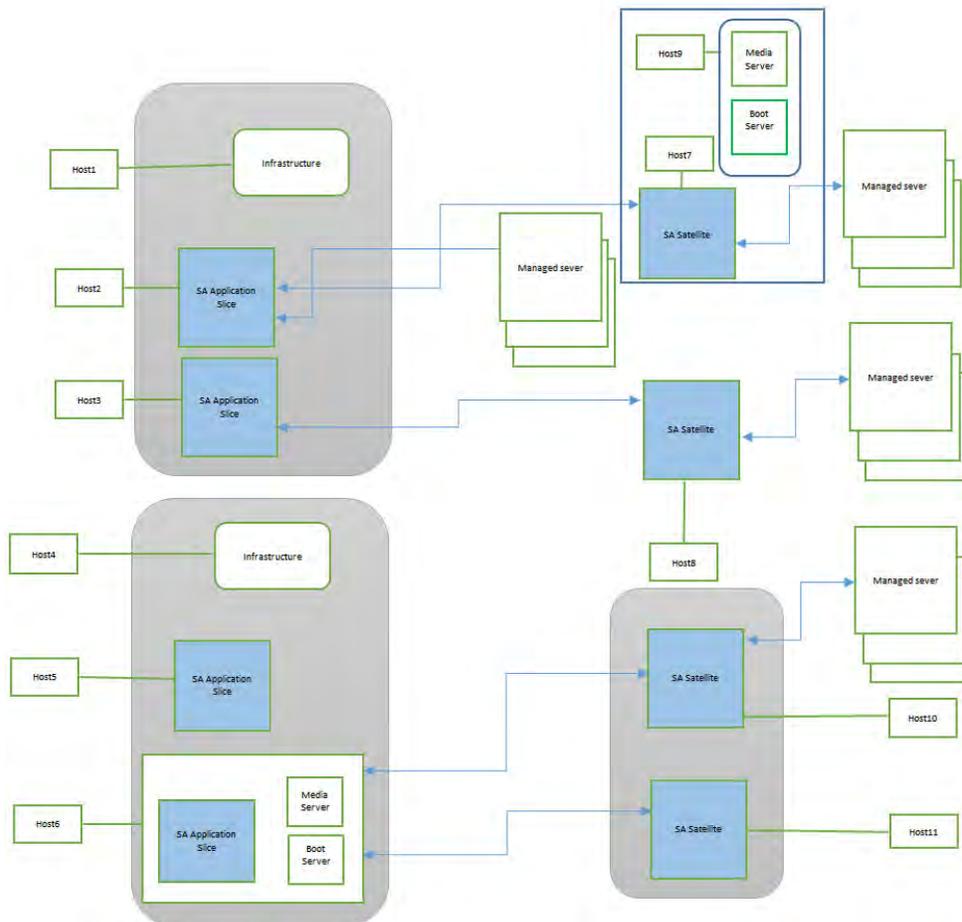
Host1, Host2, and Host3 constitute the primary core. Host4, Host5, and Host6 makes up the secondary core. For IPv6-enablement purposes, the primary and secondary cores become a single unit.

Satellite Host7 and Host9 (the OS provisioning boot server) are considered a single unit.

Satellite Host8 is considered a single unit.

The satellites on Host10 and Host11 are multiple instances on the same realm, serving to provide high availability. These satellites are considered to be a single unit.

The user can choose to:

- **Enable IPv6 on core and satellites**

  In this case, run `enable_ipv6.sh` on all hosts (Host1 through Host11).

  On all hosts except Host9, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f
  ```

  On Host9, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f –g <IPv6 Address of
  Host7>
  ```

- **Keep core as IPv4, and enable IPv6 in the satellites**

  In this case, enable IPv6 on Host7, Host8, Host9, Host10, and Host11.

  On Host7, Host8, Host10, and Host11, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f
  ```

  On Host9, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f –g <IPv6 Address of
  Host7>
  ```

- **Enable IPv6 on cores, and keep satellites as IPv4**

  On Host1, Host2, Host3, Host4, Host5, and Host6, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f
  ```

- **Enable IPv6 on some satellites, and keep cores as IPv4**

  For example, the user wants to enable IPv6 on the realm that has multiple satellite instances (e.g., Host10 and Host11).

  On Host10 and Host11, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f
  ```

Additional Network Requirements for SA Provisioning

SA Provisioning for Solaris

If you are using SA Provisioning for Solaris (JumpStart) on an isolated network, you must have a default Gateway (router) available, even if it does not route packets. For Solaris JumpStart to function properly, the IP address of the default Gateway must be sent to the installation client that is being provisioned with DHCP. When you use the SA DHCP Configuration Tool, a default Gateway is properly configured for Solaris because the tool adds the appropriate default router.

Host Name Resolution

For Windows SA Provisioning, the host name `buildmgr` must resolve on all Windows OS installation clients.

The SA Core host names must resolve using the DNS search order and DNS server information that the DHCP server provides. The DHCP server provides the DNS server IP address and the DNS search order. For each subnet you configure with the SA DHCP Configuration Tool, the DNS domain used by that subnet must have a DNS entry for `buildmgr`.

For example, you could have two subnets with the following domain names:

```
subnet1.example.com
subnet2.example.com.
```

Therefore, there must be two DNS entries for `buildmgr`:

```
buildmgr.subnet1.example.com
buildmgr.subnet2.example.com.
```

The host running the SA Provisioning Media Server must be able to resolve the IP address to the host name (reverse lookup) for any server being provisioned.

See also Host and Service Name Resolution Requirements on page 53.

Open Ports

Any server on which an OS is to be provisioned must meet the same requirements for connectivity to the SA Core network as any managed server. See "Required Open Ports" on page 50.

Windows Patch Management Tasks

This section includes post-installation tasks for the SA Windows Patch Management feature.

Import Windows Patches into the Software Repository

Before Windows patches can be installed on managed servers using SA, the patches must be imported into the Software Repository. You can import the patches with the SA Client or with the following shell script:

```
/opt/opsware/mm_wordbot/util/populate-opsware-update-library
```

This script downloads the Microsoft Patch Database and patches from the Microsoft site and imports them into the Software Repository. You should schedule the script to run weekly as a `cron` job on the Software Repository server. Non-administrative users of the SA Client will have the new patches available to them without any action on their part.

For more information about the SA-supplied Windows Patch Import script and importing Windows patches using the SA Client, see the *SA User Guide: Server Patching*.

Install Internet Explorer 6.0 or Later for Patch Management on Windows 2000

➤ The `mbsacli.exe` patch utility for patch management on Windows 2000 requires Internet Explorer 6.0 or later. Note that IE 6.0 is pre-installed on Windows Server 2003.

Automating Installation of IE 6.0 or Later

To automatically deploy IE 6.0 or later, use the Internet Explorer Administrator's Kit (IEAK) for the version of IE that you want to install. For more information on IEAK, see the following URL:

```
http://technet.microsoft.com/en-us/ie/bb219517.aspx
```

To automate deployment of IE 6.0 or later to managed servers, perform the following tasks:

1   Install IEAK on a Windows Server 2000, 2003, 2008, 2008 R2 x62 or 2012 system.

2   After you install IEAK, start the Internet Explorer Customization Wizard.

3   IEAK will prompt you to choose a Media Selection option. Select the option *Flat* (all files in one directory).

4   Accept the defaults for all other options.

5   After the wizard completes, zip the contents of the directory it created. This directory contains the automatically deployable version of IE 6.0 or later.

6   Upload the ZIP package into the SA Software Repository. See the *SA User Guide: Software Management* for instructions on importing software into the Software Repository.

   Set the following properties for the package when you import it into the Software Repository. See the *SA Policy Setter Guide* for the steps to edit the properties for a package in the SA Client.

   •   In the Installation Parameters section in the **Install Flags field**, specify the installation location:

   ```
   %SystemDrive%\IE-redist
   ```

   •   In the Installation Parameters section in the **Reboot Required field**, specify Yes.

   •   In the Install Scripts section in the **Post-Install Script tab**, enter this text:

   ```
   %SystemDrive%\IE-redist\ieX.xsetup.exe /q:a /r:n
   ```

   Where `ieX.xsetup.exe` is the IE stub installer and `X.x` identifies the version.

   The `/q:a` install option specifies quiet install mode, with no user prompts. The `/r:n` install option suppresses restarting the server after IE installation.

7   Start the SAS Web Client, create a Software Policy, and add the package you imported into the Software Repository in step 6 to that policy. See the *SA User Guide: Software Management* for the steps to create a software policy and add a package to a software policy.

8   Use the SA Client to remediate the Software Policy to your managed Windows servers. See the *SA User Guide: Software Management* for the steps to install software on a server by remediating a software policy onto a managed server.

Support for Red Hat Network Errata and Channels

The Red Hat Network (RHN) is a web-based system for administrators that assists them in patch management, updating, monitoring, and maintenance. Of particular interest to SA administrators is the ability to install and upgrade packages (RPMs) on Red Hat Linux servers.

Included with SA, the `rhn_import` CLI program allows you to download packages from the Red Hat Network, upload the packages into SA Software Repository, and create software policies that correspond to Red Hat Network patches, errata, and channels. When you remediate the software policies, the packages in the policies are installed or upgraded on the managed servers.

SA administrators can import these packages and create software policies using the SA Client. Alternatively, all these operations can be done from the command line using the `rhn_import` utility. This remediation process can be transparent to end users.

For more information on `rhn_import`, see "Automatically Importing Red Hat Network Errata" in the *SA User Guide: Software Management*.

Global File System Tasks

This section contains optional post-installation tasks for the Global File System (OGFS).

Configuring User ID Numbers for the Global File System

When you install a SA Core, you can set values to control the range of UID and GID numbers used by the Global File System. These values are used to provide unique user IDs for all SA users that are logged in to the OGFS. When the Web Services Data Access Engine creates a new user, it will use these values to determine the next available (unique) user ID that is within the range for the local data center.

To set values that control the range of UID and GID numbers, you must specify the following Web Services Data Access Engine parameters in the `params.conf` file:

- **twist.min_uid**: Contains the minimum UID number that can be used. The default value is 80001.

- **twist.default_gid**: Contains the group ID number that a user is assigned to restrict SA users from using certain ports. The default value is 70001.

These parameters are specified as global in the `params.conf` file, which means that they will be written out to the global response file (`oiresponse.global`). This file is generated when the Model Repository export is performed on the Primary Core server. When you follow the installation instructions and provide the global response file (`oiresponse.global`) as the initial response file to the Secondary Core server, SA Installer will use the specified values.

For more information, see Table 64, "Global File System Parameters," on page 294.

▶ After you make changes to these parameters, you must restart the Web Services Data Access Engine server.
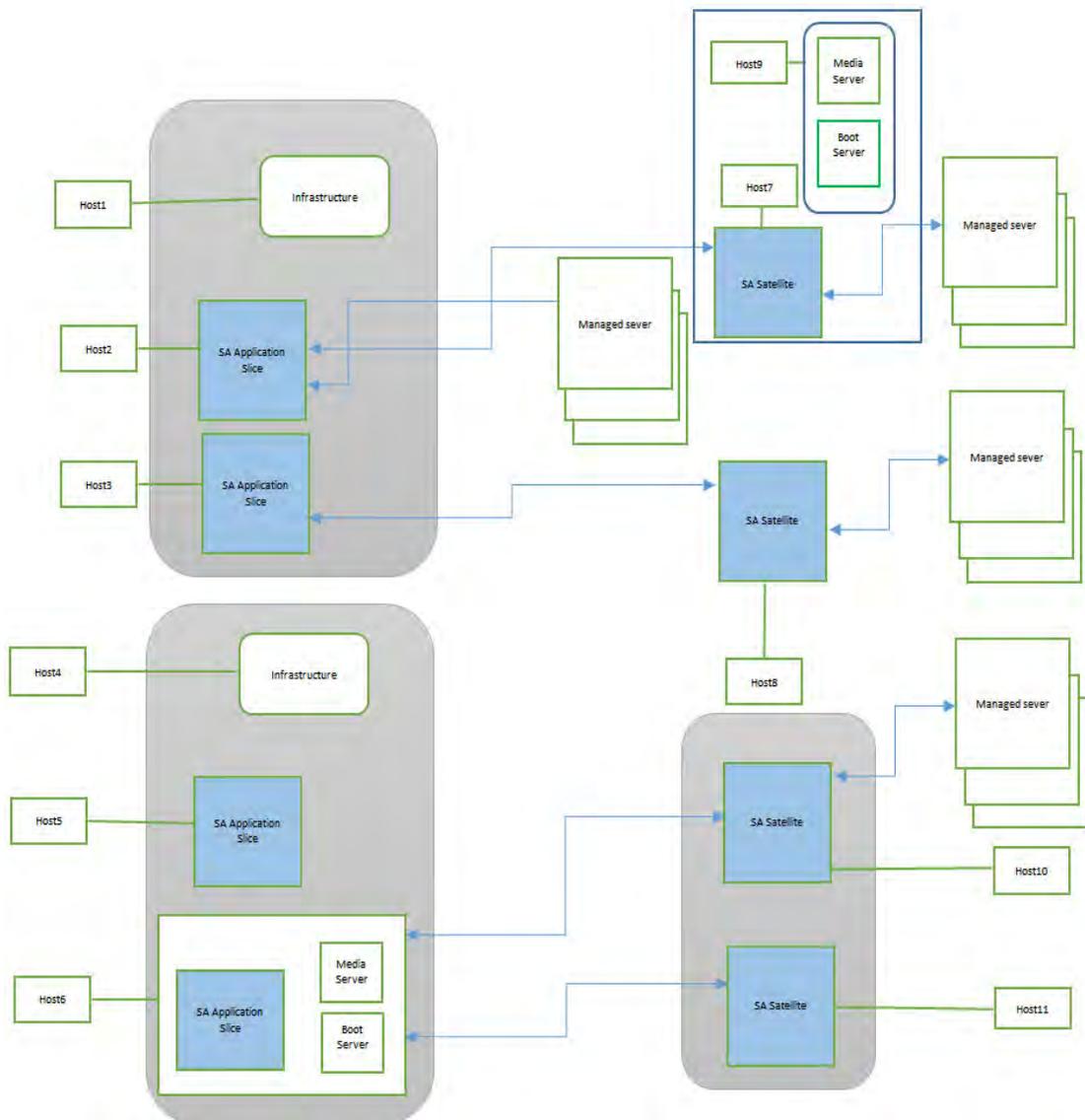
7 Satellite Installation

This section provides an overview of Satellites and Satellite installation requirements as well as instructions for installing a Satellite and post-installation tasks.

Satellite Installation Basics

A Satellite installation can be a solution for remote sites that do not have a large enough number of potential Managed Servers to justify a full SA Core installation by allowing you to install only the necessary Core Components for the remote site to function as a Satellite.

If you unsure of what a Satellite is, see the *SA Product Overview and Architecture* guide for an introduction to SA Satellites.

Installation Summary

The following is an overview of the Satellite installation process. For detailed instructions, see Satellite Installation on page 180.

1   Locate and mount the *Satellite Base Including OS Provisioning* media or NFS-mount the directory that contains a copy of the media contents

2   Run the HPSA Installer specifying the Core Definition FIle (CDF) created during the Primary Core installation. The interviewer prompts you for information about your Satellite server environment, saves the information in a new Satellite CDF and exits.

3   Re-run the SA Installer and select Satellite from the list of components to install. The Installer launches the Gateway Installer.

4   [*Optional*] Re-run the Installer to install SA Provisioning components on the Satellite.

Satellite Installation Requirements

Before you install a Satellite, verify that you meet following requirements.

• If your Satellite must be able to perform SA Provisioning in a Multimaster Mesh with an SA 9.1 Core, due to changes in SA Provisioning, the Satellite must be SA 9.0 or later. SA Provisioning does not work in a mixed Core/Satellite version installation.

• If you plan to install the SA Provisioning Boot Server and Media Server components in the Satellite, you must adhere to the requirements in SA Provisioning: DHCP Proxying on page 54.

• The required packages listed in Required Red Hat/Oracle/SUSE Linux Packages for SA Satellites in this section must be installed on the Satellite server.

- The SA Core that will provide core component services to the Satellite must be running and accessible during Satellite installation and the Satellite server must have network connectivity to that Core's Management Gateway.

- You must be a member of the *System Administrators* group as well as a member of any user group that has Manage Gateway permissions.

- You must have root privileges to parent Core's Model Repository host from which you can copy the cryptographic material and security configuration file to the Satellite server.

- The Satellite server uses UTC, as described in 11. Check the Core Host(s) Time and Locale Requirements on page 57. The Satellite server's system time **must** be synchronized with the Primary Core host.

- If you plan to locate the Satellite's Software Repository Cache on a network storage device, the user performing the installation must havewrite access over NFS to the directories in which the Software Repository Cache will be installed.

- If you already have an SA Server Agent installed on a server you plan to use for a new Satellite, you must *uninstall* it before running the Satellite Installer.

- Make note that after the installation process completes, the new Satellite server is owned by the customer "Opsware". You should take into account any effects this may have on access rights before beginning the installation.

Satellite Free Disk Space Requirements

This section describes the free disk space (in addition to the operating files system) requirements for any SA Satellite.

table 29

Satellite Component Directory	Recommended Free Disk Space
/opt/opsware	15 GB
/var/log/opsware	10 GB
/var/opt/opsware	20 GB (dependant on caching plans and the core cache size)
/osmedia	15 GB (dependant on SA Provisioning needs)

Required Red Hat/Oracle/SUSE Linux Packages for SA Satellites

The SA Installer performs an automatic prerequisite check on the SA Satellite host to ensure that environment settings are met and all required OS packages are installed. For detailed information about the SA Prerequisite Checker, see 5. Familiarize Yourself with the SA Installer Prerequisite Checker on page 41.

See also Additional Linux Requirements on page 45.

Required Open Ports

table 30   Packages that Must be Removed for SUSE Linux Enterprise Server 10

Remove Package	
chkfontpath	x86_64
desktop-file-utils	x86_64
libpng	i386
libpng	x86_64
libpng-32bit	x86_64
libxml2	x86_64
libxml2-32bit	x86_64
libxml2-python	x86_64
mkisofs	NA
ttmkfdir	x86_64
xorg-x11	x86_64
xorg-x11-font-utils	x86_64
xorg-x11-libs-32bit	x86_64
xorg-x11-libs	x86_64
xorg-x11-xauth	x86_64
xorg-x11-xfs	x86_64
xterm	x86_64

The ports listed in Table 31 must be open for use by the Satellite's Gateway. The port numbers listed in the table are default values. You can select other values during the installation.

table 31   Open Ports for a Satellites

Port	Description
1002	Agent
1003	Wordcache
1006	Wordcache
2001	The port used by a tunnel end-point listener. This port is used when you install other Gateways that tunnel to the Satellite.
3001	The proxy port on which Agents contact the Satellite.
4040	The Gateway `ident` service port, used by the Software Repository Cache.

➤ If you plan to install the SA Provisioning Boot Server and Media Server in the Satellite, then additional ports must be open. For a list of these ports, see Table 8 on page 52.

IPv6 Networking Option

To enable IPv6 networking, run the `enable_ipv6.sh` script as a post-installation or upgrade step. This enables IPv6 on HPSA core and satellite gateways and OS provisioning components on SA 10.2 or later releases. The script is available on all core, infrastructure, slices, boot servers, and satellite systems.

There are two new optional parameters for the enable_ipv6.sh script:

- -i <IPV6 address>: use specified IPV6 address instead of autodiscovered based on hostname DNS AAAA resolution.

- -n : do not start/restart SA components when making configuration file changes.

For more information, see Enabling IPv6 Networking Post-Installation.

For further information about IPv6 and the `enable_ipv6.sh` script, see "SA Remote Communications Administration" in the *SA Administration Guide*.

Satellite Installation

This section describes how to install a Satellite with the simple topology: a Satellite with a Single Core.

This topology has the following characteristics:

- The Satellite contains a single Software Repository Cache.

- The Satellite communicates with a single Management Gateway on a core server. No other gateways communicate with the Satellite. In other words, the Satellite is not part of a cascading Satellite installation in which one Satellite communicates with the core's Management Gateway while the cascaded Satellites communicate with the core using that Satellite's Gateway as an intermediary.

Required Information

Depending on the interview level you choose (simple, advanced), you will be prompted to supply the following information during the installation process as shown in Table 32. Parameters new to or renamed as of SA 9.x are indicated:

table 32   Satellite Installation Required Information Checklist

Parameter	Requirement	Description
truth.oaPwd	opsware_admin user access	The opsware_admin password.
cast.admin.pwd	SA Administrator's access	The SA Administrator's password
satellite.dcNm	The Satellite Facility identification	The name of the new Satellite's facility.
satellite.gateway_name	The name for a new or existing Satellite Gateway (name cannot contain spaces)	The name of the Gateway the Satellite will use for communications with the Primary Core management Gateway or other Satellite Gateways (in a cascaded Satellite topology).

table 32   Satellite Installation Required Information Checklist (cont'd)

Parameter	Requirement	Description
`satellite.proxy_port`	The port used by Agents to contact the new Satellite.	The port number on which agents can contact the Satellite Gateway. (Default: 3001).
`satellite.parentgw.ip`	A Core Management Gateway IP address	The IP address of a server running a Management Gateway.

`satellite.parentgw.`
`tunnel_listener_port`
	The Management Gateway's listener port	The port number through which tunnel connections to the Management Gateway will pass. (The default port is 2001.) The Management Gateway listens on this port for connection requests from the Satellite. In the Management Gateway Properties File, this port specified with the `opswgw.TunnelDst` parameter
		
		The path to the Core's Gateway Properties file is:
		
		`/etc/opt/opsware/`
		`opswgw-mgw0-<facility>/`
		`opswgw.properties`

`satellite.parentgw.` `proxy_port`	The port on which a Core's Management Gateway listens for connection requests.	The port number on which a Core's Management Gateway listens for connection requests from Satellite Gateways to SA Core Components (default 3003) or the port on which a Satellite Gateway listens for connection requests from other Satellite Gateways to SA Core Components (cascading Satellite links) (default 3001).
`decrypt_passwd`	Accessing Core cryptographic material	The password required to access the Core's cryptographic material.
`word_root`	Package Repository location (SA Provisioning)	The root directory for the Package Repository. For example: `/var/opt/opsware/word`
`word_tmp_dir`	Software Repository	Directory where Package Repository will temporarily place content during uploads. For example: `/var/opt/opsware/word`
`word.store.host`	Software Repository	The host name of the server where Software Repository content is stored.

Parameter	Requirement	Description
`media_server.` `linux_media`	Linux media location (SA Provisioning)	The pathname to the Linux media. For example: `/media/opsware/linux`
`media_server.` `sunos_media`	Solaris media location (SA Provisioning)	The pathname to the Solaris media. For example: `/media/opsware/sunos`
`media_server.` `windows_media`	Windows media location (SA Provisioning)	The pathname to the Windows media. For example: `/media/opsware/windows`
`media_server.windows_` `share_name`	Windows Media location (SA Provisioning)	The share name to use for the Windows media sharing server (note: share names that are longer than 8 characters may give errors while browsing or may not be accessible to some older clients.)
`media_server.windows_` `share_password`	Windows Media location (SA Provisioning)	The password to write-protect the Windows media share. Import_media tool will prompt for this password each time it is run.
`bootagent.host`	SA Provisioning Boot Server	The SA Provisioning Boot Server IP or hostname.
`agent_gw_list_args`	Agent- Gateway communications	The list of Gateways on which the the Satellite's agent will be installed. Specified by the IP address and port number (`ip:port`) on which Agents can contact the Gateway in the Satellite facility. Default *<satellite_gateway>*:3001.
`opswgw.ConfigPort`	Bandwidth configuration	The gateway Bandwidth Configuration Management port.
`opswgw.BwUsageChannel` `Port`	Bandwidth configuration	The gateway bandwidth usage channel port.
`agw_admin_port`	Bandwidth configuration	The port for the administrative interface of the Agent Gateway.

Satellite Installation Phases

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

table 33   Satellite Installation Phases

Phase	Description	Complete
1	Prepare for Installation	
2	Complete the Installer Interview	
3	Install the Satellite	
4	Install the SA Provisioning Components (optional)	
5	Post-Satellite Installation Tasks	

Phase 1: Prepare for Installation

1   Locate the SA *Satellite Base Including OS Provisioning* media.

2   On the server where you will install the new Satellite, mount the Satellite Base Including SA Provisioning media or NFS-mount the directory that contains a copy of the media contents.

➤ The Installer must have *read/write root* privileges to the directories where it will install the SA Core Components, including NFS-mounted network appliances.

3   In a terminal window, log in as a user with root privileges.

4   Create the Realm directory:

```
mkdir -p /var/opt/opsware/crypto/cadb/realm
```

5   If you have not already done so as described in Satellite Installation Requirements on page 177, copy the database of cryptographic material (`opsware-crypto.db.e`) from any Core server in the facility to the Satellite server. On the Core server, the database and the gzipped tar file are located in:

```
/var/opt/opsware/crypto/cadb/realm/opsware-crypto.db.e
```

➤ The database of cryptographic material must be copied to the same directory path and filenames on the Satellite server. The directory and database must be readable by the user that performs the installation.

If you initiate a Satellite installation on a server that does not have a copy of the cryptographic material, the installer will require you to copy the material to the server before it can continue.

In a Single Core installation, the cryptographic material is located in the `/var/opt/opsware/crypto/cadb/realm` directory on the Primary Core. In a Multimaster Mesh installation, the cryptographic material can be copied from the `/var/opt/opsware/crypto/cadb/realm` directory on any server that hosts a core component. If you have stored the cryptographic material on a remote, non-SA Core server, copy the file from the remote server's `/var/opt/opsware/crypto/cadb/realm` directory.

6   Create the following directory on the Satellite host:

```
/etc/opt/opsware/crypto
```

From the core to which the satellite will connect, copy the `/etc/opt/opsware/crypto/security.conf` file to the same directory on the Satellite host.

7   Create the directory `/var/opt/opsware/install_opsware/cdf/` to contain `cdf.xml`.

8 Copy the CDF from the core's Infrastructure Component bundle host:

```
/var/opt/opsware/install_opsware/cdf/cdf.xml
```

to the same location on the new Satellite host.

9 Change to the root directory:

```
cd /
```

10 Go to Phase 2.

Phase 2: Complete the Installer Interview

1 On the Satellite host, run the Installer script in interview mode by invoking it with no command-line options:

```
# <distro>/opsware_installer/hpsa_add_satellite.sh -c /var/opt/opsware/
install_opsware/cdf/cdf_<timestamp>.xml
```

You must specify the full path to the script.

2 A screen similar to the following displays:

```
Satellite Components to Install
===============================

1 ( ) Satellite
2 ( ) OS Provisioning Boot Server
3 ( ) OS Provisioning Media Server

Enter the choice number of the component you wish to add on
(<c>ontinue, <a>ll, <u>nselect all, <p>revious, <h>elp, <q>uit):
```

Press a to select all Satellite and SA Provisioning components or press the number associated with the component(s) you want to install.

➤ The SA Provisioning Boot Server and Media Server entries only appear when you have initiated the Satellite installation from the SA *Satellite Base Including OS Provisioning* media.

3 A screen similar to the following displays:

```
Interview Type
==============

1. Simple Interview
2. Advanced Interview
3. Expert Interview

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

Select 1 for a simple interview or 2 for an Advanced interview. The list in step 4 shows which parameters are modifiable in the Simple and Advanced interviews. The Expert interview is for the use of HP Technical Support or Professional Services only.

4 Provide values for parameters presented during the interview or accept defaults.

The parameter values requested during the interview depend on the interview mode:

a (truth.oaPwd)Please enter the password for the opsware_admin user
 - Simple and Advanced

b (cast.admin.pwd) Enter the password for the SA admin user
- Simple and Advanced

c (satellite.dcNm) Enter the new Satellite Facility name
-Advanced (Default is None. If you need to change this, select Advanced interview)

d (satellite.gateway_name) Enter the name of the Satellite Gateway
- Expert

e (satellite.proxy_port) Enter the port used by agents to contact the new Satellite
- Advanced

f (satellite.parentgw.ip) Enter the IP address of the First Core Management Gateway
- Simple and Advanced

g (satellite.parentgw.tunnel_listener_port) Enter the port number on which a Core's Management Gateway listens for connections from Satellite Gateways or the port on which a Satellite Gateway listens for connections from other Satellite Gateways (cascading satellite links)
- Advanced and Expert

h (satellite.parentgw.proxy_port) Enter the port on which the Management Gateway listens for Satellite connections
- Advanced and Expert

i (decrypt_passwd)Enter the password for the cryptographic material
- Expert

j (word_tmp_dir)Enter directory where Package Repository will temporarily place content during uploads. [/var/opt/opsware/wordbot_tmp/]
- Expert

k (word_root)Enter the root directory for the Package Repository [/var/opt/opsware/word]
- Advanced and Expert

l (media_server.linux_media)Enter the pathname of the Linux media [/media/opsware/linux]
- Advanced SA Provisioning

m (media_server.sunos_media)Enter the pathname of the Solaris media [/media/opsware/sunos]
- Advanced SA Provisioning

n (media_server.windows_media)Enter the pathname of the Windows media [/media/opsware/windows]
- Advanced SA Provisioning

o (media_server.windows_share_name)Enter the share name to use for the Windows media sharing server (note: share names that are longer than 8 characters may give errors while browsing or may not be accessible to some older clients.) [OSMEDIA]
-Expert

p (media_server.windows_share_password) Enter a password to write-protect the Windows media share. Import_media tool will prompt for this password each time it is run
- Expert

q (bootagent.host)Enter the OS Provisioning Boot Server ip or hostname
- Simple and Advanced SA Provisioning

> **r** (agent_gw_list_args)`Enter the IP address and port number (ip:port) on which agents can contact the gateway in this facility`
> - Advanced and Expert

5   Supply values for the parameters. When you have completed entering all of the required information, the Installer displays this message:

`All parameters have values. Do you wish to finish the interview (y/n):`

If you are satisfied with your answers, press y.

If you want to review or change your answers, press n. The installer displays the prompts again, showing in brackets [ ] the values that you just entered during the interview.

After modifying your responses, press `y` to finish the interview.

6   The Installer automatically saves your values into a CDF in `/var/tmp`.

Phase 3: Install the Satellite

The following steps apply when you use the *SA Satellite Base* media and are not installing the SA Provisioning components.

1   The `Components to Install` menu is displayed:

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

1 ( ) Satellite

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

Selection: 1
```

At the components prompt, select `1` to install the Satellite. Press `c` to continue.

2   Satellite installation begins.

When Satellite installation completes, the installer displays a message indicating that the installation was successful.

Phase 4: Install the SA Provisioning Components (Optional)

The SA Provisioning *Boot Server* and *Media Server* are required only if you want to use the SA Provisioning feature in the Satellite. The SA Provisioning Boot Server and Media Server can reside on a different server than the Satellite.

1   **[SA Provisioning Components on Satellite Host]** If you are installing the SA Provisioning components on a non-Satellite host, go to .

If you are installing the SA Provisioning components on the same host as the Satellite, invoke the Installer again with the `-c` option to specify the CDF created by the interview in :

`/opsware_system/opsware_installer/hpsa_add_satellite.sh -c <path>`

2   At the components prompt, select one or more components to install:

```
Welcome to the Opsware Installer.
Please select the components to install.
1 ( ) Satellite
```

```
2 ( ) OS Provisioning Boot Server
3 ( ) OS Provisioning Media Server

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

Selection:
```

Select `OS Provisioning Boot Server` and `OS Provisioning Media Server`. Press c to continue. the SA Installer installs the SA Provisioning components.

➤ If you plan to install the SA Provisioning Boot Server on the Satellite, but install the Media Server on a different host, select only `OS Provisioning Boot Server`, install that component then log on to the server that will host the Media Server and invoke the install script again with the CDF specified and install the Media Server.

3 **[SA Provisioning Components on non-Satellite Host]** If you are installing the SA Provisioning components on a *different* server than the Satellite, follow the instructions in this step.

    a   Copy the database of cryptographic material from the *Satellite host* to the SA Provisioning components host. These file are found on the Satellite host in the following location:

       `/var/opt/opsware/crypto/cadb/realm/opsware-crypto.db.e`

       The database of cryptographic material must have the same paths and filenames on both servers. The directory and files also need to be readable by the user that performs the installation.

    b   Copy the CDF created by the interview in step 6 on page 186 to the server that will host the SA Provisioning components.

    c   Using the *Satellite Base Including OS Provisioning* media, invoke the SA Installer again with the `-c` option and specify the CDF created by the interview in step 6 on page 186:

       `/opsware_system/opsware_installer/hpsa_add_satellite.sh -c <path>`

    d   At the components prompt, select one or more components to install:

```
Welcome to the Opsware Installer.

Please select the components to install.

1 ( ) Satellite
2 ( ) OS Provisioning Boot Server
3 ( ) OS Provisioning Media Server

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

Selection:
```

       Select `OS Provisioning Boot Server` and `OS Provisioning Media Server`. Press c to continue. The Boot Server and Media Server are installed

Phase 5: Post-Satellite Installation Tasks

After you install the Satellite, perform the tasks listed in the following sections. For more information, see the *Satellite Administration* section of the *SA Administration Guide*.

Facility Permission Settings

➤ This is an important step because until you set the facility permissions, you cannot view the new Satellite or view/modify the managed servers associated with the Satellite's facility.

The SA Gateway Installer assigns the Realm name to the facility name of the Satellite. To access managed servers in the Satellite, an SA user must belong to a group that has the necessary permissions for the Satellite's facility. For example, you might set the permissions for the Satellite facility to Read & Write for the Advanced Users group, enabling members of this group to modify the servers managed by the Satellite.

For instructions, see "Setting the Facility Permissions of a User Group" in the *SA Administration Guide*.

Checking the Satellite

To verify that the Core Management Gateway is communicating with the Satellite, perform the following steps:

1   Log in to the SA Client as a member of a user group that has the Manage Gateway permission.

2   From the Navigation panel, click **Administration ➤ Gateway**.

3   Verify that the upper left corner of the Manage Gateway page displays a link for the new Satellite.

    If the Manage Gateway page does not display the link for the Satellite, you may need to modify the Satellite properties file located in:

    `/etc/opt/opsware/opswgw-sat/opswgw.properties`

    If you modify the properties file, you must restart the Satellite:

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

4   Log in to the SA Client as a member of a user group that has Read (or Read & Write) permission for the Satellite facility.

5   From the Navigation panel, click **Servers ➤ Manage Servers**.

6   Verify that the Manage Server page displays the host name of the Satellite server.

DHCP Configuration for SA Provisioning

After you install the SA Provisioning Boot Server component, you must set up a DHCP server. For more information, see DHCP Configuration for SA Provisioning on page 161.

8 SA Configuration

SA Configuration

After you have installed the first SA Core, whether as part of a single host or Multimaster Mesh installation, the SA Core Components will be running and you will be able to log in to that core's SAS Web Client. You can now configure SA so that end users can start managing servers in their operational environment.

The following sections provide a general outline of the SA configuration tasks you will need to do and pointers to the HP documentation that contains the detailed instructions needed to complete the tasks.

Customized SA Core Configuration Files

After installing this release, you will be able modify certain SA Core configuration files and preserve those modification during subsequent core 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`)
- Model Repository (`word`)
- Command Engine (`occ`)
- Deployment Automation (`da`)
- Component of the Global File System (`hub`)
- Command Engine component (`way`)
- Model Repository Multimaster component (`vault`)
- Gateways (`opswgw`)

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

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

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

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

- `twist_custom.conf` is created for `twist.conf`

- `psrvr_custom.properties` is created for `psvr.properties`

- `waybot_custom.args` is created for `waybot.args`

New Configuration Files Created During SA 10.0 Installation

The SA component configuration files created are:

- `/etc/opt/opsware/spin/spin_custom.args`

- `/etc/opt/opsware/twist/twist_custom.conf`

- `/etc/opt/opsware/spoke/spoke_custom.conf`

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

- `/etc/opt/opsware/occ/psrvr_custom.properties`

- `/etc/opt/opsware/da/da_custom.conf`

- `/etc/opt/opsware/hub/hub_custom.conf`

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

- `/etc/opt/opsware/vault/vault_custom.conf`

- `/etc/opt/opsware/opswgw-<gateway_name>/opswgw.custom`

▶ For information about how SA handles customized core configuration files during an upgrade to SA 10.0, see the *SA Upgrade Guide*.

Configure e-mail Alerts

You can configure SA to send e-mail alerts to the SA administrator (or other designated users) when certain conditions are met, such as Managed Server error conditions or Multimaster Mesh conflicts. To do so, your e-mail administrator must configure the SA Core and Managed Servers as Sendmail clients. You should configure e-mail alerts In the SAS Web Client when you install Server Agents on your managed servers. For information about e-mail alerts, see the *SA Administration Guide*.

Set Up SA Groups and Users

You must assign the necessary access rights and permissions to SA administrators, users, and user groups. For example, to log in to the SAS Web Client, you specify a user name and password. Each user belongs to a user group, and each user group has a set of permissions that control access to features (actions), managed servers, and folders. For information about user access rights and permissions, see the "User and Group Setup and Security" chapter of the *SA Administration Guide*.

Create SA Customers

When you installed the First Core, whether Single Core or Multimaster, you specified a single default SA customer. For information about creating and assigning additional customers to a facility, see the "User and Group Setup and Security" chapter of the *SA Administration Guide*.

Define Software Management Policies

Software policies allow you to install software and configure applications simultaneously. A software policy can contain packages, RPM packages, patches, application configurations, and other software policies. After creating a software policy, you can attach it to servers or groups of servers. When you remediate a server or group of servers, the patches, packages, RPM packages, and application configurations specified in the attached policy are automatically installed and applied.

See the *SA User Guide: Software Management* for information.

Deploy Server Agents on Unmanaged Servers

After you install an Server Agent on an unmanaged server, it can be managed by Server Automation. For more information about deploying Server Agents on your unmanaged servers, see the *SA User Guide: Server Automation*.

Prepare SA for SA Provisioning

SA Provisioning is a feature that allows you to remotely install and uninstall operating systems (and related configurations, packages, and applications) on your servers. During SA Provisioning, a Server Agent is also installed, allowing the server to be immediately managed. For more information about configuring SA Provisioning, see the *SA User Guide: Provisioning*.

Prepare SA for Patch Management

The Patch Management for Windows feature enables you to identify, install, and remove Microsoft® Windows patches. With the SA Client user interface, you can identify and install patches for the Windows 2000, Windows 2003, and Windows NT4.0 operating systems. These patches include Service Packs, Update Rollups, and hotfixes. This feature also supports patching on 64 bit for Windows 2003 operating systems and for 32 bit for Windows XP operating systems.

For information about Windows patch management, see the *SA User Guide: Server Patching*.

SA Monitoring

SA provides several methods that you can use to ensure that your system is performing correctly:

— **Agent reachability tests**: to determine the current reachability of a specific Agent, you can run a Communication Test in the SA Client to find those servers that have unreachable agents. For more information about the Communications Test, see the *SA User Guide: Server Automation*.

— **System Diagnostic tests**: several system diagnostics tests are available in the SA Client that can help you determine that your SA installation is operating correctly and help you troubleshoot when there are problems. For more information about the SA System Diagnostic Tests, see the *SA Administration Guide*.

— **Core Component logs**: SA components have logs that can help you troubleshoot problems. For more information about Component Logs, see the *SA Administration Guide*.

9 SA Performance Scalability

This section provides information about improving the performance of your SA Core and its components..

You can vertically scale the SA Core Components, by adding additional CPUs and memory, or horizontally, by distributing the Core Components to multiple servers.

Table 34 and Table 35 list the recommended distribution of SA components across multiple servers. In both tables, the bundled SA Core Components are distributed in the following way:

- MR: Model Repository

- INFRA: Infrastructure Component

    — Model Repository Multimaster Component

    — Management Gateway

    — Primary Data Access Engine

- Slice(*x*):

    — Agent Gateway

    — Core Gateway

    — Command Engine

    — Software Repository

    — Command Center

    — Build Manager

    — Web Services Data Access Engine

    — Secondary Data Access engine)

    — Global File System

    — Software Repository Accelerator (`tsunami`)

    — Memcache

Core Component Distribution

The introduction of bundled components requires that you consider how to distribute the SA Core components based on the hardware and memory you have available. A typical SA 7.5 or later installation now has three main components. The Model Repository, the Infrastructure Component bundle and one Slice Component bundle in addition to the Media Server and Boot Server. Since the Media Server and Boot Server do not generate much load and often have environmental dependencies they are not listed in the tables below.

There is no infallible way to select hardware for an SA installation. However, below are some recommended SA Core Component layouts that should perform well. As you can see, scaling a core requires adding slices. Each slice adds highly available UI, API, OGFS, Build Manager and Gateway resources. Consider that, when you have a small number of core servers, it may be best to begin with two larger servers, then grow the capacity of the core by adding additional slices. In Table 34 and Table 35, the following shorthand is used:

MR — Model Repository

INFRA — Infrastructure Component bundle

Slice <X> — Slice Component bundle

OS Prov — Operating System Provisioning Component bundle. :

table 34   Small-to-Medium SA Deployment (SA 7.80 and later)

Managed Servers	SA Component Distribution by Server	
	Server 1	Server 2
500	MR, Infra, Slice 0, OS Prov	N/A
1000	MR	Infra, Slice 0, OS Prov

Server Configuration: 4 CPU cores, 16 GB RAM, 1 GB/s network

table 35   Medium-to-Large SA Deployment (SA 7.80 and later)

Managed Servers	SA Component Distribution by Server				
	Server 1*	Server 2*	Server 3*	Server 4*	Server 5*
2000	MR	Infra, Slice 0, OS Prov	N/A	N/A	N/A
4000	MR	Infra, Slice 0, OS Prov	Slice 1	N/A	N/A
6000	MR	Infra, Slice 0, OS Prov	Slice 1	Slice 2	N/A
8000	MR	Infra, Slice 0, OS Prov	Slice 1	Slice 2	Slice 3

* Server Configuration: 8 CPU Cores, 16 GB RAM, 1 GB/s network

Factors Affecting Core Performance

The hardware requirements for SA vary based on these factors:

- The number of servers that SA manages

- The number and complexity of concurrent operations

- The number of concurrent users accessing the Command Center

The number of facilities in which SA operates

Multimaster Mesh Scalability

To support global scalability, you can install an SA Core in each major facility, linking the cores in a Multimaster Mesh. The size of the SA Core in each facility can be scaled according to local requirements.

Multimaster Mesh Availability

In addition to Model Repository replication, a Multimaster Mesh supports the replication and caching of the packages stored in the Software Repository. Typically, the core in each facility owns the software that is uploaded to the core's Software Repository. To support availability, multiple copies of the packages can be maintained in remote Software Repositories. See the *SA Administration Guide* for more information.

The bundling of the Software Repository with the Slice Component bundle and the Software Repository Store with the Infrastructure Component bundle does not affect availability. The Software Repository reads the replicator configuration file to determine how to serve files from backed up directories.

Satellite Core CPU/Memory Requirements

Servers hosting SA Satellite Core installations must meet the following minimum requirement:

- 2 CPUs and 2 GB RAM per 1,500 managed servers per Satellite Core up to 4 CPUs and 4 GB RAM for 3000 managed servers per Satellite Core

The capacity of a server hosting an SA Satellite can be increased to support additional managed servers as indicated above. Workload characteristics across SA environments can vary dramatically and the carrying capacity of a given SA satellite under those workloads can vary as well. For deployments that require more than 3,000 devices behind an SA Satellite, HP recommends that you consider deploying additional SA satellites in the same realm. This solution provides increased redundancy and additionally avoids reaching the point of diminishing return from a single SA Satellite host server which requires you to continuously increase its capacity in order to support increasing load demands.

Load Balancing Additional Instances of Core Components

If SA must support a larger operational environment, you can improve performance by installing additional instances of the *Slice Component bundle* which provides you with these additional components per installation:

- Agent Gateway

- Core Gateway

- Command Center

- Software Repository

- Build Manager

- Web Services Data Access Engine

- Secondary Data Access engine

- Software Repository Accelerator (`tsunami`)

- Memcache

If you have installed multiple instances of the Slice Component bundle, load balancing between the instances occurs automatically as requests for load services are received by the Core Gateway. The Core Gateway handles incoming client connections and load balances them across the Slice Component bundles in the core.

You can also deploy a hardware load balancer for the servers that run additional instances of the Slice Component bundle. You can configure the load balancer for SSL session persistence (stickiness) with the least connections algorithm.

You can also put a load balancer in front of the Core Gateways, however, this will only load balance the Gateways, but with the added benefit that clients would have only one address to connect to and would failover gracefully in the event of a Slice Component bundle host failure.

Load Balancing does not affect validation of `httpProxy` certificates since the identity of the core is based on the address the clients use to connect, not the identity of the server that ultimately serves the request. All Slice Component bundles should be issued the same certificate and the hostname referenced in the certificate should match the DNS hostname that external clients use to connect. If a load balancer is used, this should be the hostname of the load balancer.

10 SA Core Uninstallation

This section describes how to uninstall a Single Core, remove a core from a Multimaster Mesh, and how to uninstall all cores of a Multimaster Mesh.

Uninstall Basics

There are several reasons that you might choose to uninstall an SA Core:

- Removing test installations
- Removing demonstration installations
- Merging or modifying a facility's Multimaster Mesh Cores
- Decommissioning or moving a facility

Make backups of your Model Repository, Software Repository, and your database of cryptographic material unless you are certain that you no longer need that data, because a complete core uninstallation also removes the Model Repository and the cryptographic material database and permanently deletes all the data.You can preserve the SA data in the Model Repository database by doing a database backup before uninstalling. See your Oracle documentation.

➤ Before you uninstall an SA Core, you should back up the Oracle database running on the server where that core's Model Repository is installed. See Oracle Database Backup Methods on page 261.

➤ The core's cryptographic material must be available during the uninstallation so that SA Core Components can be fully removed from the environment. If the cryptographic material is not available, the uninstallation will fail.

Procedures for Uninstalling Cores

You can perform any of the following uninstallation procedures according to your requirements:

- Uninstall a Single Core
- Uninstalling a Secondary Core in a Multimaster Mesh
- Uninstall All Cores in a Multimaster Mesh
- Decommission a Facility

Uninstall a Single Core

A single core can have all components installed on one host or may have some core components installed (distributed) on other hosts. To uninstall a single SA Core, perform the following tasks:

1   Before uninstalling a single core, you must deactivate all servers that host components for that Core using the SA Web Client. For more information about deactivating Core Component servers, see *Deactivating a Server* in the *Basic Server Management Tasks* section of the *SA User Guide: Server Automation*.

2   On the server hosting the core's Infrastructure Component bundle, log in asa user with root privileges.

3   Change to the root directory:

    cd /

4   Run the `uninstall_opsware.sh` script with the `-r` (specify response file) argument. You need to use the response file created when you installed the SA Core you are uninstalling:

    <distro>/opsware_installer/uninstall_ opsware.sh -r <response-file>

   where `<distro>` is the full path to the media. You must specify the full path the response file.

5   A menu similar to the following appears:

    Welcome to the Opsware Installer.
    Please select the components to uninstall.
    1 ( ) Software Repository - Content (install once per mesh)
    2 ( ) OS Provisioning
    3 ( ) Slice
    4 ( ) Core Infrastructure Components
    5 ( ) Model Repository, First Core
    6 ( ) Oracle RDBMS for SA

    Select one or more or all components to uninstall:

   Press `a` to select `all` components. If you must uninstall components one-at-a-time, for example due to a custom installation where core components have been distributed among multiple core component hosts, the components must be uninstalled in the order they appear on the menu above. For example, you would first log on to the SA Provisioning component host, run `uninstall_ opsware.sh -r <response-file>` and uninstall that component, then log into the Slice Component bundle host and run the uninstall script to remove that component, and so on down the list.

   You will be asked if you want to preserve the database of Cryptographic Material. If you enter `y`, the directory containing the database will not be removed during the uninstall.

   You will also see this prompt:

```
Are you absolutely sure you want to remove users' OGFS home and audit
directories? (home and audit directories will only be removed if they are
stored on the Software Repository server) (y/n)?
```

Select y if you want to remove the OGFS home and audit directories. If you press n, the directories will not be removed. Note that, if you have placed the OGFS home and audit directories on a server other than the server hosting the Software Repository, the uninstall will not remove those directories even if you press y.

6   After you have uninstalled all core components, you should remove the `/var/opt/opsware/install_opsware` directory.

▶   If you specified during the uninstall that you want to preserve the database of cryptographic material, you should *not* delete the `/var/opt/opsware/crypto` directory. This directory contains the database of your cryptographic material.

Uninstalling a Secondary Core in a Multimaster Mesh

▶   *Do not uninstall the First Core* (primary core) unless you plan to uninstall the entire Multimaster Mesh and all its cores. See Uninstall All Cores in a Multimaster Mesh on page 201 in this chapter for more information. This section describes only uninstalling *Secondary Cores* from a Multimaster Mesh.

To uninstall a single Secondary Core in a Multimaster Mesh, perform the following tasks

1   Log in to any SA Web Client available for that Mesh:

   a   If the Secondary Core to be uninstalled has a Data Access Engine that is currently serving as the Primary Data Access Engine for the core, you must first assign a Data Access Engine in another Core to serve as the Primary Data Access Engine.

      See "Reassigning the Data Access Engine to a Secondary Role" in the "SA Maintenance" chapter of the *SA Administration Guide*.

   b   Verify that all transactions have propagated to the other facilities in the Multimaster Mesh.

      For more information about verifying transaction traffic, see Verify Multimaster Transaction Traffic on page 145.

2   Decommission the facility for the core you will uninstall. 0

   a   See Decommission a Facility on page 203.

   b   On the *Infrastructure Component bundle host* in the core you are decommisioning, run the following command:

```
/opt/opsware/bin/python2
<distro>/opsware_installer/tools/reload_vaults.pyc  --certfile
/var/opt/opsware/crypto/gateway/spin.srv
```

   where <distro> is the full path to the mounted media. Successful output will be similar to this:

```
Core ID        Peers IDs Known To This Core
-------        ------------------------------
<nnn>            <nnn>
```

3   Stop and start the *Model Repository Multimaster Component* in all cores, except for the core that you will be uninstalling, by entering the following command as auser with root privileges on Infrastructure Component bundle host(s):

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

```
/etc/init.d/opsware-sas start vaultdaemon
```

4   Stop the Command Center (OCC) component (part of the Slice Component bundle). Log in as auser with root privileges to a Slice Component bundle host and enter the following command:

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

5   Stop all *Data Access Engines* (part of the Infrastructure Component bundle).

Log in as auser with root privileges to the Infrastructure Component bundle host and enter the following command:

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

➤   If the Command Center and the Data Access Engine are installed on different servers, you must also run the `stop spin` command on all Slice Component bundle hosts.

6   Stop the *Model Repository Multimaster Component*.

Log in as a user with root privileges to the Infrastructure Component bundle host and enter the following command:

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

7   On the Infrastructure Component bundle host, stop and start the *Data Access Engine* that serves as the **Primary** Data Access Engine by entering the following commands as root:

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

```
/etc/init.d/opsware-sas start spin
```

8   On Infrastructure Component bundle host for the core to be uninstalled, log in as a user with root privileges.

9   Change to the root directory:

```
cd /
```

10 Run the `uninstall_opsware.sh` script:

```
<distro</opsware_installer/uninstall_ opsware.sh -r <response-file>
```

where `<distro>` is the full path to the mounted media.

11 At the components prompt, select one or more or all components to uninstall:

```
Welcome to the Opsware Installer.
Please select the components to uninstall.
1 ( ) OS Provisioning
2 ( ) Slice
3 ( ) Infrastructure
2 ( ) Model Repository
1 ( ) Oracle RDBMS for SA
```

Select `a` for all. If you want to uninstall components separately, they must be uninstalled in the order they appear on the menu above. To do so, enter the number of the component to uninstall. For example, you would first log on to the SA Provisioning component host, run `uninstall_opsware.sh -r <response-file>` and uninstall that component, then log into the Slice Component bundle host and run the uninstall script to remove that component, and so on down the list.

12 You will be asked if you want to preserve the database of Cryptographic Material. If you respond y, the directory containing the database will not be removed during the uninstall.

You will also see this prompt:

```
Are you absolutely sure you want to remove users' OGFS home and audit
directories? (home and audit directories will only be removed if they are
stored on the Software Repository server) (y/n)?
```

Enter `y` if you want to remove the OGFS home and audit directories. If you enter `n`, the directories will not be removed. If you chose to place the OGFS home and audit directories on a server other than the server hosting the Software Repository, the uninstall will not remove those directories even if you enter y.

▶ If you installed the core using Custom Mode, it is important that you uninstall the components in the reverse order that they were installed.

13 After the uninstall has completed, remove the `/var/opt/opsware/install_opsware` directory.

▶ If you specified during the uninstall that you want to preserve the database of cryptographic material, you should *not* delete the `/var/opt/opsware/crypto` directory. This directory contains the database of cryptographic material.

Uninstall All Cores in a Multimaster Mesh

To uninstall all cores in a Multimaster Mesh, perform the following steps:

1 Stop the Command Engine (OCC) by logging on as a user with root privileges to a Slice Component bundle host and enter the following command:

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

2 Stop the Data Access Engine (`spin`).

Log in as a user with root privileges to the Infrastructure Component bundle host and enter the following command:

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

If the Command Engine and the Data Access Engine are installed on different servers, you must also run the `stop spin` command on the Slice Component bundle host(s).

3 Stop the Model Repository Multimaster Component in all cores by logging in to all Infrastructure Component bundle hosts and running the following command as a user with root privileges:

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

4 In each core, uninstall all SA components on the hosts on which they are installed. On the servers hosting the components to be uninstalled, log in as a user with root privileges.

5   Change to the root directory:

    `cd /`

6   Run the `uninstall_opsware.sh` script:

    `<distro>/opsware_installer/uninstall_ opsware.sh -r <response-file>`

    where `<distro>` is the full path to the mounted media.

7   At the components prompt, select one or more or all components to uninstall:

```
Welcome to the Opsware Installer.
Please select the components to uninstall.
1 ( ) OS Provisioning
2 ( ) Slice
3 ( ) Infrastructure
2 ( ) Model Repository
1 ( ) Oracle RDBMS for SA
```

Select `a` for all. If you want to uninstall components separately, they must be uninstalled in the order they appear on the menu above. To do so, enter the number of the component to uninstall. For example, you would first log on to the SA Provisioning component host, run `uninstall_opsware.sh -r <response-file>` and uninstall that component, then log into the Slice Component bundle host and run the uninstall script to remove that component, and so on down the list.

You will be asked if you want to preserve the database of Cryptographic Material. If you respond `y`, the directory containing the database will not be removed during the uninstall.

You will also see this prompt:

```
Are you absolutely sure you want to remove users' OGFS home and audit
directories? (home and audit directories will only be removed if they are
stored on the Software Repository server) (y/n)?
```

Enter `y` if you want to remove the Global File System (OGFS) home and audit directories. If you enter `n`, these directories will not be removed. If you placed the OGFS home and audit directories on a server other than the server hosting the Software Repository when you installed the core, the uninstall script will not remove those directories even if you enter `y`.

▶   If you installed the core using Custom Mode, it is important that you uninstall the components in the reverse order that they were installed.

8   After the uninstall has completed, remove the `/var/opt/opsware/install_opsware` directory.

▶   If you specified during the uninstall that you want to preserve the database of cryptographic material, you should *not* delete the `/var/opt/opsware/crypto` directory. This directory contains the database of cryptographic material.

Decommission a Facility

Performing this procedure does not shut down or uninstall SA in a facility. Decommission facilities with care, because this task cannot be undone.

When you decommission a facility, the facility is still listed in the SA Client, however, it is grayed out.

▶ **Note:** Short names cannot be reused, even if they belonged to a decommissioned facility.

Preliminary Steps

Before you decommission a facility, you must perform preliminary steps on that facility.

To perform preliminary steps:

1 Move managed servers from core facilities to satellites:

   a Log in to the managed server.

   b Linux: Update `/etc/opt/opsware/agent/opswgw.args`.

      Windows: Update `C:\Program files\Common\Opsware\etc\agent\opswgw.args`.

   c Change the IP address of the `opswgw.gw_list` to the satellite's IP address.

   d Restart the SA Agent.

      — Linux: `/etc/init.d/opsware-agent` restart.

      — Windows: Service, Opsware Agent: Restart

   e Run bs_hardware:

      — Linux: `/opt/opsware/agent/pylibs/cog/bs_hardware`

      — Windows: `C:\Program files\Opsware\agent\pylibs\cog\bs_hardware`

2 Manually cancel all wlm jobs and reschedule them on another mesh core.

3 Obtain the `migrate_sessions.py` and `migrate_sessions.sh` scripts from HP Support.

4 Reroute satellites associated with the decommissioned core to another core:

   a Log in to the satellite.

   b Update `/etc/opt/opsware/opswgw-<`*Name of the Satellite Facility*`>/` `opswgw.properties`

   c Change the `opswgw.TunnelSrc` Core IP address to the new Core's Infrastructure server IP address.

      — Give the new TunnelSrc an appropriate cost (optional).

   d Restart the gateway: `/etc/init.d/opsware-sas restart opswgw`

▶ **Note:** If you have cascading satellites, you only need to do this for the topmost satellite.

   e To verify, in the SA Client, navigate to Administration > Gateway > $Satellite-Facility > Tunnel. The Endpoint should display the New Core's Infrastructure server IP.

5 Move `way` jobs to another core, using the following example as a guide:

   If Core 3 is the core to be decommissioned, and Core 2 is the core where the `way` jobs will be transferred, issue the following commands from Core 3's slice server to move the `way` jobs:

   ```
   <distro>/opsware_installer/tools/migrate_sessions.sh -d 2 -f /var/tmp/
   wayjob3_2
   ```

usage:

```
migrate_sessions.sh  -d <destination_facility_id> -f <filename to hold the
session id>
```

Decommissioning

To decommission a facility with the SA Client, perform the following steps.

To decommission a facility using the SA Client:

1   In the SA Client, deactivate the SA agent on all of the core's component hosts. Make sure that the SA Agent's lifecycle displays a Deactivated status.

2   Go to Administration > Facilities.

3   In the list of facilities, right-click the core and chose Decommission. Make sure that the core's facility status is inactive.

4   Verify that all the jobs still run successfully.

After you have deactivated a facility, you must delete the deactivated core host. This prevents system diagnostic errors.

Appendix A: Oracle Setup for the Model Repository

This document explains how to install, configure, and maintain an Oracle database to support the SA Model Repository.

➤ This document is both an appendix in the SA Installation Guide and a standalone document. Sometimes the content of this document needs to be updated between releases. You can use the following URL to download the latest standalone version of this document from the HP Software Support portal after signing in with your HP Passport credentials:

> https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01253513

Supported Oracle Versions and Operating Systems

Support for the Model Repository is limited to certain versions of Oracle running on certain versions of operating systems. HP strongly recommends that you also apply the latest Oracle CPU or PSU patches.

See the *SA Support and Compatibility Matrix* associated with this release for a list of supported Oracle versions and operating systems.

➤ The *SA Support and Compatibility Matrix* is updated in every release, including minors and CORDs. You can use this URL to download the latest version from the HP Software Support portal after signing in with your HP Passport credentials:

> https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01253535

For additional versions, after logging into the HP Software Support portal, click the house icon to go to the home page, then use the SEARCH box to find any available product document.

System Requirements

The following sections list the system requirements for Oracle 11g and 12c. The SA Installer performs an automated check to ensure that these requirements are met on the Oracle host.

The system requirements and configurations listed in this section apply both to the SA-supplied Oracle RDBMS software as well as to non-SA-supplied Oracle RDBMS and software installations.

➤ If you create the database using the Oracle Universal Installer rather than the SA Installer, you must check for these packages and patches manually.

➤ The Oracle database must be installed either on its own host or on a server that has the SA Infrastructure Component bundle installed.

Database Server Time Requirements

Database servers must meet the following requirements. These time requirements do not apply to Managed Servers.

- All SA database servers must maintain synchronized system clocks. Typically, you will synchronize the system clocks through an external server that uses NTP (Network Time Protocol) services.

Linux Time Configuration

To configure the time zone on a Linux server, perform the following tasks:

1   Copy or link

    /usr/share/zoneinfo/UTC

    to

    /etc/localtime.

2   Ensure that the /etc/sysconfig/clock file contains the following lines:

    ZONE="UTC"
    UTC=true

Hostname Setup

1   You must be able to ping the database server hostname. To verify this, enter the following command:

    # ping <hostname>

2   Check that the database server name is FQDN by using the following command:

    # hostname -f

If the hostname is not configured correctly, Oracle will not start and you will encounter the following error:

    ORA-00600: internal error code, arguments: [keltnfy-ldmInit], [46], [1], [],
    [], [], [], []

Hardware Requirements

The server that will host the Oracle database for the Model Repository must meet the hardware requirements listed in this section.

Linux Requirements

The following are hardware requirements for running Oracle 11g and 12c under Linux.

- For detailed Linux requirements, see the *Oracle® Database Quick Installation Guide11g Release 2 (11.2) for Linux x86-64* (Part Number E24326-02) and *Oracle® Database Quick Installation Guide12c Release 1 (12.1) for Linux x86-64* (Part Number E17718-09) available at:

  http://docs.oracle.com

- Determine the processor type to verify that the processor's architecture matches the Oracle software release you will install. Use the following command to check system architecture:

    # uname -m

- The recommended physical memory is 16 GB or more of RAM. An HP-supplied Oracle installation will use a minimum of 2 GB memory. The Oracle SGA memory can be increased after database installation. You can use the following command to check memory status:

  ```
  grep MemTotal /proc/meminfo
  ```

- Required available swap space is shown in Table 36:

table 36   Required Available RAM Swap Space

RAM Between:	Available Swap Space
4 GB and 16 GB	Equal to the size of RAM
More than 16 GB	16 GB

You can use the following command to check swap space:

```
grep SwapTotal /proc/meminfo
```

- As of Oracle 11g, Automatic Memory Management (ASMM) requires more shared memory (`/dev/shm`) and file descriptors. Shared memory should be sized to be at least the greater of `MEMORY_MAX_TARGET` and `MEMORY_TARGET` for each Oracle instance on a database server.

  You can use the following command to check available shared memory:

  ```
  df –h /dev/shm/
  ```

- Free `tmp` space should be 1GB or more of `/tmp` directory space

  You can use the following command to check `tmp` space:

  ```
  df –h /tmp
  ```

Solaris, HP-UX and AIX Requirements

See also Oracle Solaris, HP-UX and IBM AIX Version and Package Requirements on page 217.

HP-UX and IBM

For HP-UX and IBM requirements, refer to the *Checking the Hardware Requirements* section in the following Oracle documents:

- *Oracle® Database Quick Installation Guide 11g Release 2 (11.2) for HP-UX Itanium, Part Number E24342-03*

- *Oracle® Database Quick Installation Guide 12c Release 1 (12.1) for HP-UX Itanium, Part Number E56893-01*

- *Oracle® Database Quick Installation Guide 11g Release 2 (11.2) for IBM AIX on POWER Systems (64-Bit), Part Number E24335-03*

- *Oracle® Database Quick Installation Guide 12c Release 1 (12.1) for IBM AIX on POWER Systems (64-Bit), Part Number E56891-01*

Oracle Solaris

For Oracle Solaris requirements, refer to the *Checking the Hardware Requirements* section in the following Oracle documents:

- *Oracle® Database Quick Installation Guide 11g Release 2 (11.2) for Oracle Solaris on SPARC (64-Bit), Part Number E24349-03*

- *Oracle® Database Quick Installation Guide 12c Release 1 (12.1) for Oracle Solaris on SPARC (64-Bit), Part Number E17756-08*

Model Repository (Database) Disk Space Requirements

Additional disk space is required for the Oracle software and the Model Repository data files. Keep in mind that storage requirements for the database grow as the number of managed servers and database activity grows.

As a benchmark figure, you should allow an additional 3.5 GB of database storage for every 1,000 servers in the facility that SA manages. When sizing the tablespaces, follow the general guidelines described in Table 37. If you need to determine a more precise tablespace sizing, contact your technical support representative.

table 37   Tablespace Sizes

Tablespace	MB/1000	Recommended Minimum Tablespace Size
AAA_DATA	256 MB	2000 MB
AAA_INDX	256 MB	2000 MB
AUDIT_DATA	256 MB	2000 MB
AUDIT_INDX	256 MB	2000 MB
LCREP_DATA	3000 MB	8000 MB
LCREP_INDX	2000 MB	8000 MB
TRUTH_DATA	1500 MB	4000 MB
TRUTH_INDX	500 MB	4000 MB
STRG_DATA	1300 MB	2000 MB
STRG_INDX	400 MB	2000 MB

Software Requirements

This section lists the requirements for running Oracle 11g and 12c under Red Hat Enterprise Linux, Oracle Enterprise Linux and SUSE Linux Enterprise Server.

Linux Requirements

The following are software requirements for running Oracle 11g and 12c under Red Hat Enterprise Linux, Oracle Enterprise Linux and SUSE Linux Enterprise Server:

- Required operating system version for 11g:
    - Oracle Linux 5 Update 2 (with Red Hat Compatible Kernel)
    - Oracle Linux 6 (with Red Hat Compatible Kernel)
    - Red Hat Enterprise Linux 5 Update 2
    - Red Hat Enterprise Linux 6
    - SUSE Linux Enterprise Server 10 SP2
    - SUSE Linux Enterprise Server 11
- Required operating system version for 12c:

- — Oracle Linux 5 Update 6 (with Red Hat Compatible Kernel)
- — Oracle Linux 6 (with Red Hat Compatible Kernel)
- — Red Hat Enterprise Linux 5 Update 6
- — Red Hat Enterprise Linux 6
- — SUSE Linux Enterprise Server 11 SP2

You can use the following command to determine the distribution and version of Linux installed:

```
# cat /proc/version
```

- Required Kernel version for Oracle Database 11g Release 2 (11.2):
  - — Oracle Linux 5 Update 2

    2.6.18 or later (with Red Hat Compatible Kernel)
  - — Oracle Linux 6

    2.6.32-71.el6.x86_64 or later (with Red Hat Compatible Kernel)
  - — Red Hat Enterprise Linux 6

    2.6.32-71.el6.x86_64 or later
  - — Red Hat Enterprise Linux 5 Update 2

    2.6.18 or later
  - — SUSE Linux Enterprise Server 10

    2.6.16.21 or later
  - — SUSE Linux Enterprise Server 11

    2.6.27.19 or later

- Required Kernel version for Oracle Database 12c Release 1 (12.1):
  - — Oracle Linux 5 Update 6

    2.6.18-238.0.0.0.1.el5 or later
  - — Oracle Linux 6 (with Red Hat Compatible Kernel)

    2.6.32-71.el6.x86_64 or later
  - — Red Hat Enterprise Linux 5 Update 6

    2.6.18-238.0.0.0.1.el5 or later
  - — Red Hat Enterprise Linux 6

    2.6.32-71.el6.x86_64 or later
  - — SUSE Linux Enterprise Server 11 SP2

    3.0.13-0.27 or later

You can use the following command to check the kernel versions:

```
uname -r
```

You can use the following command to check the platform:

```
uname -mi
```

You can use the following command to check the processor type:

```
grep "model name" /proc/cpuinfo
```

Linux Package Requirements

Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 for Oracle 11g

The following or later package versions for Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 (with Red Hat compatible kernel) must be installed (shaded rows indicate 32-bit packages):

➤ Starting with Oracle Database 11g Release 2 (11.2.0.2), all the *32-bit packages*, excepting `gcc-32bit-4.3`, listed in the following table are no longer required for installing a database on Linux x86-64. Only the 64-bit packages are required. However, for any Oracle Database 11g release before 11.2.0.2, both the 32-bit *and* 64-bit packages listed in the following table are required..

table 38   Required Packages for Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 for Oracle 11g

Required Packages	Version
binutils	2.17.50.0.6
compat-libstdc++	33-3.2.3
compat-libstdc++	33-3.2.3 (32-bit)
elfutils-libelf	0.125
elfutils-libelf-devel	0.125
gcc	4.1.2
gcc-c++	4.1.2
glibc	2.5-24
glibc	2.5-24 (32-bit)
glibc-common	2.5
glibc-devel	2.5
glibc-devel	2.5 (32-bit)
glibc-headers	2.5
ksh	NA
libaio	0.3.106
libaio	0.3.106 (32-bit)
libaio-devel	0.3.106
libaio-devel	0.3.106 (32-bit)
libgcc	4.1.2
libgcc	4.1.2 (32-bit)
libstdc++	4.1.2
libstdc++	4.1.2 (32-bit)
libstdc++-devel	4.1.2

table 38   Required Packages for Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 for Oracle 11g (cont'd)

Required Packages	Version
make	3.81
sysstat	7.0.2

Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 for Oracle 12c

The following or later package versions for Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 (with Red Hat compatible kernel) must be installed (shaded rows indicate 32-bit packages):

table 39   Required Packages for Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 for Oracle 12c

Required Packages	Version
binutils	2.17.50.0.6
compat-libstdc++	33-3.2.3
compat-libstdc++	33-3.2.3 (32-bit)
gcc	4.1.2
gcc-c++	4.1.2
glibc	2.5-58
glibc	2.5-58 (32-bit)
glibc-common	2.5
glibc-devel	2.5-58
glibc-devel	2.5-58 (32-bit)
ksh	NA
libaio	0.3.106
libaio	0.3.106 (32-bit)
libaio-devel	0.3.106
libaio-devel	0.3.106 (32-bit)
libgcc	4.1.2
libgcc	4.1.2 (32-bit)
libstdc++	4.1.2
libstdc++	4.1.2 (32-bit)
libstdc++-devel	4.1.2
libXext	1.0.1
libXext	1.0.1 (32-bit)
libXtst	1.0.1

Required Packages	Version
libXtst	1.0.1 (32-bit)
libX11	1.0.3
libX11	1.0.3 (32-bit)
libXau	1.0.1
libXau	1.0.1 (32-bit)
libXi	1.0.1
libXi	1.0.1 (32-bit)
make	3.81
sysstat	7.0.2

Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 for Oracle 11g

The following or later package versions for Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 (with Red Hat compatible kernel) must be installed:

table 40   Required Packages for Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 for Oracle
              11g

Required Packages	Version
binutils	2.20.51.0.2–5.11.el6 (x86_64)
compat-libcap1	1–1.10-1 (x86_64)
compat-libstdc++	33–3.2.3-69.el6 (x86_64)
compat-libstdc++	33–3.2.3-69.el6.i686
gcc	4.4.4-13.el6 (x86_64)
gcc-c++	4.4.4-13.el6 (x86_64)
glibc	2.12-1.7.el6 (x86_64)
glibc	2.12-1.7.el6 (i686)
glibc-devel	2.12-1.7.el6 (x86_64)
glibc-devel	2.12-1.7.el6.i686
ksh	NA
libaio	0.3.107-10.el6 (x86_64)
libaio	0.3.107-10.el6.i686
libaio-devel	0.3.107-10.el6 (x86_64)
libaio-devel	0.3.107-10.el6.i686
libgcc	4.4.4-13.el6 (x86_64)

table 40   **Required Packages for Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 for Oracle 11g (cont'd)**

Required Packages	Version
libgcc	4.4.4–13.el6 (i686)
libstdc++	4.4.4–13.el6 (x86_64)
libstdc++	4.4.4–13.el6.i686
libstdc++-devel	4.4.4–13.el6 (x86_64)
libstdc++-devel	4.4.4–13.el6.i686
make	3.81–19.el6
sysstat	9.0.4–11.el6 (x86_64)

Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 for Oracle 12c

The following or later package versions for Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 (with Red Hat compatible kernel) must be installed:

table 41   **Required Packages for Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 for Oracle 12c**

Required Packages	Version
binutils	2.20.51.0.2–5.11.el6 (x86_64)
compat-libcap1	1.10-1 (x86_64)
compat-libstdc++	33–3.2.3–69.el6 (x86_64)
compat-libstdc++	33–3.2.3–69.el6 (i686)
gcc	4.4.4–13.el6 (x86_64)
gcc-c++	4.4.4–13.el6 (x86_64)
glibc	2.12-1.7.el6 (x86_64)
glibc	2.12-1.7.el6 (i686)
glibc-devel	2.12-1.7.el6 (x86_64)
glibc-devel	2.12-1.7.el6 (i686)
ksh	NA
libaio	0.3.107–10.el6 (x86_64)
libaio	0.3.107–10.el6 (i686)
libaio-devel	0.3.107–10.el6 (x86_64)
libaio-devel	0.3.107–10.el6 (i686)
libgcc	4.4.4–13.el6 (x86_64)
libgcc	4.4.4–13.el6 (i686)
libstdc++	4.4.4–13.el6 (x86_64)

table 41   Required Packages for Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 for Oracle 12c (cont'd)

Required Packages	Version
libstdc++	4.4.4-13.el6 (i686)
libstdc++-devel	devel-4.4.4-13.el6 (x86_64)
libstdc++-devel	4.4.4-13.el6 (i686)
make	3.81-19.el6
sysstat	9.0.4-11.el6 (x86_64)

SUSE Linux Enterprise Server 10 for Oracle 11g

The following or later package versions for SUSE Linux Enterprise Server 10 must be installed:

table 42   Required Packages for SUSE Linux Enterprise Server 10 for Oracle 11g

Required Packages	Version
binutils	2.16.91.0.5
compat-libstdc++	5.0.7
gcc	4.1.0
gcc-c++	4.1.2
glibc	4.1.2
glibc-devel	2.4-31.63
glibc-devel	32bit-2.4-31.63
ksh	93r-12.9
libaio	0.3.104
libaio	32bit-0.3.104
libaio-devel	0.3.104
libaio-devel	32bit-0.3.104
libelf	0.8.5
libgcc	4.1.2
libstdc++	4.1.2
libstdc++-devel	4.1.2
make	3.80
numactl	0.9.6.x86_64
sysstat	8.0.4

SUSE Linux Enterprise Server 11 for Oracle 11g

The following or later package versions for SUSE Linux Enterprise Server 11 must be installed:

table 43   Required Packages for SUSE Linux Enterprise Server 11for Oracle 11g

Required Packages	Version
binutils	2.19
gcc	4.3
gcc	32bit-4.3
gcc-c++	4.3
glibc	2.9
glibc	32bit-2.9
glibc-devel	2.9
glibc-devel	32bit-2.9
ksh	93t
libaio	0.3.104
libaio	32bit-0.3.104
libaio-devel	0.3.104
libaio-devel	32bit-0.3.104
libgcc43	4.3.3_20081022
libstdc++-devel	4.3
libstdc++33	3.3.3
libstdc++33	32bit-3.3.3
libstdc++43	4.3.3_20081022
libstdc++43	32bit-4.3.3_20081022
libstdc++43-devel	4.3.3_20081022
libstdc++43-devel	32bit-4.3.3_20081022
make	3.81
sysstat	8.1.5

SUSE Linux Enterprise Server 11 for Oracle 12c

The following or later package versions for SUSE Linux Enterprise Server 11 must be installed:

table 44   Required Packages for SUSE Linux Enterprise Server 11 for Oracle 12c

Required Packages	Version
binutils	2.21.1-0.7.25
gcc	4.3-62.198
gcc-c++	4.3-62.198
glibc	2.11.3-17.31.1
glibc-devel	2.11.3-17.31.1
ksh	93u-0.6.1
libaio	0.3.109-0.1.46
libaio-devel	0.3.109-0.1.46
libcap1	1.10-6.10
libgcc46	4.6.1_20110701-0.13.9
libstdc++33	3.3.3-11.9
libstdc++33	3.3.3-11.9 (32-bit)
libstdc++43-devel	4.3.4_20091019-0.22.17
libstdc++46	4.6.1_20110701-0.13.9
make	3.81
sysstat	8.1.5-7.32.1
xorg-x11-libs	7.4 (x86_64)
xorg-x11-libs	7.4 (32-bit)
xorg-x11-libX11	7.4 (x86_64)
xorg-x11-libX11	7.4 (32-bit)
xorg-x11-libXau	7.4 (x86_64)
xorg-x11-libXau	7.4 (32-bit)
xorg-x11-libxcb	7.4 (x86_64)
xorg-x11-libxcb	7.4 (32-bit)
xorg-x11-libXext	7.4 (x86_64)
xorg-x11-libXext	7.4 (32-bit)

Verifying that Packages are Installed

To verify that RPMs are installed under Linux, enter the following command:

```
rpm -q --qf '%{NAME}-%{VERSION}-%{RELEASE} (%{ARCH})\n' <rpm_name>
```

Oracle Solaris, HP-UX and IBM AIX Version and Package Requirements

For Oracle Solaris, HP-UX and IBM AIX operating system, compiler, patch and any additional software requirements, see the *Checking the Software Requirements* section in the *Oracle® Database Quick Installation Guide* for your operating system.

Non-SA-Supplied Oracle Software and Database Setup

➤ If you plan to install the SA-supplied Oracle RDBMS software and database, you do not need to perform the tasks in this section. The SA Installer performs all the tasks discussed below. For information about installing the SA-supplied Oracle software and database, see SA-Supplied Oracle RDBMS Software and Database Setup on page 225.

If you plan to use a non-SA-supplied Oracle database with the SA Model Repository, the following steps are required for compatibility with SA. You should also review System Requirements on page 205 before preceding with this section.

Modifiable Kernel Parameters

If you manually install the Oracle database, or use an existing database, you must insure that all kernel parameter values are specified correctly for your environment but also within the limitations required by SA.

You can find additional information about kernel parameter configuration in the *Configuring Kernel Parameters* section of the *Oracle® Database Quick Installation Guide.*

Modifiable Kernel Parameter Values for Linux

This section identifies the kernel parameters you can change for supported Linux operating systems.

You can change values for the following parameters in /etc/sysctl.conf. If the current value of any parameter is higher than the value listed in this table, then do not change the value of that parameter:

```
#SA Oracle parameters begin
fs.aio-max-nr=1048576
fs.file-max=6815744
kernel.shmmax=2147483648
kernel.shmall=2097152
kernel.shmmni=4096
kernel.sem=250 32000 100 128
net.core.rmem_default=262144
net.core.rmem_max=4194304
net.core.wmem_default=262144
net.core.wmem_max=1048586
net.ipv4.ip_local_port_range=9081 65500
net.ipv4.tcp_wmem=262144 262144 262144
net.ipv4.tcp_rmem=4194304 4194304 4194304
```

```
#SA Oracle parameters end
```

You can change values for the following parameters in `/etc/security/limits.conf`:

```
#SA Oracle parameters begin
oracle soft nofile 1024
oracle hard nofile 65536
oracle soft nproc 2047
oracle hard nproc 16384
oracle soft stack 10240
oracle hard stack 32768
#SA Oracle parameters end
```

You can change values for the following parameters in `/etc/pam.d/login`:

```
session required pam_limits.so
```

You can change values for the following parameter in `/etc/fstab`:

```
shmfs /dev/shm tmpfs size=4g 0
```

You can change values for the following parameters in `/etc/selinux/config`:

```
#SA Oracle parameters begin
SELINUX=disabled
#SA Oracle parameters end
```

Modifiable Kernel Parameter Values for SUSE Linux x86_64

This section identifies additional required settings for SUSE Linux x86_64 when running Oracle 11g or 12c:

- Enter the following command to cause the system to read the `/etc/sysctl.conf` file when it restarts:

  ```
  # /sbin/chkconfig boot.sysctl on
  ```

- You must enter the GID of the `oinstall` group as the value for the parameter `/proc/sys/vm/hugetlb_shm_group`. Doing this grants members of `oinstall` a group permission to create shared memory segments. For example, where the oinstall group GID is 501:

  ```
  # echo 501 > /proc/sys/vm/hugetlb_shm_group
  ```

  After running this command, use vi to add the following text to /etc/sysctl.conf, and enable the boot.sysctl script to run on system restart:

  ```
  vm.hugetlb_shm_group=501
  ```

▶ Only one group can be defined as the `vm.hugetlb_shm_group`.

Modifiable Kernel Parameter Values for Oracle SPARC Solaris (64 bit), HP-UX and IBM AIX

Refer to the *Configuring Kernel Parameters* section in the following Oracle documents:

- *Database Quick Installation Guide for Oracle Solaris on SPARC (64 Bit)*
- *Database Quick Installation Guide for HP-UX Itanium*
- *Database Quick Installation Guide for IBM AIX on POWER Systems (64-Bit)*

Oracle Database Installation Steps

In order to install an Oracle database for use with the SA Model Repository, you must perform the following tasks which are explained in more detail in the following sections:

1 Create the database with the UTF8 database character set

2 Set the database with `TIME_ZONE` to `'+00:00'`

3 Create the database with the required initialization (`init.ora`) parameters

4 Create the database with required tablespaces

5 Create the database user `opsware_admin`

6 `tnsnames.ora` file requirements

7 File linking requirements

8 Enable Oracle Daylight Savings Time (DST)

9 `sqlnet.ora` file requirements

1. UTF8 Database Character Set

Create the database with the UTF8 database character set:

```
CHARACTER SET UTF8
```

2. Set the Database TIME_ZONE

Create the database with `TIME_ZONE` set to `'+00:00'`:

```
SET TIME_ZONE = '+00:00'
```

3. Specify the Required Initialization (init.ora) Parameters

Create the database instance with the following initialization (`init.ora`) parameters. For parameters not listed, SA assumes that the default Oracle parameters are used.

Oracle 11.2.0.x

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

```
session_cached_cursors := required to be >= 50
undo_tablespace := should be = UNDO or other UNDO tablespace
undo_management := should be = AUTO
_complex_view_merging := required to be = FALSE
```

Oracle 12.1.0.x

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

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

4. Create the Required Tablespaces

The following tablespaces must be created to support SA. For tablespace disk space requirements, see Model Repository (Database) Disk Space Requirements on page 208.

- LCREP_DATA
- LCREP_INDX
- TRUTH_DATA
- TRUTH_INDX
- AAA_DATA
- AAA_INDX
- AUDIT_DATA
- AUDIT_INDX
- STRG_DATA
- STRG_INDX

5. Create the Database User opsware_admin

Create the database user 'opsware_admin' with the following privileges.

```
SQL> create user opsware_admin identified by opsware_admin
default tablespace truth_data temporary tablespace temp
```

```
quota unlimited on truth_data;
SQL> grant alter session to opsware_admin with admin option;
SQL> grant create procedure to opsware_admin with admin option;
SQL> grant create public synonym to opsware_admin with admin option;
SQL> grant create sequence to opsware_admin with admin option;
SQL> grant create session to opsware_admin with admin option;
SQL> grant create table to opsware_admin with admin option;
SQL> grant create trigger to opsware_admin with admin option;
SQL> grant create type to opsware_admin with admin option;
SQL> grant create view to opsware_admin with admin option;
SQL> grant delete any table to opsware_admin with admin option;
SQL> grant drop public synonym to opsware_admin with admin option;
SQL> grant select any table to opsware_admin with admin option;
SQL> grant select_catalog_role to opsware_admin with admin option;
SQL> grant query rewrite to opsware_admin with admin option;
SQL> grant restricted session to opsware_admin with admin option;
SQL> grant execute on dbms_utility to opsware_admin with grant option;
SQL> grant analyze any to opsware_admin;
SQL> grant insert, update, delete, select on sys.aux_stats$ to opsware_admin;
SQL> grant gather_system_statistics to opsware_admin;
SQL> grant create job to opsware_admin with admin option;
SQL> grant create any directory to opsware_admin;
SQL> grant drop any directory to opsware_admin;
SQL> grant alter system to opsware_admin;
SQL> grant create role to opsware_admin;
SQL> grant create user to opsware_admin;
SQL> grant alter user to opsware_admin;
SQL> grant drop user to opsware_admin;
SQL> grant create profile to opsware_admin;
SQL> grant alter profile to opsware_admin;
SQL> grant drop profile to opsware_admin;
```

6. tnsnames.ora File Requirements

The `tnsnames.ora` file enables resolution of database names used internally by the core components.
SA has the following requirements for the `tnsnames.ora` file:

- The file must reside in the following locations:

  ```
  /var/opt/oracle/tnsnames.ora
  $ORACLE_HOME/network/admin
  ```

- If the core is installed across multiple servers, a copy of the file must reside on the servers hosting the following components:

  — Model Repository

  — Infrastructure Component bundle (required by the Data Access Engine, Model Repository Multimaster Component, Software Repository Store)

  — Slice Component bundle (required by the Command Center, Web Services Data Access Engine, Global File System)

- For a core installed on multiple servers, the directory path of the `tnsnames.ora` file must be the same on each server.

- In a Single Core installation, the `tnsnames.ora` file must contain an entry for the Model Repository, as in the following example:

```
truth = DESCRIPTION= (ADDRESS=(HOST=magenta.example.com)(PORT=1521)
(PROTOCOL=tcp)) (CONNECT_DATA=(SERVICE_NAME=truth)))
```

tnsnames.ora: Multimaster Mesh Requirements

In a Multimaster Mesh, the `tnsnames.ora` file must be set up for a Source Core and a Destination Core using the following guidelines.

Source Core

The `tnsnames.ora` file must contain an entry for its own Model Repository. The port number must be set to the port that you have designated that the Oracle listener process use, such as `1521` `(default)`, `1526`, and so on.

The `tnsnames.ora` file must also contain an entry that specifies the Source Core Management Gateway. This port is used by the Data Access Engine for Multimaster traffic. The port number is derived from the following formula: (20000) + (facility ID of the Destination Core).

Example: In the following example, the TNS service name of the Source Core is `orange_truth`, which runs on the host `orange.example.com`. The TNS name of the Destination Core is `cyan_truth`, which has a facility ID of `556`. Note that the entry for `cyan_truth` specifies `orange.example.com`, which is the host running the Source Core's Management Gateway.

```
orange_truth=(DESCRIPTION=(ADDRESS=(HOST=orange.example.com)(PORT=1521)
(PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
cyan_truth=(DESCRIPTION=(ADDRESS=(HOST=orange.example.com)(PORT=20556)
(PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
```

Destination Core

The `tnsnames.ora` file must contain an entry for its own Model Repository. The port number must be set to the port that you have designated that the Oracle listener process use, such as `1521` (default), `1526`, and so on. The `tnsnames.ora` file does not require any entries for other cores in the mesh.

Example: In the following example, the TNS service name of the Destination Core is `cyan_truth`, and the core runs on the host, `cyan.example.com`.

```
cyan_truth=(DESCRIPTION=(ADDRESS=(HOST=cyan.example.com)(PORT=1521)
(PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
```

7. File Linking Requirements:

After creating the database, but before installing the Model Repository with the SA Installer, perform the following tasks:

1   Create the `tnsnames.ora` file in the following directory:

```
/var/opt/oracle
```

Verify that the file conforms to the rules listed in .

2   If it does not exist, create the following directory:

```
mkdir -p /var/opt/oracle
```

3   Create the following symbolic link:

```
ln -s /var/opt/oracle/tnsnames.ora $ORACLE_HOME/network/admin/tnsnames.ora
```

4   Ensure that the oracle Unix user has read-write permission on the `tnsnames.ora` file.

For Red Hat Enterprise Linux:

1   Create another symbolic link:

```
        ln -s /etc/oratab /var/opt/oracle/oratab
```
Next:

1   Copy the sample `opsware-oracle` script to `/etc/init.d/`.

2   Link `/etc/init.d/opsware-oracle` to corresponding scripts in the `/etc/rc*` directories. For example:

```
ln -s /etc/init.d/opsware-oracle \
       /etc/rc0.d/K02opsware-oracle
ln -s /etc/init.d/opsware-oracle \
       /etc/rc1.d/K02opsware-oracle
ln -s /etc/init.d/opsware-oracle \
       /etc/rc2.d/S60opsware-oracle
ln -s /etc/init.d/opsware-oracle \
       /etc/rcS.d/K02opsware-oracle
```

8. Enable Oracle Daylight Savings Time (DST)

To enable Daylight Saving Time for the Oracle database, you must apply database tier patches. To apply these patches, perform the following steps:

1   Verify that your database is running on Oracle 11g, 12c or higher.

2   Use MetaLink Note 412160.1 to apply Oracle Database time zone fixes specific to your database version.

Use MetaLink Note 412160.1 to apply time zone fixes to the Oracle Java Virtual Machine (JVM) in the Oracle Database specific to your E-Business Suite database version.

9. sqlnet.ora requirements

Some applications in Server Automation use the oracle `classes12.jar` file to connect to the database. To enable these utilities to connect to the Oracle 12C database, create a `sqlnet.ora` in the `$ORACLE_HOME/network/admin` folder in *both* the SA Client system and the SA Core Database server with the following contents:

```
# File:         sqlnet.ora
# Certified:    Oracle 12.1.0
# Purpose:      Configuration File for all Net8 Clients
# Notes:        None

LOG_DIRECTORY_SERVER=/u01/app/oracle/product/12.1.0/db_1/network/log
LOG_FILE_SERVER=sqlnet.log
TRACE_DIRECTORY_SERVER=/u01/app/oracle/product/12.1.0/db_1/network/trace
TRACE_FILE_SERVER=sqlnet.trc
NAMES.DIRECTORY_PATH= (TNSNAMES)
SQLNET.INBOUND_CONNECT_TIMEOUT=180
SQLNET.ALLOWED_LOGON_VERSION_SERVER=8
SQLNET.ALLOWED_LOGON_VERSION_CLIENT=8
```

SA Database Installation Sample Scripts

HP Support can provide sample scripts for steps 1 through 5 of the Oracle Database Installation Steps.

Oracle/SA Installation Scripts, SQL Scripts, and Configuration Files

- **truth.sh**: A shell script that creates directories and then launches the `truth.sql` script. Running this script causes all the scripts to be run automatically, in the correct order.

- **truth.sql**: Prompts for passwords of the `SYS` and `SYSTEM` users and launches the remainder of the SQL scripts in this list.

- **CreateDB.sql**: Creates a database with the UTF8 character set and `TIME_ZONE` set to `'+00:00'`

- **CreateDBFiles.sql**: Creates the following tablespaces that are required by SA:

  ```
  LCREP_DATA
  LCREP_INDX
  TRUTH_DATA
  TRUTH_INDX
  AAA_DATA
  AAA_INDX
  AUDIT_DATA
  AUDIT_INDX
  STRG_DATA
  STRG_INDX
  ```

  See Model Repository (Database) Disk Space Requirements on page 48 for additional tablespace sizing information.

- **CreateDBCatalog.sql** : Runs Oracle scripts to create data system catalog objects.

- **JServer.sql**: Sets up the Oracle Java environment.

- **CreateAdditionalDBFiles.sql**: Adds data and index files to certain tablespaces and allocates additional disk space. This script is optional, but recommended.

- **CreateUserOpsware_Admin.sql**: Creates the `opsware_admin` database user and grants permissions (privileges) to this user (required by SA).

- **postDBCreation.sql:** Creates the `spfile` from the `pfile` (parameter file).

- **init.ora**: Contains initialization parameters for the database. See 3. Specify the Required Initialization (init.ora) Parameters on page 219.

- **tnsnames.ora**: Enables resolution of database names used internally by SA.

- **listener.ora**: Contains configuration parameters for the listener. SA by default listens on port 1521. You can change the default port during installation or by editing the tsnames.ora file.

➤ The SA-supplied Oracle 12.1.0.1 database has a new `listener.ora` parameter:

```
SUBSCRIBE_FOR_NODE_DOWN_EVENT_LISTENER=
```

Default is OFF. This parameter must be set to OFF for non-RAC installations. For more information about this parameter, see the Oracle documents IDs 372959.1 and 437598.1.

- **bash_profile** or **profile**: Sets environment variables and sets shell limits for the `oracle` Unix user.

- **opsware-oracle**: A script residing in `/etc/init.d` that starts up and shuts down the database and listener.

➤ The `/etc/init.d/opsware-sas` start script, which starts and stops the SA components, does not start and stop the database and listener. For more information on the `opsware-sas` start script, see "Start Script for SA" in the *SA Administration Guide*.

Creating the Database using the SA-Supplied Scripts

To create the Oracle database using the SA-supplied scripts, perform the following steps:

1   Obtain the database creation scripts from your HP support representative.

2   Make any required changes to the scripts.

3   As a user with root privileges, create the Unix user `oracle` and log in to the server as the user `oracle`.

4   Copy the SA-supplied files to the following directory:

`$ORACLE_BASE/admin/truth/create`

5   Change the mode of the SA-supplied `truth.sh` script:

`chmod 755 truth.sh`

6   Launch the SQL scripts that create the database by running the `truth.sh` script:

`./truth.sh`

7   After the scripts launched by `truth.sh` complete, check the log files in the following directory for errors:

`/u01/app/oracle/admin/truth/scripts/*.log`

SA-Supplied Oracle RDBMS Software and Database Setup

▶   If you plan to install the Oracle RDBMS software and database yourself, you do not need to perform the tasks in this section. See Non-SA-Supplied Oracle Software and Database Setup on page 217.

If you plan to use a SA-supplied Oracle database with the SA Model Repository, you should read the following sections for information about what the SA Installer does when installing the Oracle software and database during SA installation. The SA Installer performs all the tasks discussed below. You should also review System Requirements on page 205 before proceeding with this section.

SA-Supplied RDBMS Configuration Details

When you install the SA-supplied Oracle RDBMS using the SA Installer Oracle installation option, the installer:

- Checks that all requirements are met on the host server (see System Requirements on page 205).

- Sets certain kernel parameters to required values (see Modifiable Kernel Parameters on page 217).

- Creates the Unix user `oracle` locally in `/etc/passwd`.

- Creates the Unix groups `dba` and `oinstall` locally in `/etc/group`.

- Sets the `$ORACLE_HOME` environment variable to the following directory:

`/u01/app/oracle/product/12.1.0/db_1`

- Sets the `$ORACLE_SID` environment variable to `truth`.

- Creates a database with the UTF8 character set, `TIME_ZONE` set to `'+00:00'` and with required `init.ora` parameters.

- Creates the tablespaces and data and index files under the following directories:

```
/u01/oradata/truth
/u02/oradata/truth
/u03/oradata/truth
/u04/oradata/truth
```

The system administrator can configure the `/u01`, `/u02`, `/u03`, `/u04` directories before installing the Oracle RDBMS software.

- Gets the service name (TNS name) from the SA Installer interview (`truth.servicename` prompt) and inserts it into the `tnsnames.ora` file in `$ORACLE_HOME/network/admin` and `/var/opt/oracle`. The SA Installer changes the value of the `host` parameter in `tsnames.ora` to the value returned by the Unix `hostname` command.

- In the `$ORACLE_HOME/network/admin/listener.ora` file, changes the value of the `host` parameter to the value returned by the Unix `hostname` command.

  The listener is password protected and OS authenticated. (The default password is `opsware`.) By default, it listens on port 1521.

- Creates the `$ORACLE_HOME/network/admin/sqlnet.ora` file that allows older client versions to connect to the Oracle 12C database.

- Creates the `/etc/init.d/opsware-oracle` script, which you can use to start up and shut down the database and listener.

  This script is linked to corresponding scripts in the `/etc/rc*.d` directories.

- Creates the user `opsware_admin` with the required privileges.

- After installation is complete, you can examine the logs that are created here:

  `/var/log/opsware/install_opsware`

Security

SA recommends that you change the default passwords for the following:

- the Unix user `oracle`

- the Oracle database users SYS and SYSTEM

  SA does not use the SYS and SYSTEM users.

- the Oracle listener

  In the `/$ORACLE_HOME/network/admin/listener.ora` file, SA sets the value of the host parameter to the value returned by the Unix hostname command. The listener is password protected and OS authenticated. The default password is `opsware`. By default, the Oracle listener uses port 1521.

SA-Supplied Oracle Installation Procedure

SA supports the following SA/Oracle database configurations:

- SA Core and Oracle database on a single host

- SA Core with the Oracle database on a remote database server

See Chapter 2, "SA Core Configurations Supported For Customer Installation" for a description of supported SA Core/Oracle database configurations and Chapter 5, "SA Core Installation" for installation instructions.

Installing the Model Repository Database on a Remote Server

To install or upgrade the Model Repository Oracle database on a remote server, perform the following tasks:

1   Perform the following tasks on the server on which you will run the SA Installer:

   a   Install the Oracle Full Client software.

       The steps below use `/u01/app/oracle/product/12.1.0/client_1` as the Oracle Full Client home.

▶   The Oracle Full Client must be the same version as the Oracle database.

   b   Ensure that the Oracle Full Client software is owned by the OS user `oracle`.

   c   Copy the database server's `/var/opt/oracle/tnsnames.ora` file to the client machine's `/var/opt/oracle/tnsnames.ora`. Ensure that the hostname in the file resolves properly.

   d   If it does not exist, create the following directory:

       `mkdir -p /var/opt/oracle`

   e   Create the following symbolic link:

       `# ln -s /var/opt/oracle/tnsnames.ora $ORACLE_HOME/network/admin/tnsnames.ora`

   f   Ensure that the Unix user `oracle` has read-write permission on the `tnsnames.ora` file.

   g   Ensure that the `$ORACLE_HOME/network/admin/sqlnet.ora` file is created in both the client as well as the Oracle Database Server as described in step 9 under the section Oracle Database Installation Steps on page 219.

   h   Ensure that the SA Installer Core Definition File (CDF) has the correct path to the client `tnsnames.ora` file (`%truth.tnsdir`), oracle client home (`%db.orahome`), database server name/IP (`%db.host`), listener port (`%db.port`), SA Installer machines subdomain (`%truth.dcSubDom`), and so on. Based on the above steps your parameter values will be:

       –   `%truth.tnsdir=/var/opt/oracle`

       –   `%db.orahome=/u01/app/oracle/product/12.1.0/client_1`

       –   `%db.port=1521`

       –   `%truth.dcSubDom=prod.example.com`

       –   `db.host=192.168.9.99` (server on which the Oracle database is installed)

   i   Ensure that the `COMPATIBLE` parameter is set correctly and that it matches the database version. For example, for database software that is version 12.1.0.1 ensure that `COMPATIBLE=12.1.0.1`. SA uses Oracle's Export Data Pump and Import Data Pump utilities during secondary core creation. These utilities require the `COMPATIBLE` parameter be specified correctly.

2   Perform the following tasks on the Model Repository host:

   a   Log in as the user `oracle`.

   b   Ensure that the listener is started with the command:

       `lsnrctl start <your_listener_name>`

Oracle RAC Support

SA supports Oracle Real Application Clusters (RAC).

➤ Oracle RAC support requires a new installation of both Oracle and SA. Therefore, in order to enable Oracle RAC support in SA, you must first install Oracle RAC 11g or Oracle RAC 12c, configured as described in the following sections.

Supported Oracle Versions and Operating Systems

Support for the Model Repository is limited to certain versions of Oracle running on certain versions of operating systems. HP strongly recommends that you also apply the latest Oracle CPU or PSU patches.

- See the *SA 10.2 Support and Compatibility Matrix* for a list of supported Oracle versions and operating systems.

➤ The *SA Support and Compatibility Matrix* is updated in every release, including minors and CORDs. You can use this URL to download the latest SA10.2x version of the from the HP Software Support portal after signing in with your HP Passport credentials:

https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01253535

For additional versions, after logging into the HP Software Support portal, click the house icon to go to the home page, then use the SEARCH box to find any available product document.

System Requirements

Set up the Oracle RAC Database/Instances

SA supports any valid Oracle RAC configuration, such as any number of nodes, ASM or regular disks, and so on.

However, the Oracle database must be configured for use with SA. You may require your Oracle DBA's help to configure the Oracle RAC/instances, the required initialization parameters, the required tablespaces, the `opsware_admin` database user, and the `listener.ora`, `sqlnet.ora`, and `tnsnames.ora` files.

Create the Database with the Required Initialization Parameters

Follow the procedure described in Non-SA-Supplied Oracle Software and Database Setup on page 217.

You should perform the following tasks listed in the Non-SA-Supplied Oracle Software and Database Setup section:

- Modifiable Kernel Parameters
- Oracle Database Installation Steps
    - a Create the database with the UTF8 database character set
    - b Set the database with `TIME_ZONE` to `'+00:00'`
    - c Create the database with the required initialization (`init.ora`) parameters
    - d Create the database with required tablespaces

    e   Create the database user `opsware_admin`

➤ Use the `tnsnames.ora` file and file linking requirements listed in the following sections since they differ for the Oracle RAC environment from those listed in Non-SA-Supplied Oracle Software and Database Setup.

Installing the Model Repository

In most production environments with Oracle RAC, you can perform the Model Repository installation from any SA server. The database server or RAC nodes in this case are considered to be remote.

The examples used in the following sections assume an SA server (`rac1sa.dev.opsware.com`) on which SA will be installed and a 2 node RAC configuration shown in Table 45

table 45   **Example RAC Configurations**

Identity	Host Note	Name	Type	Address	Address Static or Dynamic	Resolved By
Node 1 Public	rac1pub	rac1pub	Public	192.168.173.210	Static	DNS
Node 1 Virtual	Selected by Oracle Clusterware	rac1-vip	Virtual	192.168.173.212	Static	DNS and/or host file
Node 1 Private	rac1pub	rac1prv	Private	172.16.1.100	Static	DNS, host file or none
Node 2 Public	rac2pub	rac2pub	Public	192.168.173.211	Static	DNS
Node 2 Virtual	Selected by Oracle Clusterware	rac2-vip	Virtual	192.168.173.213	Static	DNS and/or host file
Node 2 Private	rac2pub	rac2prv	Private	172.16.1.101	Static	DNS, host file or none
SCAN vip 1	Selected by Oracle Clusterware	sa_cluster1-scan	Virtual	192.168.173.216	Static	DNS
SCAN vip 2	Selected by Oracle Clusterware	sa_cluster1-scan	Virtual	192.168.173.217	Static	DNS
SCAN vip 3	Selected by Oracle Clusterware	sa_cluster1-scan	Virtual	192.168.173.218	Static	DNS

Installing the Model Repository in a RACed Environment

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

Perform the following tasks on the SA server on which you will run the SA Installer, for example `rac1sa.dev.opsware.com`.

1   **Model Repository Hostname Resolution**

Ensure that all the public, VIP and SCAN addresses are resolvable by using `nslookup`. If you are not using `nslookup`, then update the `/etc/hosts` file with those names.

Example:

```
# nslookup rac1-vip.dev.opsware.com
```

```
# nslookup sa_cluster1-scan.dev.opsware.com
```

On the server where you will run the SA Installer, ensure that the Model Repository hostname `truth` resolves to the remote database server, not to the server on which you will be running the SA Installer:

In `/etc/hosts`, enter the public IP address of one of the RAC nodes/instances. For example the `/etc/hosts` file on `rac1sa.dev.opsware.com` would have the following entry:

```
192.168.173.210 truth rac1pub rac1pub.dev.opsware.com
```

➤ If you have set up Oracle Clusterware, you should use the Clusterware IP address rather than a single database node IP address. For example:

```
192.168.173.216 truth sa_cluster1-scan sa_cluster1-scan.dev.opsware.com
```

If you have set up SCAN name, you should use the SCAN address rather than the database node IP address.

2 Install the Oracle 11g or Oracle 12c Full Client on the SA Server

➤ For Oracle 12.1.0.1, use the Oracle Full Client Version 12.1.0.1.

a The SA Installer uses the Oracle Full Client to connect to the SA server and install the Model Repository. Below are sample commands for installing the Oracle full client.

Create the database user `oracle` for the Oracle Full Client installation:

```
root@rac1sa ~]# mkdir -p /u01/app/oracle
root@rac1sa ~]# mkdir -p /u01/app/oraInventory
root@rac1sa ~]# groupadd oinstall
root@rac1sa ~]# groupadd dba
root@rac1sa ~]# useradd -c "Oracle Client software owner" -g oinstall
-G
dba -d /u01/app/oracle -s /bin/bash oracle
root@rac1sa ~]# chown -R oracle:oinstall /u01/app
root@rac1sa ~]# chmod -R 775 /u01/app
root@rac1sa ~]#passwd oracle (change oracle user password)
```

b Create the `.bash_profile` file

In `/u01/app/oracle` create the `.bash_profile` file.

Temporarily comment out `ORACLE_HOME` and `ORACLE_PATH`. You will uncomment these entries after the Oracle client installation is complete.

Sample .bash_profile File

```
# .bash_profile
# Get the aliases and functions
if [ -f ~/.bashrc ]; then
. ~/.bashrc
fi

# User specific environment and startup programs
PATH=$PATH:$HOME/bin
```

```
export PATH

#SA-OracleRAC parameters begin
#unset USERNAME
export ORACLE_BASE=/u01/app/oracle
# export ORACLE_HOME=$ORACLE_BASE/product/11.2.0/client_1 (for 11g Client) or
# export ORACLE_HOME=$ORACLE_BASE/product/12.1.0/client_1 (for 12c Client)
#PATH=$ORACLE_HOME/bin:$ORACLE_HOME/OPatch:$PATH
export PATH

if [ -t ]; then
stty intr ^C
fi

umask 022
#SA-OracleRAC parameters end
```

c Install the Oracle Full Client.

Install the Oracle Full Client as described in your Oracle documentation. You can create a share to access the Oracle Full Client binaries.

d Set Up Terminals.

You will need two X window terminals to install the Oracle Full Client:

Terminal 1: log in as a user with root privileges and enter the commands:

```
Terminal 1> xhost +
Terminal 2:  ssh -X oracle@<new_oracle_full_client_host>
```

e Start Oracle Full Client installation

From Terminal 2, run the Oracle Universal Installer (OUI). The Oracle Full Client is installed in:

```
/u01/app/oracle/product/12.1.0/client_1
```

f Run the Oracle Universal Installer to install Oracle Full Client. The directories in this example assume an Oracle 12c Full Client on Linux.

1. `cd /<location_of_oracle_full_client>`

2. `./runInstaller`

3. At the Welcome Screen, click Next.

4. Specify the Inventory Directory and Credentials (`/u01/app/oraInventory` and `/u01/app/oinstall`).

5. For Select Installation Type, choose Administrator, click Next.

6. For `ORACLE_BASE` select: `/u01/app/oracle`, click Next.

7. The Oracle Universal Installer performs some checks. If the checks are not successful, fix the issue and re-run this step. If the checks are successful click Next.

8. The Oracle OUI will list the products that are to be installed. Click Install.

9. The OUI shows the progress bar while installing.

10. On the 'Welcome to Oracle Net Configuration Assistant' window click on Next.

11. Click Finish when the installation completes.

12. You must run the following two configuration scripts as a user with root privileges after the installation completes:

```
-/u01/app/oraInventory/orainstRoot.sh

-/u01/app/oracle/product/12.1.0/client_1/root.sh
```

g   Verify that the `.bash_profile` file for the user `oracle` is correct.

h   Uncomment `$ORACLE_HOME` and `$ORACLE_PATH`.

3   Making Changes to tnsnames.ora on an SA Server (Use tnsnames.ora-install_upgrade File)

By default SA expects the `tnsnames.ora` file to be located in `/var/opt/oracle`.

a   Log in as a user with root privileges on the SA server from which the installer will be run.

b   Enter the command:

```
mkdir -p /var/opt/oracle
```

c   Copy `tnsnames.ora` from the remote database server to the directory you created above.

For the RAC environment, copy `tnsnames.ora` from RAC Node 1 (for example, `rac1pub.dev.opsware.com`).

To accommodate the remote Model Repository installation process, two sets of `tnsnames.ora` files are required on the SA server.

— **tnsnames.ora-install_upgrade** – this copy of `tnsnames.ora` is used during SA installation/upgrade. The file can be renamed.

— **tnsnames.ora-operational** – this copy of `tnsnames.ora` is used during normal SA operation. The file can be renamed.

You can use softlinks to point `tnsnames.ora` to either `tnsnames.ora-install_upgrade` or `tnsnames.ora-operational`. For example:

```
ln -s tnsnames.ora-install_upgrade tnsnames.ora
```

tnsnames.ora-install_upgrade Sample File

```
# tnsnames.ora Network Configuration File: /u01/app/oracle/product/
12.1.0/db_1/network/admin/tnsnames.ora
# Generated by Oracle configuration tools.
RAC1SA_TRUTH =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)
(PORT = 1521))
(CONNECT_DATA =
(UR=A)
(SERVER = DEDICATED)
(SERVICE_NAME = truth)
)
)
RAC2SA_TRUTH=(DESCRIPTION=(ADDRESS=(HOST=192.168.173.214)(PORT=20002)(
PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
```

d   Ensure that the `$ORACLE_HOME/network/admin/sqlnet.ora` file is created in both the client as well as the Oracle Database Server as described in step 9 under the section Oracle Database Installation Steps on page 219.

Testing the Connection from the SA host to the Database

Before starting the Model Repository installation/upgrade, you can perform the following tests to verify that your `tnsnames.ora` file is configured correctly and if the SA Installer can connect to the database.

1 Verify that the SA server's `/var/opt/oracle/tnsnames.ora` file is configured correctly as described in Making Changes to tnsnames.ora on an SA Server (Use tnsnames.ora-install_upgrade File) on page 232.

2 On the SA server:

    a Log in as `oracle` or as a user with root privileges or `su - twist/spin` – if these users exist.

    b `export ORACLE_HOME=/u01/app/oracle/product/12.1.0/client_1` (or where you installed the Oracle Full Client)

    c `export LD_LIBRARY_PATH=$ORACLE_HOME/lib`

    d `export TNS_ADMIN=/var/opt/oracle`

    e `set $PATH $ORACLE_HOME/bin path`

    f `sqlplus sys/password@RAC1SA_TRUTH as sysdba;`

       where `rac1sa_truth` is the `service_name` or entry from the `tnsnames.ora` file

    g `connect opsware_admin/<password>@RAC1SA_truth`

       If you are able to logon to the database then all files are configured correctly.

SA Installer Core Definition File (CDF)

You can now start the installation of the SA Model Repository. Ensure that you have the correct parameters values for the installation interview or that you have a previous Core Definition File (CDF).

- `%db.sid: truth1` (Oracle SID of the instance where SA installer is going to connect to.)
- `%db.orahome: /u01/app/oracle/product/12.1.0/client_1` (Oracle client home)
- `%db.port: 1521` (Oracle listener port)
- `%db.host: 192.168.173.210` (IP address of a node where ORACLE RDBMS is installed)
- `%truth.servicename: rac1sa_truth` (value of service name from `tnsnames.ora` file)

You can now install the SA Core as described in the Chapter 5, "SA Core Installation".

Post SA Installation Process

After you install the SA Core, perform the following tasks in order to use all the nodes in the Oracle RAC environment.

Making Changes to tnsnames.ora on the SA Server (Use tnsnames.ora-operational File)

After SA Core installation is complete, the `tnsnames.ora` file should point/link to the `tnsnames.ora-operational file`.

In an Oracle RAC environment, only one of the RAC nodes or instances 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 database installation process, two sets of `tnsnames.ora` files are required on the SA server.

- **tnsnames.ora-install_upgrade** – this copy of `tnsnames.ora` is used during SA installation/upgrade. You can rename the file.

- **tnsnames.ora-operational** – this copy of `tnames.ora` is used during normal SA operation. You can rename the file.

  You can use softlinks to point `tnsnames.ora` to either tnsnames.ora-install_upgrade or `tnsnames.ora-operational`:

  ```
  ln -s tnsnames.ora-operational tnsnames.ora
  ```

tnsnames.ora-operational Sample File

➤ If you have set up Oracle Clusterware, you should use the Clusterware IP address rather than a single database node IP address. If you have set up SCAN name, you should use the SCAN address rather than the database node IP address.

Make a note of the text that is in **bold** letters. This `tnsnames.ora` file is used during normal SA operation and contains the RAC parameters.

tnsnames.ora-operational sample File - with Clusterware Setup

If you have set up Oracle Clusterware, use the following:

#This entry is for connecting to RAC virtual machines. This entry is used by SA during operation of SA.

```
RAC1SA_TRUTH =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = sa_cluster1-scan.dev.opsware.com)(PORT =
1521))
(LOAD_BALANCE = yes)
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = truth)
(FAILOVER_MODE =
(TYPE = SELECT)
(METHOD = Preconnect)
(RETRIES = 180)
(DELAY = 5))
)
)
```

#This entry is for connecting to node2 via `service_name`. This is for DBA convenience. This is not used by SA.

```
TRUTH2 =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = rac2pub.dev.opsware.com)(PORT = 1521))
(CONNECT_DATA =
(UR=A)
(SERVER = DEDICATED)
(SERVICE_NAME = truth)
)
)
```

#This entry is for connecting to node1 via `service_name`. This is for DBA convenience. This is not used by SA.

```
TRUTH1 =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = rac1pub.dev.opsware.com)(PORT = 1521))
(CONNECT_DATA =
(UR=A)
(SERVER = DEDICATED)
(SERVICE_NAME = truth)
```

```
)
)
```

During installation, the SA Installer adds an SA Gateway entry into `tnsnames.ora` file (linked to `tnsnames.ora.install-upgrade`) on the Primary SA Core.

After installation completes, copy that entry into the `tnsname.ora.operational` file. If this entry is not present in the `tnsname.ora.operational` file, Multimaster Mesh transactions will not flow. The following is a sample gateway entry from `tnsnames.ora`:

```
RAC2SA_TRUTH=(DESCRIPTION=(ADDRESS=(HOST=192.168.173.214)
(PORT=20002)
(PROTOCOL=tcp))
(CONNECT_DATA=(SERVICE_NAME=truth)))
```

tnsnames.ora-operational Sample File - Without Clusterware Setup

If you have not set up Oracle Clusterware, use the following:

#This entry is for connecting to RAC virtual machines.

```
RAC1SA_TRUTH =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521))
(ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.dev.opsware.com)(PORT = 1521))
(LOAD_BALANCE = yes)
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = truth)
(FAILOVER_MODE =)
(TYPE = SELECT)
(METHOD = Preconnect)
(RETRIES = 180)
(DELAY = 5))
)
)
LISTENERS_TRUTH =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521))
(ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.dev.opsware.com)(PORT = 1521))
)
```

#This entry is for connecting to node2 via `service_name`. This entry is optional. This is for DBA convenience. This is not used by SA.

```
RAC2SA_TRUTH =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.dev.opsware.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = truth)
(INSTANCE_NAME = truth2)
)
)
LISTENER_TRUTH2 =
(ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.dev.opsware.com)(PORT = 1521))
```

#This entry is for connecting to node1 using `service_name`. This entry is optional. This is for DBA convenience. This is not used by SA.

```
RAC1SA_TRUTH =
```

```
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = truth)
(INSTANCE_NAME = truth1)
)
)
LISTENER_TRUTH1 =
(ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521))
```

During installation, the SA Installer adds an SA Gateway entry into `tnsnames.ora` file (linked to `tnsnames.ora.install-upgrade`) on the Primary SA Core.

After installation completes, copy that entry into the `tnsname.ora.operational` file. If this entry is not present in the `tnsname.ora.operational` file, Multimaster Mesh transactions will not flow. The following is a sample gateway entry from `tnsnames.ora`:

```
RAC2SA_TRUTH=(DESCRIPTION=(ADDRESS=(HOST=192.168.173.214)
(PORT=20002) (PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
```

Use softlinks to link the file to `tnsnames.ora` file after SA installation is complete and you are ready to start SA in operational mode.

```
ln -s tnsnames.ora-operational tnsnames.ora
```

vault.conf File Changes

If you have set up Oracle Clusterware, you should use the Clusterware IP address rather than a single database node IP address. If you have set up SCAN name, you should use the SCAN address rather than the database node IP address.

In an Oracle RAC environment, the `vault.conf` file must be modified after SA installation is complete. Modify `/etc/opt/opsware/vault/vault.conf` to specify the complete `tnsname.ora` definition instead of the SID. For example:

- *If you have set up Oracle Clusterware, use the following:*
  - Before:

    ```
    db.sid: truth
    ```
  - After:

    ```
    #truth.sid: truth1
    truth.sid: (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)
    (HOST = sa_cluster1-scan.dev.opsware.com)(PORT = 1521))
    (LOAD_BALANCE = yes)
    (CONNECT_DATA =(SERVER = DEDICATED)
    (SERVICE_NAME = truth)
    (FAILOVER_MODE = (TYPE = SELECT)
    (METHOD = Preconnect)(RETRIES = 180)(DELAY = 5))))
    ```

- *If Oracle Clusterware is not set up, use the following:*

  ```
  #truth.sid: truth1
  truth.sid:(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)
  (HOST =rac1-vip.dev.opsware.com)(PORT = 1521)) (ADDRESS = (PROTOCOL = TCP)
  (HOST = rac2-vip.dev.opsware.com)(PORT = 1521))
  (LOAD_BALANCE = yes)
  ```

```
(CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = truth)
(FAILOVER_MODE = (TYPE = SELECT)
(METHOD = Preconnect) (RETRIES = 180)(DELAY = 5))))
```

- Also, ensure that these values are correct:

```
truth.port: 1521
truth.host: 192.168.173.210 (database server IP)
truth.servicename: rac1sa_truth (tnsnames.ora enter)
```

- Restart the vaultdaemon:

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

da.conf File Changes

As of SA 9.10 and later, the Application Deployment Manager reads database connection information from the `tnsnames.ora` file.

In SA 9.10 and 9.1x, the default was `SID =Truth` unless changed by the user, for example, in `/etc/opt/opsware/da/da.conf`:

```
truth.sid=truth1 (this is the Oracle SID of the instance on RAC node)
```

opsware_start.config File Changes

This file is located in:

```
/opt/opsware/oi_util/startup/opsware_start.config
```

➤ If you have set up Oracle Clusterware, you should use the Clusterware IP address rather than a single database node IP address. If you have set up SCAN name, you should use the SCAN address rather than the database node IP address.

- `TRUTH_HOST="192.168.173.210"` - If Clusterware is not set up, then set the `TRUTH_HOST` value to one of the node's hostnames or public IPs.

- `TRUTH_HOST="sa_cluster1-scan.dev.opsware.com"` - If Clusterware is set up, then set the `TRUTH_HOST` value to the Clusterware scan name.

Setting up a Secondary SA core in an Oracle RACed environment.

During the interview process the installer asks for the secondary cores' database host information. Enter the IP or host name of the secondary cores single RACed node. During the install process the installer connects to the database via a single node only.

Upgrading the Model Repository in a RACed Environment

You must perform *pre-upgrade* steps before you upgrade the repository, and *post-upgrade* steps after you upgrade.

Pre-upgrade steps:

1 Backup `vault.conf` and `opsware_start.config` files or they will be overwritten by the installer.

These files were modified for Oracle RAC.

```
/etc/opt/opsware/vault/vault.conf
/opt/opsware/oi_util/startup/opsware_start.config
```

2   Update the `tnsnames.ora` file.

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.

— `tnsnames.ora-operational`

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

During the upgrade process, you can use soft links to point the `tnsnames.ora` file to `tnsnames.ora-install_upgrade`.

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

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

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

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

3   Start SA.

Post-Upgrade Steps:

1   Verify `vault.conf` and `opsware_start.config` files.

Prior to the upgrade these files were backed up. Look at section '`vault.conf File Changes`' and the backed up files and replace the value of `truth.sid`.

The installer may try to re-start the Vault during the upgrade process and it might fail due to an incorrect `truth.aid` value. In that case, make the changes to `vault.conf` and then re-start the installer.

2   Update `tnsnames.ora` file

After the entire SA upgrade is done, 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 node.

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

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

— You can use softlinks to point `tnsnames.ora` to `tnsnames.ora-operational`.

  For example, `$ln -s tnsnames.ora-operational tnsnames.ora`

3   Start SA.

Setting the Oracle Database Server OS To Non-UTC Time

HP recommends that all servers including the Oracle database server be set to UTC. However, if you must set the database server to a non-UTC time zone, you can use the following procedure.

Requirements

- The steps in this section apply only to the Oracle *database server* used for SA. All other SA servers are required to be set to the UTC time zone.

- The process listed in this section is only for Oracle Standard and Enterprise Edition. *It is not certified for Oracle RAC.*

- This section is applicable for SA10.20. It is not applicable for lower versions of SA.

- The process is applicable to fresh core installations.

- Once the database is set up for non-UTC support as described in this section, the DBA must log on to the database using the `tnsnames.ora`'s service name/aliases. For example:

  `sqlplus <userid>/password@<tns_service_name>`

  Do not use local connections to log into the database. Refer to the section Logging into the Database on page 246 for more details.

- The SA application and Oracle RDBMS software must be installed on a supported OS. See the *SA Support and Compatibility Matrix* for supported OS's and versions.

- The Oracle database server's OS time zone can be set to a non-UTC time zone, for example PST, EST etc.

- The Primary and Secondary Core database servers can be set to different time zones.

Non-UTC Support Set Up for SA Oracle Database Server

The steps in this section refer to various machines, IP's and host names. The following table lists the Core environment used for the steps including Core names and machine information.

table 46   Core Names

Core Name	Facility ID/Core ID
Core 1	1
Core 2	2

table 47   Host Details

Host Name	IP Address	Purpose
Core 1		
db.pri.cpe.opsware.com	192.168.209.41	Primary Core Oracle database server
pri.aus.cpe.opsware.com	192.168.209.42	Primary Core Host
prisat1.aus.cpe.opsware.com	192.168.209.43	Primary Core Satellite
Core 2		
db.sla.cpe.opsware.com	192.168.210.24	Secondary Core Oracle database server
sla.aus.cpe.opsware.com	192.168.210.25	Secondary Core Host
slasat1.aus.cpe.opsware.com	192.168.210.26	Secondary Core Satellite

Non-UTC Setup Procedure

The following steps must be performed to set up a non-UTC time zone for the SA Oracle database server.

➤ If you allow the SA Installer to install the SA-supplied Oracle database, you can skip Steps 1 and 2.

1   Install the Oracle Software and create SA Oracle database

2   Create the database user `opsware_admin`.

➤ See System Requirements on page 205for Oracle database set up Requirements. You can install Oracle Software, and create the SA database using Oracle Corporation's install utilities or you can allow the SA Installer to install the SA-supplied Oracle database. The requirements for database user `opsware_admin` are listed in 5. Create the Database User opsware_admin on page 220.

3   Create a logon trigger and modify the `listener.ora` file.

table 48

Step	Action	Details	Comments

1	Create the logon trigger to set SA database user sessions to UTC.	This command must be executed from the database server.
		
		See Trigger for Setting SA DB User's Session Time Zone on page 247.
			Example showing correct `CURRENT_TIMESTAMP` and `LOCALTIMESTAMP` after the `HPSA_LOGON_ZONE_UTC` trigger is created.
			
			`$sqlplus opsware_admin/`
			`opsware_admin@`
			`truth.AusPri`
			
			`SQL> SELECT DBTIMEZONE,`
			`SESSIONTIMEZONE FROM`
			`DUAL;`
			
			`DBTIME SESSIONTIMEZONE`
			
			`------ ------------`
			
			`-07:00 +`**`00:00`**
			
			`SQL> select`
			`CURRENT_TIMESTAMP,`
			`LOCALTIMESTAMP from dual;`
			
			`CURRENT_TIMESTAMP`
			`LOCALTIMESTAMP`
			
			`------------------------`
			`--------------`
			`------------------------`
			`-----`
			
			`30-JUN-14 05.48.51.146919`
			`PM +00:00     30-JUN-14`
			`05.48.51.146919 PM`
			`(correct time in UTC)`

table 48

Step	Action	Details	Comments

2	Modify the `listener.ora` file	**Note**: You can see a sample `listener.ora` in Sample listener.ora File for a Non-UTC Environment on page 246.
		
		a Shutdown the Oracle listener:
		`$lsnrctl stop`
		
		b Add ENVS variable to the file i.e. (`ENVS='TZ=UTC'`), UTC is required by SA.
		
		c Specify the PORT to be other than the default1521.
		
		d Restart the listener:
		`$lsnrctl start`
			a The database server's listener files was changed based on the Oracle document 'How To setup TNS listener to Show More Than one Time zone (Doc ID 399448.1)'
			
			b `listerner.ora`'s PORT number must be something other than the SA default 1521.
			
			c `listener.ora`'s connection must be via SID.
			
			d `listener.ora`'s connections are made using the static handler (`SID_DESC`).
			
			e Ensure that the database parameter `LOCAL_LISTENER` is not set to dynamically register any database that requires a different `TZ` or statically defined `SID_DESC` in the `listener.ora` file. To verify use `show parameter local_listener` in SQL*Plus.

table 48

Step	Action	Details	Comments

3	Verify the listener settings	To verify that the `listener.ora` settings:
		
		`$ su - oracle`
		`$ lsnrctl`
		`LSNRCTL> set displaymode verbose`
		`LSNRCTL> services`
		`Connecting to`
		`(ADDRESS=(PROTOCOL=tcp)(HOST=db.`
		`pri.cpe.opsware.com)(PORT=1524))`
		`Services Summary...`
		`Service "truth" has 1`
		`instance(s).`
		`  Instance "truth", status`
		`UNKNOWN, has 1 handler(s) for`
		`this service...`
		`    Handler(s):`
		`      "DEDICATED" established:2`
		`refused:0`
		`          LOCAL SERVER`
		
		`(ADDRESS=(PROTOCOL=beq)(PROGRAM=`
		`/u01/app/oracle/product/11.2.0/`
		`db_2/bin/`
		`oracle)(`**`ENVS='TZ=UTC`**`,ORACLE_HOME=/`
		`u01/app/oracle/product/11.2.0/`
		`db_2,ORACLE_SID=truth')(ARGV0=or`
		`acletruth)(ARGS='(LOCAL=NO)'))`
		`The command completed`
		`successfully`
		`LSNRCTL> exit`
			This step ensures that all the remote connections going through the listener will have the TZ=UTC setting.

4	Modify all `tnsnames.ora` files on database host and Core server hosts	Ensure that the `tnsnames.ora` files on the database server and all the SA Core component hosts have the correct PORT specified.
		
		`truth.AusPri=(DESCRIPTION=(ADDRE`
		`SS=(HOST=db.pri.cpe.opsware.com)`
		`(PORT=`**`1524`**`)(PROTOCOL=tcp))(CONNE`
		`CT_DATA=(SERVICE_NAME=truth)))`	

4 Run the SA Installer and install the Model Repository and other SA components using the "Expert Interview" mode. The Expert interview mode allows you to set the Oracle listener port to a non-default port. By default the Oracle listener is set to 1521. When setting the database server to other than UTC time, `listerner.ora`'s PORT number must be a value other than the SA default 1521.

➤ **Note**: If you install the Model Repository without setting the `listener.ora` file, the SA Installer issues a warning that the database server is not set to the required UTC time zone. Also, the data inserted in the database will have incorrect time. It is necessary to make the changes listed in the previous section before installing any of the SA components.

After installing all the SA components, logon to the database as the `spin` or `twist` database user and verify the time.:

table 49   Verify Time

Step	Actions	Details	Comments

1	Verify the time.
	
	Log on as one of the SA database users and verify the time from any of the SA Core component hosts or the database server.
		```set line 150```
		```col SESSIONTIMEZONE format a25```
		```col SYSTIMESTAMP format a40```
		```col CURRENT_TIMESTAMP format a40```
		```col LOCALTIMESTAMP format a30```
		```col SYSDATE_FORMATTED format a30```
		
		```SELECT DBTIMEZONE,```
		```SESSIONTIMEZONE FROM DUAL;```
		
		```SELECT```
		```TO_CHAR(SYSDATE,'DD-MON-YY```
		```HH:MI:SSAM') SYSDATE_FORMATTED,```
		```SYSTIMESTAMP FROM DUAL;```
		```Select CURRENT_TIMESTAMP,```
		```LOCALTIMESTAMP from dual;```
		
		```! date```
			Example of verifying the date-time from an SA component host:
			
			```$ su - oracle```
			```$sqlplus spin/```
			```<spin_password>@```
			```truth.AusPri```
			
			```SQL> set line 150```
			```SQL> col SESSIONTIMEZONE```
			```format a25```
			```SQL> col SYSTIMESTAMP```
			```format a40```
			```SQL> col CURRENT_TIMESTAMP```
			```format a40```
			```SQL> col LOCALTIMESTAMP```
			```format a30```
			```SQL> col SYSDATE_FORMATTED```
			```format a30```
			
			```SQL> SELECT DBTIMEZONE,```
			```SESSIONTIMEZONE FROM DUAL;```

table 49   **Verify Time**

Step	Actions	Details	Comments

2			Ensure that the SESSIONTIMEZONE is +00:00
			
			`DBTIME SESSIONTIMEZONE`
			`------`
			`-----------------------`
			`-07:00 +`**`00:00`**
			
			`SQL> SELECT`
			`TO_CHAR(SYSDATE,'DD-MON-YY`
			`HH:MI:SSAM')`
			`SYSDATE_FORMATTED,`
			`SYSTIMESTAMP FROM DUAL;`
			
			`SYSDATE_FORMATTED`
			`SYSTIMESTAMP`
			`---------------------------`
			`-`
			`---------------------------`
			`-----------`
			`30-JUN-14 06:32:22PM`
			`30-JUN-14 06.32.22.609631 PM`
			`+00:00`
			
			`SQL> select`
			`CURRENT_TIMESTAMP,`
			`LOCALTIMESTAMP from dual;`
			
			`CURRENT_TIMESTAMP`
			`LOCALTIMESTAMP`
			`---------------------------`
			`-----------`
			`---------------------------`
			`-`
			`30-JUN-14 06.32.22.612416 PM`
			`+00:00      30-JUN-14`
			`06.32.22.612416 PM`

Post Installation Steps and Notes

In addition to the above, perform these tasks or be aware of the following after the installation.

Oracle's dba_scheduler jobs

SA has several jobs that are run using Oracle's `dba_scheduler`. See also Garbage Collection on page 248 and Changes to the Database Statistics Job on page 257 . The `dba_scheduler` jobs are run based on the database server time, but the job timings can be easily changed to a suitable time. Garbage Collection on page 248 lists the commands that can be used to change the job run time.

Oracle's alert.log

Oracle's `alert.log` and other log files will continue to show the machine/OS time.

SA Logs

All SA logs will show the time in UTC.

Logging into the Database

The DBA should always connect to the database using the `tnsnames.ora` entry, which connects to the database using the Oracle listener. You should not connect the database using a local connection. The `listener.ora` file has been modified to include the TZ=UTC parameter. The listener connections set the correct time zone value.

Correct:

`sqlplus <userid>/password@<tns_service_name>`

For example:

`$sqlplus opsware_admin/opsware_admin@truth.AusPri`

Incorrect:

`sqlplus <userid>/password`

For example:

`$sqlplus opsware_admin/opsware_admin`

Setting up a Secondary Core

After the primary core is setup in a non-UTC environment, it is important to wait for a day before setting up a secondary core. During the secondary core creation, if 'add_dc_to_mesh' runs into errors similar to the following in Oracle's alert.log file:

```
ORA-31693: Table data object "TRUTH"."<table_name>" failed to load/unload
and is being skipped due to error:
ORA-02354: error in exporting/importing data
ORA-08186: invalid timestamp specified
ORA-06512: at "SYS.TIMESTAMP_TO_SCN", line 1
```

...then, wait for a day, and then give the following grants in sqlplus and kickoff the installer's add_dc_to_mesh command once again:

```
$ su - oracle
$ sqlplus  "/ as sysdba"
SQL> grant create session to vault, gcadmin, twist, spin, lcrep, aaa,
truth;
SQL> exit;
```

Sample listener.ora File for a Non-UTC Environment

The following is a sample `listener.ora` file from a primary core:

```
Sample listener.ora from primary core
# File:      listener.ora
# Purpose:   Listener specifications
# Notes:     None

LISTENER =
 (ADDRESS_LIST=
```

```
              (ADDRESS=(PROTOCOL=tcp)(HOST=db.pri.cpe.opsware.com)(PORT=1524))
              (ADDRESS=(PROTOCOL=ipc)(KEY=PNPKEY)))

    SID_LIST_LISTENER=
      (SID_LIST=
        (SID_DESC=
            (ENVS='TZ=UTC')
            (SID_NAME=truth)
            (ORACLE_HOME=/u01/app/oracle/product/12.1.0/db_1)
        )
      )
    LOG_DIRECTORY_LISTENER=/u01/app/oracle/product/12.1.0/db_1/network/log
    LOG_FILE_LISTENER=listener.log
    TRACE_DIRECTORY_LISTENER=/u01/app/oracle/product/12.1.0/db_1/network/trace
    TRACE_FILE_LISTENER=listener.trc
    INBOUND_CONNECT_TIMEOUT_LISTENER=120
    # subscribe_for_node_down_event entry should be removed for RAC env.
    SUBSCRIBE_FOR_NODE_DOWN_EVENT_LISTENER=OFF
    #LOCAL_OS_AUTHENTICATION_LISTENER=OFF

    #----ADDED BY TNSLSNR 04-OCT-2005 23:06:20---
    SAVE_CONFIG_ON_STOP_LISTENER = ON
    #-------------------------------------------

    #----ADDED BY TNSLSNR 04-OCT-2005 23:09:20---
    PASSWORDS_LISTENER = CEE9A6452943F605
    #-------------------------------------------
```

Sample tsnames.ora File for a Non-UTC Environment

The following is sample `tnsnames.ora` file from primary core:

```
truth.AusPrimary=(DESCRIPTION=(ADDRESS=(HOST=db.pri.cpe.opsware.com)(PORT=152
4)(PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
truth.AusSecondary=(DESCRIPTION=(ADDRESS=(HOST=192.168.209.42)(PORT=20002)(PR
OTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
```

Note: The `truth.AusSecondary` entry is added by the SA installer and is used for the Multimaster Mesh replication process.

Trigger for Setting SA DB User's Session Time Zone

```
$ su - oracle
$ sqlplus / as sysdba
CREATE OR REPLACE TRIGGER HPSA_LOGON_ZONE_UTC
AFTER LOGON ON DATABASE

DECLARE
            v_user varchar2(30):=user;
            sql_stmt1 varchar2(256) :='ALTER SESSION SET
TIME_ZONE=''+00:00''';
begin
            if
            (
```

```
                                    USER IN
                                    (
                                                'AAA',
                                                'AAA_USER',
                                                'GCADMIN',
                                                'LCREP',
                                                'OPSWARE_ADMIN',
                                                'OPSWARE_PUBLIC_VIEWS',
                                                'TRUTH',
                            'SPIN',                 'TWIST',

                                                'VAULT'
                                    )
                        )
                        THEN
                        execute immediate sql_stmt1;
        end if;
end;
/
/
```

Garbage Collection

The Garbage Collector (GC) is a stored procedure written in PL/SQL that runs in the database on a schedule. The GC procedures look at the AUDIT_PARAMS table to determine the retention period to use to delete the old data. The GC PL/SQL procedures are managed by Oracle's dba_scheduler_jobs.

Data Retention Period

When GC runs, it looks at the values in the AUDIT_PARAMS table to determine what retention period to use when deleting objects.

▶ The AUDIT_PARAMS table is not replicated, so there is a possibility that these retention periods may become unsynchronized, which can cause severe Multimaster conflict issues. You must ensure that the values in the AUDIT_PARAMS table are exactly the same for all the cores in a mesh.

```
# sqlplus "/ as sysdba"
SQL> col name format a20;
SQL> col value format a20;
SQL> col AUDIT_PARAM_ID format a15;
SQL> select AUDIT_PARAM_ID, NAME, VALUE from audit_params;
```

The parameters from `AUDIT_PARAMS` table and their default values are:

```
AUDIT_PARAM_ID    NAME                 VALUE
--------------    ------------------   --------------------------
2                 DAYS_WAY             30         (These are the completed way sessions)
3                 DAYS_CHANGE_LOG      180        (These are the server history events)
4                 LAST_DATE_WAY        02-NOV-14
5                 LAST_DATE_CHANGE_LOG 05-JUN-14
6                 DAYS_AUDIT_LOG       180        (These are the audit logs)
7                 LAST_DATE_AUDIT_LOG  05-JUN-14
8                 DAYS_WLM             30         (These are completed WLM jobs)
9                 LAST_DATE_WLM        02-NOV-14
```

▶ As of SA 9.10, the `DAY_TRAN` parameter that controlled retention time for transactions was removed. To control transaction retention time, instead use the system configuration parameter `vault.garbageCollector.daysToPreserve`.

Select the **Administration** tab in the SA Client, then select System Configuration in the navigation panel. Select Model Repository Multimaster Component. Locate and change the value of the above parameter. The default value is 7. Select the Save button to save your change.

Modifying the Retention Period Values

To update the data, run a SQL command similar to the following example as user `LCREP`:

```
# su - oracle
# sqlplus "/ as sysdba"
SQL> grant create session to lcrep;
SQL> connect lcrep/<password>
SQL> update AUDIT_PARAMS set value=30 where name = 'DAYS_AUDIT_LOG';
```

▶ The values in the `AUDIT_PARAMS` table must be exactly the same for all the cores in a mesh.

Viewing GC DBA_SCHEDULER_JOBS

When the Model Repository is installed, the SA Installer sets up these jobs, which perform garbage collection.

GC jobs can be viewed by logging in to SQL*Plus and running the following SQL commands:

```
# su - oracle
# sqlplus "/ as sysdba"
SQL> set line 200
SQL> col job_name format a50
SQL> col owner format a14
SQL> col last_date format a17
SQL> col next_date format a17
SQL> col job_action format a50

SQL>select job_name, owner, to_char(LAST_START_DATE, 'MM/DD/YY HH:MI:SS')
last_date,to_char(next_run_date, 'MM/DD/YY HH:MI:SS') next_date, job_action
from dba_scheduler_jobs where owner='GCADMIN';
```

```
JOB_NAME                      OWNER     LAST_DATE          NEXT_DATE          JOB_ACTION
----------------------------  -------   ----------------   ----------------   ---------------------------
WLMPURGE_GC                   GCADMIN   04/02/12 09:00:02  04/04/12 09:00:00  WLMPURGE.GC_JOBS
STORAGEINITIATORPURGE_GC      GCADMIN   04/02/12 09:47:30  04/03/12 10:47:30  STORAGEINITIATORPURGE.GC_STORAGE
                                                                              INITIATORS
AUDITPURGE_GC                 GCADMIN   04/02/12 09:00:02  04/04/12 09:00:00  AUDITPURGE.GC_AUDITLOGS
CHANGELOGPURGE_GC             GCADMIN   04/02/12 09:00:02  04/04/12 09:00:00  CHANGELOGPURGE.GC_CHANGELOGS
WAYPURGE_GC                   GCADMIN   04/02/12 09:00:02  04/04/12 09:00:00  WAYPURGE.GC_SESSIONS
```

where:

`WAYPURGE.GC_SESSIONS` - Performs `sessions` garbage collection

`CHANGELOGPURGE.GC_CHANGELOGS` - Performs `changelogs` garbage collection

`AUDITPURGE.GC_AUDITLOGS` - Performs `auditlogs` garbage collection

`STORAGEINITIATORPURGE.GC_STORAGEINITIATORS` - Performs `storage data` garbage collection

`WLMPURGE.GC_JOBS` - Performs WLM garbage collection

Manually Running GC Jobs

You can run GC jobs by logging in to SQL*Plus and entering the following:

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

SQL> grant create session to gcadmin
SQL> connect gcadmin/<password>
SQL> exec dbms_scheduler.run_job('<job_name_value>');
```

For example, this sample command runs the `waypurge_gc` job:

```
SQL> exec dbms_scheduler.run_job('WAYPURGE_GC');
```

Database Monitoring Strategy

Because the Model Repository is a critical component of SA, the DBA should implement a monitoring strategy. The DBA can write custom monitoring scripts or use third-party products.

This section contains example commands for monitoring the Oracle database used by the Model Repository. When issuing the commands shown in this section, you must be logged on to the server as the user `oracle`:

```
$ su - oracle
```

The SQL commands shown in this section are entered in the `sqlplus` command-line utility. To run `sqlplus`, log on as `oracle` and enter the following command:

```
$ sqlplus "/ as sysdba"
```

Verify that the Database Instances are Up and Responding

To verify that the Database Instances are up and running, perform the following steps:

1   Check to see if the Oracle processes are running by entering the following command:

```
$ ps -ef | grep ora_
```

This `ps` command should generate output similar to the following lines:

```
oracle   14674     1  0 Apr18 ?        00:00:00 ora_pmon_truth
oracle   14676     1  0 Apr18 ?        00:00:00 ora_psp0_truth
oracle   14678     1  0 Apr18 ?        00:00:00 ora_vktm_truth
oracle   14682     1  0 Apr18 ?        00:00:00 ora_gen0_truth
oracle   14684     1  0 Apr18 ?        00:00:00 ora_diag_truth
oracle   14686     1  0 Apr18 ?        00:00:00 ora_dbrm_truth
oracle   14688     1  0 Apr18 ?        00:05:57 ora_dia0_truth
oracle   14690     1  0 Apr18 ?        00:00:00 ora_mman_truth
oracle   14692     1  0 Apr18 ?        00:00:00 ora_dbw0_truth
oracle   14694     1  0 Apr18 ?        00:00:01 ora_lgwr_truth
oracle   14696     1  0 Apr18 ?        00:00:28 ora_ckpt_truth
oracle   14698     1  0 Apr18 ?        00:00:04 ora_smon_truth
oracle   14700     1  0 Apr18 ?        00:00:00 ora_reco_truth
oracle   14702     1  0 Apr18 ?        00:00:13 ora_mmon_truth
oracle   14704     1  0 Apr18 ?        00:00:13 ora_mmnl_truth
oracle   14728     1  0 Apr18 ?        00:00:00 ora_qmnc_truth
oracle   14775     1  0 Apr18 ?        00:00:01 ora_cjq0_truth
oracle   14779     1  0 Apr18 ?        00:00:00 ora_q000_truth
oracle   14781     1  0 Apr18 ?        00:00:00 ora_q001_truth
oracle   14832     1  0 Apr18 ?        00:00:00 ora_smco_truth
oracle   22619     1  0 22:38 ?        00:00:00 ora_w000_truth
```

2   Verify that the database status is ACTIVE by entering the following command in `sqlplus`:

```
SQL>select database_status from v$instance;
```

3   Verify that the open mode is READ WRITE by entering the following command in `sqlplus`:

```
SQL>select name, log_mode, open_mode from v$database;
```

Verify that the Data Files are Online

To verify that the data files are online, in SQL*Plus, enter the following commands:

```
SQL>Col file_name format a50
SQL>Col status format a10
SQL>Set line 200
SQL>Select file_id, status, bytes, file_name from dba_data_files order by
SQL>tablespace_name;
```

The status should be AVAILABLE for all the data files.

Verify That the Listener is Running

To verify that the listener is running, perform the following steps:

1   Check to see if the Oracle listener processes are running by entering the following command:

```
$ ps -ef | grep tns

oracle   11664     1  0 Mar22 ?        00:08:05 /u01/app/oracle/product/
12.1.0/db_1/bin/tnslsnr LISTENER -inherit
oracle   22725 22706  0 22:44 pts/2    00:00:00 grep tns
```

2   Check the status of the listener with the `lsnrctl` command:

```
$ lsnrctl status
```

The listener should be listening on port 1521 (default), or on the port that you have designated that the Oracle listener process use, with the TCP protocol, and should be handling the instance named truth. The `lsnrctl` command should generate output similar to the following lines:

```
. . .
Connecting to (ADDRESS=(PROTOCOL=tcp)
(HOST=per1.performance.qa.example.com)(PORT=1521))
. . .
Instance "truth", status READY, has 1 handler(s) for this service...
```

3   Test connectivity to the instance from the Data Access Engine (spin) and Web Services Data Access Engine (twist) hosts by running the `tnsping` utility:

```
$ tnsping truth
```

The `OK` statement displayed by the `tnsping` utility confirms that the listener is up and can connect to the instance. The `tnsping` utility should generate output similar to the following lines:

```
. . .
Used parameter files:

Used HOSTNAME adapter to resolve the alias
Attempting to contact
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=truth.performance.qa.example.com
))(ADDRESS=(PROTOCOL=TCP)(HOST=192.168.165.178)(PORT=1521)))
OK (0 msec)


Attempting to contact
(DESCRIPTION=(ADDRESS=(HOST=localhost)(PORT=1521)(PROTOCOL=tcp))(CONNECT_
DATA=(SERVICE_NAME=truth)))
OK (0 msec)
```

As an alternative to running the `tnsping` utility in this step, you can check the connectivity by running `sqlplus` and connecting to the database instance with the service name (TNS alias), for example:

```
$ sqlplus myuser/mypass@truth
```

Examine the Log Files

To examine the log files, perform the following steps:

1   Look for errors in the `alert.log` file.

For each instance, locate the `alert.log` file in the background dump destination directory:

`$ORACLE_BASE/diag/rdbms/<SID>/<SID>/trace/`

This is an example `bdump` directory for an instance with the `truth` SID:

`/u01/app/oracle/diag/rdbms/truth/truth/trace/`

2   Look for errors in the other log and trace files, located in various directories under:

`$ORACLE_BASE/diag/rdbms/<SID>/<SID>`

Check for Sufficient Free Disk Space in the Tablespaces

To check for sufficient disk space, perform the following steps:

1 Enter the following commands in `sqlplus`:

```
SQL>set line 200
SQL>column dummy noprint
SQL>column pct_used format 999.9 heading "Pct|Used"
SQL>column name format a16 heading "Tablespace Name"
SQL>column mbytes format 999,999,999 heading "Current|File Size|MB"
SQL>column used format 999,999,999 heading "Used MB "
SQL>column free format 999,999,999 heading "Free MB"
SQL>column largest format 999,999,999 heading "Largest|Contigous|MB"
SQL>column max_size format 999,999,999 heading "Max Possible|MB"
SQL>column pct_max_used format 999.999 heading "Pct|Max|Used"
SQL>break on report
SQL>compute sum of Mbytes on report
SQL>compute sum of free on report
SQL>compute sum of used on report


SQL>SELECT
    nvl(df.tablespace_name,'UNKOWN') name, df.mbytes_alloc Mbytes,
    df.mbytes_alloc-nvl(fs.mbytes_free,0) used, nvl(fs.mbytes_free,0)
free,
    ((df.mbytes_alloc-nvl(fs.mbytes_free,0)) / df.mbytes_alloc) * 100
pct_used,
    nvl(df.largest,0) largest, nvl(df.mbytes_max,df.mbytes_alloc)
Max_Size,
    ((df.mbytes_alloc-nvl(fs.mbytes_free,0)) / df.mbytes_max) * 100
pct_max_used
FROM
    (   SELECT tablespace_name, sum(bytes)/1024/1024 Mbytes_alloc,
max(bytes)/1024/1024 largest,

sum(decode(autoextensible,'YES',greatest(bytes,maxbytes),bytes))/1024/
1024 Mbytes_max
        FROM
            dba_data_files GROUP BY tablespace_name
    ) df,
    ( SELECT tablespace_name, sum(bytes)/1024/1024 Mbytes_free
        FROM dba_free_space GROUP BY tablespace_name
    ) fs
WHERE
    df.tablespace_name = fs.tablespace_name(+)
UNION
SELECT
    D.tablespace_name name, D.mbytes_alloc Mbytes, ((ss.used_blocks *
F.block_size) / 1024 / 1024) used,
    D.mbytes_alloc - ((ss.used_blocks * F.block_size) / 1024 / 1024) free,
    ((D.mbytes_alloc-nvl((D.mbytes_alloc - ((ss.used_blocks *
F.block_size) / 1024 / 1024)),0)) / D.mbytes_alloc) * 100 pct_used,
    nvl(((G.max_blocks * F.block_size) / 1024 / 1024),0) largest,
Max_Mbytes Max_Size,
```

```
          ((D.mbytes_alloc-nvl((D.mbytes_alloc - ((ss.used_blocks *
    F.block_size) / 1024 / 1024)),0)) / D.Max_Mbytes) * 100 pct_pct_used
    FROM
        (   SELECT tablespace_name, used_blocks, free_blocks, max_size
            FROM v$sort_segment
        ) ss,
        (   SELECT tablespace_name, sum(bytes)/1024/1024 Mbytes_alloc,

    sum(decode(autoextensible,'YES',greatest(bytes,maxbytes),bytes))/1024/
    1024 Max_Mbytes
            FROM dba_temp_files GROUP BY tablespace_name
        ) D,
        (   SELECT B.name, C.block_size, SUM (C.bytes) / 1024 / 1024 mb_total
            FROM v$tablespace B, v$tempfile C
            WHERE B.ts#= C.ts# GROUP BY B.name, C.block_size
        ) F,
        (   SELECT B.name, max(blocks) max_blocks, sum(blocks) total_blocks
            FROM v$tablespace B, v$tempfile C
            WHERE B.ts#= C.ts# GROUP BY B.name
        ) G
    WHERE ss.tablespace_name = D.tablespace_name and ss.tablespace_name =
    F.name and ss.tablespace_name = G.name;
```

In the output generated by the preceding commands, compare the numbers under the `Used` and `Free` headings.

2   To list the existing data, index, and temporary files, enter the following commands in `sqlplus`:

```
SQL>Select file_id, bytes, file_name from dba_data_files;
```

3   If a tablespace has auto-extended to its maximum size and is running out of disk space, then add new data files by entering the `ALTER TABLESPACE` command in `sqlplus`.

The following example commands add data files to four of the tablespaces. For a full list of tablespaces and data files, see the output generated by the commands in the preceding two steps.

```
SQL>ALTER TABLESPACE "AAA_DATA"
SQL>ADD DATAFILE '/u01/oradata/truth/aaa_data10.dbf'
SQL>SIZE 32M AUTOEXTEND ON NEXT 128M MAXSIZE 4000M ;

SQL>ALTER TABLESPACE "AAA_INDX"
SQL>ADD DATAFILE '/u02/oradata/truth/aaa_indx11.dbf'
SQL>SIZE 32M AUTOEXTEND ON NEXT 128M MAXSIZE 4000M ;

SQL>ALTER TABLESPACE "UNDO"
SQL>ADD DATAFILE '/u03/oradata/truth/undo12.dbf' SIZE 32M AUTOEXTEND ON
NEXT 128M MAXSIZE 4000M ;

SQL>ALTER TABLESPACE "TEMP" ADD
SQL>TEMPFILE '/u04/oradata/truth/temp14.dbf' SIZE 32M AUTOEXTEND ON NEXT
128M MAXSIZE 4000M ;
```

Enable Oracle Automatic Optimizer Statistics Collection

As of SA 10.0 the schema and index statistics collection for SA database user AAA, TRUTH etc. has been moved from `dba_jobs` to Oracle's Automatic Optimizer Statistics Collection.

SA relies on Oracle's Automatic Optimizer statistics collection to collect schema statistics used to avoid database performance degradation. By default, Oracle's Automatic optimizer statistics collection should be enabled.

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

1   Enter the following commands in SQL*Plus:

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

SQL>set line 200
SQL>col status format a10
SQL>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
```

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

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

Manually Collecting Schema Statistics

Although you have moved to the Oracle's Automatic Optimizer Statistics Collection, there are times when you may need to collect statistics manually.

To collect the statistics manually:

Enter the following commands in SQL*Plus:

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


SQL> begin
    dbms_stats.gather_schema_stats (ownname=>'TRUTH',
        estimate_percent=>DBMS_STATS.AUTO_SAMPLE_SIZE,
        cascade=>TRUE,
        options=>'GATHER AUTO');
end;
/
```

Replace the ownname from TRUTH to the other SA schemas like AAA, LCREP, GCADMIN, OPSWARE_ADMIN.

Verify that the Database Jobs (System/Index Statistics and Garbage Collection) Ran Successfully

When the Model Repository is installed, the SA Installer sets up the System/Index Statistics and the Garbage Collection jobs in Oracle's `dba_scheduler_jobs` which then runs these jobs at specified time-intervals. The jobs perform system/ index statistics collection and garbage collection. If the system/ index statistics collection jobs do not run successfully, database performance degrades. If the garbage collection jobs do not run, old data accumulates and requires additional disk space. Performance can also be affected.

To verify that the Jobs in `DBA_SCHEDULER_JOBS` ran successfully, perform the following steps:

1   Enter the following commands in SQL*Plus:

```
SQL>set line 200
SQL>col job_name format a50
SQL>col owner format a14
SQL>col last format a17
SQL>col next format a17
SQL>col state format a10
SQL>col job_action format a50

SQL>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 looks like this:

```
JOB_NAME                    OWNER          LAST              NEXT              STATE      JOB_ACTION
-------------------         ------------   ---------------   ---------------   ---------  ----------------------
WLMPURGE_GC                 GCADMIN        12/02/14 09:00:01 12/03/14 09:00:00 SCHEDULED  WLMPURGE.GC_JOBS
STORAGEINITIATORPURGE_GC    GCADMIN        12/02/14 09:00:01 12/03/14 09:00:00 SCHEDULED  STORAGEINITIATORPURGE.GC
                                                                                          _STORAGEINITIATORS
AUDITPURGE_GC               GCADMIN        12/02/14 09:00:01 12/03/14 09:00:00 SCHEDULED  AUDITPURGE.GC_AUDITLOGS
CHANGELOGPURGE_GC           GCADMIN        12/02/14 09:00:01 12/03/14 09:00:00 SCHEDULED  CHANGELOGPURGE.GC_CHANGE
                                                                                          LOGS
WAYPURGE_GC                 GCADMIN        12/02/14 09:00:01 12/03/14 09:00:00 SCHEDULED  WAYPURGE.GC_SESSIONS
LCREP_INDEX_STATS           LCREP          12/02/14 11:00:00 12/04/14 11:00:00 SCHEDULED  gather_lcrep_stats
OPSWARE_ADMIN_SYSTEM_STATS  OPSWARE_ADMIN  12/01/14 06:00:02 12/08/14 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

Starting with Oracle 10g, the DBMS_JOB package was superceded by the improved Oracle Scheduler (dbms_scheduler) package. Although Oracle still supports the DBMS_JOB package for backward compatibility, Oracle will make no further enhancements to the package. Since the DBMS_SCHEDULER provides better functionality, all the SA jobs that used the DBMS_JOB package have been redesigned in this release to use the DBMS_SCHEDULER package. The affected jobs can be found in the dba_scheduler_jobs table. These changes are only relevant to new SA 10.x Cores and cores upgraded to SA 10.x.

To view the jobs and changes made, you can run the following from SQL*Plus:

```
# su - oracle
# sqlplus "/ as sysdba"
SQL>set line 200
SQL>col owner format a14
SQL>col job_action format a50
SQL>col job_name format a50
SQL>select job_name, owner, job_action from dba_scheduler_jobs where owner in
('OPSWARE_ADMIN', 'LCREP', 'GCADMIN');
```

Your output should be as follows:

```
JOB_NAME                          OWNER         JOB_ACTION
------------------------------    -----------   -------------------------
WLMPURGE_GC                       GCADMIN       WLMPURGE.GC_JOBS
STORAGEINITIATORPURGE_GC          GCADMIN       STORAGEINITIATORPURGE.GC_STORAGEINITIATORS
AUDITPURGE_GC                     GCADMIN       AUDITPURGE.GC_AUDITLOGS
CHANGELOGPURGE_GC                 GCADMIN       CHANGELOGPURGE.GC_CHANGELOGS
WAYPURGE_GC                       GCADMIN       WAYPURGE.GC_SESSIONS
LCREP_INDEX_STATS                 LCREP         gather_lcrep_stats
OPSWARE_ADMIN_SYSTEM_STATS        OPSWARE_ADMIN gather_opsware_admin_sys_stats

7 rows selected.
```

Running dba_scheduler_jobs manually

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

```
SQL> grant create session to lcrep, gcadmin;
```

To run the statistics collection jobs manually in SQL*Plus, use the commands shown below. If you copy and paste the following command examples, replace the variables like schema_user_value with the values of the **schema_user** column displayed by the preceding select statement. Substitute the variables such as job_name_value with the values of the job column displayed by the same select statement.

```
SQL> connect <schema_user_value>/<password>
SQL> exec dbms_scheduler.run_job('<job_name_value>');
```

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

```
SQL> revoke create session from lcrep, gcadmin;
```

Changing the Time Jobs are Run

dba_scheduler_jobs are run at UTC time. To change the time at which the jobs are run, follow these instructions:

```
# su - oracle
$ sqlplus "/ as sysdba"
SQL>set line 300
SQL>col job_name format a30
SQL>col owner format a14
SQL>col last format a17
SQL>col next format a17
SQL>col repeat_interval format a40
SQL>col job_action format a30

SQL>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, repeat_interval,
job_action from dba_scheduler_jobs where owner in ('OPSWARE_ADMIN', 'LCREP',
'GCADMIN');
```

The above statement provides information about a job. Note the job name and the owner that has the privilege to run this job.

The output of the above statement is similar to the following (formatting is compressed due to space limitations):

```
JOB_NAME              OWNER    LAST            NEXT            REPEAT_INTERVAL        JOB_ACTION
-----------           -------  --------------  --------------  --------------------   ---------------------
WLMPURGE_GC           GCADMIN  12/02/14 09:00:01  12/03/14 09:00:00  TRUNC(SYSDATE+1)+9/24   WLMPURGE.GC_JOBS
STORAGEINITIATORPURGE GCADMIN  12/02/14 09:00:01  12/03/14 09:00:00  TRUNC(SYSDATE+1)+9/24   STORAGEINITIATORPURGE.GC
_GC                                                                                         _STORAGEINITIATORS
AUDITPURGE_GC         GCADMIN  12/02/14 09:00:01  12/03/14 09:00:00  TRUNC(SYSDATE+1)+9/24   AUDITPURGE.GC_AUDITLOGS
CHANGELOGPURGE_GC     GCADMIN  12/02/14 09:00:01  12/03/14 09:00:00  TRUNC(SYSDATE+1)+9/24   CHANGELOGPURGE.GC_CHANGE
                                                                                            LOGS
WAYPURGE_GC           GCADMIN  12/02/14 09:00:01  12/03/14 09:00:00  TRUNC(SYSDATE+1)+9/24   WAYPURGE.GC_SESSIONS
LCREP_INDEX_STATS     LCREP    12/02/14 11:00:00  12/04/14 11:00:00  TRUNC(SYSDATE+2)+11/24  gather_lcrep_stats
OPSWARE_ADMIN_SYSTEM_ OPSWARE_ 12/01/14 06:00:02  12/08/14 06:00:00  TRUNC(SYSDATE+1) + 18/  gather_opsware_admin_sys
STATS                 ADMIN                                          24 +                   _stats
                                                                     mod(abs(to_number(to_c
                                                                     har(sysdate + 1,'D'))
                                                                     - 7) + 2,  7")
```

In this example the user `lcrep` changes the time/interval at which the job is run. Any other user can be substituted for the user `lcrep`.

```
# su - oracle
$ sqlplus "/ as sysdba"
SQL> grant create session to lcrep;
Grant succeeded.
```

In the example:

• job name=LCREP_INDEX_STATS

• owner = lcrep

In this example, the job LCREP_INDEX_STATS runs at 11:00 a.m. UTC. To change this to 9:00 a.m. UTC, the command is:

```
SQL> connect lcrep/<password_for_lcrep>
Connected.

SQL> exec dbms_scheduler.set_attribute('LCREP_INDEX_STATS',
attribute=>'REPEAT_INTERVAL', value=>'TRUNC(SYSDATE+2)+9/24');
```

Monitoring Database Users

To monitor database users, perform the following steps:

1   To check the database users, enter the following command in `sqlplus`:

```
# su - oracle
$ sqlplus "/ as sysdba"
SQL>Select username, account_status, default_tablespace,
temporary_tablespace from dba_users;
```

Monitoring the ERROR_INTERNAL_MSG Table

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

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

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

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

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

Rebuilding the SHADOW_FOLDER_UNIT Table

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

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

```
SQL>exec SHADOW_FOLDER_UNIT_UTIL.SHADOW_FOLDER_UNIT_RELOAD
```

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

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

do the following:

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

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

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

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

3   Run the SQL from Monitoring the ERROR_INTERNAL_MSG Table on page 259 and check if the procedure has listed any faulty records.
SHADOW_FOLDER_UNIT_UTIL.SHADOW_FOLDER_UNIT_RELOAD is idem potent therefore the faulty records can be fixed and you can rerun SHADOW_FOLDER_UNIT_UTIL.SHADOW_FOLDER_UNIT_RELOAD.

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

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

4   Revoke the permissions given to user `truth`:

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

Oracle Database Backup Methods

It is important that you back up the database on a regular basis. Be sure to use more than one backup method and to test your recovery process.

You can use the following methods to back up the Oracle database:

- **Export-Import**: An export extracts logical definitions and data from the database and writes the information to a file. Export-import does not support point-in-time recoveries. Do not use Export-Import as your only backup and recovery strategy.

- **Cold or Off-Line Backups**: This procedure shuts the database down and backs up all data, index, log, and control files. Cold or off-line backups do not support point-in-time recoveries.

- **Hot or Online Backups**: During these backups, the database must be available and in `ARCHIVELOG` mode. The tablespaces are set to backup mode. This procedure backs up tablespace files, control files, and archived redo log files. Hot or online backups support point-in-time recoveries.

- **RMAN Backups**: While the database is either off-line or on-line, use the `rman` utility to back up the database.

Regardless of your backup strategy, remember to back up all required Oracle software libraries, parameter files, password files, and so forth. If your database is in `ARCHIVELOG` mode, you also need to back up the archived log files.

For more information on backing up Oracle databases, see the following Oracle documents:

- *Oracle Database 2 Day DBA*

- *Oracle Database Concepts*

- *Oracle Database Administrator's Guide*

These guides are on the Oracle web site at the following URL:

`http://www.oracle.com/technology/documentation/index.html`

Troubleshooting System Diagnosis Errors

If an additional privilege (permission) has been made manually to the database, when SA performs a system diagnosis on the Data Access Engine, an error message might be generated. For example, if an additional grant has been made to the `truth.facilities` table, the following error appears:

```
Test Information
Test Name: Model Repository Schema
Description: Verifies that the Data Access Engine's version of the schema
matches the Model Repository's version.
Component device: Data Access Engine (spin.blue.qa.example.com)
Test Results: The following tables differ between the Data Access Engine
and the Model Repository:  facilities.
```

To fix this problem, revoke the grant. For example, if you need to revoke a grant on the `truth.facilities` table, log on to the server with the database and enter the following commands:

```
# su - oracle
$ sqlplus "/ as sysdba"
SQL>grant create session to truth;
SQL>connect truth/<truth passwd>;
SQL>revoke select on truth.facilities from spin;
SQL>exit
sqlplus "/ as sysdba"
SQL>revoke create session from truth;
```

Useful SQL

The following SQL commands help you manage information in the Oracle database.

BIN$ Objects

If the SA Installer discovers the existence of BIN$ objects in the database, enter the following SQL commands:

```
SQL>show parameter recyclebin;
SQL>SELECT owner,original_name,operation,type FROM dba_recyclebin;
connect <owner>/password
SQL>purge recyclebin;
```

or

```
SQL>purge table BIN$xxx;
```

By default, `recyclebin` is set to OFF.

Appendix B: SA Core Parameter Reference

This section describes configuration parameters that you will be required to specify values for during an SA Core installation.

Depending on the type of installation you are performing, Single-host, Simple or Advanced, you will be prompted to provide certain required parameter values.

These parameters provide values for:

- Passwords (SA Administrator, Database Administrator, etc.)

- Service Names (TNS name)

- Configuration parameter values

- Path names for programs, configuration file, logs

- IP Addresses for Core hosts and devices hosting Core Components

- Gateway port numbers, and so on.

The values you provide are used for the current installation and are saved to a *Core Definition File (CDF)* that you will use again later when upgrading the SA Core and when adding Secondary Cores for a Multimaster Mesh. This file is autmatically saved during installation to `/var/tmp` and given a timestamp to aid you in identifying the file.

During installation, theHPSA Installer displays a series of parameters, some with default values that you can accept or modify, and other parameters that you must supply values for.

The number of parameters varies depending on whether you choose a single-host, standard, or advanced installation.

SA Installation Configuration Parameters

You can use the following reference to gather the information that you will need for the SA installation.

The tables below, list the various parameters that you may be asked to provide values for. The parameters are labeled with the type of installation in which they appear (Single-host, Simple, and Advanced).

When you run the SA Installation script, the Installer prompts you to choose either the **Simple** or **Advanced** interview. If you choose Simple mode, the default values are used for certain values, for example, passwords for the Oracle database, the Model Repository (`truth`) and Data Access Engine (`spin`) user, ports used by the Gateways, among others. In Advanced Mode, you can select values other than the default, giving you finer control.

Configuration Parameters by Installation Type

The configuration parameters you are asked to provide values for during the SA Installer Interview depends on the installation method you select:

- Single-Host

- Simple

- Advanced

- Uninstall

Table 50 through Table 54 list the parameters you will see based upon the type of installation. Table 55 through Table 66 list the parameters by their SA function.

Single-Host Installation Configuration Parameters

Table 50 lists the Single-Host installation configuration parameters and the expected values.

table 50   Single-Host Installation Configuration Parameters

Parameter	Description
Please enter the database password for the `opsware_admin` user. This password is used to connect to the Oracle database. **Parameter:** `truth.oaPwd`	Specify the `opsware_admin` password created by your database administrator. `opsware_admin` is an Oracle user that the Installer uses during installation to perform required tasks. If you are installing the HP-supplied Oracle database created by the Installer, the password you provide here will be associated with `opsware_admin` during installation of the database. If you have an existing Oracle database installation, this must be the password that your DBA set for the `opsware_admin` user when setting up the Oracle instance on the server. **Source:** Oracle DBA
Enter the short name of the facility where the SA Installer is being run (no spaces). **Parameter:** `truth.dcNm`	Specify the short name of the facility where the Installer is being run. This would also be the location of the First Core. Some SA processes use this name internally. It must be in uppercase, less than 25 characters, and cannot contain spaces or special characters (underscores are allowed, dashes are *not* allowed). **Source:** Variable **Example:** HEADQUARTERS

table 50 Single-Host Installation Configuration Parameters (cont'd)

Parameter	Description
Enter the directory that contains the Microsoft patching utilities. (Press Ctrl-I for a list of required files) or enter "none" if you do not wish to upload these utilities. **Parameter:** `windows_util_loc`	Specify the directory to which you have already copied the Microsoft utilities required for Window's Patch Management or enter "none" if you do not plan to perform Windows patching and do not want to upload these files. Should you decide later that you need to perform Windows patching, you will need to install the required Windows Patch Management files either by using the SA Client's Import feature or the `populate-opsware-update-library` command line script as described in the *SA User Guide: Server Patching*. **Source:** Variable, however, this directory *must* exist on the same server as the Software Repository (part of the Slice Component bundle). **Example:** `/tmp`
Enter the hashing algorithm [SHA1 or SHA256] for the SA cryptographic module. [SHA1]: **Parameter:** `crypto.hash_algorithm`	Specify the hashing algorithm that SA should use for the cryptographic module. **Source:** Variable **Valid Values:** SHA1 or SHA256.
Enter the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module. [2048]: **Parameter:** `crypto.key_length`	Specify the key length to use for the cryptographic module hashing algorithm. **Source:** Variable **Valid Values:** 2048 or 4096

Simple Installation Configuration Parameters

Table 51 lists the Simple installation configuration parameters and the expected values.

table 51   Simple Installation Configuration Parameters

Parameter	Description
Please enter the database password for the `opsware_admin` user. This password is used to connect to the Oracle database. **Parameter:** `truth.oaPwd`	Specify the `opsware_admin` password created by your database administrator. `opsware_admin` is an Oracle user that the Installer uses during installation to perform required tasks. If you are installing the HP-supplied Oracle database created by the Installer, the password you provide here will be associated with `opsware_admin` during installation of the database. If you have an existing Oracle database installation, this must be the password that your DBA set for the `opsware_admin` user when setting up the Oracle instance on the server. **Source:** Oracle DBA
Enter the short name of the facility where the SA Installer is being run (no spaces). **Parameter:** `truth.dcNm`	Specify the short name of the facility where the Installer is being run. This would also be the location of the First Core. Some SA processes use this name internally. It must be in uppercase, less than 25 characters, and cannot contain spaces or special characters (underscores are allowed, dashes are *not* allowed). **Source:** Variable **Example:** HEADQUARTERS
Enter the directory that contains the Microsoft patching utilities. (Press Ctrl-I for a list of required files) or enter "none" if you do not wish to upload these utilities. **Parameter**: `windows_util_loc`	Specify the directory to which you have already copied the Microsoft utilities required for Window's Patch Management or enter "none" if you do not plan to perform Windows patching and do not want to upload these files. Should you decide later that you need to perform Windows patching, you will need to install the required Windows Patch Management files either by using the SA Client's Import feature or the `populate-opsware-update-library` command line script as described in the *SA User Guide: Server Patching*. **Source:** Variable, however, this directory *must* exist on the same server as the Software Repository (part of the Slice Component bundle). **Example:** `/tmp`

table 51   Simple Installation Configuration Parameters (cont'd)

Parameter	Description
Please enter the IP address of the Management Gateway. **Parameter:** `mgw_address`	Specify the IP address of the Management Gateway. The Management Gateway manages Core-to-Core communications. Core Gateways installed on Secondary Cores and/or Satellite Gateways also communicate with the Management Gateway. **Source:** Variable **Example:** `192.168.165.242`
Enter the hashing algorithm [SHA1 or SHA256] for the SA cryptographic module. [SHA1]: **Parameter**: `crypto.hash_algorithm`	Specify the hashing algorithm that SA should use for the cryptographic module. **Source**: Variable **Valid Values**: SHA1 or SHA256.
Enter the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module. [2048]: **Parameter**: `crypto.key_length`	Specify the key length to use for the cryptographic module hashing algorithm. **Source**: Variable **Valid Values**: 2048 or 4096
Enter the path of the Oracle home directory. **Parameter:** `db.orahome`	Specify the base directory of the Oracle database installation. If you are installing the HP-supplied Oracle database created by the Installer, the default location of `ORACLE_HOME` is `/u01/app/oracle/product/12.1.0/db_1`. If you have an existing HP-supplied Oracle database, you will not be prompted for this parameter. For an existing non-HP-supplied Oracle database, you can determine the Oracle home directory by logging in as the `oracle user` on the Model Repository server, and checking the value of the `$ORACLE_HOME` environment variable. (For a remote database installation, this parameter refers to the Oracle Client on the Model Repository server.) **Source:** The DBA who created the Oracle database. **Example:** `/u01/app/oracle/product/12.1.0/db_1`
Please enter the host (NFS server) where Software Repository Content resides. **Parameter** `word.store.host`	Specify the host name of the server where Software Repository content is stored. **Source:** Variable **Example:** `192.168.165.243`

table 51   Simple Installation Configuration Parameters (cont'd)

Parameter	Description
Please enter the path to the server where Software Respiratory content resides. **Parameter** `word.store.path`	Specify the path to the server where Software repository content is stored. This will be to the server specified in word.store.host. **Source**: Variable
Please enter the OS Provisioning Boot Server IP address or hostname. **Parameter:** `bootagent.host`	Specify the IP address for server on which you installed the SA Provisioning Boot Server. Important: You must provide a valid IP address or host name that can be resolved from the server on which you installed the SA Provisioning Boot Server component and the Build Manager. Additionally, the host name must be resolvable by SA managed servers for SA Provisioning. **Source**: Variable **Example**: `foo.example.com`

Advanced Installation Configuration Parameters

Table 52 lists the Advanced installation configuration parameters and the expected values.

table 52   **Advanced Installation Configuration Parameters**

Parameter	Description
Please enter the database password for the `opsware_admin` user. This password is used to connect to the Oracle database. **Parameter:** `truth.oaPwd`	Specify the `opsware_admin` password created by your database administrator. `opsware_admin` is an Oracle user that the Installer uses during installation to perform required tasks. If you are installing the HP-supplied Oracle database created by the Installer, the password you provide here will be associated with `opsware_admin` during installation of the database. If you have an existing Oracle database installation, this must be the password that your DBA set for the `opsware_admin` user when setting up the Oracle instance on the server. **Source**: Oracle DBA

table 52   Advanced Installation Configuration Parameters (cont'd)

Parameter	Description
Enter the short name of the facility where the SA Installer is being run (no spaces). **Parameter:** `truth.dcNm`	Specify the short name of the facility where the Installer is being run. This would also be the location of the First Core. Some SA processes use this name internally. It must be in uppercase, less than 25 characters, and cannot contain spaces or special characters (underscores are allowed, dashes are *not* allowed). **Source:** Variable **Example:** HEADQUARTERS
Enter the hashing algorithm [SHA1 or SHA256] for the SA cryptographic module. [SHA1]: **Parameter**: `crypto.hash_algorithm`	Specify the hashing algorithm that SA should use for the cryptographic module. **Source**: Variable **Valid Values**: SHA1 or SHA256.
Enter the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module. [2048]: **Parameter**: `crypto.key_length`	Specify the key length to use for the cryptographic module hashing algorithm. **Source**: Variable **Valid Values**: 2048 or 4096
Enter the directory that contains the Microsoft patching utilities. (Press Ctrl-I for a list of required files) or enter "none" if you do not wish to upload these utilities. **Parameter**: `windows_util_loc`	Specify the directory to which you have already copied the Microsoft utilities required for Window's Patch Management or enter "none" if you do not plan to perform Windows patching and do not want to upload these files. Should you decide later that you need to perform Windows patching, you will need to install the required Windows Patch Management files either by using the SA Client's Import feature or the `populate-opsware-update-library` command line script as described in the *SA User Guide: Server Patching*. **Source**: Variable, however, this directory *must* exist on the same server as the Software Repository (part of the Slice Component bundle). **Example:** `/tmp`
Please enter the IP address of the Management Gateway. **Parameter**: `mgw_address`	Specify the IP address of the Management Gateway. The Management Gateway manages Core-to-Core communications. Core Gateways installed on Secondary Cores and/or Satellite Gateways also communicate with the Management Gateway. **Source:** Variable **Example:** `192.168.165.242`

table 52   Advanced Installation Configuration Parameters (cont'd)

Parameter	Description
Please enter the password for the cryptographic material. **Parameter:** `decrypt_passwd`	Specify the password to use for decrypting cryptographic material. This password must be the same across all cores in a Multimaster Mesh. If you have an existing SA installation, this must be the password previously set for decrypting cryptographic material. **Password Restrictions**: The password cannot contain spaces and it must be between 4 and 20 characters long. **Source:** Variable **Example:** `x145_pwd03`
Enter the path of the Oracle home directory. **Parameter:** `db.orahome`	Specify the base directory of the Oracle database installation. If you are installing the HP-supplied Oracle database created by the Installer, the default location of `ORACLE_HOME` is `/u01/app/oracle/product/12.1.0/db_1.` If you have an existing HP-supplied Oracle database, you will not be prompted for this parameter. For an existing non-HP-supplied Oracle database, you can determine the Oracle home directory by logging in as the `oracle user` on the Model Repository server, and checking the value of the `$ORACLE_HOME` environment variable. (For a remote database installation, this parameter refers to the Oracle Client on the Model Repository server.) **Source:** The DBA who created the Oracle database. **Example:** `/u01/app/oracle/product/ 12.1.0/db_1`
Please enter the host (NFS server) where Software Repository Content resides. **Parameter** `word.store.host`	Specify the host name of the server where Software Repository content is stored. **Source:** Variable **Example:** `192.168.165.243`
Please enter the path to the server where Software Respiratory content resides. **Parameter** `word.store.path`	Specify the path to the server where Software repository content is stored. This will be to the server specified in word.store.host. **Source:** Variable

table 52   Advanced Installation Configuration Parameters (cont'd)

Parameter	Description
Please enter the OS Provisioning Boot Server IP address or hostname. **Parameter:** `bootagent.host`	Specify the IP address for server on which you installed the SA Provisioning Boot Server. Important: You must provide a valid IP address or host name that can be resolved from the server on which you installed the SA Provisioning Boot Server component and the Build Manager. Additionally, the host name must be resolvable by SA managed servers for SA Provisioning. **Source**: Variable **Example**: `foo.example.com`
Please enter the password for the cryptographic material. **Parameter:** `decrypt_passwd`	Specify the password to use for decrypting cryptographic material. This password must be the same across all cores in a Multimaster Mesh. If you have an existing SA installation, this must be the password previously set for decrypting cryptographic material. **Password Restrictions**: The password cannot contain spaces and it must be between 4 and 20 characters long. Source: Variable **Example:** `x145_pwd03`
Please enter the password for the SA `admin` user. this is the password that will be used to authenticate the user `admin` to SA. **Parameter:** `cast.admin_pwd`	Specify the password for the SA `admin` user. **Password Restrictions**: This password cannot contain spaces. The Installer automatically creates the `admin` user. The first time you log in to the SAS Web Client to access a new Facility, you must log in as the `admin` user. Source: Variable **Example:** `x145_pwd03`

table 52   Advanced Installation Configuration Parameters (cont'd)

Parameter	Description
Enter the fully qualified path to the directory where the export file will be saved. **Parameter:** `truth.dest`	*You must create this directory on the Model Repository server before you run the Installer.* Specify the directory in which the database export file will be saved. This directory must reside on the Model Repository server in the source facility. You will see this prompt only when installing a new First Core. **Note:** When adding a facility to a Multimaster Mesh, you must export the Model Repository from the source facility, then copy it to the destination facility. **Source:** Variable **Default:** `/var/opt/opsware/truth/`
Enter the fully qualified path to the directory that contains the export file. **Parameter:** `truth.sourcePath`	*This parameter is used when a new facility is added to a Multimaster Mesh and the source export file is copied to the new facility. This directory must exist on the server and contain the database export file before you run the Installer on the server.* Specify the directory on the destination facility's Model Repository server to which you copied the export data file from the source facility. **Source:** Variable **Default:** `/var/opt/opsware/truth/`
Please enter the Facility ID (number only, less than or equal to 950, with no leading zeros). **Parameter:** `truth.dcId`	Specify an ID that uniquely identifies the facility. When you install the First Core, you will be prompted to provide this ID. When you install Secondary Cores in the same Multimaster Mesh, SA automatically generates the Facility ID when you add a new facility using the SAS Web Client. You can determine the Secondary Core's Facility ID by logging in to the SAS Web Client at the First Core facility, then select **Opsware Facilities** under **Environment** in the Navigation pane and click the facility's name. **ID Restrictions:** The Facility ID value is capped at 950. Therefore, you must specify a number for the first facility that is far enough below 950 that you will have sufficient IDs available to continue adding facilities to your Multimaster Mesh. **Source:** Variable for the first facility; set by the SA for subsequent facilities. **Default:** 1

Parameter	Description
Would you like this facility to mirror all Software Repository content in the mesh? **Parameter**: `word.enable_content_mirroring`	Enables mirroring (replication) of the Software Repository (word). **Source**: Variable **Default**: Y
Enter the SID of the Oracle instance that contains the Data Model Repository. **Parameter**: `db.sid`	Specify the database system ID (SID) that was set when Oracle was installed on the server where the Model Repository is installed. If you are installing the HP-supplied Oracle database created by the Installer, the SID is `truth`. If you have an existing HP-supplied Oracle database, you will not be asked to supply this parameter. For an existing non-HP-supplied Oracle database, you can find the SID by looking in the `tnsnames.ora` file. The location of this file can vary, so check with your DBA if you are not sure where to look. **Source**: The DBA who created the Oracle database. **Default**: truth **Example**: `DTC05`

table 52   Advanced Installation Configuration Parameters (cont'd)

Parameter	Description
Enter the fully-qualified path to the TNS admin directory (where the `tnsnames.ora` file resides). **Parameter:** `truth.tnsdir`	Specify the directory that contains the `tnsnames.ora` file. **Note:** This directory and path must be the same on all servers in a core. For example, since the Data Access Engine must access the `tnsnames.ora` file to connect to the Model Repository, the location of `tnsnames.ora` directory on the Data Access Engine server must be the same as the directory location on the Model Repository server. If you are installing the HP-supplied Oracle database created by the Installer, the `tnsnames.ora` file will be installed under `/var/opt/oracle.` If you have an existing HP-supplied Oracle database installed, you will not be prompted for this parameter. If you have an existing non-HP-supplied Oracle database, the location of the `tnsnames.ora` file can vary, so check with your DBA if you are not sure where to look. **Source:** The DBA who created the Oracle database. **Example:** `/var/opt/oracle`
Please enter the port on which the Model Repository database is listening. **Parameter:** `db.port`	Specify the port on which the Model Repository database listens: **Source:** Variable **Default:** 1521
Please enter the absolute path on the NFS server for the Opsware Global File System (`/user`, `/home`, and `/tmp` directories). This value should be different from `ogfs.audit.path` and `word.store.path`. **Parameter:** `ogfs.store.path`	Specify the absolute path on the NFS server for the Global File System (`/user`, `/home`, and `/tmp` directories). This value should be different from `ogfs.audit.path` and `word.store.path`. **Source:** Variable **Default:** `/var/opt/opsware/ogfs/export/store`
Please enter the absolute path on the NFS server for the Opsware Global File System where the audit streams will be stored. This value should be different from `ogfs.store.path` and `word.store.path`. **Parameter:** `ogfs.audit.path`	Specify the absolute path on the NFS server for the Global File System where the audit streams will be stored. This value should be different from `ogfs.store.path` and `word.store.path`. **Source:** Variable **Default:** `/var/opt/opsware/ogfs/export/audit`

table 52   Advanced Installation Configuration Parameters (cont'd)

Parameter	Description
Please enter the port on which Management Gateway in the First Core listens for connections from other Gateways (this value should match the value of `mgw_tunnel_listener_port` parameter in First Core's CDF. Typically it's set to 2001.) **Parameter**: `masterCore.mgw_tunnel_ listener_port`	Specify the port on which Management Gateway in the First Core listens for connections from other Gateways (this value should match the value of `mgw_tunnel_listener_port` parameter in First Core's CDF. **Source**: Variable **Default**: None
Enter the port on which the Management Gateway will listen for connections from other gateways. **Parameter:** `mgw_tunnel_listener_port`	Specify the port on which the First and Secondary Cores' Management Gateways will listen for connections from other Core and Satellite gateways. **Source**: Variable **Example**: 2001
Please enter the port on which Agents can contact the Agent Gateway to request connections to Core Components. **Parameter**: `agw_proxy_port`	Specify the port that agents should use to connect to the SA Core. **Source**: Variable **Default**: 3001
Please enter the pathname to the Linux media. **Parameter:** `media_server.linux_media`	Specify the path to the Linux OS media on the server on which the Media Server will be installed. Providing the path to the Linux OS media does not actually copy the media to the Media Server. See the *SA User Guide: OS Provisioning* for the steps required to set up the media on the Media Server for SA Provisioning. **Source**: Variable, however, this directory must exist on the server where the Media Server is installed. **Default**: `/media/opsware/linux`
Please enter the pathname to the Solaris OS media. **Parameter:** `media_server.sunos_media`	Specify the path to the Sun Solaris OS media on the server on which the Media Server will be installed. Providing the path to the Solaris OS media does not actually copy the media to the Media Server See the *SA User Guide: OS Provisioning* for the steps required to set up the media on the Media Server for SA Provisioning. **Source**: Variable, however, this directory must exist on the server where the Media Server is installed. **Default**: `/media/opsware/solaris/`

table 52   Advanced Installation Configuration Parameters (cont'd)

Parameter	Description
Please enter the pathname to the Windows OS media. **Parameter:** `media_server.windows_media`	Specify the path to the Microsoft Windows OS media on the server on which the Media Server will be installed. The SA Provisioning feature exports Windows OS media to SMB clients through a Samba share. Providing the path to the Windows OS media does not actually copy the media to the Media Server. See the *SA User Guide: OS Provisioning* for the steps required to set up the media on the Media Server for SA Provisioning. **Source**: Variable, however, this directory must exist on the server where the Media Server is installed. **Default**: `/media/opsware/windows/`
Please enter the host name or IP address of the Network Automation (NA) server. (Enter "none" if NA is not installed.) **Parameter:** `twist.nasdata.host`	Specify the host name or IP address of the server running HP Network Automation (NA), if installed. If NA is not installed, accept the default value `none`. Enter a value without spaces. **Source**: The network administrator/SA administrator who installed HP Network Automation. **Example**: `192.168.165.242`
Please enter the username used to connect to HP Live Network. (Leave as "none" if HPLN is not being configured.) **Parameter**: `hpln_user_name`	Specify the username used to connect to the HP Live Network (HPLN). The value should adhere to HPLN's standard. A minimum of 5 characters and it cannot contain the special characters `&`, `|`, or `*`. Also, any of the invalid characters defined for the SA install also apply, such as leading `#`, quotes, and so on **Source**: Variable **Default**: None
Please enter the password associated with the username used to connect to HP Live Network. (Leave as "none" if HPLN is not being configured.) **Parameter**: `hpln_password`	Specify the HPLN user password used to connect to the HP Live Network (HPLN). The value must follow the same rules as `hpln_user_name`, except the minimum characters accepted is 6. **Source**: Variable **Default**: None

table 52   Advanced Installation Configuration Parameters (cont'd)

Parameter	Description
Please enter the address of the proxy used to connect to the HP Live Network. (Leave as "none" if HPLN is not being configured or no proxy is needed to connect to HP Live Network.) **Parameter**: `hpln_proxy`	Specify the IP address or hostname of the proxy used to connect to the HP Live Network (HPLN) The value must follow the following format: `<protocol>://<host>` or `<protocol>://<host>:<port>`. If no `<port>` value is provided, the default 3128 is used. **Source**: Variable **Default**: None
Please enter the username of the proxy user required to connect to the HP Live Network. (Leave as "none" if HPLN is not being configured, no proxy is configured or if no username is needed.) **Parameter**: `hpln_proxy_user`	Specify the username for the HPLN proxy user. The invalid characters for this parameter follow the SA convention for usernames, such as no leading #, no quotes, no whitespace, and so on. **Source**: Variable **Default**: None
Please enter the password of the proxy user required to connect to the HP Live Network. (Leave as "none" if HPLN is not being configured, no proxy is configured or if no username is needed.) **Parameter**: `hpln_proxy_pwd`	Specify the password for the HPLN proxy user. The invalid characters for this parameter follow the SA convention for usernames, such as no leading #, no quotes, no whitespace, and so on. **Source**: Variable **Default**: None
Please enter the gateway Bandwidth Configuration Management for remote connections port. **Parameter:** `opswgw.ConfigPort`	Specify the port to be used for pushing bandwidth configurations to Satellite Gateways. **Source**: Variable **Default**: None
Please enter the gateway bandwidth usage channel port. **Parameter**: `opswgw.BwUsageChannelPort`	Specify the port to be used for retrieving Satellite Gateway bandwidth usage information. **Source**: Variable **Default**: None

SA Installation Configuration Parameters Listed by Function

Define New Facility Parameters

Table 53 lists the parameters you see when defining a new Facility and the expected values.

table 53   **Define New Facility Parameters**

Parameter	Description
Advanced only Enter the short name of the new facility you would like to define **Parameter:** `newCore.dcNm`	Specify the default facility name for the Secondary Core. Some SA processes use this name internally. It must be less than 25 characters, and cannot contain spaces or special characters (both dashes and underscores are allowed). **Source:** Variable **Example:** NORTHSIDE
Advanced only Enter the IP address of the host where you want to install the Model Repository in the new facility. **Parameter:** `newCore.dbHost`	Specify the IP address of the host on which you will install the Model Repository for the new target core. **Source:** Variable **Example:** `192.168.165.242`
Advanced only Please enter the IP address of the device where you are planning to install the Infrastructure component in the new facility (or where the management gateway will be installed). **Parameter**: `newCore.mgwIP`	Specify the IP address of the host on which you will install the Infrastructure Component bundle or the host on which the Management Gateway will be installed. **Source**: Variable **Example**: 192.168.165.202
Advanced only Enter the subdomain for the facility you are about to create (lowercase, no spaces). **Parameter:** `newCore.dcSubDom`	Specify the fully-qualified DNS subdomain where the Destination Multimaster Core is to be deployed. This value must be *unique* for each core in the Multimaster Mesh, both Source and Destination Cores. The value is based on the VLAN for the facility in which you are installing the Multimaster core. The subdomain name must be in lowercase with no spaces, less than 50 characters, and in subdomain format. **Source:** Your network administrator. **Example:** `dc2.example.com`

table 53   Define New Facility Parameters (cont'd)

Parameter	Description
Advanced only Enter the service name (aka TNS name) of the Model Repository instance. **Parameter:** `newCore.servicename`	Specify the service name, also known as the *alias*, for the core's Model Repository. You will see this prompt only when installing a new First Core. If this is a new installation, the service name you specify will be associated with the Model Repository during installation. If you plan to use an existing Model Repository, you can find the service name by looking in the `tnsnames.ora` file on the Model Repository instance. The location of this file can vary, so check with your DBA if you are not sure where to look. **Source:** The DBA who created the Oracle database. **Example:** `truth02.example.com`

SA Core Uninstallation Parameters

Table 54 lists the SA Core uninstallation parameters and the expected values.

table 54   SA Core Uninstallation Parameters

Parameter	Description
Are you absolutely sure you want to remove all packages in the repository? [Y/N] **Parameter:** `word.remove_files`	If you answer *Yes*, the packages, logs, and cryptographic material for the Software Repository are removed. **Default:** `None`
Are you absolutely sure you want to remove users' OGFS home and audit directories? (home and audit directories will only be removed if they are stored on the Software Repository server) (Y/N)? **Parameter**: `ogfs.remove_home_dirs`	Respond *Yes* if you want the uninstall to remove all users' OGFS home and audit directories. Backup any information you want to retain. **Source**: Variable **Default**: None
Do you need to preserve any of the data in this database? [Y/N] **Parameter:** `truth.uninstall.needdata`	Uninstalling the Model Repository permanently deletes all data in the database, therefore, the uninstallation process stops if you reply *Yes* to this prompt. If you want to do an uninstallation, backup your data, run the uninstallation again and answer *No* to this prompt. Remember, the Installer *does not* preserve any data. **Default:** `Y`

table 54   SA Core Uninstallation Parameters (cont'd)

Parameter	Description
Are you sure you want to remove all data and schema from this database? [Y/N **Parameter:** `truth.uninstall.aresure`	Uninstalling the Model Repository by responding *Yes* permanently deletes all data in the database. You can stop the uninstallation by responding *No* to this prompt. **Default**: None
Would you like to preserve the database of cryptographic material? [Y/N] **Parameter**: `save_crypto`	If you answer *Yes*, the database of cryptographic material is saved. If you answer *No*, the material is deleted as part of the uninstallation. **Default**: None
Would you like to preserve the HPLN content? (Y/N) **Parameter**: `hpln.uninstall.keepcontent`	Responding *No* uninstalls all HP Live Network content. **Source**: Variable **Default**: None

Model Repository Parameters

The Model Repository is the database that stores information about the hardware and software deployed in the operational environment. Most of the Model Repository parameters apply only to a Single-host or First Core installation.

Table 55 lists the Model Repository parameters and the expected values.

table 55   Model Repository Parameters

Parameter	Description
Install Method: Advanced Please enter the service name (aka TNS name) of the Model Repository instance in the facility where the SA Installer is being run. **Parameter**: `truth.servicename`	Specify the service name, also known as the *alias*, for the Model Repository. For a Single Core, this is the server on which you are running the Installer. If you are installing the default Oracle database created by the Installer, the service name you provide here will be associated with the database during installation. If you intend to use an existing Oracle database, you can find the service name by looking in the `tnsnames.ora` file on the Model Repository instance. The service name is the value before the first equals sign (=) in the file. The location of this file can vary, so check with your DBA if you are not sure where to look. **Source**: The DBA who created the Oracle database. **Example**: `truth.example.com`
Install Method: Simple, Advanced Enter the service name (aka TNS name) of the Model Repository instance. **Parameter:** `newCore.servicename`	Specify the service name, also known as the *alias*, for the core's Model Repository. You will see this prompt only when installing a new First Core. If this is a new installation, the service name you specify will be associated with the Model Repository during installation. If you plan to use an existing Model Repository, you can find the service name by looking in the `tnsnames.ora` file on the Model Repository instance. The location of this file can vary, so check with your DBA if you are not sure where to look. **Source**: The DBA who created the Oracle database. **Example**: `truth02.example.com`
Install Method: Advanced Enter the SID of the Oracle instance that contains the Data Model Repository. **Parameter**: `db.sid`	Specify the database system ID (SID) that was set when Oracle was installed on the server where the Model Repository is installed. If you are installing the HP-supplied Oracle database created by the Installer, the SID is `truth`. If you have an existing HP-supplied Oracle database, you will not be asked to supply this parameter. For an existing non-HP-supplied Oracle database, you can find the SID by looking in the `tnsnames.ora` file. The location of this file can vary, so check with your DBA if you are not sure where to look. **Source**: The DBA who created the Oracle database. **Default**: truth **Example**: `DTC05`

table 55   Model Repository Parameters (cont'd)

Parameter	Description
Install Method: Simple and Advanced Enter the path of the Oracle home directory. **Parameter:** `db.orahome`	Specify the base directory of the Oracle database installation. If you are installing the HP-supplied Oracle database created by the Installer, the default location of `ORACLE_HOME` is `/u01/app/oracle/product/12.1.0/db_1`. If you have an existing HP-supplied Oracle database, you will not be prompted for this parameter. For an existing non-HP-supplied Oracle database, you can determine the Oracle home directory by logging in as the `oracle user` on the Model Repository server, and checking the value of the `$ORACLE_HOME` environment variable. (For a remote database installation, this parameter refers to the Oracle Client on the Model Repository server.) **Source**: The DBA who created the Oracle database. **Example**: `/u01/app/oracle/product/12.1.0/db_1`
Install Method: Advanced Enter the fully-qualified path to the TNS admin directory (where the `tnsnames.ora` file resides). **Parameter:** `truth.tnsdir`	Specify the directory that contains the `tnsnames.ora` file. **Note**: This directory and path must be the same on all servers in a core. For example, since the Data Access Engine must access the `tnsnames.ora` file to connect to the Model Repository, the location of `tnsnames.ora` directory on the Data Access Engine server must be the same as the directory location on the Model Repository server. If you are installing the HP-supplied Oracle database created by the Installer, the `tnsnames.ora` file will be installed under `/var/opt/oracle`. If you have an existing HP-supplied Oracle database installed, you will not be prompted for this parameter. If you have an existing non-HP-supplied Oracle database, the location of the `tnsnames.ora` file can vary, so check with your DBA if you are not sure where to look. **Source**: The DBA who created the Oracle database. **Example**: `/var/opt/oracle`
Install Method: Advanced Please enter the port on which the Model Repository database is listening. **Parameter**: `db.port`	Specify the port on which the Model Repository database listens: **Source**: Variable **Default**: 1521

table 55   **Model Repository Parameters (cont'd)**

Parameter	Description
Install Method: Advanced Enter the fully qualified path to the directory where the export file will be saved. **Parameter:** `truth.dest`	Specify the directory in which the database export file will be saved. This directory must reside on the Model Repository server in the source facility. You will see this prompt only when installing a new First Core. Note: When adding a facility to a Multimaster Mesh, you must export the Model Repository from the source facility, then copy it to the destination facility. **Source**: Variable **Default**: `/var/opt/opsware/truth/`
Install Method: Advanced Enter the fully qualified path to the directory that contains the export file. **Parameter:** `truth.sourcePath`	*This parameter is used when a new facility is added to a Multimaster Mesh and the source export file is copied to the new facility. This directory must exist on the server and contain the database export file before you run the Installer on the server.* Specify the directory on the destination facility's Model Repository server to which you copied the export data file from the source facility. **Source**: Variable **Default**: `/var/opt/opsware/truth/`
Install Method: Simple, Advanced Enter the IP address of the host where you want to install the Model Repository in the new facility. **Parameter**: `newCore.dbHost`	Specify the IP address of the host on which you will install the Model Repository for the new target core. **Source**: Variable **Example**: `192.168.165.242`
Install Method: Simple, Advanced Please enter the IP address of the device where you are planning to install the Infrastructure component in the new facility (or where the management gateway will be installed). **Parameter**: `newCore.mgwIP`	Specify the IP address of the host on which you will install the Infrastructure Component bundle or the host on which the Management Gateway will be installed. **Source**: Variable **Example**: 192.168.165.202

Database (Model Repository) Password Parameters

The Installer prompts you to specify passwords for required Oracle user accounts. The passwords must meet the following standard Oracle criteria:

- The password cannot contain an Oracle reserved word (see Oracle's documentation for a full list).

- The password must be between 1 and 30 characters long.

- The password must start with a letter and use only alphanumeric and underscore (_) characters.

Table 56 lists the Database parameters and the expected values.

table 56   Database Password Parameters

Parameter	Description
Install Method: Single-Host, Simple, Advanced Please enter the database password for the `opsware_admin` user. This password is used to connect to the Oracle database. **Parameter:** `truth.oaPwd`	Specify the `opsware_admin` password created by your database administrator. `opsware_admin` is an Oracle user that the Installer uses during installation to perform required tasks. If you are installing the HP-supplied Oracle database created by the Installer, the password you provide here will be associated with `opsware_admin` during installation of the database. If you have an existing Oracle database installation, this must be the password that your DBA set for the `opsware_admin` user when setting up the Oracle instance on the server. **Source**: Oracle DBA

Software Repository Parameters

Table 57 lists the password parameters for the Software Repository and the expected values.

table 57   Software Repository Parameters

Parameter	Description
Install Method: Advanced Would you like this facility to mirror all Software Repository content in the mesh? **Parameter**: `word.enable_content_mirroring`	Enables mirroring (replication) of the Software Repository (word). **Source**: Variable **Default**: Y
Install Method: Advanced Please enter the location where the Software Repository temporarily places content during uploads. **Parameter** `word_tmp_dir`	Specify the fully qualified location for the temporary storage of content during Software Repository uploads. **Source**: Variable **Default**: `/var/opt/opsware/wordbot_tmp/`

table 57   Software Repository Parameters

Parameter	Description
Install Method: Simple and Advanced Please enter the host (NFS server) where Software Repository Content resides. **Parameter** `word.store.host`	Specify the host name of the server where Software Repository content is stored. **Source**: Variable **Example**: `192.168.165.243`
Install Method: Simple and Advanced Please enter the path to the server where Software Respiratory content resides. **Parameter** `word.store.path`	Specify the path to the server where Software repository content is stored. This will be to the server specified in word.store.host. **Source**: Variable

SA Cryptographic Material Parameters

Table 58 lists the cryptographic materials parameters and the expected values.

table 58   Cryptographic Materials Parameters

Parameter	Description
Enter the hashing algorithm [SHA1 or SHA256] for the SA cryptographic module. [SHA1]: **Parameter**: `crypto.hash_algorithm`	Specify the hashing algorithm that SA should use for the cryptographic module. **Source**: Variable **Valid Values**: SHA1 or SHA256.
Enter the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module. [2048]: **Parameter**: `crypto.key_length`	Specify the key length to use for the cryptographic module hashing algorithm. **Source**: Variable **Valid Values**: 2048 or 4096

SA Component Password Parameters

Table 59 lists the password parameters for components other than the Model Repository and the expected values.

➤ If this installation is for a Multimaster Mesh, the following passwords must be the same for all cores belonging to the mesh.

table 59   Component User and Password Parameters

Parameter	Description
Install Method: Advanced Please enter the password for the cryptographic material. **Parameter:** `decrypt_passwd`	Specify the password to use for decrypting cryptographic material. This password must be the same across all cores in a Multimaster Mesh. If you have an existing SA installation, this must be the password previously set for decrypting cryptographic material. **Password Restrictions**: The password cannot contain spaces and it must be between 4 and 20 characters long. **Source**: Variable **Example**: `x145_pwd03`
Install Method: Advanced Please enter the password for the SA `admin` user. this is the password that will be used to authenticate the user `admin` to SA. **Parameter:** `cast.admin_pwd`	Specify the password for the SA `admin` user. **Password Restrictions**: This password cannot contain spaces. The Installer automatically creates the `admin` user. The first time you log in to the SAS Web Client to access a new Facility, you must log in as the `admin` user. **Source**: Variable **Example**: `x145_pwd03`

Facility Parameters

A *Facility* is a system object that represents a specific geographical location (such as Sunnyvale, Plano, Sacramento, or a data center). Servers and users are often associated with a facility as a means to enforce access rights and privileges. If you are performing a Single Core installation, your deployment is a single facility. Multimaster installations, however, consist of two or more facilities.

In this section, the first core installed in a Multimaster Mesh is called the *First Core*, and is the core that has the first Model Repository installed. *Secondary Cores* are the second, third, and fourth (and so on) cores installed in the mesh. For historical reasons, First Cores are sometimes referred to in parameter names as *Master* and Secondary Cores as *Slave*.

Table 60 lists the Facility parameters and the expected values.

table 60   Facility Parameters

Parameter	Description
Install Method: Advanced Please enter the subdomain for this facility (lowercase, no spaces). **Parameter:** `truth.dcSubDom`	Specify the fully-qualified DNS subdomain where the core is to be deployed. This is the facility where you run the Installer. This value must be unique for each core in the Multimaster Mesh. The value is based on the VLAN for the facility in which you are installing the core. The subdomain name must be in lowercase, less than 50 characters long, and in subdomain format. **Source**: Your network administrator. **Example:** `dc1.example.com`
Install Method: Simple, Advanced Enter the subdomain for the facility you are about to create (lowercase, no spaces). **Parameter:** `newCore.dcSubDom`	Specify the fully-qualified DNS subdomain where the Destination Multimaster Core is to be deployed. This value must be *unique* for each core in the Multimaster Mesh, both Source and Destination Cores. The value is based on the VLAN for the facility in which you are installing the Multimaster core. The subdomain name must be in lowercase with no spaces, less than 50 characters, and in subdomain format. **Source**: Your network administrator. **Example:** `dc2.example.com`

table 60 **Facility Parameters (cont'd)**

Parameter	Description
Install Method: Single-Host, Simple, Advanced Enter the short name of the facility where the SA Installer is being run (no spaces). **Parameter:** `truth.dcNm`	Specify the short name of the facility where the Installer is being run. This would also be the location of the First Core. Some SA processes use this name internally. It must be in uppercase, less than 25 characters, and cannot contain spaces or special characters (underscores are allowed, dashes are *not* allowed). **Source:** Variable **Example:** HEADQUARTERS
Install Method: Simple, Advanced **Secondary Core Install only** Enter the short name of the new facility you would like to define **Parameter:** `newCore.dcNm`	Specify the default facility name for the Secondary Core. Some SA processes use this name internally. It must be less than 25 characters, and cannot contain spaces or special characters (both dashes and underscores are allowed). **Source:** Variable **Example:** NORTHSIDE
Install Method: Advanced Please enter the Facility ID (number only, less than or equal to 950, with no leading zeros). **Parameter:** `truth.dcId`	Specify an ID that uniquely identifies the facility. When you install the First Core, you will be prompted to provide this ID. When you install Secondary Cores in the same Multimaster Mesh, SA automatically generates the Facility ID when you add a new facility using the SAS Web Clientt. You can determine the Secondary Core's Facility ID by logging in to the SAS Web Client at the First Core facility, then select **Opsware Facilities** under **Environment** in the Navigation pane and click the facility's name. **ID Restrictions:** The Facility ID value is capped at 950. Therefore, you must specify a number for the first facility that is far enough below 950 that you will have sufficient IDs available to continue adding facilities to your Multimaster Mesh. **Source:** Variable for the first facility; set by the SA for Secondary facilities. **Default:** 1

SA OS/Software Provisioning and NA Integration Parameters

The values specified for the following parameters will be used to configure SA Provisioning, Software Provisioning, Patch Management, and Network Automation (NA) integration. Table 61 lists the OS/Software Provisioning and NA Integration parameters and the expected values.

table 61   SA OS/Software Provisioning and NA Integration Parameters

Parameter	Description
Install Method: Single-Host, Simple, Advanced Enter the directory that contains the Microsoft patching utilities. (Press Ctrl-I for a list of required files) or enter "none" if you do not wish to upload these utilities. **Parameter**: `windows_util_loc`	Specify the directory to which you have already copied the Microsoft utilities required for Window's Patch Management or enter "none" if you do not plan to perform Windows patching and do not want to upload these files. Should you decide later that you need to perform Windows patching, you will need to install the required Windows Patch Management files either by using the SA Client's Import feature or the `populate-opsware-update-library` command line script as described in the *SA User Guide: Server Patching*. **Source**: Variable, however, this directory *must* exist on the same server as the Software Repository (part of the Slice Component bundle). **Example**: `/tmp`
Install Method: Simple and Advanced Please enter the OS Provisioning Boot Server IP address or hostname. **Parameter**: `bootagent.host`	Specify the IP address for server on which you installed the SA Provisioning Boot Server. Important: You must provide a valid IP address or host name that can be resolved from the server on which you installed the SA Provisioning Boot Server component and the Build Manager. Additionally, the host name must be resolvable by SA managed servers for SA Provisioning. **Source**: Variable **Example**: `foo.example.com`
Install Method: Advanced Please enter the pathname to the Linux media. **Parameter**: `media_server.linux_media`	Specify the path to the Linux OS media on the server on which the Media Server will be installed. Providing the path to the Linux OS media does not actually copy the media to the Media Server. See the *SA User Guide: OS Provisioning* for the steps required to set up the media on the Media Server for SA Provisioning. **Source**: Variable, however, this directory must exist on the server where the Media Server is installed. **Default**: `/media/opsware/linux`

Parameter	Description
Install Method: Advanced Please enter the pathname to the Solaris OS media. **Parameter**: `media_server.sunos_media`	Specify the path to the Sun Solaris OS media on the server on which the Media Server will be installed. Providing the path to the Solaris OS media does not actually copy the media to the Media Server See the *SA User Guide: OS Provisioning* for the steps required to set up the media on the Media Server for SA Provisioning. **Source**: Variable, however, this directory must exist on the server where the Media Server is installed. **Default**: `/media/opsware/solaris/`
Install Method: Advanced Please enter the pathname to the Windows OS media. **Parameter**: `media_server.windows_media`	Specify the path to the Microsoft Windows OS media on the server on which the Media Server will be installed. The SA Provisioning feature exports Windows OS media to SMB clients through a Samba share. Providing the path to the Windows OS media does not actually copy the media to the Media Server. See the *SA User Guide: OS Provisioning* for the steps required to set up the media on the Media Server for SA Provisioning. **Source**: Variable, however, this directory must exist on the server where the Media Server is installed. **Default**: `/media/opsware/windows/`
Install Method: Advanced Please enter the host name or IP address of the Network Automation (NA) server. (Enter "none" if NA is not installed.) **Parameter**: `twist.nasdata.host`	Specify the host name or IP address of the server running HP Network Automation (NA), if installed. If NA is not installed, accept the default value `none`. Enter a value without spaces. **Source**: The network administrator/SA administrator who installed HP Network Automation. **Example**: `192.168.165.242`
Install Method: Advanced Please enter the location where the Software Repository temporarily places content during uploads. **Parameter** `word_tmp_dir`	Specify the fully qualified location for the temporary storage of content during Software Repository uploads. **Source**: Variable **Default**: `/var/opt/opsware/wordbot_tmp/`

SA Gateway Parameters

The values specified for the following parameters are used to configure the IP addresses and ports at which SA Gateways can be contacted by Core Components, Agents, or other gateways.

Table 62 lists the gateway parameters and expected values.

➤ You can use only port numbers below 64001.

table 62   SA Gateway Parameters

Parameter	Description
Install Method: Simple and Advanced Please enter the IP address of the Management Gateway. **Parameter**: `mgw_address`	Specify the IP address of the Management Gateway. The Management Gateway manages Core-to-Core communications. Core Gateways installed on Secondary Cores and/or Satellite Gateways also communicate with the Management Gateway. **Source**: Variable **Example**: `192.168.165.242`
Install Method: Advanced Enter the port on which the Management Gateway will listen for connections from other gateways. **Parameter**: `mgw_tunnel_listener_port`	Specify the port on which the First and Secondary Cores' Management Gateways will listen for connections from other Core and Satellite gateways. **Source**: Variable **Example**: 2001

table 62   SA Gateway Parameters (cont'd)

Parameter	Description
Install Method: Advanced Enter the port on which the Management Gateway can be contacted to request connections to Core Components. *Parameter:* `mgw_proxy_port`	Specify the port number through which Core Components can request tunneled connections to other components through the Management Gateway. Source: Variable Example: 3003
Install Method: Advanced Please enter the port on which Agents can contact the Agent Gateway to request connections to Core Components. **Parameter**: `agw_proxy_port`	Specify the port that agents should use to connect to the SA Core. **Source**: Variable **Default**: 3001
Install Method: Advanced Please enter the port on which Management Gateway in the First core listens for connections from other Gateways (this value should match the value of `mgw_tunnel_listener_port` parameter in First Core's CDF. Typically it's set to 2001.) **Parameter**: `masterCore.mgw_tunnel_ listener_port`	Specify the port on which Management Gateway in the First core listens for connections from other Gateways (this value should match the value of `mgw_tunnel_listener_port` parameter in First Core's CDF. **Source**: Variable **Default**: 2001

Satellite Gateway Bandwidth Configuration Management Parameters

The values specified for the following parameters are used to configure Satellite Gateway Bandwidth Configuration Management.

Table 63 lists the Global File System parameters and the expected values.

table 63   **Satellite Gateway Bandwidth Configuration Management Parameters**

Parameter	Description
Install Method: Simple and Advanced Please enter the gateway Bandwidth Configuration Management for remote connections port. **Parameter:** `opswgw.ConfigPort`	Specify the port to be used for pushing bandwidth configurations to Satellite Gateways. **Source**: Variable **Default**: 8086
Install Method: Simple and Advanced Please enter the gateway bandwidth usage channel port. **Parameter**: `opswgw.BwUsageChannelPort`	Specify the port to be used for retrieving Satellite Gateway bandwidth usage information. **Source**: Variable **Default**: 8084
Install Method: Expert Please enter the port for the administrative interface of the Agent Gateway. **Parameter**: `agw_admin_port`	Specify the port for the Bandwidth Configuration Management tool administrative interface. **Source**: Variable **Default**: 8089

Global File System Parameters

The values specified for the following parameters are used to configure IP addresses and directories for the Global File System.

Table 64 lists the Global File System parameters and the expected values.

table 64   Global File System Parameters

Parameter	Description
Install Method: Advanced Please enter the pathname of where you wish the local cache of snapshots and audits to be. This will require a large amount of disk space (4 Gb by default). **Parameter**: `spoke.cachedir`	Specify the directory in which the Global File System service will cache snapshots and audits for quick access. **Default**: `/var/opt/opsware/compliancecache` **Source**: Variable **Example**: `/var/opt/opsware/compliancecache`
Install Method: Advanced Please enter the absolute path on the NFS server for the Opsware Global File System (`/user`, `/home`, and `/tmp` directories). This value should be different from `ogfs.audit.path` and `word.store.path`. **Parameter**: `ogfs.store.path`	Specify the absolute path on the NFS server for the Global File System (`/user`, `/home`, and `/tmp` directories). This value should be different from `ogfs.audit.path` and `word.store.path`. **Source**: Variable **Default**: `/var/opt/opsware/ogfs/export/store`
Install Method: Advanced Please enter the absolute path on the NFS server for the Opsware Global File System where the audit streams will be stored. This value should be different from `ogfs.store.path` and `word.store.path`. **Parameter**: `ogfs.audit.path`	Specify the absolute path on the NFS server for the Global File System where the audit streams will be stored. This value should be different from `ogfs.store.path` and `word.store.path`. **Source**: Variable **Default**: `/var/opt/opsware/ogfs/export/audit`

HP Live Network (HPLN) Parameters

Table 65 lists the parameters and expected values for the HP Live Network (HPLN).

table 65   HP Live Network (HPLN) Parameters

Parameter	Description
Install Method: Advanced Please enter the username used to connect to HP Live Network. (Leave as "none" if HPLN is not being configured.) **Parameter**: `hpln_user_name`	Specify the username used to connect to the HP Live Network (HPLN). The value should adhere to HPLN's standard. A minimum of 5 characters and it cannot contain the special characters `&`, `|`, or `*`. Also, any of the invalid characters defined for the SA install also apply, such as leading `#`, quotes, and so on **Source**: Variable **Default**: None

table 65   HP Live Network (HPLN) Parameters

Parameter	Description
Install Method: Advanced Please enter the password associated with the username used to connect to HP Live Network. (Leave as "none" if HPLN is not being configured.) **Parameter**: `hpln_password`	Specify the HPLN user password used to connect to the HP Live Network (HPLN). The value must follow the same rules as `hpln_user_name`, except the minimum characters accepted is 6. **Source**: Variable **Default**: None
Install Method: Advanced Please enter the address of the proxy used to connect to the HP Live Network. (Leave as "none" if HPLN is not being configured or no proxy is needed to connect to HP Live Network.) **Parameter**: `hpln_proxy`	Specify the IP address or hostname of the proxy used to connect to the HP Live Network (HPLN) The value must follow the following format: `<protocol>://<host>` or `<protocol>://<host>:<port>`. If no `<port>` value is provided, the default 3128 is used. **Source**: Variable **Default**: None
Install Method: Advanced Please enter the username of the proxy user required to connect to the HP Live Network. (Leave as "none" if HPLN is not being configured, no proxy is configured or if no username is needed.) **Parameter**: `hpln_proxy_user`	Specify the username for the HPLN proxy user. The invalid characters for this parameter follow the SA convention for usernames, such as no leading #, no quotes, no whitespace, and so on. **Source**: Variable **Default**: None
Install Method: Advanced Please enter the password of the proxy user required to connect to the HP Live Network. (Leave as "none" if HPLN is not being configured, no proxy is configured or if no username is needed.) **Parameter**: `hpln_proxy_pwd`	Specify the password for the HPLN proxy user. The invalid characters for this parameter follow the SA convention for usernames, such as no leading #, no quotes, no whitespace, and so on. **Source**: Variable **Default**: None
Install Method: Uninstall This is an uninstallation parameter **Parameter**: `hpln.uninstall.keepcontent`	See Uninstallation Parameters on page 296

Uninstallation Parameters

Table 66 lists the parameters and expected values for an SA Core uninstallation.

table 66   Uninstallation Parameters

Parameter	Description
Install Method: Uninstall Do you need to preserve any of the data in this database? [Y/N] **Parameter:** `truth.uninstall.needdata`	Uninstalling the Model Repository permanently deletes all data in the database, therefore, the uninstallation process stops if you reply *Yes* to this prompt. If you want to do an uninstallation, backup your data, run the uninstallation again and answer *No* to this prompt. Remember, the Installer *does not* preserve any data. **Default**: Y
Install Method: Uninstall Are you sure you want to remove all data and schema from this database? [Y/N **Parameter:** `truth.uninstall.aresure`	Uninstalling the Model Repository by responding *Yes* permanently deletes all data in the database. You can stop the uninstallation by responding *No* to this prompt. **Default**: None
Install Method: Uninstall Would you like to preserve the database of cryptographic material? [Y/N] **Parameter:** `save_crypto`	If you answer *Yes*, the database of cryptographic material is saved. If you answer *No*, the material is deleted as part of the uninstallation. **Default**: None
Install Method: Uninstall Are you absolutely sure you want to remove all packages in the repository? [Y/N] **Parameter:** `word.remove_files`	If you answer *Yes*, the packages, logs, and cryptographic material for the Software Repository are removed. **Default**: None
Install Method: Uninstall Are you absolutely sure you want to remove users' OGFS home and audit directories? (home and audit directories will only be removed if they are stored on the Software Repository server) (Y/N)? **Parameter**: `ogfs.remove_home_dirs`	Respond *Yes* if you want the uninstall to remove all users' OGFS home and audit directories. Backup any information you want to retain. **Source**: Variable **Default**: None
Install Method: Uninstall Would you like to preserve the HPLN content? (Y/N) **Parameter**: `hpln.uninstall.keepcontent`	Responding *No* uninstalls all HP Live Network content. **Source**: Variable **Default**: None

Full SA Core Configuration Parameter Listing

The HP SA Installer provides an Expert level interview which displays and allows modifications of all SA Core configuration parameters, some of which are not displayed during the Simple or Advanced interviews. Modifying these parameters requires extensive knowledge of SA Core capabilities and configuration and applying incorrect values will cause unexpected results.

Table 67 lists all SA Core configuration parameters as seen when you perform an installation using the Expert level interview.

For a detailed description of these parameters their values and ranges, see SA Core Parameter Reference on page 263.

table 67   **Full** SA **Core Configuration Parameter List**

Parameter	Default Value	Description
agw_proxy_port	3001	This port must be open between the Agents in this facility and the Agent Gateway. Agents will contact the Agent Gateway on this port to request connections to core components
bootagent.host	Infrastructure Components host	Specify the SA Provisioning Boot Server IP address or hostname.
cast.admin_pwd	opsware	Specify the password for the SA admin user. The Installer automatically creates the admin user. The first time you log in to the SA Web Client to access a new Facility, you must log in as the admin user. **Password Restrictions**: This password cannot contain spaces.
cgw_admin_port	8085	Specify the port for the administrative interface of the core Gateway. The Gateway has a browser-based administrative interface that allows you to view configuration and monitor traffic.
cgw_proxy_port	3002	Specify the port on which core components can contact this core Gateway to request tunneled connections.
cgw_slice_tunnel_ listener_port	2003	Specify the port on which the core Gateway on the Slice Component bundle will listen for connections from other Gateways (only used if the Infrastructure component bundle is installed on the same box as the Slice Component bundle).
crypto.hash_algorithm	SHA1	Specify the hashing algorithm [SHA1 or SHA256] for SA cryptographic module.
crypto.key_length	2048	Specify the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module.
db.host	none	Specify the hostname/IP address of the Oracle database server.

table 67   Full SA **Core Configuration Parameter List (cont'd)**

Parameter	Default Value	Description
`db.orahome`	`/u01/app/ oracle/ product/ <version>/ db_2`	Specify the path of the `ORACLE_HOME` directory of your Model Repository (truth) server.
`db.port`	**1521**	Specify the port on which the database listens for incoming connections. This value is recorded in the `tnsnames.ora` file.
`db.sid`	truth	Specify the SID of the Oracle instance containing the Model Repository.
`decrypt_passwd`	crypto	Specify the password for the cryptographic material. This password must be the same across all cores in a Multimaster Mesh. If you have an existing SA installation, this must be the password previously set for decrypting cryptographic material. **Password Restrictions**: The password cannot contain spaces and it must be between 4 and 20 characters long.
`hpln_password`	none	Specify the user password used to connect to the HP Live Network (HPLN). Specify "none" if HPLN is not being configured. The value must follow the same rules as `hpln_user_name`, except the minimum characters accepted is 6.
`hpln_proxy`	3128	Specify the IP address or hostname of the proxy used to connect to the HP Live Network (HPLN). Specify "none" if HPLN is not being configured or no proxy is needed to connect to HP Live Network. The value must follow the following format: `<protocol>://<host>` or `<protocol>://<host>:<port>`. If no `<port>` value is provided, the default 3128 is used.
`hpln_proxy_pwd`	none	Specify the password for the HPLN proxy user. Specify "none" if HPLN is not being configured, no proxy is configured, or no password is required. The invalid characters for this parameter follow the SA convention for usernames, such as no leading #, no quotes, no whitespace, and so on.

table 67   Full SA Core Configuration Parameter List (cont'd)

Parameter	Default Value	Description
hpln_proxy_user	none	Specify the username for the HPLN proxy user. Specify "none" if HPLN is not being configured, no proxy is configured, or no username is required. The invalid characters for this parameter follow the SA convention for usernames, such as no leading #, no quotes, no whitespace, and so on.
hpln_user_name	none	Specify the username used to connect to the HP Live Network (HPLN). Specify "none" if HPLN is not being configured. The value should adhere to HPLN's standard. A minimum of 5 characters and it cannot contain the special characters &, |, or *. Also, any of the invalid characters defined for the SA install also apply, such as leading #, quotes, and so on.
masterCore.mgw_tunnel_listener_port	none	Specify the port on which Management Gateway in the First Core listens for connections from other Gateways (this value should match the value of the mgw_tunnel_listener_port parameter for the First Core (typically 2001).
media_server.linux_media	/media/opsware/linux	Specify the path to the location on the Media Server where the Linux media shouldbe placed when SA Provisioning components are installed. **Note**: Providing the path to the Linux OS media does not actually copy the media to the Media Server. See the *SA User Guide: OS Provisioning* for the steps required to set up media on the Media Server. This directory must exist on the Media Server host.
media_server.sunos_media	/media/opsware/solaris/	Specify the path to the location on the Media Server where the Oracle Solaris OS media should be placed when SA Provisioning components are installed. **Note**: Providing the path to the Solaris OS media does not actually copy the media to the Media Server See the *SA User Guide: OS Provisioning* for the steps required to set up media on the Media Server. This directory must exist on the Media Server host.

table 67   Full SA **Core Configuration Parameter List (cont'd)**

Parameter	Default Value	Description
`media_server.windows_media`	`/media/ opsware/ windows`	Specify the path to the location on the Media Server where the Windows OS media should be placed when SA Provisioning components are installed. The SA Provisioning feature exports Windows OS media to SMB clients through a Samba share. **Note**: Providing the path to the Windows OS media does not actually copy the media to the Media Server See the *SA User Guide: OS Provisioning* for the steps required to set up media on the Media Server. This directory must exist on the Media Server host.
`media_server.windows_share_name`	OSMEDIA	Specify the share name to use for the Windows media sharing server (**note**: share names that are longer than 8 characters may give errors while browsing or may not be accessible to some older clients.)
`media_server.windows_share_password`	opsware	Specify a password to write-protect the Windows media share. The `import_media` tool will prompt for this password each time it is run.
`mgw_address`	none	Specify the IP address of the Management Gateway.
`mgw_proxy_port`	3003	Specify the port number through which Core Components can request tunneled connections to other components through the Management Gateway.
`mgw_tunnel_listener_port`	2001	Specify the port on which the First and Subsequent Cores' Management Gateways will listen for connections from other Core and Satellite gateways.
`ogfs.audit.host.ip`	none	Specify the IP address of the NFS server for the Global File System where audit streams will be stored.
`ogfs.audit.path`	`/var/opt/ opsware/ogfs/ export/audit`	the absolute path on the nfs server for the Opsware Global File System where the audit streams will be stored. This value should be different from `ogfs.store.path` and `word.store.path`
`ogfs.store.host.ip`	none	Specify the IP address of the NFS server for the Opsware Global File System (user, home, and tmp directories).
`ogfs.store.path`	`/var/opt/ opsware/ogfs/ export/store`	Specify the absolute path on the NFS server for the Global File System (user, home, and tmp directories). This value should be different from `ogfs.audit.path` and `word.store.path`

table 67   **Full** SA **Core Configuration Parameter List (cont'd)**

Parameter	Default Value	Description
`spoke.cachedir`	`/var/opt/ opsware/ compliance cache`	Specify the directory in which the Global File System service will cache snapshots and audits for quick access. This directory can require a large amount of disk space (4Gb by default)
`truth.aaaPwd`	database password	Enter database password for the `AAA` user.
`truth.authDom`	MY. CUSTOMER. COM	Enter the authorization domain used by the Access and Authentication Directory.
`truth.dcNm`	none	Specify the short name of the facility in which the SA Installer is being run (no spaces).
`truth.dcSubDom`	none	Specify the subdomain for the facility in which the SA Installer is being run (lowercase, no spaces). The value must be a valid domain name (for example, SUB.DOMAIN.COM) and is limited to 50 characters.
`truth.detuserpwd`	opsware	Specify the password to use for the DCML exchange tool (DET) user.
`truth.gcPwd`	opsware	Spe ify database password for the `gcadmin` user.
`truth.lcrepPwd`	opsware	Specify the database password for the `lcrep` user.
`truth.oaPwd`	opsware	Specify the password for the `opsware_admin` user. This is the password used to connect to the Oracle database. If you are installing Oracle with SA, this password is set to "`opsware`" during installation. If you are using your own Oracle installation, ask your DBA for the password.
`truth.pubViewsPwd`	opsware	Specify the database password for the `public views` user.
`truth.servicename`	none	Specify the service name of the Model Repository instance in the facility where SA Installer is being run. For Oracle, you can identify the service name by looking in the `tnsnames.ora` file on the Model Respository instance. Locate the appropriate TNS entry in this file for the Model Repository and note the value before the first "=" sign. For example, if the database name is "`truth`", the entry may look like "`truth=(DESCRIPTION=(...))`". The location and contents of this file can vary, check with your DBA if you are not sure where to look.

table 67   **Full** SA **Core Configuration Parameter List (cont'd)**

Parameter	Default Value	Description
`truth.sourcePath`	`/var/opt/ opsware/truth`	Specify the full path to the directory containing the `source_db_charset.txt` file. When adding a facility to a multimaster mesh, the Model Respository (truth) data must be exported from the source facility, then copied to the destination facility. The destination directory path must be the same as the directory on the Model Repository (truth) server as the source directory path.
`truth.spinPwd`	database password (opsware)	Specify the database password for the `spin` user.
`truth.tnsdir`	`/var/opt/ oracle`	Specify the path to the TNS admin directory (where the `tnsnames.ora` file resides)
`truth.truthPwd`	database password (opsware)	Specify the database password for the `truth` user.
`truth.twistPwd`	database password (opsware)	Specify the database password for the `twist` user.
`truth.vaultPwd`	database password (opsware)	Specify the database password for the `vault` user.
`twist.buildmgr.passwd`	database password (opsware)	Specify the database password for the `buildmgr` user.
`twist.default_gid`	70001	Specify the default UNIX Group ID to assign to SA users (number only, no less than 1024 and no greater than 90000000, with no leading zeros
`twist.integration.pas swd`	database password (opsware)	Specify the password for the `Integration` user.
`twist.min_uid`	80001	Specify the the minimum ID to use when assigning UNIX User IDs to Opsware users (number only, no less than 1024 and no greater than 90000000, with no leading zeros). UNIX UIDs are generated automatically for each SA user. UIDs are allocated counting up from the minimum specified in this parameter.
`twist.nasdata.host`	none	Specify the hostname or IP address of the NA (Network Automation) server (Enter "none" if NA is not installed).

table 67   Full SA Core Configuration Parameter List (cont'd)

Parameter	Default Value	Description
`windows_util_loc`	none	Specify the path to the directory in which SA should install the Microsoft patching utilities or, if you have already manually downloaded the utilities, the path to the directory that contains the files. For a list of required files, press Ctrl-I at the prompt. Enter "none" if you do not wish to install the utilities.
`word.enable_content_mirroring`	Y(es)	Enable/disable mirroring of all Software Repository content in a Multimaster Mesh.
`word.store.host`	none	Specify the IP address of the NFS server for the Software Repository. For satellite installs, enter the IP address of the Software Repository Cache. Storage for the Software Repository will be mounted from the server specified in this parameter..
`word.store.path`	`/var/opt/ opsware/word`	Specify the absolute path on the NFS server for the Software Repository. Storage for the Software Repository will be mounted from this directory on the server specified by the `word.store.host` parameter. Ensure that this directory has sufficient free disk space. This value should be different from `ogfs.store.path` and `ogfs.audit.path`
`word_root`	`/var/opt/ opsware/word`	Specify the mount point for the Software Repository root directory. For satellite installs, enter the root directory of the Software Repository Cache. Package Repository contents will be mounted from the server and directory specified by `word.store.host` and `word.store.path` parameters, respectively. **Note**: During installation, the SA Installer creates a number of default directories/folders with a default naming format. For example: `/var/opt/opsware/word/Package Repository` These directory/folder names are required and must not be changed. If changed, you may have problems when upgrading your SA Core.
`word_tmp_dir`	`/var/opt/ opsware/ wordbot_ tmp/`	Specify the directory where the Package Repository will temporarily place content during uploads.

Appendix C: SA Management Console

From SA 10.2 and later, SA provides the Management Console, a command line tool that you can use to:

- Remove SA CORD patches (rollback to the major release level)
- Shut down an SA Core
- Reset the SA Administrative passwords

SA Management Console Usage

To invoke the console, enter the command:

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

Arguments

The Management Console accepts the following arguments:

table 68

Argument	Description
`-c <filename>`	The path to CDF used to install the SA Core.
`--debug`	Run the Management Console in debug mode which causes more information to be displayed on the console.

Removing a Cord Patch

1 Invoke the Management Console:

```
<distro>/opsware_installer/hpsa_mgmt_console.sh --debug
-c <distro>/var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml
```

2 You see the following screen:

```
Utility Type
============

1. Remove Patch (Rollback to GA build)
2. Shutdown HPSA service
3. Reset HPSA Password

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

3 Select 1 to Remove Patch:

```
Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit): 1
```

4 You see the following message (this example assumes all SA Core Components are installed on a single host; if there is more than one server in the core, patches are removed in parallel):

```
--------------------------------------
remove_patch will be performed on the following identified core host(s).
If there is any inconsistency then try again with the correct CDF.

<IP_address>  (word_uploads, slice, infrastructure, oracle_sas, osprov,
truth_mm_overlay)


--------------------------------------
Do you want to continue (Y/N) [Y]:
```

5 Press Y to begin the patch uninstallation. You will see messages similar to the following:

```
Setting up NFS
Install media mounted from <hostname>:<distro>/disk001
Distribution local - linking to /var/tmp/hpsa_media
Collecting inventory from <IP_address>
Verifying that "/etc/init.d/opsware-sas" exist on <IP_address>...
Running primary core status check on <IP_address>...
Removing opsware_patch on <IP_address>...
******* Removing opsware_patch from device <IP_address>.
...............

Cleaning up NFS
<IP_address> is an address on the machine <IP_address>
Creating temporary CDF [/var/tmp/cdf_tmp.xml]
Copying [/var/tmp/cdf_tmp.xml] to [/var/opt/opsware/install_opsware/cdf/
cdf.xml] on <IP_address>
Copying [/var/tmp/cdf_tmp.xml] to [/var/opt/opsware/install_opsware/cdf/
cdf_<timestamp>.xml] on <IP_address>
Remaining threads after stop:
[<_MainThread(MainThread, started)>]

Script done on <timestamp>
```

Shutting Down an SA Core

1 Invoke the Management Console:

```
<distro>/opsware_installer/hpsa_mgmt_console.sh --debug
-c <distro>/var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml
```

2 You see the following screen:

```
Utility Type
============

1. Remove Patch (Rollback to GA build)
2. Shutdown HPSA service
3. Reset HPSA Password
```

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

3   Select 2 to shutdown an SA Core:

```
Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit): 2
```

4   At this point, the SA Core is shut down normally.

Resetting the SA Administrative Passwords

Prerequisites

- The user DETUSER login must have already been manually changed using the SAS Web Client or the SA Client.

- All interview parameters must have same password because this option assumes that all passwords are derived from `truth.oaPwd`.

- You can invoke the Management Console on the Infrastructure Component bundle host where the default CDF will be loaded from the default CDF location directory or, if invoked from a different host, you can specify the location of most recent CDF used to install the core.

Perform the following tasks to reset the SA Administrator password:

1   Invoke the Management Console:

```
<distro>/opsware_installer/hpsa_mgmt_console.sh --debug
-c <distro>/var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml
```

2   You see the following screen:

```
Utility Type
============

1. Remove Patch (Rollback to GA build)
2. Shutdown HPSA service
3. Reset HPSA Password

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

3   Select 3 to reset the SA Administrator password:

```
Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit): 3
```

4   You see messages similar to the following:

```
Setting up NFS
Distro nfs mounted from:
    <IP_address>:/mydistro to /tmp/dist
Install media mounted from <IP_address>:/mydistro/oi_rhel6/
opsware_<version>-primary/disk001
<IP_address> is an address on the machine <IP_address>
Distribution local - linking to /var/tmp/hpsa_media

Parameter 1 of 2
new truth.oaPwd []: **********
```

```
Parameter 2 of 2
db.orahome []: /u01/app/oracle/product/12.1.0/db_1


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

..................


Cleaning up NFS
<IP_address> is an address on the machine <IP_address>
Creating temporary CDF [/var/tmp/cdf_tmp.xml]
Copying [/var/tmp/cdf_tmp.xml] to [/var/opt/opsware/install_opsware/cdf/
cdf.xml] on <IP_address>
Copying [/var/tmp/cdf_tmp.xml] to [/var/opt/opsware/install_opsware/cdf/
cdf_<timestamp>.xml] on <IP_address>
Remaining threads after stop:
[<_MainThread(MainThread, started)>]

Script done on <timestamp>
```

As the Management Console processes the core components, it updates the file
/var/opt/opsware/install_opsware/sa_password_reset.inv. If a problem occurs, the
Management Console will use this file to determine where to restart when invoked again. Each core
server will have a local copy of this file listing components already processed on that host. The
sa_password_reset.inv file will contain entries similar to the following:

```
# cat /var/opt/opsware/install_opsware/sa_password_reset.inv
File created ........
VAULT
SPIN
CDF
TWIST
USERS
DETUSER
```

Appendix D: SA Hotfix Tool

From SA 10.2 and later, SA provides the Hotfix tool which simplifies installation and uninstallation of SA hotfixes.

The SA Hotfix tool is installed with the SA Core and can be found in the following directory:

`TBD`

The Hotfix tool is a Python script.

Usage

From the command line, invoke the SA Hotfix tool:

`sa_hotfix.py [-l, -i <hotfix archive>, -u <hotfix id>, -f <hotfix id> ] <-v>`

where `<hotfix archive>` is the filename of the SA provided hotfix. `<hotfix id>` is the hotfix's unique ID. Hotfix IDs are in the format qc*nnnnn*.

Arguments

Table shows the valid arguments for sa_hotfix.py.

table 69   SA Hotfix Tool Arguments

Argument	Description
`-h`	Prints the help message.
`-l`	Lists hotfixes registered on the current system.
`d <hotfix ID>`	Prints the details for the hotfix with the specified ID. For example, `qc12345`.
`-i <hotfix_filename>.zip`	Installs the hotfix packaged in file `<hotifix_filename>.zip`
`-u <hotfix ID>`	Uninstalls the hotfix with the specified ID. For example, `qc12345`.
`-f <hotfix ID>`	Forces the uninstall of the hotfix with the specified ID. For example, `qc12345`.
`-v`	Verbose: prints additional script output messages.

Installing a Hotfix

```
sa_hotfix.py -i <filename>.zip
```

Invoking the Hotfix tool as shown performs the following:

1 Backs up all the original files in `/var/opt/opsware/OPSWhotfix/<hotfix_id>/`.

2 Executes the pre-install script

3 Copies the files from the hotfix ZIP to the correct locations

4 Executes the post-install script.

If the hotfix file specifies multiple targets for a file, SA only backs up the first original file since it is assumed that the file is the same in all locations in the core. If a backup of an original file fails, SA will not proceed with the hotfix installation, and you must determine the reason for the failure and attempt the installation again. If a file is already present in the backup location, it will not be backed up again.

If a failure occurs after the backup step, then run the hotfix installer with

```
sa_hotfix.py -f <hotfix id>
```

which attempts to force uninstallation of the hotfix file, then retry the installation.

You should not rerun this Hotfix tool command again on the same core unless:

• The Hotfix tool failed to backup the original files.

• The hotfix does not appear in the list generated by the command `sa_hotfix.py -l`.

Listing Available Hotfixes

```
sa_hotfix.py -l
```

Prints a list of all hotfixes that have been installed on the core. If a hotfix has been uninstalled, the entry is marked as uninstalled.

Uninstalling a Hotfix

```
sa_hotfix.py -u <hotfix id>
```

▶ `<hotfix id>` is case sensitive.

Runs the pre-uninstall script, restores the backed up original files to their original locations and runs the post-install script. When completed, the hotfix is marked as uninstalled.

You should not rerun this Hotfix tool command again on the same core. If the pre-uninstall script fails, contact HP Technical Support.

Forcing a Hotfix Uninstallation

```
sa_hotfix.py -f <hotfix id>
```

▶ `<hotfix id>` is case sensitive.

This command is the same as `-u` with two exceptions.

- The Hotfix tool attempts to remove the hotfix even if it is not listed as INSTALLED.

- The Hotfix tool removes the hotfix even if the `md5sum` of the file currently installed does not match the `md5sum` listed in the hotfix manifest.

Appendix E: Advanced SA Installation Information

> The information in this section is only for the use HP Professional Services, HP-certified consultants. and/or HP Technical Support.

Distributing Core Components

If you plan to perform a custom installation in order to distribute SA Core Components in a layout other than those listed in Chapter 2, "SA Core Configurations Supported For Customer Installation", you must be aware of the following restrictions.

Additional Slice Component Bundles

When installing additional Slice Component bundles, due to SA Core Component boot order requirements, the Slice Component bundles cannot be installed on the Oracle database host unless the Multimaster Infrastructure Components are installed on the Oracle host.

Core Component Distribution Restrictions

Due to SA Core Component start up order requirements (certain components must be up and running before certain other components can be started), the following core component layouts are valid and show component start order (A first, B second, etc.):

table 70   Supported Custom Core Component Layouts

Server	Core Components
A	Custom (customer installed) database
B	Model repository, software repository
C	Infrastructure Component bundle, Slice Component bundle
D	SA Provisioning components
A	Model repository, SA-supplied database, software repository
B	Infrastructure Component bundle, Slice Component bundle
C	SA Provisioning components
A	Custom (customer installed) database

table 70   Supported Custom Core Component Layouts (cont'd)

Server	Core Components
B	Model repository, software repository
C	Infrastructure Component bundle
D	Slice Component bundle
E	SA Provisioning components

Installing a Satellite with SA Provisioning Components on Separate Hosts

If you have a requirement that the SA Provisioning components be installed on a host other than the Satellite host, contact HP Professional Services for assistance.

Extending a Satellite Realm

➤ It is very important that you understand how peer SA Agent Gateways work before attempting to extend a Satellite Realm. Misconfiguration could lead to significant, intermittent connectivity problems. If you require an extended Realm but do not have the required expertise to do so, contact HP Professional Services or a certified HP consultant.

Realms are a sub-component of SA facilities. A single Facility can contain multiple realms, but a realm can reference only one Facility.

Realms are typically used to allow overlapping IP address space within a Facility in order to keep all SA Agents within a logical Facility (permissions boundary) while still providing flexibility for network reachability. For example, you may have two distinctly separate 10.0.1.x subnets that you must manage in SA under the same logical Facility. Facilities are security boundaries, while Realms inherit the boundaries of their parent facility.

Facility/realm relationships are unique to an Agent Gateway instance or peer group. If you have a facility with two realms, each facility/realm combination is managed by a completely separate group of Agent Gateways. Therefore, realms are a purely logical grouping construct for Agent Gateway configurations.

Typically when a core is installed, you assign a facility name. Then SA automatically creates a standard set of core Realms based on the facility name (`<facility_name>-agents`, `<facility_name>-mm`, etc). When you install an SA Satellite, you can choose either to start a new facility for the Satellite or to join an existing facility.

When you configure a Satellite with realm name `<facility_name>-agents`, you are effectively adding that Satellite as a peer to the SA Core's Agent Gateways that control the facility's `<facility_name>-agents` Realm which is the default Realm for agent management.

In some cases, you may need to extend a Realm. This can be done only by running the SA Installer in Expert mode to install the Satellite, which exposes all SA configuration parameters where you can then specify the extended Realm.

Appendix F: HP SA FIPS 140-2 Compliance Statement

HP Server Automation (SA) complies with the Federal Information Processing Standards publication 140-2, a security standard that enables government entities to procure equipment that uses validated cryptographic modules.

This document describes how HP SA complies with FIPS 140-2 and the methods used to make SA FIPS 140-2 compliant. This document contains these sections:

- Overview
- About FIPS 140-2
- FIPS 140-2-Compliant Technologies
- Supported SA Core and Satellite Operating Systems
- Supported Managed Server Operating Systems
- Supported FIPS 140-2 Security Level
- Acronyms
- Related Industry Documentation

Overview

This section describes the SA Core, Satellite and managed servers that comply with FIPS 140-2.

SA Core

An SA Core is a set of Core Components that work together to allow you to discover servers on your network, add those servers to a Managed Server Pool, and then provision, monitor, configure, audit, and maintain those servers from a centralized SA Web Client or SA Client interface. These clients provide a GUI interface to the information and management capabilities of SA.

The servers that the Core Components are installed on are called Core Servers. Core Components, even if distributed to multiple hosts are still considered part of a single SA Core. Core Components can all be installed on a single host or distributed across several hosts, however, the typical SA installation uses Core Component bundling which installs certain components together on the same server for performance and maintainability purposes.

In order to communicate and perform certain server management activities, SA installs Server Agents on each Managed Server and communicates with the Managed Servers through Gateways that are part of the SA Core Components. Server Agents also perform certain actions on Managed Servers as directed by user input from the SA Client or SA Web Client.

SA Agent

An SA Agent is intelligent software that is installed on a server that you want to manage using SA. After an agent is installed on an unmanaged server, it registers with the SA Core which can then add that server to its pool of Managed Servers. The SA Agent also receives commands from the Core and initiates the appropriate action on its local server, such as software installation and removal, software and hardware configuration, server status reporting, auditing, and so on.

During agent registration, SA assigns each server a unique ID (the Machine ID (MID)) and stores this ID in the Model Repository. Servers can also be uniquely identified by their MAC Address (the network interface card's unique hexadecimal hardware identifier, which is used as the device's physical address on the network).

SA Gateway

SA Gateways manage communication between Managed Servers and an SA Core, between multiple cores, and between Satellite installations and an SA Core.

There are several types of gateways:

- **Management Gateway**

  This gateway manages communication between SA Cores and between SA Cores and Satellites.

- **Core Gateway/Agent Gateway**

  These gateways work together to facilitate communication between the SA Core and Agents.

- **Satellite Gateway**

  This gateway communicates with the SA Core through the Management Gateway or the Core Gateway depending on your configuration.

SA Satellite

A Satellite installation can be a solution for remote sites that do not have a large enough number of potentially Managed Servers to justify a full SA Core installation. A Satellite installation allows you to install only the minimum necessary Core Components on the Satellite host which then accesses the Primary Core's database and other services through an SA Gateway connection.

A Satellite installation can also relieve bandwidth problems for remote sites that may be connected to a primary facility through a limited network connection. You can cap a Satellite's use of network bandwidth to a specified bit rate limit. This allows you to insure that Satellite network traffic will not interfere with your other critical systems network bandwidth requirements on the same pipe.

A Satellite installation typically consists of, at minimum, an Satellite Gateway and a Software Repository Cache and still allows you to fully manage servers at a remote facility. The Software Repository Cache contains local copies of software packages to be installed on Managed Servers in the Satellite while the Satellite Gateway handles communication with the Primary Core.

SA Managed Server

An SA Managed Server is a server that has an installed SA Agent and is actively under SA management.

About FIPS 140-2

The Federal Information Processing Standards Publication (FIPS) 140-2, "Security Requirements for Cryptographic Modules," was issued by the National Institute of Standards and Technology (NIST) in May, 2001. The standard specifies the security requirements for cryptographic modules utilized within a security system that protects sensitive, but unclassified information. FIPS 140-2 is one of the standards adopted by the governments of the U.S. and Canada to promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment that complies with the standard and contains validated cryptographic modules.

HP Server Automation (SA) supports FIPS 140-2 by using FIPS-compliant cryptographic modules.

FIPS 140-2-Compliant Technologies

SA achieves FIPS 140-2 compliance by using cryptographic modules that have already gone through the NIST certification process. SA uses the following FIPS 140-2-compliant technologies.

NSS Cryptographic Module

SA employs the FIPS 140-2 certified Network Security Services (NSS) cryptographic module, an open-source, general purpose cryptographic library under the Mozilla Public License.

The NSS cryptographic module contains an API based on the industry standard Public-Key Cryptography Standards (PKCS) #11 cryptographic token interface version 2.20 published by RSA, the security division of EMC Corporation.

TLS/SSL Transport Protocol

SA also makes use of Transport Layer Security (TLS), the next generation of Secure Sockets Layer (SSL).

The SA platform is composed of multiple distributed components that communicate sensitive information over insecure networks. SSL is a proven industry standard that provides:

- Encryption to ensure that data (events/user interaction) cannot be sniffed

- Data integrity (MAC) to prevent intentional or accidental data modification on the wire

- Authentication to prevent credentials from leaking across the wire

Because the function of TLS and SSL is the same, the protocols are referred to jointly as TLS/ SSL, although they use different algorithms to establish secure key exchange.

The SSL 2.0 and 3.0 protocols are not FIPS 140-2 compliant. TLS is the only SSL variant that incorporates FIPS 140-2-approved algorithms based upon Internet Engineering Task Force (IETF) standards.

SHA-128

Secure Hash Algorithm (SHA)-128 is a cryptographic hash algorithm with a 128-bit digest designed by the National Security Agency (NSA) and published by NIST as a U.S. Federal Information Processing Standard. SA uses SHA-128.

Supported SA Core and Satellite Operating Systems

FIPS 140-2 enabled SA Cores are supported on all supported SA managed platforms.

Supported Managed Server Operating Systems

FIPS 140-2 enabled managed servers are supported on all supported SA managed platforms except for the following:

- Red Hat Enterprise Linux 5 on IA 64
- Red Hat Enterprise Linux 5 and 6 on S390X platform (Z Series)
- SUSE Linux Enterprise Server 10 and 11 on S390X platform (Z Series)
- HPUX PA-RISC 11.11, 11.23, 11.31
- HPUS IA64 11.11, 11.23, 11.31
- Windows Server 2008 R2 on IA 64

Supported FIPS 140-2 Security Level

table 71   FIPS 140-2 Security Level

SA Component	Supported FIPS 140-2 Security Level	NSS Version	OpenSSL Version
SA 10.10 and later	Level 1	3.15.1	1.0.1h (2.0.5 FIPS module)

SA Cryptography Modes

SA offers two cryptographic modes:

- FIPS 140-2 mode (sensitive, but unclassified information)
- ESM Standard Cryptography (default mode)

FIPS 140-2 Mode

FIPS 140-2 mode enables security for information that is sensitive, but unclassified (SBU). FIPS 140-2 mode means that the NSS cryptographic module has been deployed and enabled on all the relevant SA components that connect to and exchange data with the SA Core.

FIPS 140-2 mode is based on RSA public-key encryption technology, and is a separate and secure cryptography system apart from ESM's standard cryptography system. Once FIPS 140-2 mode is enabled, ESM's standard cryptography system is not used.

ESM Standard Cryptography

To support deployments for which FIPS 140-2 cryptography is not a requirement, SA continues using its existing cryptographic algorithms and key store formats.

Acronyms

ESM   Enterprise Security Management

FIPS   Federal Information Processing Standards

HMAC   Keyed-Hash Message Authentication Codes

HTTPS Secure Hypertext Transfer Protocol (over TLS/SSL)

ECDSA Elliptical Curve Digital Signature Algorithm. Used for support of Suite B security for information classified up to top secret.

IDS   Intrusion Detection System

IEC   International Electrotechnical Commission

IETF   Internet Engineering Task Force

ISO   International Organization for Standardization

MD5   Message-Digest Algorithm 5

NIST   National Institute of Standards and Technology

NSA   National Security Agency

NSS   Network Security Services

PKCS   Public Key Cryptography Standards

RSA   A public-key encryption technology developed by RSA Security, Inc., the Security Division of EMC Corporation. The acronym stands for Rivest, Shamir, and Adelman, the inventors of the technique.

SBU   Sensitive But Unclassified. Refers to information to be protected by a cryptographic method.

SHA   Secure Hash Algorithm

SSL   Secure Sockets Layer; related to TLS

TSL   Transport Security Layer; the next generation of SSL

W3C   World Wide Web Consortium

Related Industry Documentation

Refer to the following industry resources for more about the FIPS 140-2 standard, and the OpenSSL cryptographic module and its underlying technology.

table 72   Related Industry Documentation

Topic	Resource
FIPS PUB 140-2	Information Processing Standards (FIPS) document published by the Information Technology Laboratory of the National Institute of Standards and Technology (NIST). Issued May 25, 2001. *http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf*
OpenSSL Cryptographic Module	The FIPS 140-2 Non-Proprietary Security Policy Level 1 and 2 Validation for the OpenSSL Cryptographic Module version 0.9.8j, published by OpenSSL.org. *http://www.openssl.org/docs/fips/fipsvalidation.html* *http://www.openssl.org/docs/fips/UserGuide-2.0.pdf*
Approved Cryptographic Modules	A list of all cryptographic modules approved by NIST. *http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140valall.htm*
PKCS #11	A description of the Public Key Cryptographic Standards (PKCS) #11. Describes the cryptographic token interface API, which allows device independence and resource sharing among multiple applications that access multiple devices. *http://www.rsa.com/rsalabs/node.asp?id=2133*
Transport Layer Protocol (TLS)	An overview of Transport Layer Protocol (TLS), the next generation of Secure Sockets Layer, (SSL). *http://en.wikipedia.org/wiki/Transport_Layer_Security* Notes about how and why TLS is implemented: Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations published by NIST in 2005: *http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf*
Internet Engineering Task Force (IETF)	An overview of the IETF, the organization that developed of the TLS protocol, which promotes Internet standards recognized by the World Wide Web Consortium (W3C), International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC): *http://en.wikipedia.org/wiki/IETF* The IETF web site: *http://www.ietf.org/*

Index

W