Quick Reference: Pre-Installation Requirements for SA

This reference document is intended to quickly familiarize you with the basic requirements for installing SA, including the supported operating systems and their required packages, supported versions of Oracle, network requirements, and time and locale requirements.

This document discusses the following topics:

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

Hardware Requirements for SA Core Servers

An SA core server is a computer running one or more SA core components. You can install all of the SA core components on a single server or you can distribute the components across multiple servers. This section describes the hardware requirements for SA core servers.

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 1 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 1 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)

Table 1 SA Disk Space Requirements (cont'd)

sa component directory	recommended disk space	Requirement origin
/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/mnt	20 GB	The home directory for the Global File System (OGFS) enabled SA user accounts.

* The entries in Table 1 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 2. If you need to determine a more precise tablespace sizing, contact your technical support representative.

Table 2 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 3 and Table 4 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 3 and Table 4, 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 3 Example Component Distribution: Two Large Servers and Additional Smaller Servers

Number of Managed Servers	**Number of Users**	**Number of Core Servers**	**SA Core Component Distribution by Server**				
			8 CPU Cores 8GB RAM	8 CPU Cores 8GB RAM	4 CPU Cores 8GB RAM	4 CPU Cores 8GB RAM	4 CPU Cores 8GB RAM
960	40	1	MR INFRA Slice 0 OS Prov				
2250	90	2	MR	INFRA Slice 0 OS Prov			
4500	180	3	MR	INFRA Slice 0 OS Prov	Slice 1		
7200	280	4	MR	INFRA Slice 0 OS Prov	Slice 1	Slice 2	
8000	300	5	MR	INFRA Slice 0 OS Prov	Slice 1	Slice 2	Slice 3

If your Oracle database deployment must run on four CPU cores due to licensing restriction, use Table 4.

Table 4 Example Core Component Distribution when Limited to Four CPU Cores

Number of Managed Servers	Number of Users	Number of Core Servers	SA Core Component Distribution by Server				
			4 CPU Cores 8GB RAM	4 CPU Cores 8GB RAM	4 CPU Cores 8GB RAM	4 CPU Cores 8GB RAM	4 CPU Cores 8GB RAM
480	20	1	MR INFRA Slice 0 OS Prov				
1125	45	2	MR	INFRA Slice 0 OS Prov			
2250	90	3	MR	INFRA Slice 0 OS Prov	Slice 1		
3600	144	4	MR	INFRA Slice 0 OS Prov	Slice 1	Slice 2	
4000	160	5	MR	INFRA Slice 0 OS Prov	Slice 1	Slice 2	Slice 3

Small Core Server Capacity

For small test/demonstration environments, the following single server core implementations are feasible. These configurations *are not* appropriate for production environments.

- 1 core server with 4 CPU cores, 8 GB RAM: 480 managed servers
- 1 core server with 2 CPU cores, 8 GB RAM: 150 managed servers

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.

Supported Operating Systems: SA Core Server

Table 5 lists the supported operating systems for SA Client Core and Satellite Components.

For a list of supported Oracle versions for the Model Repository, see Appendix A in the *SA Planning and Installation Guide***.**

SA Core Supported Operating Systems

Platforms with a (*) are deprecated in this release. For more information on platform deperecation in SA in this releasse, see Operating System Deprecation and End of Support on page 25.

Table 5 SA Core Supported Operating Systems

Supported os for SA core	Versions	Architecture	SA Components
Sun Solaris			
Sun Solaris	Solaris 10 (Updates 1, 2, 3, 4, 5 and 6)	Sun SPARC 4u, 4v(*) **Note**: The SA Core is also supported on Sun Dynamic System Domains.	All components
Red Hat Linux			
	Red Hat Enterprise Linux 3* AS	x86_32	All components
	Red Hat Enterprise Linux 4 AS	x86_64	All components
	Red Hat Enterprise Linux 5.2, 5.3	x86_64	All components
SUSE Linux			
	SUSE Linux Enterprise Server 10 SP2	x86_64	All components

A guest OS (virtual machine) of a VMWare ESX server *is not supported* as an SA Core server. SA Core servers may not be installed in Solaris Local Zones and Solaris Local Zones may not be installed on a server where an SA Core is installed.

SA Satellite Supported Operating Systems

Table 6 lists the supported operating systems for these SA Satellite Components:

- Satellite Gateway
- Software Repository Cache
- OS Provisioning Boot Server (*optional*)
- OS Provisioning Media Server (*optional*)

Platforms with a (*) are deprecated in this release.

Table 6 SA Satellite Supported Operating Systems

Supported operating systems for SA satellite	Versions	Architecture
Sun Solaris		
	Solaris 10 (Updates 1, 2, 3, 4, 5 and 6)	Sun SPARC 4u, 4v*
Red Hat Linux		
	Red Hat Enterprise Linux 3* AS	x86_32
	Red Hat Enterprise Linux 4 AS	x86_64
	Red Hat Enterprise Linux 5.2, 5.3	x86_64
SUSE Linux		
	SUSE Linux Enterprise Server 9*	x86_32
	SUSE Linux Enterprise Server 10 SP2	x86_64

Veritas File System (VxFS)

SA does not currently support the Veritas File System (VxFS). If you attempt to install SA components on a system running VxFS, the installation will fail and need to be backed out.

Supported Oracle Versions

Support for the Model Repository is limited to certain versions of Oracle running on certain versions of operating systems. HP strongly recommends that you also apply the latest Oracle CPU patches. For manual installations, SA supports both the Oracle Standard Edition, Standard Edition One, and the Oracle Enterprise Edition. Table 7 lists the supported Oracle versions.

Table 7 Supported Operating Systems and Oracle Versions

Operating System	Supported Oracle Versions (Standard or Enterprise Edition)
SunOS 10 x86_64	10.2.0.2, 10.2.0.4, 11.1.0.7
Red Hat Enterprise Linux AS 3 x86_32	10.2.0.2, 10.2.0.4
Red Hat Enterprise Linux AS 4 x86_64	10.2.0.2, 10.2.0.4, 11.1.0.7
Red Hat Enterprise Linux AS 5 x86_64	10.2.0.4, 11.1.0.7
SUSE Linux Enterprise Server 10 x86_64	10.2.0.4, 11.1.0.7

Oracle 10.2.0.3 is not supported by SA due to known incompatibilities.

Multiple Oracle Versions and Multimaster Cores

For the database export to succeed during the installation of a Multimaster core, the version of the target database cannot be 10.x if the source database is 11.x. Table 8 lists these allowed version combinations.

Table 8 Database Versions Allowed for Multimaster

source db version	target db version	allowed?
10	10	Y
10	11	Y
11	10	N
11	11	Y

Solaris and Linux Requirements for 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.

Solaris Requirements

If you will be installing an SA Core Server under Solaris, you must ensure that the packages listed in Table 9 are installed. Table 10 lists recommended packages and Table 11 lists packages that must *not* be installed.

Table 9 Packages Required for Solaris

required packages for solaris		
SUNWCreq (cluster)	SUNWeurf	SUNWeudiv
SUNWadmap	SUNWi2rf	SUNWeudlg
SUNWadmc	SUNWi4rf	SUNWeudmg
SUNWdoc	SUNWi5rf	SUNWeuezt
SUNWesu	SUNWi7rf	SUNWeuhed
SUNWman	SUNWi8rf	SUNWeuluf
SUNWmkcdS	SUNWi9rf	SUNWeulux
SUNWswmt	SUNWi13rf	SUNWeuodf
SUNWtoo	SUNWi15rf	SUNWeuxwe
SUNWtoox**	SUNWtxfnt	SUNWuiu8
SUNWadmfw	SUNWinttf	SUNWuiu8x
SUNWlibC	SUNW5xmft	SUNWulcf
SUNWlibCx**	SUNWcxmft	SUNWulcfx
SUNWinst	SUNWjxmft	SUNWulocf
SUNWucbt	SUNWkxmft	SUNWuxlcf
SUNWucbtx**	SUNWeu8df	SUNWuxlcx
SUNWscpu	SUNWeu8os	SUNWeudbd
SUNWscpux**	SUNWeu8ox	SUNWeudhs
SUNWtcsh	SUNWeudba	SUNWeusru
SUNWsacom	SUNWeudda	SUNWuium
SUNWntpr	SUNWeudhr	NSCPeu8cm
SUNWntpu	SUNWeudis	
SUNWarrf		

** These packages are required only for Solaris 8 and Solaris 9.

Table 10 Packages Recommended for Solaris 8 and 9

recommended packages for solaris		
SUNWisolc	SUNWi1of	SUNWiniu8
SUNWisolx	SUNWjiu8	SUNWiniu8x
SUNWislcc	SUNWjiu8	
SUNWislcx	SUNWkiu8	
SUNWciu8	SUNWkiu8x	
SUNWciu8x	SUNWtiu8	
SUNWhiu8	SUNWtiu8x	
SUNWhiu8x		

Table 11 Packages That Must Be Removed from Solaris

packages That must be 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 9 servers, you must install the time zone patch 113225-07 or later, and libc patch 112874-33 or later. To download these patches, search for the patch ID at *http://www.sun.com/*.
- 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/*.

Linux Package Requirements

For Red Hat Linux AS 3 32-bit x_86, an SA Core Server must have the packages listed in Table 12 installed. For Red Hat Linux AS 4 32-bit x86 and Red Hat Linux Server 5 x_86, an SA Core Server must have the packages listed in Table 13 installed. For both and Red Hat Linux AS4 32-bit x86 and Red Hat Linux AS4 64-bit x86, the packages listed in Table 14 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 12 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

Table 12 Required Packages For Linux As3 32-bit x_86

Required Packages	Architecture
iptables	32-bit x86
kernel-source	32-bit x86
libcap	32-bit x86
libxml2-python	32-bit x86
libstdc++	32-bit x86
libstdc++-devel **	32-bit x86
mkisofs *	32-bit x86
ncompress (contains uncompress utility)	32-bit x86
nfs-utils	32-bit x86
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”.

** Required for Oracle database (Model Repository)

.

Table 13 Packages Required for Linux AS 4 x_64 and AS 5 x_64

Required Packages	Architecture
binutils	x86_64
chkfontpath	x86_64
compat-db	i386
compat-db	x86_64
cpp	x86_64

Table 13 Packages Required for Linux AS 4 x_64 and AS 5 x_64 (cont'd)

Required Packages	Architecture
desktop-file-utils	x86_64
elfutils-libelf (Red Hat 5 only)	x86_64
elfutils-libelf-devel (Red Hat 5 only)	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
glibc-kernheaders (AS 4 only)	x86_64
iptables	x86_64
kernel (Red Hat 5 only)	x86_64
kernel-smp (AS 4 only)	x86_64
kernal-dev (Red Hat 5 only)	x86_64
kernel-smp-devel (AS 4 only)	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

Table 13 Packages Required for Linux AS 4 x_64 and AS 5 x_64 (cont'd)

Required Packages	Architecture
libstdc++	x86_64
libstdc++-deve (Red Hat 5 only)	x86_64
libtermcap	i386
libtermcap	x86_64
libxml2	i386
libxml2	x86_64
libxml2-python	x86_64
make	x86_64
mesa-libGL (Red Hat 5 only)	i386
mesa-libGL (Red Hat 5 only)	x86_64
mesa-libGLU (Red Hat 5 only)	i386
mesa-libGLU (Red Hat 5 only)	x86_64
mkisofs	x86_64
ncompress	x86_64
nfs-utils	x86_64
ntp	x86_64
openmotif (Red Hat 5 only)	
openmotif21 (AS 4 only)	
openmotif21	i386
patch	x86_64
patchutils	x86_64
pdksh	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
tcp_wrappers	i386

Table 13 Packages Required for Linux AS 4 x_64 and AS 5 x_64 (cont'd)

Required Packages	Architecture
tcp_wrappers	x86_64
ttmkfdir	x86_64
unzip	x86_64
vim-enhanced	x86_64
vnc	x86_64
vnc-server	x86_64
xinetd	x86_64
xinitrc	noarch
xorg-x11 (AS 4 only)	x86_64
xorg-x11-Mesa-libGL (AS 4 only)	i386
xorg-x11-Mesa-libGL	x86_64
xorg-x11-Mesa-libGLU (AS 4 only)	i386
xorg-x11-Mesa-libGLU (AS 4 only)	x86_64
xorg-x11-Xvfb (AS 4 only)	x86_64
xorg-x11-deprecated-libs (AS 4 only)	i386
xorg-x11-deprecated-libs (AS 4 only)	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 14 Packages That Must Be Removed for Linux

Packages		
samba	rsync	tftp (AS 3 and 4 only) **
apache	httpd	tftp-server (Red Hat 5 only)
yast2-dhcp-server (SLES 10 only)	yast2-samba-server (SLES 10 only)	dhcp**
	yast2-tftp-server (SLES 10 only)	

** 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'
    ```

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 15 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 15 Open Ports on a Firewall Protecting an SA Core

port	component	Purpose
80 (TCP)	Command Center	HTTP redirector
443 (TCP)	Command Center	HTTPS Proxy for SAS Web Client UI, SAS Client, SA Web Services (2.2)
1003	Software Repository (`word`)	
1004	Data Access Engine (`spin`)	
1018	Command Engine (`way`)	
1032	Web Services Data Access Engine (`twist`)	
1521	Model Repository (`truth`)	
2001 (TCP)	Management Gateway/ Core Gateways	Inbound tunnels from other Gateways (If Port 2001 is in use, rolls over to 2003)
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 SAS Client

Table 16 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 16 Open Ports for the OS 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 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 segregrate the OS Provisioning Boot Server and Media Server components onto their own DMZ network. When you segregate these components, the ports listed in Table 16 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 17 shows the Managed Server port that must be open for SA Core Server connections.

Table 17 Open Ports on Managed Servers

port	component
1002 (TCP)	Server 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.

Additionally, a Core Server must be able to resolve both the fully qualified and unqualified names of the SA Services. (Each service name represents an SA Core Component.) For example, both `truth` (unqualified) and `truth.acct.buzzcorp.com` (fully qualified) must resolve to the IP address of the server containing the Model Repository.

The list of fully qualified names of the SA services follows:

- `truth.`*`subdomain`* — Model Repository
- `way.`*`subdomain`* — Command Engine
- `spin.`*`subdomain`* — Primary Data Access Engine
- `theword.`*`subdomain`* — Software Repository
- `wordcache.`*`subdomain`* — Software Repository Multimaster Component The name `wordcache` must resolve to the core server running the Software Repository (Slice Component bundle).

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.

On Solaris 10, an OGFS installation requires the actual host name of the OGFS host. In the `dfstab` file on the Software Repository host, specify the actual hostname of the OGFS host.

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 OS Provisioning” in the *SA Planning and 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 7.50

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.

- wsusscn2.cab

  The `wsusscn2.cab` file contains the Microsoft patch database. To download the package containing `wsusscn2.cab`, search for “`wsusscn2.cab`” at *http://www.microsoft.com* .

- 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`".

- mbsacli.exe **(version 2.1)**

  This file is packaged with the MBSA 2.1 setup file, `MBSASetup-x86-EN.msi`, that you must download by searching for “`MBSA 2.1`” at *http://www.microsoft.com* .

  After the download, on a Windows machine run `MBSASetup-x86-EN.msi` to install MBSA 2.1. In the directory where you installed MBSA 2.1, locate the `mbsacli.exe` file. By default, the file is installed here:

  ```
  %program files%\Microsoft Baseline Security
  Analyzer 2\mbsacli.exe
  ```

- wusscan.dll

  The `wusscan.dll` file is in the directory where you installed MBSA 2.1. By default, the file is here:

- ```
  %program files%\Microsoft Baseline Security
  Analyzer 2\wusscan.dll
  ```

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:

  ```
  mbsacli.exe
  WindowsUpdateAgent-x86.exe
  WindowsUpdateAgent-x64.exe
  ```
  ```

```
WindowsUpdateAgent-ia64
qchain.exe
wsusscn2.cab
wusscan.dll
```

4 Write down the name of the directory containing the files. When you run the Installer, during the Software Repository installation, you will prompted to provide the fully qualified directory path. The location you provide will be stored in the parameter, `windows_util_loc`.

These patch management files will be copied to Windows servers during SA Agent deployment. If you upload newer versions of the files to the Software Repository later, they will be downloaded to the 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 SAS Client. For more information, see the *SA Planning and Installation Guide*.

For information on Windows Patch Management, see the *SA User's Guide: Application Automation*.

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"
```