Quick Reference: Pre-Installation Requirements for Opsware SAS 6.1.1

This reference document is intended to quickly familiarize you with the basic requirements for installing Opsware SAS, 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:

- Supported Operating Systems

- Supported Versions of Oracle

- SAS Core Server Package Requirements

  - Solaris Requirements

  - Linux Requirements

- Network Requirements

  - Network Requirements Within a Facility

  - Open Ports

- Core Time Requirements

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

Supported Operating Systems

Table 1-1 lists the platform-specific requirements for installing Opsware SAS.

Table 1-1: Supported Operating Systems for Installing Opsware SAS

SUPPORTED OS	VERSION	ARCHITECTURE
Sun Solaris	Solaris 8, 9, 10	SPARC
Linux	Red Hat Enterprise Linux 3 AS	32 bit x 86

Supported Versions of Oracle

Support for the Model Repository (truth) is limited to certain versions of Oracle running on certain versions of operating systems. Table 1-2 lists the supported Oracle versions.

Table 1-2: Supported Oracle Versions for the Model Repository

ORACLE EDITION	ORACLE VERSION
Oracle Standard Edition	9.2.0.4 9.2.0.6 9.2.0.7 9.2.0.8 10.2.0.2
Oracle Enterprise Edition	9.2.0.4 9.2.0.6 9.2.0.7 9.2.0.8 10.2.0.2

SAS Core Server Package Requirements

Solaris Requirements

For Solaris, the Opsware core servers must meet the requirements listed in Table 1-3, Table 1-4, and Table 1-5.

Table 1-3: Packages Required for Solaris

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

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

Table 1-4: Packages Recommended for Solaris

RECOMMENDED PACKAGES FOR SOLARIS		
SUNWisolc	SUNWjiu8	SUNWkiu8x
SUNWisolx	SUNWkiu8	SUNWtiu8x
SUNWislcc	SUNWtiu8	SUNWi1of
SUNWislcx	SUNWciu8x	SUNWiniu8
SUNWciu8	SUNWhiu8x	SUNWiniu8x
SUNWhiu8	SUNWjiu8x	

Table 1-5: Packages That Must Be Removed for Solaris

PACKAGES THAT MUST BE REMOVED FROM SOLARIS
SUNWCpm

Table 1-6 lists the packages required for a Solaris core server that has the en_US.UTF-8 locale installed.

Table 1-6: Package Requirements for the en_US_.UTF-8 Locale

REQUIRED	RECOMMENDED (OPTIONAL)	MUST REMOVE
SUNWarrf	SUNWkxmft	SUNWeuodf
SUNWeurf	SUNWeu8df	SUNWeuxwe
SUNWi2rf	SUNWeu8os	SUNWuiu8
SUNWi4rf	SUNWeu8ox	SUNWuiu8x
SUNWi5rf	SUNWeudba	SUNWulcf
SUNWi7rf	SUNWeudda	SUNWulcfx
SUNWi8rf	SUNWeudhr	SUNWulocf
SUNWi9rf	SUNWeudis	SUNWuxlcf
SUNWi13rf	SUNWeudiv	SUNWuxlcx
SUNWi15rf	SUNWeudlg	SUNWeudbd
SUNWtxfnt	SUNWeudmg	SUNWeudhs
SUNWinttf	SUNWeuezt	SUNWeusru
SUNW5xmft	SUNWeuhed	SUNWuium
SUNWcxmft	SUNWeuluf	NSCPeu8cm
SUNWjxmft	SUNWeulux	

Other Solaris Requirements

On the server where you will install the SAS Web Client component, you must install the J2SE Cluster Patches for Solaris. You can download these patches from the following location:

```
http://sunsolve.sun.com/pub-cgi/show.pl?target=patches
/patch-access
```

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.

You can download these patches from the following locations:

```
http://sunsolve.sun.com/search/
document.do?assetkey=urn:cds:docid:1-21-113225-07-1
```

```
http://sunsolve.sun.com/search/
document.do?assetkey=urn:cds:docid:1-21-112874-33-1
```

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.

You can download these patches from the following locations:

```
http://sunsolve.sun.com/search/
document.do?assetkey=urn:cds:docid:1-21-122032-03-1
```

```
http://sunsolve.sun.com/search/
document.do?assetkey=urn:cds:docid:1-21-119689-07-1
```

For more information about DST changes, see `http://sunsolve.sun.com/search/document.do?assetkey=1-26-102775-1`.

Linux Requirements

For Linux, the Opsware core servers must meet the requirements listed in Table 1-7 and Table 1-8.

Table 1-7: Packages Required for Linux

REQUIRED PACKAGES FOR LINUX		
at	glibc-headers	ncompress (contains
compat-db	glibc-kernheaders	uncompress utility)
compat-libstdc++	iptables	nfs-utils
coreutils	kernel-source	ntp
cpp	libcap	patch
expat	libxml2-python	patchutils
gcc	libstdc++	sharutils
glibc-devel	libstdc++-devel	strace

Table 1-8: Packages That Must Be Removed for Linux

PACKAGES THAT MUST BE REMOVED FROM LINUX		
samba	rsync	tftp**
apache	httpd	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 Opsware core servers that do not have the OS Provisioning Boot Server component.

Network Requirements

This section discusses the following network requirements within a facility, open ports required for core components, and name resolution requirements. These requirements must be met for both standalone and multimaster cores.

Network Requirements Within a Facility

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

• The Opsware core servers must be on the same Local Area Network (LAN or VLAN).

• The Opsware core servers must have network connectivity to the servers that the Opsware core manages, and vice versa.

• The Opsware core servers cannot use the Network Information Service (NIS) for password and group databases. The Opsware components check for the existence of certain target accounts before creating them during installation.

• When using network storage for Opsware components, such as the Software Repository or Media Server, the network storage configuration must allow the root user to have write access over NFS to the directories where the components are to be installed.

• The speed and duplex mode of the NIC adapters of the Opsware core and managed servers must match the switch they are connected to. A mismatch causes poor network performance between the core and managed servers, making Opsware SAS unusable.

Open Ports

Table 1-9 shows the ports that must be open on firewalls that protect the Opsware core components. The Gateway ports listed are the default values, which can be changed during the installation.

Table 1-9: Open Ports on a Firewall Protecting an Opsware Core

PORT	COMPONENT	PURPOSE
80 (TCP)	SAS Web Client	HTTP redirector
443 (TCP)	SAS Web Client	SAS Web Client UI, SAS Client, Opsware web services
2001 (TCP)	Core Gateway	Inbound tunnels from other Gateways

Table 1-9: Open Ports on a Firewall Protecting an Opsware Core (continued)

PORT	COMPONENT	PURPOSE
2222 (TCP)	Opsware Global File System	Global shell session from an SSH client
3001 (TCP)	Agent Gateway	Inbound Agent connections
7580, 7581 (TCP)	Model Repository Multimaster Component	TIBCO Rendezvous web client
8017 (UDP, TCP)	Agent Gateway	Interface to the Build Manager
8080 (TCP)	SAS Web Client	OGFS Gateway for the SAS Client

Table 1-10 shows the ports for the OS provisioning components that are accessed by servers during the provisioning process. (In Opsware SAS, provisioning refers to the installation of an operating system on a server.)

Table 1-10: 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*	Boot Server, Media Server	`rpc.mountd`, required for NFS
2049 (UDP, TCP)	Boot Server, Media Server	NFS

* The `rpc.mountd` process runs on a dynamic port and is not fixed. Therefore, if a firewall is in place, it must be an application layer firewall that can understand the RPC request that the client uses to locate the port for `mountd`. The firewall must dynamically open that port.

Table 1-11 shows the ports that must be open on managed servers so that Opsware core servers can connect to managed servers.

Table 1-11: Open Ports on Managed Servers

PORT	COMPONENT
1002 (TCP)	Opsware Agent

DHCP Proxying

If network provisioning occurs on a separate network from the Opsware core components, you must set up DHCP proxying (for example, with Cisco IP Helper) to the DHCP server. If you set up DHCP proxying, the server/router performing the DHCP proxying must be the router for the network so that PXE will function correctly in the Opsware OS Provisioning Feature.

The Opsware Boot Server component includes a DHCP server, but does not include a DHCP proxy. You configure the DHCP server after installation by using the Opsware DHCP Network Configuration Tool.

DMZ Network

The Boot Server and Media Server run various services (such as portmapper and rpc.mountd) that have been susceptible to network attacks. Opsware Inc. recommends 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 previously) 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.

Core Time Requirements

Opsware core servers (either standalone or multimaster) and Opsware Satellite servers must meet the following requirements. These time requirements do not apply to managed servers (that is, servers with Opsware Agents).

• Opsware core servers must maintain synchronized clocks. For example, you can synchronize the system clocks with an external server that uses NTP (Network Time Protocol) services.

• Opsware core servers must have their time zone set to Coordinated Universal Time (UTC).

On Linux servers, to configure the time zone, perform the following steps:

• Copy or link `/usr/share/zoneinfo/UTC` to `/etc/localtime`.

• Make sure that `/etc/sysconfig/clock` contains the following lines:

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

On Solaris servers, to configure the time zone, verify that `/etc/TIMEZONE` contains the following line: TZ=UTC