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.

This document discusses the following topics:

- Copying the DVDs to a Local Disk
- Dual Layer DVD Requirements
- Supported Operating Systems for SA Cores, Agents, and Satellites
- SA Cores on VMs
- Agent Installation on Windows Server 2000, Windows Server 2003, and Windows Server 2008
- Veritas File System (VxFS)
- The SA Prerequisite Check
- Required Solaris and Linux Packages for SA Core Servers
- Requirements for Installing Oracle 11g using the SA Installer
- Disk Space Requirements
- SA Core Performance Scalability
- Network Requirements
- Windows Patch Management Requirements
- Configuration Tracking Requirements
- Global File System (OGFS) Requirements
- Time and Locale RequirementsUser and Group Requirements For Solaris and Linux

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

Copying the DVDs to a Local Disk

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

Dual Layer DVD Requirements

All SA installation DVDs require a DVD drive that supports dual layer.

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 SAS Web Client), see *SA Supported Platforms* provided in the documentation directory of the distribution media or available for download at

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

SA Cores on VMs

SA Cores are certified for VMware VMs running Red Hat Linux 4AS (update 6 or later) and Red Hat 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 Supported Platforms* provided in the documentation directory of the distribution media or available for download from:

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

The Model Repository must be installed on a physical server while the rest of the Core Components can be installed on the VM. For a list of supported Oracle versions for the Model Repository, see “Oracle Setup for the Model Repository” in the *SA Simple/Advanced Installation Guide*.

VM CPU and Memory Requirements

Table 1 shows the minimum number of CPUs and required memory to run SA Cores on VMs:

Table 1 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	
1	Infrastructure Component bundle OS Provisioning bundle Slice Component bundle		960
2	Infrastructure Component bundle OS 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 2 lists provides the minimum number of CPUs and required memory to run SA Satellites on VMs:

Table 2 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, 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.

The Model Repository must be installed on a physical server while the rest of the Core Components can be installed on the VM.

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

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 and Linux Server 5 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.

The SA Prerequisite Check

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** - diskspace, 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

- **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
- **Diskspace Requirements** - checks that minimum diskspace 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) and locale (`en_US.UTF-8` or equivalent)
  - Run level (Linux only)
  - NFS versions
  - No VxFS (Linux 3AS and 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 3AS, 4AS, and 5Server only)
  - Verification that no critical file paths contain symbolic links
  - Red Hat update 5 or later (Linux 4AS 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.

The prerequisite check validates both required and recommended items. Required items, such as required packages and Oracle settings, must be corrected if the validation fails.

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" in the *SA Simple/Advanced 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/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.

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 response file 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`

Unzipping this file will create a sub-directory, `OPSWprereqs-<version>` which contains the script `preinstall_requisites.sh`.

Usage

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

where:

Table 3 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 response file
`--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.
`--resp_file`	Specifies the path to a valid Installer response file for the current installation. When specified, certain values that might be specified during the install process are taken from the response file, such as Oracle installation values.
`--verbose | --silent`	`verbose` displays 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.

Required Solaris and Linux Packages for SA Core Servers

This section describes platform-specific packages and utilities that must be installed for the operating system on the server that will host an SA Core.

Required Solaris Packages

If you will be installing an SA Core Server under Solaris, you must ensure that the packages listed in Table 4are installed. Table 4 lists recommended packages and Table 5 lists packages that must *not* be installed.

Table 4 Packages Required for Solaris

Required Packages for Solaris		
SUNW5xmft	SUNWeudlg	SUNWjxmft
SUNWadmap	SUNWeudmg	SUNWkxmft
SUNWadmc	SUNWeuezt	SUNWlibC
SUNWadmfw	SUNWeuhed	SUNWman
SUNWarrf	SUNWeuluf	SUNWntpr
SUNWbash	SUNWeuodf	SUNWntpu
SUNWcxmft	SUNWeurf	SUNWsacom
SUNWdoc	SUNWeuxwe	SUNWscpu
SUNWesu	SUNWi13rf	SUNWswmt
SUNWeu8df	SUNWi15rf	SUNWtcsh
SUNWeu8os	SUNWi2rf	SUNWtoo
SUNWeudba	SUNWi4rf	SUNWtxfnt
SUNWeudbd	SUNWi5rf	SUNWucbt
SUNWeudda	SUNWi7rf	SUNWuiu8
SUNWeudhr	SUNWi8rf	SUNWuium
SUNWeudhs	SUNWi9rf	SUNWulcf
SUNWeudis	SUNWinst	SUNWuxlcf
SUNWeudiv	SUNWinttf	

Table 5 Packages That Must Be Removed from Solaris

Packages That Must Me Removed From Solaris
SUNWCpm

Other Solaris Requirements

The SA Core Server must also meet the following requirements:

- On the server where you will install the SAS Web Client component, you must install the J2SE Cluster Patches for Solaris. To download these patches, search for “J2SE Cluster Patches” for your version of Solaris at *http://www.sun.com/*.
- On all core servers, verify that the Network File System (NFS) is configured and running.

- For Daylight Saving Time (DST) on Solaris 10 servers, you must install the time zone patch 122032-03 or later, and `libc` patch 119689-07 or later. To download these patches, search for the patch ID at *http://www.sun.com/*.

  For more information about DST changes, search for “Daylight Saving Time (DST)” at *http://www.sun.com/*.

Required Linux Packages

For Red Hat Linux AS 3 32-bit x_86, an SA Core Server must have the packages listed in Table 6 installed. For Red Hat Linux AS 4 32-bit x86 an SA Core Server must have the packages listed in Table 7 installed. For Red Hat Linux Server 5 x_86 an SA Core Server must have the packages listed in Table 8 installed. For both and Red Hat Linux AS4 32-bit x86 and Red Hat Linux AS4 64-bit x86, the packages listed in Table 9 must *not* be installed.

Due to a known Linux AS4 64-bit x86 kernel bug, you must have Update 5 or later installed on all servers that will host an SA Core

Table 6 Required Packages For Linux As3 32-bit x_86

Required Packages	Architecture
at	32-bit x86
compat-db	32-bit x86
compat-libstdc++	32-bit x86
coreutils	32-bit x86
cpp	32-bit x86
expat	32-bit x86
gcc	32-bit x86
glibc-devel	32-bit x86
glibc-headers	32-bit x86
glibc-kernheaders	32-bit x86
iptables	32-bit x86
kernel-source	32-bit x86
libaio	32-bit x86
libcap	32-bit x86
libstdc++	32-bit x86
libxml2-python	32-bit x86
mkisofs *	32-bit x86
ncompress (contains uncompress utility)	32-bit x86
nfs-utils	32-bit x86

Table 6 Required Packages For Linux As3 32-bit x_86

Required Packages	Architecture
ntp	32-bit x86
patch	32-bit x86
patchutils	32-bit x86
sharutils	32-bit x86
strace	32-bit x86
unzip	32-bit x86
XFree86-libs	32-bit x86
XFree86-libs-data	32-bit x86
XFree86-Mesa-libGL	32-bit x86
xinetd	32-bit x86
zip	32-bit x86
* mkisofs is used for premastering ISO 9660 file systems used on CDROMs. It is open source and available at *http://freshmeat.net*, search for “mkisofs”.	

.

Table 7 Packages Required for Linux AS 4 x_64

Required Packages	Architecture
binutils	x86_64
chkfontpath	x86_64
compat-db	i386
compat-db	x86_64
cpp	x86_64
desktop-file-utils	x86_64
expat	i386
expat	x86_64
gamin-devel	x86_64
gcc	x86_64
gcc-c++	x86_64
glibc	i686
glibc	x86_64
glibc-common	x86_64
glibc-devel	i386

Table 7 Packages Required for Linux AS 4 x_64 (cont'd)

Required Packages	Architecture
glibc-devel	x86_64
glibc-headers	x86_64
glibc-kernheaders	x86_64
iptables	x86_64
kernel-smp	x86_64
kernel-smp-devel	x86_64
libaio	i386
libaio	x86_64
libcap	i386
libcap	x86_64
libgcc	i386
libgcc	x86_64
libpng	i386
libpng	x86_64
libpng10	i386
libpng10	x86_64
libstdc++	i386
libstdc++	x86_64
libtermcap	i386
libtermcap	x86_64
libxml2	i386
libxml2	x86_64
libxml2-python	x86_64
make	x86_64
mkisofs	x86_64
ncompress	x86_64
nfs-utils	x86_64
ntp	x86_64
patch	x86_64
patchutils	x86_64
pdksh	x86_64

Table 7 Packages Required for Linux AS 4 x_64 (cont'd)

Required Packages	Architecture
popt	i386
popt	x86_64
readline	i386
readline	x86_64
rpm-build	x86_64
sharutils	x86_64
strace	x86_64
sysstat	x86_64
tcp_wrappers	i386
tcp_wrappers	x86_64
ttmkfdir	x86_64
unzip	x86_64
xinetd	x86_64
xinitrc	noarch
xorg-x11	x86_64
xorg-x11-Mesa-libGL	i386
xorg-x11-Mesa-libGL	x86_64
xorg-x11-Mesa-libGLU	i386
xorg-x11-Mesa-libGLU	x86_64
xorg-x11-Xvfb	x86_64
xorg-x11-deprecated-libs	i386
xorg-x11-deprecated-libs	x86_64
xorg-x11-font-utils	x86_64
xorg-x11-libs	i386
xorg-x11-libs	x86_64
xorg-x11-xauth	x86_64
xorg-x11-xfs	x86_64
xterm	x86_64
zip	x86_64
zlib	i386
zlib	x86_64

.

Table 8 Packages Required for Linux AS 5 x_64

Required Packages	Architecture
binutils	x86_64
chkfontpath	x86_64
compat-db	i386
compat-db	x86_64
cpp	x86_64
desktop-file-utils	x86_64
elfutils-libelf	x86_64
elfutils-libelf-devel	x86_64
expat	i386
expat	x86_64
gamin-devel	x86_64
gcc	x86_64
gcc-c++	x86_64
glibc	i686
glibc	x86_64
glibc-common	x86_64
glibc-devel	i386
glibc-devel	x86_64
glibc-headers	x86_64
iptables	x86_64
kernel	x86_64
kernel-devel	x86_64
kernel-headers	x86_64
libaio	i386
libaio	x86_64
libaio-devel	x86_64
libcap	i386
libcap	x86_64
libgcc	i386
libgcc	x86_64

Table 8 Packages Required for Linux AS 5 x_64 (cont'd)

Required Packages	Architecture
libpng	i386
libpng	x86_64
libstdc++	i386
libstdc++	x86_64
libstdc++-devel	x86_64
libtermcap	i386
libtermcap	x86_64
libxml2	i386
libxml2	x86_64
libxml2-python	x86_64
make	x86_64
mesa-libGL	i386
mesa-libGL	x86_64
mesa-libGLU	i386
mesa-libGLU	x86_64
mkisofs	x86_64
ncompress	x86_64
nfs-utils	x86_64
ntp	x86_64
openmotif	i386
openmotif	x86_64
patch	x86_64
patchutils	x86_64
popt	i386
popt	x86_64
readline	i386
readline	x86_64
rpm-build	x86_64
sharutils	x86_64
strace	x86_64
sysstat	x86_64

Table 8 Packages Required for Linux AS 5 x_64 (cont'd)

Required Packages	Architecture
tcp_wrappers	i386
tcp_wrappers	x86_64
ttmkfdir	x86_64
unzip	x86_64
xinetd	x86_64
xorg-x11-font-utils	x86_64
xorg-x11-server-Xvfb	x86_64
xorg-x11-xauth	x86_64
xorg-x11-xinit	x86_64
xorg-x11-xfs	x86_64
xterm	x86_64
zip	x86_64
zlib	i386
zlib	x86_64

Table 9 Packages That Must Be Removed for Red Hat Linux

Packages		
samba	rsync	tftp (AS 4 only)**
apache	httpd	tftp-server (AS 5 only) dhcp**

** Existing versions of the `tftp` and `dhcp` packages cannot reside on the same server as the OS Provisioning Boot Server component; however, they can reside on SA Core Servers that do not have the OS Provisioning Boot Server component.

To verify that the `samba` package, for example, is installed, enter the following command:

```
# rpm -qa | grep samba
```

You can obtain the latest versions of these packages from the Red Hat errata web site.

To remove packages, enter the following command:

```
# rpm -e package_name
```

Some packages in this list may be depended on by other packages that are installed on your system. For example, the default Red Hat installation includes `mod_python` and `mod_perl` that depend on `httpd` being installed. In order to remove packages that fulfill dependencies, you must simultaneously remove the packages that create the dependencies. In this example, you would need to enter the following command:

```
# rpm -e httpd mod_python mod_perl
```

If `rpm` identifies an additional dependency, it will note which packages have dependencies on the components to be removed and fail. These packages must be added to the uninstall command line. If the chain of dependencies cannot be suitably resolved, enter the `rpm -e --nodeps` command to remove the desired packages without considering dependencies.

Additional Linux Requirements

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

- Red Hat Enterprise Linux 4 AS must be at least Update 5.
- 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 `root` 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.

  b. 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.

- Disable the Security-Enhanced Linux kernel (SELinux) on all core servers running Linux AS4 64-bit x86.
- For Daylight Saving Time (DST) on Red Hat Enterprise Linux AS 3 and AS 4, you must install the latest time zone data. You can download these time zone updates from the following location:

  https://rhn.redhat.com/errata/RHEA-2006-0745.html

- For Daylight Saving Time (DST) on SUSE Linux Enterprise Server 9, you must install the latest time zone data. You can download these updates from the following location:

  http://www.novell.com/support/

- For Daylight Saving Time (DST) on Sun Solaris, you must install the latest time zone data. You can download these updates from *http://www.sun.com*.
- If you are using a Linux NFS server, be aware that, by default, Linux enables NFSv3, which prevents Solaris servers from entering the server pool. You can either disable NFSv3 on the Linux NFS server or you can add DHCP options to force Solaris 10 to use NFSv2:

  — To force the Solaris `miniroot` to use NFSv2, add the following lines to your DHCP configuration file:

    – In the generic section of the DHCP configuration file, add the following lines:

```
# added for nfs 2 miniroot
option SUNW.SrootOpt code 1 = text;
# end of nfs 2 miniroot stuff
```

– In the `solaris-sun4u`, `solaris-sun4us`, and solaris-specific-kernel classes, add the following lines:

```
# added for nfs 2 miniroot
option SUNW.SrootOpt "vers=2";
# end of nfs 2 miniroot stuff
```

— To disable NFSv3 on the Linux NFS server add the following lines to the `/etc/sysconfig/nfs` file and then restart NFS:

```
MOUNTD_NFS_V3=no
MOUNTD_NFS_V2=yes
RPCNFSDARGS='--no-nfs-version 4'
```

Required SUSE Linux Enterprise Server 10 Packages

For SUSE Linux Enterprise Server 10 64-bit x_86, an SA Core Server must have the packages listed in Table 10 installed.

Table 10 SUSE Linux Enterprise Server 10 Required Packages

Required Packages	Architecture
binutils	x86_64
cpp	x86_64
desktop-file-utils	x86_64
expat	x86_64
gcc-c++	x86_64
gcc	x86_64
glibc	x86_64
glibc-32bit	x86_64
glibc-devel	x86_64
glibc-devel-32bit	x86_64
iptables	x86_64
kernel-smp	x86_64
kernel-source	x86_64
libaio	x86_64
libaio-32bit	x86_64
libaio-devel	x86_64
libcap	x86_64
libcap-32bit	x86_64

Table 10 SUSE Linux Enterprise Server 10 Required Packages

Required Packages	Architecture
libelf	x86_64
libgcc	x86_64
libstdc++	x86_64
libstdc++-devel	x86_64
libpng	x86_64
libpng-32bit	x86_64
libxml2	x86_64
libxml2-32bit	x86_64
libxml2-python	x86_64
make	x86_64
mDNSResponder-lib	x86_64
mkisofs	x86_64
ncompress	x86_64
nfs-utils	x86_64
patch	x86_64
popt	x86_64
popt-32bit	x86_64
readline	x86_64
readline-32bit	x86_64
rpm	x86_64
sharutils	x86_64
strace	x86_64
sysstat	x86_64
termcap	x86_64
unzip	x86_64
vim	x86_64
xinetd	x86_64
xntp	x86_64
xorg-x11-libs	x86_64
xorg-x11-libs-32bit	x86_64
xorg-x11	x86_64

Table 10 SUSE Linux Enterprise Server 10 Required Packages

Required Packages	Architecture
xterm	x86_64
zip	x86_64
zlib	x86_64
zlib-32bit	x86_64

Table 11 shows packages *must not* be installed on a SUSE Linux Enterprise Server 10 hosting an SA Core:

Table 11 Packages Not Supported on SUSE Linux Enterprise Server 10 Core Hosts

Package	Package
rsync	yast2-dhcp-server
samba	yast2-samba-server
samba-32bit	yast2-tftp-server

These packages are reinstalled during an operating system upgrade from SUSE Enterprise Linux SP2 to SP3 and therefore must be removed for proper SA Core operation after upgrade.

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, you should see “Oracle Setup for the Model Repository” in the *SA Simple/Advanced Installation Guide* for more information.

Disk Space Requirements

An SA *Core Server* is a computer hosting one or more *SA Core Components*. You have the option to install all of the SA Core Components on a single server or distribute them across multiple servers. This section describes the hardware requirements for any SA Core Server.

Core Server Disk Space Requirements

On each Core Server, the root directory must have at least 72 GB available hard disk space. SA components are installed in the `/opt/opsware` directory. Table 12 lists the recommended disk space requirements for installing and running SA Core Components. These sizes are recommended for the primary production data. Additional storage for backups must be calculated separately.

Table 12 SA Disk Space Requirements

SA Component Directory	Recommended 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 AS3 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)
/var/log/opsware	10 GB	The total log space used by all SA Core Components. (Fixed disk usage)
/var/opt/opsware	10 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 12 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 13. If you need to determine a more precise tablespace sizing, contact your technical support representative.

Table 13 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 OS Provisioning requirements. This component requires sufficient disk space for the OS media for all the operating system versions you intend to provision.

SA Core Performance Scalability

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 14 and Table 15 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

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 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 14 and Table 15, 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 14 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, 8 GB RAM, 1 GB/s network		

Table 15 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, 8 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 requirements:

- 2 CPUs per 1,500 managed servers per Satellite Core
- 2 GB RAM per 1,500 managed servers per Satellite Core

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
- Global File System

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.

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 both First Cores, Multimaster Mesh installations, and Satellite cores.

Network Requirements within a Facility

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

- All SA Core Servers must be on the same Local Area Network (LAN or VLAN).
- 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.
- If you plan to use 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.

Open Ports

You must configure any firewalls protecting your Core Servers to allow the ports shown in Table 16 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 16 Open Ports on a Firewall Protecting an SA Core

Port	Component	Purpose
80 (TCP)	Command Center	HTTP redirector

Table 16 Open Ports on a Firewall Protecting an SA Core (cont'd)

Port	Component	Purpose
443 (TCP)	Command Center	HTTPS Proxy for SAS Web Client UI, SAS Client, SA Web Services (2.2)
1003 (TCP)	Software Repository (`word`)	Core Communications
1004 (TCP)	Data Access Engine (`spin`)	Core Communications
1018 (TCP)	Command Engine (`way`)	Core Communications
1032 (TCP)	Web Services Data Access Engine (`twist`)	Core Communications
1521 (TCP)*	Model Repository (`truth`)	Database Communications *This port is user configurable.*
2001 (TCP)	Management Gateway/Core Gateways	Inbound tunnels from other Gateways (If Port 2001 is in use, rolls over to 2003) *This port is user configurable*
2222 (TCP)	Global File System	Global shell session from an SSH client
8017 (UDP, TCP)	Agent Gateway	Interface to the Build Manager
8080 (TCP)	Command Center	Load Balancing Gateway for the SA Client

* 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.

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 17 shows the ports used by the OS Provisioning components that are accessed by servers during the provisioning process. (In SA, OS provisioning refers to the installation of an operating system on a server.)

Table 17 Open Ports for the OS Provisioning Components

Port	Component	Service
67 (UDP)	Boot Server	DHCP
69 (UDP)	Boot Server	TFTP

Table 17 Open Ports for the OS Provisioning Components (cont'd)

Port	Component	Service
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 OS 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 OS Provisioning Boot Server and Media Server components onto their own DMZ network. When you segregate these components, the ports listed in Table 17 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 18 shows the Managed Server port that must be open for SA Core Server connections.

Table 18 Open Ports on Managed Servers

Port	Component
1002 (TCP)	SA 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 7.0), 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 the *SA Simple/Advanced Installation Guide*.

Windows Patch Management Requirements

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

Supported Platforms

- Windows 2000
- Windows XP
- Windows Server 2003 x86 and x64
- Windows Server 2008 x86 and 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. This update is required for MBSA 2.1 to run properly.

Requirements

The Managed Servers meet the following Windows patching requirements:

- Windows Installer 3.1 must be installed
- MSXML 3+ must be installed
- 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.

Installing MBSA 2.1 for SA 9.0

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

1 Obtain the following files from Microsoft:

- qchain.exe

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

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

- WindowsUpdateAgent-x86.exe

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

- WindowsUpdateAgent-x64.exe

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

- WindowsUpdateAgent-ia64.exe

  The `WindowsUpdateAgent30-ia64.exe` file is required by the `mbsacli.exe` utility.

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

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

   ```
   /opsw/win_util
   ```

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

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

4. Write down the name of the directory containing the 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's Guide: Application Automation*.

Configuration Tracking Requirements

The Configuration Tracking feature tracks, backs up, and recovers critical software and system configuration information across Unix and Windows servers. When you enable the SA Configuration Tracking feature for a facility, by default, a separate partition is created on the server running the Software Repository. That partition will contain this Configuration Tracking backup directory:

```
/var/opt/opsware/word/<facility-name>/acsbar
```

You can optionally specify that the backup directory be created under the Software Repository root directory during SA installation.

The Configuration Tracking feature uses this directory to store backups of tracked configuration files and databases. The configuration tracking backup directory is relative to the Software Repository root directory:

```
<word_root>/<facility_name>/acsbar
```

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 interviewer 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 Simple/Advanced 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) filesystems are mounted after the network is available. Slice Component bundle installation will fail otherwise. The services can be diasabled 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.

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
   ```

Solaris Time Configuration

To configure the time zone on a Solaris server, verify that the `/etc/TIMEZONE` file contains the following line:

```
TZ=UTC
```

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.

To enable non-English locales for Windows patching, follow the instructions in “Locales for Windows Patching” in the *SA User’s Guide: Application Automation*.

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"
```

User and Group Requirements For Solaris and Linux

During installation on Solaris and Linux servers, the SA Installer creates two users (if you are installing OMDB, its installer will also add a user).

For Solaris, these users and groups are:

Table 19 Users and Groups Created During an SA/Solaris Install

userid	group	groupid	home directory	shell
twist	twist	other	/var/opt/opsware/twist	/bin/sh twist
occ	occ	occ	/var/opt/opsware/occ	/bin/sh occ
opswgw	opswgw	na	/var/opt/opsware/ opswgw-<gw name>	na

For Linux, these users and groups are:

Table 20 Users and Groups Created During an SA/Linux Install

userid	group	uid	groupid	home directory	shell
twist	twist		users	/var/opt/opsware/twist	/bin/sh twist
occ	occ		occ	/var/opt/opsware/occ	/bin/sh occ