Quick Reference:
SA Installation Requirements

This reference is provided to familiarize you with many of the basic requirements that should be met before you attempt to install SA. It is intended as a reference and does not replace the *SA Installation Guide*. There may be additional installation/upgrade prerequisites; see the release notes for this SA version.

This document covers the following topics:

- Disk Space Requirements
- Network Requirements
- SA Core Performance Scalability
- Windows Patch Management Files
- Global File System (OGFS) Requirements

For more detailed documentation about any of these topics, see the *SA Installation Guide*.

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 3, 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 10.1 from the directory `/cust/SA/T8900-15063`.

Supported Operating Systems for SA Cores, Agents, and Satellites

For a complete listing of all platforms supported for SA Cores, Agents (managed servers), Satellites, and Clients (SA Client and SA Web Client), see the *SA Support and Compatibility Matrix* document provided in the documentation directory of the 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 (for example, Red Hat Enterprise Linux 5 U1 and Red Hat Enterprise Linux 5 U2) are supported on hosts within the same core. In a multiple core mesh, each distinct core can be running under a different operating system (for example, Core 1 running Red Hat Enterprise Linux 5 and Core 2 running Solaris 10) but all hosts in each distinct core must be running the same operating system.

You must verify that your SA Core, managed server, and satellite host servers meet the requirements listed in *SA Installation Guide*. 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 one or more Secondary Core that manage 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 the *SA Installation Guide*.

If you are installing the First (Primary) Core of a Multimaster Mesh, you must complete the tasks described in the section titled 8. SA First (Primary) Core with a Secondary Core (Multimaster Mesh) of the *SA Installation Guide* to add 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 components required to be the primary core of a Multimaster Mesh. You 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 the section titled Deciding on an SA Core Configuration for your Facility in the *SA Installation Guide*.
- 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 ISOs, Primary, Oracle_sas and Upload

- invoke the SA Installer only from a mounted copy of the ISO

For more information, see Chapter 4, "Pre-installation System Requirement Checks" in the *SA Installation Guide*.

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 *self-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 in the *SA Installation Guide*.

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 Definition 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" in the *SA Installation Guide*.

➤ If the SA Installer encounters a correctable error, the installation stops. Correct the error and retry the installation. For information about restarting an interrupted installation, see the section titled Restarting an Interrupted Installation in the *SA Installation Guide*.

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 preconfigure 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 the section titled SA-Supplied Oracle RDBMS Software and Database Setup in the *SA Installation Guide*.
- 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 the section titled Non-SA-Supplied Oracle Software and Database Setup in the *SA Installation Guide*. 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 the section titled Non-SA-Supplied Oracle Software and Database Setup in the *SA Installation Guide*.

  You may need to contact your local Oracle DBA for assistance in integrating SA with your preexisting 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.

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.

If you want to use cryptographic material from a previous SA installation, you can do so by copying the material to `/var/opt/opsware/crypto/cadb/realm/opsware-crypto.db.e` 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.

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" in the *SA Installation Guide*.

Invoking the SA Installer

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

- `uninstall_opsware.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.
  For more information about uninstalling an SA Core, see "SA Core Uninstallation" in the *SA Installation Guide*.
- `uninstall_opsware.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 all servers specified during installation are to be encrypted and accessed by a master password that you specify. See Master Passwords on page 9.
`--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 14.

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, such as 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

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 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 CDF on page 11. 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 reenter 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.

➤ Ensure that the CDF you specify is valid and not empty.

If you specify a CDF that is empty or that contains invalid entries, either you will be required to enter all required parameter values during the installation or installation may fail.

Master Passwords

As of SA 9.0, you can specify a master password to be used to access the encrypted root passwords of all core hosts specified during the installation of a new SA Core.

To encrypt server root passwords specified during installation, invoke the installation with the `--pwsave` argument. When you begin an installation with the `--pwsave` argument specified, the installer encrypts root passwords and saves them in the final CDF on completion of the installation whether a successful or failed install. See Invoking the SA Installer on page 6.

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 that is saved on each host as `root_user_password`.

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

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

master.password []:


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


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

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

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

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


master.password []:
```

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

The SA Password Utility

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

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

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

Invoke the password utility as follows:

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

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

`/<mountpoint>/primary/disk001/opsware_installer/hpsa_install.sh –verbose`

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

Concluding the Interview

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

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

Reusing a 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

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

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

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

   Use the latest CDF as determined by the time stamp. See How and When CDFs are Saved on page 10.

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 root password for each host specified as path 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`

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 Chapter 4, "Pre-installation System Requirement Checks" in the *SA Installation 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" in the *SA Installation Guide* for more information

3 **Prerequisite Information for the HPSA 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 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 the "SA Core Parameter Reference" appendix in the *SA Installation Guide*.

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**: see "1. SA Core with a Local HP-supplied Database" in the *SA Installation Guide*

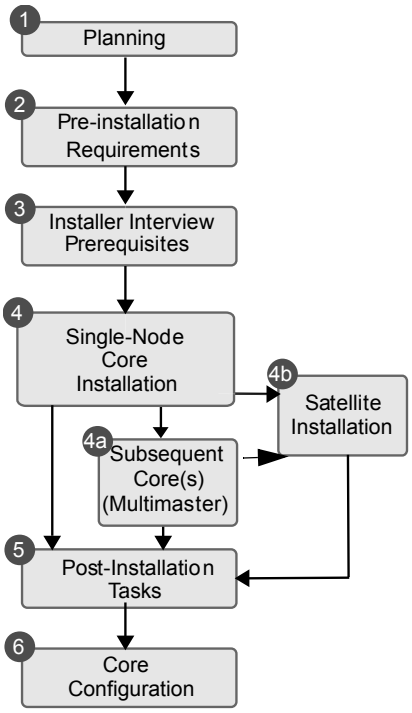
   — **Secondary Core Installations for a Multimaster Mesh:** "8. SA First (Primary) Core with a Secondary Core (Multimaster Mesh)" in the *SA Installation Guide*

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

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 shows the overall process of an SA core installation.

SA Core Installation Process Flow



The SA Installer Prerequisite Check Phase

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
- **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 (Red Hat Linux 5 AS and 6 AS only)
- Verification that no critical file paths contain symbolic links
- 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 Appendix A: *Oracle Setup for the Model Repository* in the *SA Planning and Installation Guide*. 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/5AS-X86_64 using
/tmp/OPSWprereqs-40.0.0.0.54/Linux_oracle_rqmts.conf
    Checking 'required' packages for Linux/5AS-X86_64
    Checking 'required' patches for LINUX/5AS-X86_64
    Checking 'recommended' packages for LINUX/5AS-X86_64
    Checking 'absent' packages for LINUX/5AS-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 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:

`/<mountpoint>/primary/disk001/opsware_installer/OPSWprereqs-<version>.zip`

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 2 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 CDF
`--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.

table 2 Prerequisite Check Script Arguments (cont'd)

Argument	Description
`--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.
        FAILURE 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 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.

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"
```

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

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 3 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

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

table 4 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 4 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 5 lists provides the minimum number of CPUs and required memory to run SA Satellites on VMs:

table 5 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 23, 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.

Agent Installation on Windows Server 2000, 2003, 2008 and 2008 R2 x64

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

Veritas File System (VxFS)

SA supports the Veritas File System (VxFS) for Linux AS4 x86_64, Linux Server 5 x86_64 and Solaris 10. 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.

You must not install the following packages on a Red Hat Enterprise Linux AS 5 x64 core host:

- apache
- dhcp (cores that have the OS Provisioning components installed only)
- httpd

Requirements for Installing Oracle 11g using the SA Installer

The Model Repository requires an installed Oracle database. You can use the SA Installer to install the HP-supplied Oracle 11g database on a Solaris 10 x86_64 server or on a Red Hat Enterprise Linux 4 AS x86_64, Red Hat Enterprise Linux 5 AS x86_64, or SUSE Linux Enterprise Server 10 x86_64 server. You can also use a pre-existing Oracle installation. Whatever method you choose, see “Oracle Setup for the Model Repository” in the *SA Installation Guide* for more information.

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 30. 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
```

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 6 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 6 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	**OS 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	15 GB	The base directory for all SA Core services. (Fixed disk usage)
/u01/oradata /u02/oradata /u*nn*/oradata ...	20 GB	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)

table 6 SA Disk Space Requirements (cont'd)

SA Component Directory	Recommended Free Disk Space	Requirement Origin
/var/log/opsware/word	80 GB	The total log space used by all SA Core Components. (Fixed disk usage)
/var/opt/opsware/word	80 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	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.
/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 6 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.
- 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 7. If you need to determine a more precise tablespace sizing, contact your technical support representative.

table 7 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

table 7 Tablespace Sizes (cont'd)

Tablespace	MB/1000 Servers	Minimum Size
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 OS Provisioning requirements. This component requires sufficient disk space for the OS media for all the operating system versions you intend to provision.

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" in the *SA Installation Guide*.
- When using network storage for Core Components, such as the Software Repository or OS Provisioning Media Server, you must ensure that the `root` user 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 SA Web Client; for example, restrictive Linux `iptables` rules. Ensure these operating system/network settings allow required SA 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 8 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 8 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

table 8 Open Ports on a Firewall Protecting an SA Core (cont'd)

Source	Destination	Open Port(s)	Notes
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`).
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 9 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 9 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 9 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 10 shows the Managed Server port that must be open for SA Core Server connections.

table 10 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 11 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.

OS Provisioning: DHCP Proxying

If you plan to install your OS 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 OS 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" the *SA Installation Guide*.

SA Core 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 12 and Table 13 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
- 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 12 and Table 13, 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 12 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 13 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
- 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.

Windows Patch Management Files

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

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

Installing the Required Windows Patch Management Files in an Existing Core

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

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

Global File System (OGFS) Requirements

This section discusses requirements for the Global File System (OGFS).

OGFS Store and Audit Hosts

When you run the SA Installer interview in advanced mode, you can specify values for the `ogfs.store.host.ip` and `ogfs.audit.host.ip` parameters. (See the "SA Installation Parameter Reference" in the *SA Installation Guide*.) 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.

a. On a Solaris host, modify the `/etc/dfs/dfstab` file, similar to this:

```
# Begin Opsware ogfs export
share -F nfs -o anon=0,rw=1.2.3.4:1.2.3.5 /export/ogfs/store
share -F nfs -o anon=0,rw=1.2.3.4:1.2.3.5 /export/ogfs/audit
# 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.

b. 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) file systems 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.