Sun™ Internet Mail Server™ 4.0 Installation Guide

THE NETWORK IS THE COMPUTER™

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
(650) 960-1300 Fax 650 969-9131

Part No. 805-7655-11
Revision A, September 1999

Contents

Figures

Tables

Preface

The *Sun Internet Mail Server 4.0 Installation Guide* describes how to plan, install, and configure the Sun™ Internet Mail Server™ (SIMS) 4.0 software on Solaris™ SPARC™ systems and Intel Pentium platforms.

Topics in this chapter include:

- Who should use this book
- Conventions
- Related documentation
- Shell prompts in command examples
- Graphical user interface conventions
- Notice

Who Should Use This Book

The intended audience for this installation guide are the system administrators who are moderately experienced with managing a network of Sun Workstations™, PCs, Apple computers, or IBM mainframes. Previous experience in planning, installing, configuring, maintaining, and troubleshooting an enterprise email system also helps to efficiently use this guide.

Conventions

TABLE P-1 describes the typographic conventions used in this guide.

TABLE P-1 Typographic Conventions

Convention	Meaning	Example
`courier font`	Names of commands, files, on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% test.doc.`
italics	Book titles, new terms, words to be emphasized, variables that you replace with a real name or value	Read Chapter 6 in *User's Guide.* These are called *class* options. You *must* be root to do this. Type `rm` *filename* to delete a file.
`boldface courier font`	What you type	`machine_name%` **`su`** `Password:`
italics	Command-line placeholder	

Related Documentation

SIMS 4.0 Documentation Set

The *Sun Internet Mail Server 4.0 Installation Guide* manual is a companion document to the following manuals in the SIMS documentation set:

Sun Internet Mail Server 4.0 Concepts Guide—Provides a conceptual understanding of the SIMS product. By understanding how SIMS works on a conceptual level, readers will more easily understand the administrative tasks described in the *Sun Internet Mail Server Administrator Guide and Sun Internet Mail Server Reference Guide.*

Sun Internet Mail Server 4.0 Provisioning Guides—Describes how to provision the SIMS LDAP directory with users, distribution lists, administrators, and domains by creating and importing LDIF records.

Sun Internet Mail Server 4.0 Administrator's Guide—Describes how to fine-tune the default configuration, and to maintain, monitor, and troubleshoot your mail server by using the SIMS Administration Console, a graphical user interface (GUI) tool.

Sun Internet Mail Server 4.0 Reference Manual—Provides detailed information on command-line options and configuration files that can be edited by the administrator, system architecture, supported standards, and location of software files.

Sun Internet Mail Server 4.0 Delegated Management Guide—Describes the SIMS Delegated Management Console and the tasks associated with the console. In particular, it describes how a delegated administrator for a hosted domain performs tasks on users and distribution lists.

Sun Internet Mail Server 4.0 Reference manual pages (man pages)—Describe command-line utilities and detailed information about the arguments and attributes relevant to each command.

Sun Internet Mail Server 4.0 Release Notes—Covers open issues and late-breaking installation, administration, and reference information that is not published in the product books.

Other Related Sun Documentation

Sun Internet Mail Server 4.0 Web site (located at http://www.sun.com/sims)—Offers up-to-date information on a variety of topics, including: online product documentation and late-breaking updates, product information, technical white papers, press coverage, and customer success stories.

Sun Directory Services 3.1 Administration Guide (http://docs.sun.com:80/ab2/coll.297.1/@Ab2CollToc?subject=sysadmin)—Describes the Sun Directory Services.

Netscape Directory Services documentation (http://home.netscape.com/eng/server/directory)—Describes the Netscape Directory Services.

Shell Prompts in Command Examples

TABLE P-2 shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P-2 Shell Prompts

Shell	Prompt
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	`#`

Graphical User Interface Conventions

This section describes the terminologies used to describe the installation graphical user interface for the installation or for the SIMS Administration Console. TABLE P-3 defines terms used in procedures associated with the installation or the SIMS Administration Console.

TABLE P-3 Graphical User Interface Terminology

Term	Explanation	Example
Check box	A yes / no or on / off control. A square box that appears highlighted and pushed in when on or pushed out when off. Usually, all check boxes in a group can be selected.	To enable the logging of each message, click the check box.
Radio button	A yes / no or on / off control. A diamond or circle that appears highlighted and pushed in when on or pushed out when off. Usually, only one radio button in a group can be selected.	You can enable the channel to ignore nonstandard encoding headers by clicking the appropriate radio button.
Click	Press and release a mouse button without moving the pointer.	Click Start.
Double-click	Click a mouse button twice quickly without moving the pointer.	Double-click the SMTP channel name from the list of channels

Notice

To better illustrate the process being discussed, SIMS manuals contain examples of data that might be used in daily business operations. The examples might include names of individuals, companies, brands, and products. SIMS manuals use only fictitious names, and any similarity to the names of individuals, companies, brands, and products used by any business enterprise is purely coincidental.

CHAPTER 1

Overview of Sun Internet Mail Server 4.0

Sun™ Internet Mail Server™ (SIMS) 4.0 provides a mail solution for the service providers (SPs), enabling them to expand their service offerings from residential to business outsourcing.

SIMS 4.0's key functionality includes virtual hosted domains and delegated management capabilities.

Topics in this chapter include:

- What has changed in SIMS 4.0
- SIMS 4.0 product features

What Has Changed in SIMS 4.0

The following is a list of changes from SIMS 3.5 to SIMS 4.0:

- Addition of new features included in the “SIMS 4.0 Product Features”
- Delegated Management capabilities—provisioning and utilities
- Support for hosted domain in all components
- Support of DC DIT tree structure
- Removal of the OSI DIT tree structure
- Support for the Netscape Directory Services server
- Support of the Netscape browser for the SIMS Administration Console
- Support of the remote LDAP server
- Support of the SIMS optional features for the SIMS High Availability
- Replacement of Java Web Server for Sun Web Access with Sun Web Server
- Replacement of SunDS 1.0 with SunDS 3.1
- Support of services-level restrictions
- Removal of the Enterprise edition
- Removal of the Departmental edition
- Removal of software-enforced licensing
- Removal of pure-proxy SIMS installation
- Removal of migration from SIMS 3.x to SIMS 4.0
- Support of Solaris 2.6 and Solaris 2.7 operating environments
- Support of the SIMS High Availability system with SunCluster 2.2
- Migration tools for migrating directory data from previous releases available by contacting Sun
- Removal of product support for optional Sun Messaging Connectivity Services, which is now available through a 3rd part provider.

SIMS 4.0 Product Features

This section shows the features that the SIMS 4.0 product offers based on its individual components. Items that are identified as *New* are specific to the 4.0 release.

Internet Message Transfer Agent (IMTA)

- Powerful anti-spam configuration with anti-relaying
- SMTP authentication
- POP before SMTP authentication *New*
- Scalable channel architecture
- Domain hosting support *New*
- DNS canonicalization to qualify non-FQDN names and normalize hostname aliases *New*
- SDK for custom application development
- Extensive address rewriting (including address reversal) and channel management facilities
- Pipe channels supporting the IMTA through native Solaris programs

Message Store / Message Access

- Domain hosting support *New*
- Multithreaded POP3 / IMAP4 Server
- APOP authentication for POP3 *New*
- POP before SMTP connection *New*
- Concurrent access to any message folder *New*
- Secure Socket Layer (SSL) messages access *New*
- Integrated proxy server
- Integrated backup / restore utilities

Sun Web Access Server

- Domain hosting support *New*
- Domain and user provision *New*
- HTML-based
- Brandable
- Single integrated UI to view email, directory, and calendar

- Message attachment support
- Sun Web Access server support *New*
- High Availability support *New*

Delegated Management Console **New**

- Domain-level user creation and management
- Domain-level distribution list and management
- End-user personal preferences setup
- Customizable and brandable
- HTML-based application

SIMS Administration Console

- Netscape browser support *New*
- Domain creation and deletion *New*
- Domain service restrictions set up *New*
- Domain-level user creation and management *New*
- Distribution list setup and management *New*
- Server statistics
- Server components configuration
- Server monitoring and queue status
- Starting and stopping server
- Purging deleted entries

Administration Utilities

- Domain creation and management *New*
- Domain and user authorized service restrictions *New*
- Domain-level user creation and management *New*
- Delegated administrator creation *New*
- Bulk-loading new domain-level users *New*
- Changing user authorized services *New*
- Distribution list setup and management *New*
- Service and performance monitoring *New*

Directory Services

- Netscape Directory Services 4.1 support *New*
- Sun Directory Services 3.1 support *New*
- Multiprotocol, distributed, scalable, client/server-based global directory
- LDAP v3 server *New*
- Server failure rollover *New*
- LDAP address referral in master/slave configuration *New*
- Remote LDAP sever support *New*
- Remote user authentication *New*
- Domain Component (DC) tree structure support *New*

Other Optional Features

- Message Transfer Agent SDK
- SIMS 4.0 Documentation Set
- Remote Administration Console

CHAPTER 2

System Requirements

This chapter provides the information specific to the hardware and software requirements for installing Sun™ Internet Mail Server™ 4.0.

Topics in this chapter include:

- Platform requirements
- CPU requirements
- Disk space requirements
- Swap space requirements
- Memory requirements
- Client system configuration requirements
- Sun Directory Services 3.1 requirements

Platform Requirements

The SIMS software is available on SPARC™ and Intel-based systems running the operating system versions indicated in TABLE 2-1.

TABLE 2-1 Supported Platforms and Operating System Environments

Platform	Operating System
SPARCstation 20 or higher	Sun™ Solaris™ SPARC 2.6 and 2.7
Intel Pentium 200 MHz-based systems	Sun Solaris Intel 2.6 and 2.7

CPU Requirements

Although the SIMS software can operate on any mail server with a single CPU, your mail server should be equipped with multiple CPUs to take advantage of the multithreaded capabilities of the product and for improved performance.

Disk Space Requirements

This section lists the disk space requirements for SIMS 4.0 core components. On the designated mail server, make sure that you allocate adequate free space on the file system that contains the directories listed in TABLE 2-2. This table does not account for Netscape Directory Services, Sun Web Access, or SDK. Use the `df` command to check the free disk space.

TABLE 2-2 SIMS 4.0 Storage Requirements

Directory Path	SIMS Core Requirement
`/opt`	90 MB
`/var`	20 MB
`/usr`	10.5 MB

Swap Space Requirements

Although the minimum recommendation swap space is 128 megabytes, better performance can be achieved on systems with more swap space such as 192 megabytes. The recommended swap space is 2.5 times the physical memory in the computer. The amount of swap space varies depending on the swap space needed for running other software on the server.

Memory Requirements

The minimum required RAM is 64 megabytes. TABLE 2-3 below lists the memory requirements for IMAP- and POP3-based systems.

TABLE 2-3 Memory Requirements for IMAP and POP3 Systems

Number of Users	Physical Memory for IMAP4	Physical Memory for POP3
100	178 MB	165 MB
500	375 MB	320 MB
1,000	622 MB	492 MB
5,000	2.6 GB	2.0 GB

Client Requirements

TABLE 2-4 shows the clients that are supported by SIMS 4.0.

TABLE 2-4 Client Requirements

Client	Requirement
Sun Web Access	HTML v3.2 compliant GUI Web browser which supports HTML frames and cookies
MAPI Providers	Microsoft Windows Messaging inbox, Microsoft Outlook 97

See Chapter 5, “SIMS Architecture” in the *Sun Internet Mail Server 4.0 Concepts Guide* for descriptions of supported clients that you could use with SIMS.

Sun Directory Services 3.1 Requirements

Sun Directory Services 3.1 requires the following system configurations:

- Solaris 2.6 for SPARC or Solaris 2.6 for x86/Pentium® platforms
- CD-ROM drive for software installation.
- 64 MB disk space and 64 MB memory.
- An X Window System window manager is required to use the graphical configuration and management tools.

CHAPTER 3

Software and Configuration Requirements

This chapter provides a list of software that are required for installing your Sun™ Internet Mail Server™ (SIMS) 4.0 as well as the SIMS High Availability system.

Topics in this chapter include:

- Software requirements
- Configuration requirements

Software Requirements

SIMS 4.0 requires that the software packages listed in TABLE 3-1 and TABLE 3-2 (for HA systems only) be installed. SIMS installation automatically installs the application listed in TABLE 3-1 if they are not available on your system.

TABLE 3-1 SIMS Software Requirements

Application	Required for
Sun Web Server 2.1	SIMS Administration Console, Web Access
Netscape Browser 4.06 or higher (required but not installed automatically)	SIMS Admin. Console
HTML 2.0 complaint browser or higher	SIMS Administration Console, Web Access
Secure Sockets Layer (SSL)	Secure POP3/IMAP4
Core Java Packages	SIMS Administration Console, utilities
LDAP Package	SIMS access to the directory

TABLE 3-2 shows the required applications for the SIMS High Availability systems.

TABLE 3-2 SIMS/HA Software Requirements

Application	Volume Manger	File System	Operating System
SunCluster 2.2	VxVM 3.0.1	VxFS File 3.3.2	Solaris 2.6, 2.7
SunCluster 2.2	DiskSuite 4.2	UFS	Solaris 2.6, 2.7

TABLE 3-3 provides descriptions for these applications that are required by the SIMS High Availability system.

TABLE 3-3 Description for SIMS/HA Requirements

Application	Description
SunCluster 2.2	Switch between nodes in the cluster
VxVM or DiskSuite 4.2 Volume Manger	Configure the shared disk
VxFS or UFS file systems	Logging file systems

Configuration Requirements

Before installing SIMS, you need to make sure the following requirements have been met:

DNS Configuration Files

Before installing SIMS, be sure that the two configuration files `/etc/nsswitch.conf` and `/etc/resolv.conf` are set up correctly. See “Configuring the DNS Setup” on page 92 in Chapter 11, “Troubleshooting the Sun Internet Mail Server," for detailed instructions for setting up your DNS configuration

You need to make sure that the DNS is installed and running before installing SIMS.

Naming Services Requirement

The name service (NIS or NIS+) requires that the machine designated as the mail server uses a fully qualified DNS name.

File System Requirement

SIMS requires that the message store be installed on a local disk and not on an NFS or other remote file system mounted partition in Solaris 2.6 or 2.7.

Logical Host Name Configuration for High Availability Systems

The logical host name for High Availability systems must have its own IP address which is different from its physical host IP address. This host name must be a Domain Name Server (DNS) alias of another host name.

CHAPTER 4

Preparing to Install SIMS 4.0

This chapter provides information on how to prepare your system before installing the Sun™ Internet Mail Server™ (SIMS) 4.0.

Topics in this chapter include:

- Preparing to install SIMS with remote LDAP
- Preparing to install the Netscape Directory Services for SIMS
- Preparing a clean system
- Preparing to install LDAP rollover
- Preparing to install patches

Preparing to Install SIMS with Remote LDAP

SIMS 4.0 allows using a remote LDAP server. You could use either the Netscape Directory Services or the Sun Directory Services remotely. See Appendix A, “Installing Netscape Directory Services for SIMS," if you are installing SIMS on a remote server where Netscape Directory Services are installed. If, however, you are installing on a remote server where Sun Directory Services are installed, do the instructions covered in this section. The following shows three different scenarios:

▼ To install SunDS *before* installing SIMS

1. **Install the LDAP server on a remote machine where SIMS is not installed**
2. **Add the SIMS schema package which includes the SIMS 4.0 configuration files, indexes, and Access Control Lists (ACLs) to your LDAP server.**

```
# cd /cdrom/sun_internet_mail_4_0/products/sims/Image/all
# /usr/sbin/pkgadd -d . SUNWimsch
```

3. **Install SIMS.**

   See Chapter 7, “Installing SIMS 4.0," for instructions for installing SIMS 4.0.

▼ To install SunDS *after* installing SIMS

1. **Install SIMS on a local server.**
2. **Install SunDS on a remote server.**
3. **Add the SIMS schema package which includes the SIMS 4.0 configuration files, indexes, and Access Control Lists (ACLs) to your LDAP server.**

```
# cd /cdrom/sun_internet_mail_4_0/products/sims/Image/all
# /usr/sbin/pkgadd -d . SUNWimsch
```

4. **Create the SIMS Directory Information Tree (DIT) for your server.**

```
# /opt/SUNWconn/bin/ldapadd -c -h <hostname> -p <portnumber> -D
“cn=<Directory Administrator>,o=<dcroot>” -w <passwd> -f /etc/opt/
SUNWmail/slapd.ldif
```

Where,

<*Directory Administrator*> is the name assigned to the administrator who configures the directory server,

<*passwd*> is the password associated with the Directory Administrator, and

<*dcroot*> is the node name for the root of the Domain Component (DC) tree for which SIMS is installed. The default is `internet`.

▼ To install SIMS with an existing remote SunDS

1. **Install SIMS on a local server.**
2. **Add the SIMS schema package which includes the SIMS 4.0 configuration files, indexes, and Access Control Lists (ACLs) to your LDAP server.**

```
# cd /cdrom/sun_internet_mail_4_0/products/sims/Image/all
# /usr/sbin/pkgadd -d . SUNWimsch
```

3. **Create the SIMS Directory Information Tree (DIT) for your server.**

```
# /opt/SUNWconn/bin/ldapadd -c -h <hostname> -p <portnumber> -D
“cn=<Directory Administrator>,o=<dcroot>” -w <passwd> -f /etc/opt/
SUNWmail/slapd.ldif
```

Preparing to Install the Netscape Directory Services for SIMS

SIMS 4.0 supports the Netscape Directory Services (NSDS).

Note – Be sure to install NSDS before installing SIMS.

To install NSDS with SIMS:

1. **Install NSDS 4.1.**
2. **Add the SIMS schema files to the NSDS configuration directory.**
3. **Disable the NSDS uid uniqueness.**
4. **Install SIMS 4.0.**

   See Appendix A, “Installing Netscape Directory Services for SIMS," for a complete set of instructions to install NSDS for SIMS.

Preparing a Clean System

If you are reinstalling your SIMS system, you can manually clean up your system by using the `uninstall` command along with the appropriate options that are shown in TABLE 4-1.

TABLE 4-1 The `uninstall` Command Options

Type of Installation	Option used with uninstall	Action Taken by uninstall
Fresh	`-d`	Removes the entire SIMS system along with your data and configuration files, including the directory structure.
Upgrade	`-c`	Removes the SIMS binary files, but *keeps* your data and configuration files, including the directory structure.

See the *Sun Internet Mail Server* man pages for more information on the `uninstall` command.
You may use the `pkginfo` command to list the packages already installed on your system.

Note – Do not remove the packages individually.

▼ To remove SIMS

1. **Log in as root.**

```
$su
Password: <Enter your root password>
```

2. **Enter one of the following.**

```
# /opt/SUNWmail/sbin/uninstall -d sims
OR
# /opt/SUNWmail/sbin/uninstall -c sims
```

Note – The `uninstall` command does not remove the `SUNWlldap` LDAP library packages which is part of Solaris 2.7. You may remove this package by using the `pkgrm` command.

Note – At the end of `uninstall`, `sendmail` will be restored. You will then need to start `sendmail` either manually or by rebooting. Also, package remove leaves the Sun™ Web Server™ running. Either reboot your system or stop the `httpd` daemon.

Using `uninstall` on HA Systems

If SIMS is installed on a High Availability system, the `uninstall` command is also placed in directory `/opt/SUNWimha/sbin/uninstall`. If you wish to remove SIMS from the additional machines on an HA cluster, you need to use the `uninstall` command from this directory.

Preparing to Install LDAP Rollover

When an LDAP server fails, a series of alternative LDAP servers to which the server could contact needs to be provided.

To accomplish this, before installing SIMS you need to modify the `/etc/opt/SUNWmail/sims.cnf` file and enter the LDAP servers.

The following shows an example of a `sims.cnf` file.

```
#@(#)COPYRIGHT SMI
#---- WARNING --- WARNING --- WARNING ---- WARNING ---
#
#      PLEASE DO NOT EDIT THIS FILE BY HAND
#
#---- WARNING --- WARNING --- WARNING ---- WARNING ---
#Mon Jun 07 11:55:22 PDT 1999
dcRoot=o=internet
adminBindDN=cn=
Administrator,ou=People,dc=test,dc=com,o=internet
loginSeparator=+
logicalHostname=
ldapServer=host1.domain.com:389,host2.domain.com:389
defaultDomain=
spmServer=
```

Note – `LdapServer` is where you would add the servers on which LDAP is running.

Preparing to Install Patches

This section discusses two types of patches: first, the *required* patches to ensure that SIMS operates properly; second, the *recommended* patches to the Solaris™ operating system that address a variety of system stability issues.

Required Patches

TABLE 4-2 shows a list of patches that are required for SIMS 4.0 to install and operate properly. If these patches, or newer versions of them, are not found on the targeted system, they will be installed automatically. The required patches are located in the directory `/etc/patches` on the CD.

TABLE 4-2 SIMS Required Solaris Patches

Patch ID	Operating System	Type of Patch
106621-04 sparc **106622-04 i386**	**Solaris 2.6/2.7**	**Sun Directory Services 3.1 patch**
106125-04 sparc **106126-04 i386**	**Solaris 2.6**	**`patchadd` and `patchrm` patch**
105181-04 sparc **105182-04 i386**	**Solaris 2.6**	**Kernel update patch**
105568-06 sparc **105569-06 i386**	**Solaris 2.6**	**`/usr/lib/libthread.so.1` patch**
105755-03 sparc **105756-03 i386**	**Solaris 2.6**	**`in.named` and `libresolv` patches**
105490-04 sparc **105491-04 i386**	**Solaris 2.6**	**Linker patch**
106613-01 sparc **106614-01 i386**	**Solaris 2.6**	**Japanese `UTF-8` `iconv` patch**
106618-01 sparc[1] **106619-01 i386**	**Solaris 2.6**	**ISO-2022-CN UTF-8 iconv** **(version # 6.0,REV=1.0.33)**
106556-01 sparc **106594-02 i386**	**Solaris 2.6**	**ISO-2022-CN UTF-8 iconv** **(version # 6.0,REV=1.0.38)**

1. Two different versions of the package `SUNWciu8` were shipped with Solaris 2.6. To find out which version you have, run the command `pkginfo -l SUNWciu8` and then look at the line "VERSION=".

Recommended Patches

SIMS recommends that the clusters of patches that were used during quality assurance testing of SIMS be installed. These patch clusters are available in the directory `/patches` on the SIMS CD.

In addition to the recommended patch cluster, the following two patches are also recommended. They are located on the directory `/patches/additional_2.6` on the SIMS CD.

TABLE 4-3 SIMS Additional Recommended Patches

Patch ID	Operating System	Type of Patch
106439-01 sparc 106440-01 i386	Solaris 2.6	System log patch

Installing Recommended Patch Cluster

This section shows how the `install_cluster` script installs the Solaris patches. Refer to the `CLUSTER_README` file for a list of the specific patches and installation conditions. Be sure the patch cluster has been uncompressed and extracted if you received the cluster as a `tar.Z` file.

1. **Decide the method to install the cluster.**

   By default the Save Feature option is selected, which saves the original objects being patched. Selecting the No Save option disables backing out individual patches.

2. **Run the `install_cluster` script.**

```
% cd <patch cluster directory>
% su
<enter your root password>
# ./install_cluster
```

   A message displays, asking the user to check for minimum disk space requirements. To suppress this interactive message, use the `-q` (quiet) command when you invoke the `install_cluster` script.

3. **Verify the installed patch IDs.**

```
% /usr/bin/showrev -p
```

Refer to individual patch README files for more patch detail.

4. **Check the log file if you get any error messages and need more details.**

```
% more /var/sadm/install_data/<cluster name>_log
```

If this log file already exists, the latest cluster installation data will be concatenated to this file.

Though some of the patches in the cluster will not be needed if you are installing the cluster on an Ultra machine, the installation program will assume that they need to be installed. When you check the log file, you will see errors for the patches that were not installed.

5. **Reboot the machine for all patches to take effect.**

CHAPTER 5

Planning to Install SIMS 4.0

This chapter covers different configurations that you need to consider before installing your Sun™ Internet Mail Server™ 4.0 system.

Topics in this chapter include:

- SIMS as a proxy considerations
- SIMS in SP environments considerations
- Internet Message Transfer Agent considerations

SIMS as a Proxy Considerations

If you are installing SIMS as a proxy, you need to consider the following guidelines. See Appendix A, "SIMS as a Proxy Considerations," in the *Sun Internet Mail Server 4.0 Administrator's Guide* for different proxy scenarios, models, and configurations.

Why using SIMS as a Proxy?

The proxy servers provides two real solutions: one provides security by putting the proxy on the firewall and the backend mail server on the other side. The other is for the horizontal scalability to use multiple backend servers and multiple proxies.

See the *Sun Internet Mail Server 4.0 Concepts Guide* for definitions of the horizontal scalability, where large scale virtual hosting SP configurations is implemented. This guide also provides you with a horizontal scaleability scenario.

How Does a SIMS Proxy Work?

Typically, each user has a well-defined backend mail server but accesses a random proxy via a Domain Name System (DNS) round-robin. The advantage compared with just multiple servers without proxies is that all users access one single server name rather than each user having to configure their own mail host.

Once the client is authenticated on the proxy, it will contact the real mail host and redo the login using the same user name and password. After login, however, the proxy switches to a passive relay mode in which everything that comes from the client is passed onto the backend mail host and vice-versa without any interruption on the part of the proxy. Overly large machines should not be required for the proxies.

What to Consider to Install SIMS as a Proxy

When configuring for a number of users, you must look again at the total concurrent users planned for, the total number of users, the percentages of POP3 and IMAP4 that will be concurrent at peak times, and the size of the users' mailboxes. From this you can estimate the needs of the backend mail server or servers. The number of proxy servers that you need depends upon the model you choose; that is, corporate versus SP.

Note – Be sure that you install SIMS as a proxy on a clean system where no SIMS files are installed.

SIMS in SP Environments Considerations

The Sun Internet Mail Server (SIMS) product meets the needs of the corporate outsourcing services providers (SPs), by providing the following services:

- Virtual hosting support
- Vertical and horizontal scale ability support
- Delegated administration capability
- Provisioning tools
- Monitoring tools

See the *Sun Internet Mail Server 4.0 Concepts Guide* for the key features of SIMS, domain hosting capability, and different deployment scenarios for which SIMS could be installed.

Internet Message Transfer Agent Considerations

The IMTA component of SIMS requires the following information. Be sure that you have this information ready before you begin the installation by identifying the following:

1. If the message transfer agent is behind a firewall. If yes, which system will be responsible to route messages through the firewall.
2. Mail server domain name.
3. Organization top level domain name.

Role of an IMTA

Before you install an ensemble of mail servers, you should determine what role you will assign to the message transfer agent for each of the servers.

Two factors can help determine the role of an IMTA:

1. The IMTA's ability to route messages to a group of email users either by delivering the IMTA mail directly to local recipients or by forwarding the messages to the recipient's appropriate mail server for non local recipients.
2. The relative position of the mail server to the company's firewall. That is, whether the mail server is separated from the public Internet by a firewall machine, or the mail server is not separated from the public Internet by a firewall machine. In this case, your company does not have a machine serving as the firewall; or your mail server also serves as the firewall system.

IMTA's Ability to Route Messages

The SIMS product classifies the IMTA's ability to route messages in the following three ways:

1. The mail server does not support a user community. This setup is typical if your mail server is a backbone IMTA that routes messages between domains. It does not know of each mail user, but uses the host or domain specifications to forward the message to the appropriate mail server for delivery. For example, if a message

is sent to <*user*>@eng.stream.com, the IMTA knows to forward this message to mailhost.eng.stream.com. Similarly, it can forward a message addressed to <*user*>@qa.eng.stream.com to mailhost.qa.eng.stream.com.

2. The IMTA can only deliver messages to local users and not to non-local users. If a message arrives that is not addressed to a local user, the To: envelope address is not canonical and fully qualified (that is, it does not specify the address's information as <user>@host.domain), the IMTA forwards the message to a specified smart host. The smart host is more likely to be able to forward the message to the recipient's mail server.

3. The IMTA can route messages within its Internet domain or a specified set of domains. The mail server can forward a message to the recipient's mail server if the recipient belongs to one of the specified domains.

IMTA's Location Relative to a Firewall

If your company has not implemented a firewall around your mail network, the mail server queries the local or a public Internet domain name server before it forwards a message. However, if your mail server is located behind a firewall system, all messages to mail users outside your company's private mail network have to travel through the firewall's IMTA. Since your IMTA is not a firewall IMTA, it also cannot query the public DNS.

This means that each mail server's IMTA depends on a smarter IMTA (except the firewall machine's IMTA) that resides on the firewall machine or a smart host, to forward all messages that it cannot route directly. The smart host may or may not serve as the firewall system. If you have two separate machines, one serving as the smart host and the other serving as the firewall system, the IMTA can forward a message to a recipient in another subdomain to the smart host, and mail addressed to a recipient outside your organization to the firewall machine.

For example, the Stream Corporation, has implemented a firewall. If a user, joan@eng.stream.com, sends a message to pierre@sales.stream.com, the message is handled by Joan's mail server. Since Joan's mail server can route only to users within eng.stream.com domain, it forwards the message to its configured smart host, mailhost.stream.com. If mailhost.stream.com has the ability to route messages to stream.com, this mail will be routed directly to Pierre's mail server. However, if mailhost.stream.com serves as a pure backbone IMTA, with no ability to route messages directly to users, it will transit the message to a configured IMTA (specified in the mailhost.stream.com 's configuration) that can route directly within Pierre's mail domain, sales.stream.com.

In this example, `mailhost.stream.com` does not necessarily serve as the company's firewall system. So, if a message arrives addressed to `youri@net.com`, `mailhost.stream.com` will forward this message to the firewall machine. The firewall machine will then route the message across the public Internet to the `net.com` domain.

For information on how to configure an IMTA's location relative to a firewall and how to configure a smart host, see "To Configure IMTA Position Relative to the Internet" in Chapter 5, "Internet Message Transport Agent (IMTA) Administration" in the *Sun Internet Mail Server 4.0 Administrator's Guide*.

Sample IMTA Scenarios

Use the IMTA scenario that best matches your company's mail server setup plans in this section.

Mail Server Supporting Few Users in a Single Domain

The Stream Corporation has 1000 mail users and is part of the `stream.com` domain. Based on average mail use, Stream Corporation designates one machine as the mail server, `mailserver.acme.com`.

Since there is only one mail server for the entire company, it has to be able to route messages sent to any user in the `stream.com` domain.

If Stream Corporation has a firewall, locating the corporate mail server and the firewall on different machines is preferable. In this way, the firewall IMTA can be responsible for merely forwarding messages to and from the Internet to `mailserver.stream.com`. The `mailserver.stream.com` machine handles the task of distributing the mail to its user community.

Mail Server Supporting Many Mail Users in a Single Domain

Bravo Corporation has a larger mail community than Stream Corporation. As a result, it requires multiple mail servers to support its mail traffic. In this case, the company can designate multiple mail servers such as `mailserver1.bravo.com` and `mailserver2.bravo.com`.

Each mail user is assigned to one of these mail servers, either `mailserver1.brovo.com` or `mailserver2.bravo.com`. In other words, for a given user, a single mail server delivers its messages.

To route messages from one mail server to the other, at least one of the two mail servers must have the ability to route to every user in `bravo.com`. Bravo Corporation can also specify more than one IMTA with the ability to route with the `bravo.com` domain. This will increase the database lookup times (since the amount of addressing information cached by the average IMTA is greater) but reduce the message transfer time (by reducing the average number of hops messages have to go through to travel across the network).

Mail Server Supporting Mail Users in a Single Domain Divided into Subdomains

Net International Corporation has split its parent `xyx.com` domain into several subdomains. Each of the subdomains has at least one IMTA capable of resolving all addresses in the `xyx.com` domain.

Net Corporation has implemented a firewall that provides a single entry point for all incoming and outgoing mail from the corporation. The firewall machine is also the corporate backbone server.

If all incoming mail is addressed to one of the subdomains, the firewall IMTA can serve as a proxy IMTA. It can route messages to the various subdomains without looking up individual users. To set up your company mail distribution in a similar manner, configure your mail server to route to one channel per subdomain.

On the contrary, if an incoming message is addressed to <*user*>`@net.com`, the corporate IMTA must have the ability to resolve these addresses in order to forward messages to the appropriate subdomains. As the router IMTA, it also needs information on any additional configured SMTP router channels. SWAPNA decide on the following:

Creating A New Rewrite Rule Versus Creating A New Channel

Typically, if you want particular messages to be placed in a particular Internet Message Transfer Agent (IMTA) channel queue, you can create a new domain rewriting rule. For example, imagine that you want messages addressed to <*user*>`@corp.stream.com` to go into the Sun Message Store channel queue. Domain rewriting rules (or from this point forward, *rewrite rules*) are a tool that the IMTA uses to route messages to the correct queue and thereafter, host. For more information on rewrite rules, see the *Sun Internet Mail Server 4.0 Administrator's Guide*.

There are some situations in which rather than creating a new rewrite rule for an existing channel, creating a new channel may better serve your purposes. The following are examples of such situations:

- When you wish to isolate heavy message traffic to and from a particular address in the event of a mail server failure
- When your domain is divided into subdomains, you have implemented a smart host in each subdomain, and you wish to monitor mail traffic addressed to and from these subdomains

To illustrate the situation described in the first bullet, imagine that a large number of messages pass daily between two companies, Stream Corporation and Bravo Corporation. Stream's email administrator can elect to isolate message traffic addressed to and from Bravo by creating an SMTP channel that handles Bravo message traffic only. In this situation, if a problem arises with Bravo's mail server, Bravo's messages will back up in Stream's Bravo-exclusive SMTP channel only and will not affect message traffic in other channels.

To illustrate the situation described in the second bullet, imagine that Bravo Corporation has implemented multiple subdomains, for example, Corp, Eng, and Sales. In turn, Bravo has implemented a smart host in each subdomain. (A *smart host* is an IMTA in a particular domain to which other IMTAs acting as routers forward messages if they do not recognize the recipient.) Bravo's email administrator can elect to isolate messages routed to the smart hosts in the Corp, Eng, and Sales subdomains by creating a channel that handles mail traffic addressed to and from each of these subdomains. In this situation, the email administrator can monitor the volume of email addressed to and from each of these subdomains for any patterns, changes, and so on.

Unique User Identification

You must implement a unique user ID for each user in the following ways:

- If your organization is not divided into subdomains, you must implement a unique user ID for each user in the domain. For example, if Stream Corporation is composed of the domain `stream.com`, the user ID for each user, for example, `hgreen`, must be unique.
- If your organization is divided into subdomains, at a minimum, you must specify a unique user ID for each user in each subdomain. For example, imagine that the Bravo Corporation is composed of the domain `bravo.com` and `bravo.com` is further divided into the subdomains `eng.bravo.com`, `corp.bravo.com`, and `sales.bravo.com`. The email user Harold Green exists in the `eng.bravo.com` subdomain, Harvey Green exists in the `corp.bravo.com` subdomain, and Harry Green exists in the `sales.bravo.com` subdomain. You can implement the same user ID (`hgreen`) for each of these email users since they exist in separate subdomains. Their email addresses, respectively, would be `hgreen@eng.bravo.com`, `hgreen@corp.bravo.com`, and `hgreen@sales.bravo.com`. Alternatively, you can implement a unique user ID for each user in the domain. Using the same example, you could implement `haroldg`, `harveyg`, and `harryg`, respectively. Their email addresses,

respectively, would be `haroldg@bravo.com`, `harveyg@bravo.com`, and `harryg@bravo.com`. Note that when implementing unique IDs in a domain, email users would not have to specify a subdomain(s).

Sun also recommends that when email users specify addresses for email recipients, they specify a fully qualified domain name for each recipient. For example, to specify Harry Green from Bravo Corporation as the recipient of an email, Sun recommends specifying the following:

```
harry.green@sales.bravo.com
```

Specifying a fully qualified domain name minimizes email address ambiguities that in the worst case scenario could lead to an email being delivered to the wrong recipient.

Not specifying a fully qualified domain name places the responsibility of fully qualifying email addresses on the IMTA. The IMTA must be configured to perform this task via rewrite rules.

CHAPTER 6

What SIMS 4.0 Installs

This chapter shows the directories where Sun™ Internet Mail Server™ 4.0 packages, configuration files, and data files are stored. It also provides a list of packages as well as the scripts that Sun Internet Mail Server 4.0 installs.

- Contents directories
- Components packages
- Startup scripts

SIMS 4.0 Contents Directories

SIMS 4.0 installs packages, configuration and data files for each component of SIMS in the directories listed in TABLE 6-1.

TABLE 6-1 SIMS 4.0 Contents Directories

Type	Directory Path
Packages	`/opt/SUNWmail`
Configuration files	`/etc/opt/SUNWmail`
Data files	`/var/opt/SUNWmail`

See Chapter 3, “SIMS Software Requirements," for a list of software applications that are automatically installed if they don’t exist on the system already.

See Chapter 10, “Configuration Files," for a list of configuration files that Sun Internet Mail Server 4.0 installs.

SIMS 4.0 Installed Packages

TABLE 6-2 shows packages that are installed for the following SIMS components:

- Administration Console
- Administrative Command Line Interface
- Delegated Management Console
- Delegated Management Command Line Interface
- Internet Message Transfer Agent
- Message Transfer Agent SDK
- Message Store / Message Access
- Sun Directory Services
- Sun Web Access Server
- Sun Web Server
- SIMS Documentation
- SIMS High Availability

Note – Since Sun Directory Services (SunDS), Sun Web Access Server, and Sun Web Server (SWS) are not SIMS components, they are not installed in the `/opt/SUNWmail` directory mentioned in TABLE 6-1.

See Chapter 5, "SIMS Architecture," in the *Sun Internet Mail Server 4.0 Concepts Guide* for descriptions of each component of the Sun Internet Mail Server 4.0 along with their associated features.

TABLE 6-2 SIMS 4.0 Packages

SIMS Component Name Package Name	**Package Description**
SIMS Common Package	
SUNWimcom	Sun Internet Mail Server Common Package
SUNWimsch	Sun Internet Mail Server schema
SUNWimcoi	Sun Internet Mail Server startup scripts
Administration Console	
SUNWimads	Sun Internet Mail Administration Services Server side files
SUNWimadc	Sun Internet Mail Administration Services Client side files
Administrative Command Line Interface	
SUNWimclq	Sun Internet Mail Site Admin CLI Utilities platform binaries
SUNWimclj	Sun Internet Mail Site Admin CLI Utilities
SUNWimcln	Sun Internet Mail Site Admin CLI Utilities man pages
Delegated Management Console	
SUNWimdml	Delegated Management API Library
SUNWimdmp	Delegated Management CGI Program
SUNWimdms	Delegated Management Server
SUNWimdmi	Delegated Management Machine Independent files
SUNWimdmr	Delegated Management Configuration files
Delegated Management Command Line Interface	
SUNWimclr	Sun Internet Mail Administrative CLI utilities configuration
SUNWimclp	Sun Internet Mail Admin CLI Utilities platform binaries
SUNWimcli	Sun Internet Mail Administrative CLI Utilities
SUNWimclm	Sun Internet Mail Administrative CLI Utilities man pages
Message Transfer Agent	

TABLE 6-2 SIMS 4.0 Packages *(Continued)*

SIMS Component Name Package Name	**Package Description**
SUNWbbmto	Internet MTA Program Files
SUNWbbmtr	Internet MTA Configuration Files
SUNWimmtm	Internet MTA Man Pages, Common Pages
SUNWbbmtm	Internet MTA Man pkages
SUNWimmtv	Internet MTA, Data Files
Message Transfer Agent SDK	
SUNWimsdk	Sun Internet Mail SDK
SUNWimsdd	Sun Internet Mail SDK–documentation
SUNWimsdh	Sun Internet Mail SDK–developer package
Message Store/Message Access	
SUNWimimo	Internet Mail Message Store Libraries and Programs
SUNWimimr	Internet Mail Message Store Configuration
SUNWimimm	Sun Internet Mail Message Store man pages
Sun Directory Services (SunDS)	
SUNWsds	Sun Directory Services
SUNWsdsc	Sun Directory Services Client tools
Web Acess Server	
SUNWwa	Sun Web Access classes, images, html files, etc.
SIMS Documentation	
SUNWimols SUNWimola SUNWimolc SUNWimold SUNWimoli SUNWimolp SUNWimolf SUNWimoln SUNWimolw	Sun Internet Mail Server online documentation
High Availability	
SUNWimha	Sun Internet Mail Server High Availability package

Startup Scripts

SIMS provides the startup script `/etc/init.d/im.server`, which in turn executes the scripts listed in TABLE 6-3.

After installing SIMS, the administrator needs to run the `im.server` script to startup the SIMS server.

See Chapter 9, “Post Installation Tasks," for more information on the `im.server` script.

TABLE 6-3 Required Scripts Run by `im.server`

Script Name	Application Name
`mt.scheduler`	Message Store / Proxy server
`dsserv`	SunDS daemon (if SunDS is installed)
`httpd`	Web Server
`lic_mgr`	License Manager
`dsweb`	Web Gateway (if SunDS is installed)
`imta`	SIMS Internet Message Transfer Agent
`dm.server`	Delegated Management Server

CHAPTER 7

Installing SIMS 4.0

This chapter contains the instructions for installing Sun™ Internet Mail Server™ 4.0 by using the graphical interface (GUI).

Topics in this chapter include:

- Before installing SIMS 4.0
- Installing SIMS 4.0
- Installing SIMS optional features
- Installing the remote SIMS Administration console
- Installing the SIMS High Availability system
- After installing SIMS 4.0

If you are installing the SIMS High Availability system, refer to the Sun Cluster 2.2 documentation set to ensure that you have installed the necessary software and hardware required by the Sun Cluster.

You can revise the information you have provided during installation by using the SIMS Administration Console. See the *Sun Internet Mail Server 4.0 Concepts Guide* for information on the SIMS Administration Console and its capabilities.

Before Installing SIMS 4.0

Before installing SIMS 4.0, make sure that you have read the following chapters:

TABLE 7-1 Chapters Required before Installing SIMS 4.0

Chapter Number, Name	To Learn About...
1, Overview of SIMS 4.0	SIMS 4.0 changes, features
2, System Requirements	Platform, space, memory, client, SDS 3.1 requirements
3, Software and Configuration Requirements	SIMS and SIMS/HA software requirements, DNS configuration
4, Preparing to Install SIMS 4.0	NSDS, LDAP rollover, remote LDAP, clean system, patches
5, Planning to Configure SIMS 4.0	SIMS as a proxy, SP environment, and IMTA considerations
6, What SIMS 4.0 Installs	Lists of SIMS 4.0 packages and startup scripts

Installing SIMS 4.0

This section provides step-by-step instructions to install your Sun Internet Mail Server 4.0.

The installation steps are:

1. Run the `setup` installation script.
2. Select the optional features.
3. Specify the LDAP server information.
4. Specify the server configuration information.
5. Start the Setup script.

See “Installing SIMS Optional Features” on page 54 to install SIMS optional and add on features on your existing SIMS system.

See “Installing the SIMS High Availability System” on page 59 for instructions on installing the SIMS High Availability system.

See Appendix A, “Installing Netscape Directory Services for SIMS," for instructions to install NSDS with SIMS 4.0.

See Appendix B, “Installing Netscape Directory Services for SIMS High Availability," for instructions to install NSDS with the SIMS High Availability system 4.0.

Note – SIMS installation log files are located in `/var/opt/SUNWmail/log/SIMS_installation_log.`*n after* installation is complete, and are in `/tmp` *while* installation is in progress.

Running the Installation Script

1. **Log in as a non-root user.**
2. **Ensure that you have set the** `DISPLAY` **variable.**
3. **Insert the SIMS CD-ROM into the disk drive.**

   Make sure that your CD is mounted to the `/cdrom` directory.
4. **Change to the SIMS product directory.**

```
% cd /cdrom/sun_internet_mail_4_0
```

5. **Run the `setup` script from the software CD-ROM as non-root.**

```
% setup
```

This launches a web browser and then displays the first page of the SIMS 4.0 installation interface, as shown in FIGURE 7-1.

FIGURE 7-1 SIMS 4.0 Installation Top Page

Note – Running `setup` results in cleaning up the `/tmp` directory.

---

6. **Review the information pages and then click `Install` to install the SIMS 4.0 core and optional features.**

Note – See Chapter 1, “Overview of Sun Internet Mail Server 4.0," for a complete list features that comprise SIMS 4.0.

Selecting SIMS Optional Features

The next step after starting the installation process is to select the SIMS optional components that you can add to your SIMS server, as shown in FIGURE 7-2.

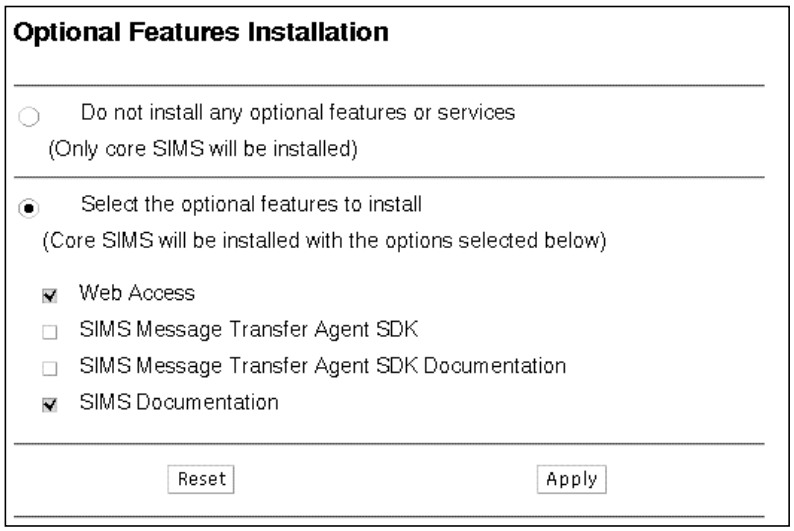


FIGURE 7-2 SIMS Optional Features

7. **Select the SIMS optional features that you wish to add to your SIMS server.**

   If you don't select any options, only the SIMS core components will be installed.

8. **Click `Apply` to go to the Directory Services Information page**.

FIGURE 7-3 The Directory Information Page

9. **Enter the required information on the Directory Services Information page.**

   Directory Services Server Name—The fully qualified domain name of the server on which the LDAP directory services are available; that is, either the Netscape Directory Services (NSDS) or the Sun Directory Services (SunDS).

   Directory Services Server Port—The port number of which the LDAP server uses. For NSDS, this is the port number that you used during the NSDS installation.

Note – If you would like your SIMS server to use a remote LDAP server (instead of using the local LDAP server), you need to specify the fully qualified domain name (FQDN) and the port number of the remote LDAP server as the Directory Services Server Name and the Directory Services Server Port number here. Be sure that your LDAP server is configured and run before you click `Apply` here.

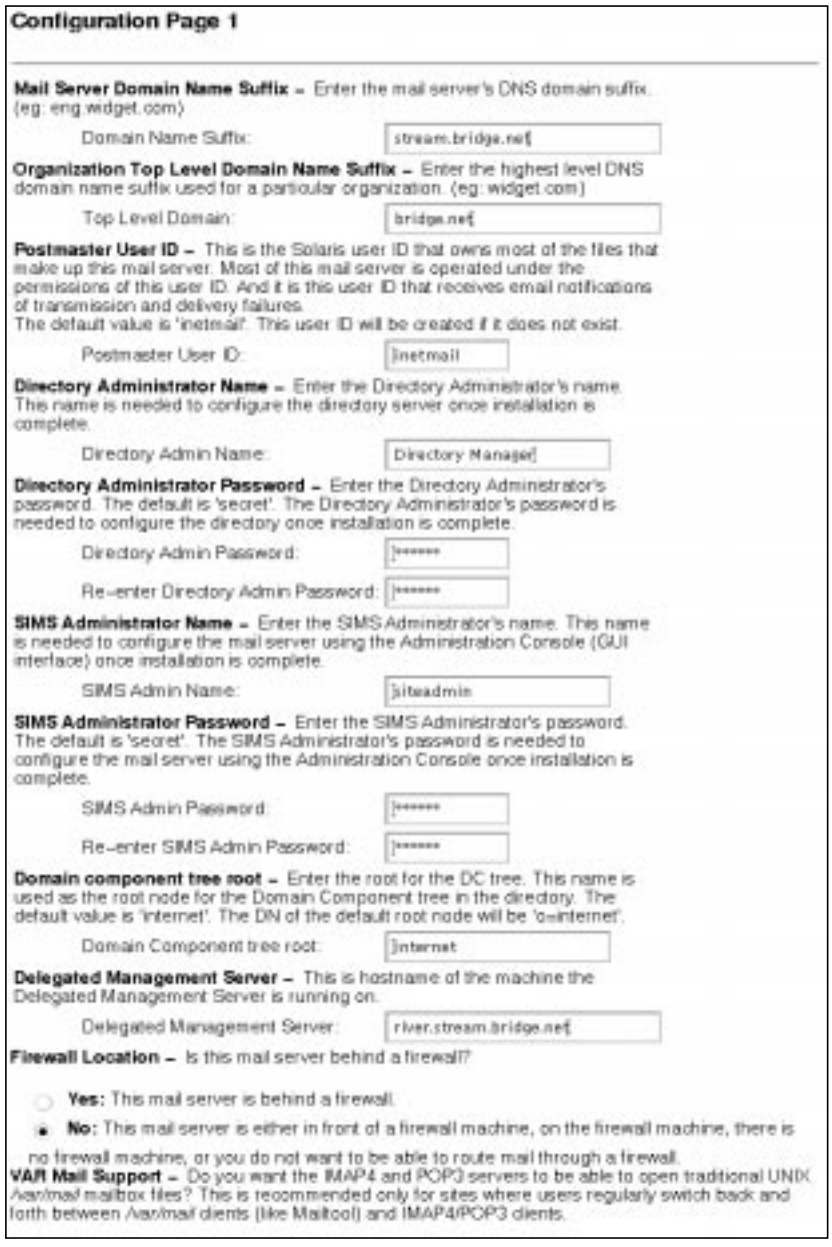
Note – If the local NSDS LDAP server, the remote NSDS, or the remote SunDS is not configured with the SIMS 4.0 schema, a warning displays at the top of the screen. Although you may choose to click `Apply` and continue the installation, you will need to manually perform certain configurations, as covered in "Preparing to Install SIMS with Remote LDAP" in Chapter 4, "Preparing to Install SIMS 4.0."

---

10. **Directory Services Type**—The directory services of your choice: Netscape Directory Services or Sun Directory Services. The Netscape Directory Services is the preferred directory to use with SIMS 4.0.

Specifying the Server Configuration

After entering the LDAP information, next you will be specifying your SIMS server configuration. FIGURE 7-4 shows the first page of the two server configuration pages.



Configuration Page 1

Mail Server Domain Name Suffix – Enter the mail server's DNS domain suffix. (eg: eng.widget.com)

Domain Name Suffix: stream.bridge.net

Organization Top Level Domain Name Suffix – Enter the highest level DNS domain name suffix used for a particular organization. (eg: widget.com)

Top Level Domain: bridge.net

Postmaster User ID – This is the Solaris user ID that owns most of the files that make up this mail server. Most of this mail server is operated under the permissions of this user ID. And it is this user ID that receives email notifications of transmission and delivery failures.
The default value is 'inetmail'. This user ID will be created if it does not exist.

Postmaster User ID: inetmail

Directory Administrator Name – Enter the Directory Administrator's name. This name is needed to configure the directory server once installation is complete.

Directory Admin Name: Directory Manager

Directory Administrator Password – Enter the Directory Administrator's password. The default is 'secret'. The Directory Administrator's password is needed to configure the directory once installation is complete.

Directory Admin Password: ******

Re-enter Directory Admin Password: ******

SIMS Administrator Name – Enter the SIMS Administrator's name. This name is needed to configure the mail server using the Administration Console (GUI interface) once installation is complete.

SIMS Admin Name: siteadmin

SIMS Administrator Password – Enter the SIMS Administrator's password. The default is 'secret'. The SIMS Administrator's password is needed to configure the mail server using the Administration Console once installation is complete.

SIMS Admin Password: ******

Re-enter SIMS Admin Password: ******

Domain component tree root – Enter the root for the DC tree. This name is used as the root node for the Domain Component tree in the directory. The default value is 'internet'. The DN of the default root node will be 'o=internet'.

Domain Component tree root: internet

Delegated Management Server – This is hostname of the machine the Delegated Management Server is running on.

Delegated Management Server: river.stream.bridge.net

Firewall Location – Is this mail server behind a firewall?

○ **Yes:** This mail server is behind a firewall.

● **No:** This mail server is either in front of a firewall machine, on the firewall machine, there is no firewall machine, or you do not want to be able to route mail through a firewall.

/var/mail Support – Do you want the IMAP4 and POP3 servers to be able to open traditional UNIX /var/mail mailbox files? This is recommended only for sites where users regularly switch back and forth between /var/mail clients (like Mailtool) and IMAP4/POP3 clients.

FIGURE 7-4 Configuration Page 1

11. Enter the values in the first SIMS configuration page.

You may accept the default configuration values if they meet the requirements of your mail server.

Mail Server Domain Name Suffix—The domain name of the mail server on which SIMS is being installed. For example, if this server resides in the `stream` domain at the site `bridge`, then specify `stream.bridge.net` in this field. This parameter has no default value. However, if installation can determine the domain name from `resolv.conf`, this value will be automatically supplied. This value can be the same as the Organization Top Level Domain Name field.

Note – SIMS 4.0 checks for a fully qualified domain name and will display error messages, depending on its finding. See Chapter 11, “Troubleshooting the Sun Internet Mail Server," for more information on configuring DNS setup.

Organization Top Level Domain Name Suffix—The highest level domain name used within your organization. For example, the top level domain name for an SP provider could be `bridge.net`. This value can be the same as the Mail Server Domain Name.

Postmaster User ID—The Solaris™ user listed in this field has permission to run all SIMS commands, programs, and `start` or `stop` daemons on the mail server. You will need this postmaster name to administer the mail server after installing SIMS. By default the installation assigns `inetmail` as the postmaster (the reserved user ID 72). Your input in this field should not exceed 64 characters. Although it is recommended that you use `inetmail`, you can change the default user name during the installation. You do not need to provide a password. However, the first time the postmaster logs into the mail server, the postmaster will be prompted for a new password before being able to execute any SIMS commands on the mail server.

Directory Administrator Name—The user name of the directory server administrator. The default name is `Directory Manager` for NSDS and `admin` for SunDS. After the installation is complete, the administrator can use the SIMS Administration Console to configure the directory server. Your input in this field should not exceed 64 characters. The name you provide in this field is logged in the directory configuration file so that the administrator always has access to the directory. This enables the administrator to solve problems associated with access control.

Directory Administrator Password—The password for the directory server administrator. The default password is `secret` for SunDS. For NSDS, you enter the password that you provided for the `Directory Manger`. Once the installation is complete, the Directory Administrator’s password is needed to configure the directory server using the SIMS Administration Console. The password you provide in this field is logged in the directory configuration file. By default, this password is stored encrypted.

SIMS Administrator Name—The user name for the SIMS Administrator at the site who administers the SIMS server, including performing delegated management tasks. The SIMS Administrator is a real user in the directory and has been granted access to the entire LDAP directory through special Access Control Lists (ACLs).

SIMS Administrator Password—The password associated with the SIMS administrator. The default password is `secret`.

Domain Component Tree Root—The node name for the root of the Domain Component (DC) tree for which SIMS is installed. The default is `internet`. This will cause the DC tree to be rooted at the node `o=internet`. See the *Sun Internet Mail Server 4.0 Concepts Guide* for more information on the DC tree structure for SIMS 4.0.

Delegated Management Server—The fully qualified domain name (FQDN) of the Delegated Management server from which all requests from the hosted domains are accessed.

Firewall Location—Choose the button that best indicates the location of your mail server in relationship to your company's firewall machine. The firewall controls access between the Internet and your company's internal network.

No—Indicates that your mail server is on or outside the firewall, or if your company has no firewall.

Yes—Indicates that your mail server is behind a firewall. You will then be asked to specify the name of the smart host, which is the machine with more routing information and capabilities than your mail server.

Smart Host—If you chose to put your mail server behind a firewall, you need to enter the fully qualified host name of the machine that has the routing information about your mail server. If your mail server cannot route mail to a recipient's address, it forwards the message to its smart host.

A smart host usually knows how to route messages through your company's firewall. Without routing information, the mail server cannot forward messages *outside* the firewall. It may only be able to communicate with machines in its own domain, specified domains, or with its peers. In small companies, the smart host may also serve as the firewall machine, providing a communication link between the company and the outside mail community. If neither the smart host nor the firewall machine can route a recipient's address, they return the message to the sender with a non delivery notice.

VAR Mail Support— Click on the button that best indicates your company's plans for this mail server. SIMS supports both `/var/mail` and Sun Message Store users. Sun Message Store that runs under the user id `inetmail` is more secure than `/var/mail` that runs as root. Refer to the *Sun Internet Mail Server 4.0 Administrator's Guide* for migration instructions.

Note – `/var/mail/` is only supported for the default domain and not for the hosted domains.

---

12. **Click `Apply` to go to the second page of the configuration pages.**

    Your input in the form fields is saved to a file and the next configuration page displays.

13. **Enter information on the Configuration Page 2.**

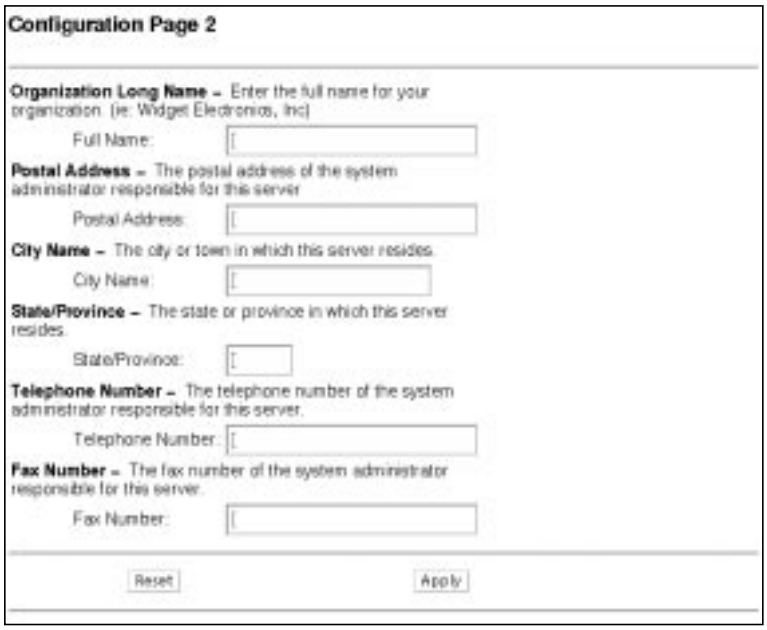


FIGURE 7-5 Configuration Page 2

Your input in this form is optional.

Organization Long Name—Enter your full company name.

Note – This should not be the same as Organization Name shown in Step 13 above.

Postal Address—Enter the street address of the individual who administers this mail server.

City Name—Enter the city name in which your mail server resides. Your input in this field should not exceed 128 characters.

State/Province—Enter the state name in which your mail server resides. Your input in this field should not exceed 128 characters.

Telephone Number—Enter the telephone number of the individual administering this mail server.

Fax Number—Enter the fax number of the individual who administers this mail server.

14. **Click `Apply` to go to the Configuration Summary page.**

    This page shows how you specified the configuration of your SIMS system.

Running the Setup Installation

After selecting SIMS optional components and specifying configurations for both core and optional components, you are now ready to begin installing SIMS 4.0.

15. **Click `Start Install` in the Configuration Summary page, if the information you provided in all the forms is accurate.**

    If the command tool is not invoked automatically, verify that your `DISPLAY` variable is set correctly. You will then need to restart the software. If the command tool is not available, an error message will be displayed. Check the patch to the command tool or your operating system setup.

16. **Enter the root password at the password prompt.**

17. **Enter the SIMS Postmaster's password.**

    You may not see the screen to enter your password during your installation session. This screen will only appear if the user `inetmail` does not exist on your system.

    Look for any warnings or error messages that may display as the installation proceeds.

18. **Press `Enter` to exit the command tool window when prompted.**

    The Installation Summary page displays.

19. **Select `Exit` from the browser File menu to quit out of the GUI installation interface.**

    You have now successfully installed SIMS 4.0.

20. **If you have installed any patches during the installation, reboot your system now. Otherwise, go directly to Step 18.**

```
# sync; sync; init 6
```

21. **If you choose to reboot your system later, start the mail server.**

```
# /etc/init.d/im.server start
```

See “After Installing SIMS 4.0” on page 68 for a roadmap of post installation configurations and tasks.

Installing SIMS Optional Features

The following are SIMS 4.0 optional features that you may choose to add to your SIMS core server. Additionally, you can install these features as standalone components on servers where SIMS is not installed.

- Sun Web Access
- Message Transfer Agent SDK
- SIMS 4.0 Documentation Set
- Remote Administration Console

See Chapter 5, "SIMS Architecture," in the *Sun Internet Mail Server 4.0 Concepts Guide* for overviews of each components of SIMS.

To install SIMS optional features:

1. **Follow steps 1 through 6 in "Running the Installation Script" on page 43 under the heading "Installing SIMS 4.0" on page 42.**

   The Optional Features Installation page displays, as shown in FIGURE 7-6.

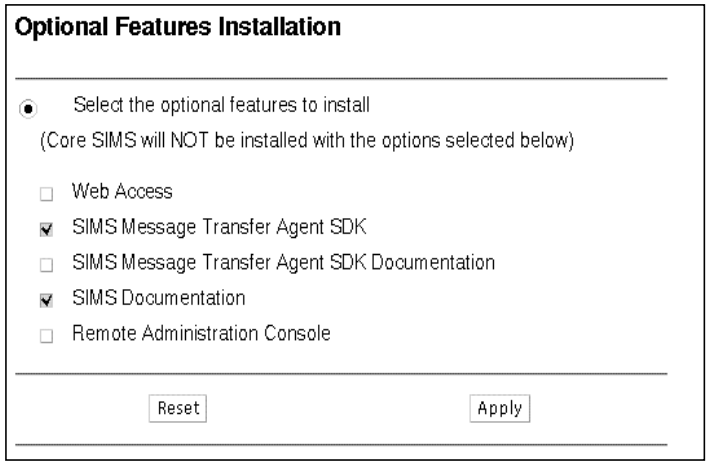


FIGURE 7-6 SIMS Optional and Add On Features

2. **Select the SIMS optional feature that you wish to add to your SIMS server or install as an standalone component.**
3. **Click `Apply` to go to the Directory Services Information page.**
4. **Follow steps 8 through 10 in "Specifying the LDAP Server Configuration" on page 46 under the heading "Installing SIMS 4.0" on page 42.**

5. **Click `Apply` to go to the Configuration Page 1.**

   The Configuration Page 1 for the SIMS optional features is shown in FIGURE 7-7.

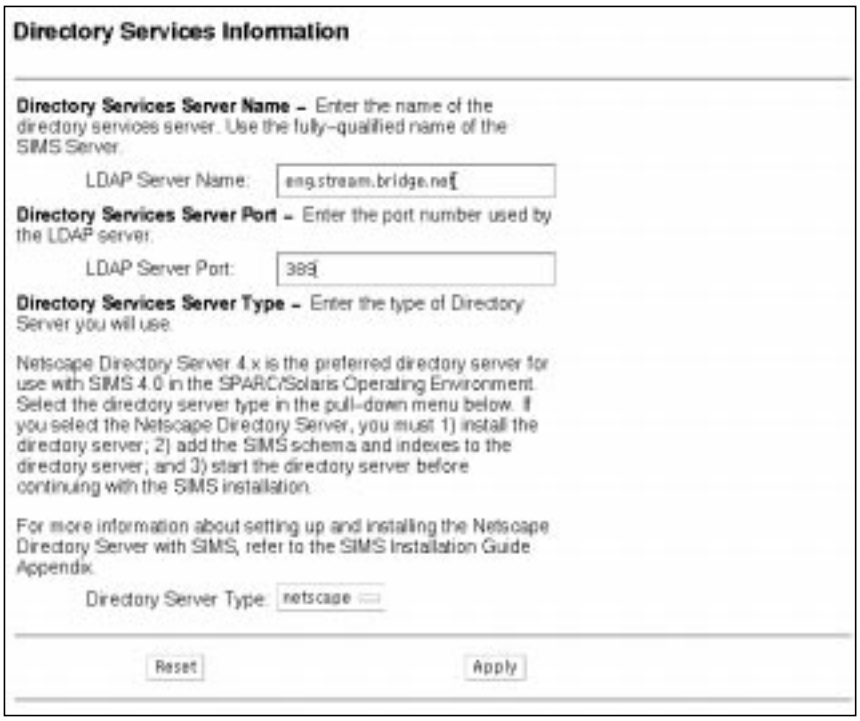


FIGURE 7-7 Configuration Page 1 Screen for SIMS Optional Features

6. **Specify the server configuration on which the optional or standalone component will be installed.**

   Mail Server Domain Name Suffix—The domain name of the mail server on which the optional feature or standalone component is being installed. For example, if this server resides in the `stream` domain at the site `bridge`, then specify `stream.bridge.net` in this field. This parameter has no default value. However, if installation can determine the domain name from `resolv.conf`, this value will be automatically supplied. This value can be the same as the Organization Top Level Domain Name field.

   Organization Top Level Domain Name Suffix—The highest level domain name used within your organization. For example, the top level domain name for an SP provider could be `bridge.net`. This value can be the same as the Mail Server Domain Name.

Postmaster User ID—The Solaris™ user listed in this field has permission to run all SIMS commands, programs, and start or stop daemons on the mail server. You will need this postmaster name to administer the mail server after installing SIMS. By default, the installation assigns `inetmail` as the postmaster (the reserved user ID 72). Your input in this field should not exceed 64 characters. Although it is recommended that you use `inetmail`, you can change the default user name during the installation. You do not need to provide a password. However, the first time the postmaster logs into the mail server, the postmaster will be prompted for a new password before being able to execute any SIMS commands on the mail server.

Domain Component Tree Root—The node name for the root of the Domain Component (DC) tree for the server on which SIMS optional features or standalone components are being installed. The default is `internet`. This will cause the DC tree to be rooted at the node `o=internet`. See the *Sun Internet Mail Server Concepts Guide* for more information on the DC tree structure for SIMS 4.0.

7. **Click `Apply` to go to the Configuration Summary page.**
8. **Follow steps 15 through 21 in “Running the Setup Installation” on page 52 under the heading “Installing SIMS 4.0” on page 42.**

Installing the Remote SIMS Administration Console

You can administer the SIMS product from either Microsoft Windows 95, Windows NT 4.0, or Solaris™ systems.

Note – It is recommended that you do not run the SIMS Administration console on a dual boot machine running *both* Windows 95 and Windows NT. The console will experience a `NullPointerException` error, which will cause problems loading the main page.

▼ To install on Windows 95 or Windows NT 4.0

1. **Insert the SIMS 4.0 CD-ROM into the CD-ROM drive.**

   The CD-ROM Autoplay starts, displaying two options: View README and Install. If the Autoplay screen does not appear after a few seconds, then continue with step 3 below.

2. **Click the `Install` button.**

3. **Click the `Start` button.**

4. **Click the `Run` button.**

5. **Run the `setup` script.**

   ```
   <cdrom_drive_letter>:\win35\setup.exe
   ```

   Running the `setup` script begins the installation program.

▼ To install on Solaris™ systems

1. **Follow steps 1 through 6 in "Running the Installation Script" on page 43 under the heading "Installing SIMS 4.0" on page 42.**

   This starts the SIMS GUI Installation `setup` script as a non-root user.

2. **Click `Install`.**

   FIGURE 7-8 displays.

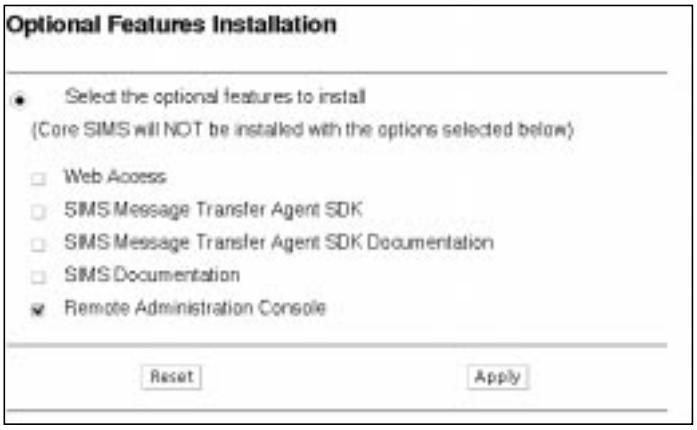


FIGURE 7-8 SIMS Optional Features Screen

3. **Select the Remote Administration Console feature.**

4. **Click `Apply`.**

   The Summary page displays as shown in FIGURE 7-9.

FIGURE 7-9 Remote Administration Console Configuration Summary Page

5. **Click `Start Install` by following the steps 15 through 21 in "Running the Setup Installation" on page 52 under the heading "Installing SIMS 4.0" on page 42.**

Installing the SIMS High Availability System

Installing the SIMS High Availability system must be done as a new installation followed by migrating users to the High Availability system. An existing SIMS installation cannot be simply upgraded to an HA installation.

SIMS High Availability installation is controlled by the SIMS installation script. If you are installing SIMS on an HA cluster, the SIMS installation script provides the HA installation.

Your SIMS software will be installed in the directory `/opt`. The HA software, however, will be installed in directory `<ha-dir>/opt`, where `<ha-dir>` is defined by you during the installation.

This section contains the instructions for installing the SIMS High Availability by using the graphical user interface (GUI). First you will be installing the SIMS High Availability on the machine where HA will be primarily used. Next, you will install HA on the machine where HA will be used as a backup to the primary machine.

See Chapter 12, “SIMS Asymmetric High Availability System," for information on the SIMS High Availability system configuration and fail over information.

See the Sun Cluster documentation set for information on commands that are used in this section and for information on packages installed by Sun Cluster.

Note – SIMS High Availability installation must be fresh and cannot be upgraded.

▼ To prepare before installing SIMS/HA

Before installing the SIMS High Availability system, make sure that you have completed the following steps:

1. **Install SunOS.**
2. **Install the Sun Cluster 2.2 software.**
3. **Install Veritas File System (VxFS) 3.3.2 (or later release).**
4. **Start the cluster.**
5. **Set up a logical host name for your HA machine.**

   Use the Sun Cluster documentation set to set up this host name. The disk group or groups that belong to this logical host name must contain sufficient space to store the SIMS product, configuration files, message store, message queues, and directory.

6. **Remove any existing SIMS software as root to allow fresh installation of SIMS/HA**.

   See for instructions on how to remove the SIMS/HA system.

7. **Ensure that the following shared volumes names were not used:**

   ```
   /opt/SUNWmail
   /opt/SUNWconn
   /var/opt/SUNWmail
   /var/opt/SUNWconn
   /etc/opt/SUNWmail
   /etc/opt/SUNWconn
   ```

8. **Ensure that multiple shared volumes for shared files were not used.**

   The SIMS High Availability installs all shared files on only one shared volume. For example, you cannot have `/opt/SUNWmail` on one volume and `/opt/SUNWconn` on another volume.

▼ To install the SIMS High Availability system

Installing the SIMS High Availability involves installing the software first on the machine where SIMS/HA will be primarily used. The next step is to install SIMS/HA on the machine that will be used as a backup for the SIMS/HA system. The steps are as follow:

1. **Login as root.**

   ```
   $su
   Password: <Enter your root password>
   ```

   Note – Use your system administration console screen to monitor the steps for installing SIMS on both primary and secondary machines.

2. **Change the directory to where your Sun Cluster software resides.**

3. **Check if you are already on the master machine where HA will be primary used.**

   ```
   # ./haget -f mastered
   ```

   If this command returns a logical host name, you are already on the master machine and can skip to step 5. But if you are not on the master machine, it returns nothing.

Caution – If the logical host name returned above is not known to DNS, SIMS/HA will not install. Additionally, the logical host name must NOT be a DNS alias.

4. **Switch over to the primary HA machine.**

```
# ./haswitch <local-machine> <ha-logical-hostname>
```

Where,
local-machine is the logical host name for the machine on which the SIMS High Availability will be primarily used, for example, *ha-primary*, and
ha-logical-hostname is the logical host name assigned to the HA machine, for example *active-ha*.

5. **Follow steps 1 through 6 in "Running the Installation Script" on page 43 under the heading "Installing SIMS 4.0" on page 42.**

This starts the SIMS GUI Installation `setup` script as a non-root user.

6. **Click `Install` next to install the SIMS core and optional features.**

7. **Select the High Availability option, as shown in** FIGURE 7-10**.**

FIGURE 7-10 SIMS High Availability System

8. **Follow steps 8 through 10 in “Specifying the LDAP Server Configuration” on page 46.**

9. **Select the logical host name of the machine on which you install SIMS.**

   An HA cluster can support several logical hosts that are *mastered* on the same physical host. During a *failover*, the logical host is moved from the physical host that is failing to another available physical host. As part of this switch over process, all the services running on the logical host also get transferred to the new physical host. This question allows you to select the logical host name with which SIMS services are to be associated.

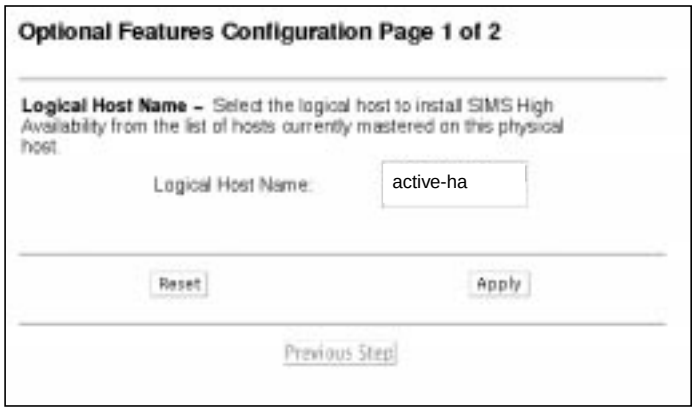


FIGURE 7-11 SIMS/HA Logical Host Name

10. **Specify the shared file system where the SIMS 4.0 HA software will reside.**

    This is the location of the shared disk on which the HA and SIMS software will reside. As shown in FIGURE 7-12**, s**elect a shared disk from the list of available shared disks on your system, for example, */active-ha/disk1*. These available shared disks should have already been specified by Sun Cluster.

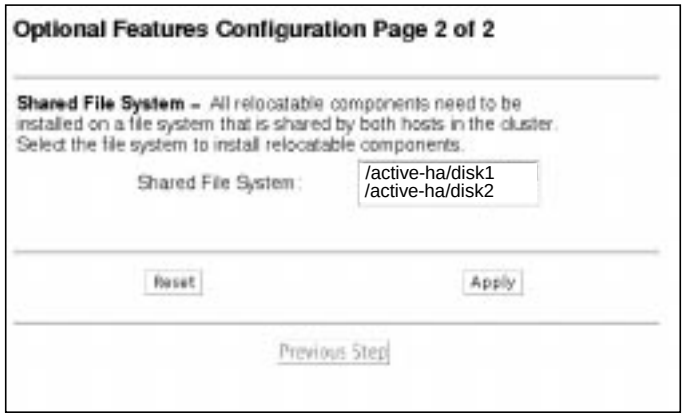


FIGURE 7-12 SIMS / HA Shared File System

During installation, SIMS checks to ensure that the shared file system has sufficient disk space.

Note – Record the name of the shared disk that you are selecting. Use the same name during SIMS / HA installation on the secondary machine.

---

11. **Follow steps 15 through 21 in "Running the Installation Script" on page 43 under the heading "Installing SIMS 4.0" on page 42.**

    This displays the summary page and runs the `setup` script.

    You are now done with installing the SIM High Availability on the primary machine. Next, you will be installing the SIMS High Availability on the secondary machine.

12. **Switch over to the secondary HA machine.**

```
# ./haswitch <local-machine> <ha-logical-hostname>
```

    Where,
    local-machine is the host name of the machine on which SIMS / HA will be used as the secondary machine, for example, *ha-secondary*, and
    ha-logical-hostname is the logical name assigned to the HA machine, for example *active-ha*. This is the same host name that you selected in step 9 above.

13. **Install SIMS/HA on the secondary machine from the command-line.**

```
% ./setup_tty.secondary -f <shared-file-system>
```

Where *shared-file-system* is the shared disk that you selected in step 10 above. As in the example shown in FIGURE 7-12, you may have selected */active-ha/disk1* as the shared disk on which HA and SIMS files were stored.

14. **If you have installed patches, you need to stop the node before rebooting.**

If you did not install any patches, skip to the next step following next.

```
# /opt/SUNWcluster/bin/scadmin stopnode
```

15. **Reboot the machine on which you have installed the patches.**

If you did not install any patches, skip to the next step.

16. **Start up the SIMS services under the HA framework.**

```
# /opt/SUNWhadf/bin/hareg -y Sun_Internet_Mail
```

You are now done with installing the SIMS High Availability on both primary and secondary machines.

FIGURE 7-13 illustrates the SIMS High Availability system after it is fully installed on both the primary and secondary machines.

Note – SIMS supports failure detection and consequent fail over at the hardware and operating system level. Failure at the SIMS service level, such as message access becoming unavailable while the rest of the system remains functional, are not detected and do not cause automatic fail over.

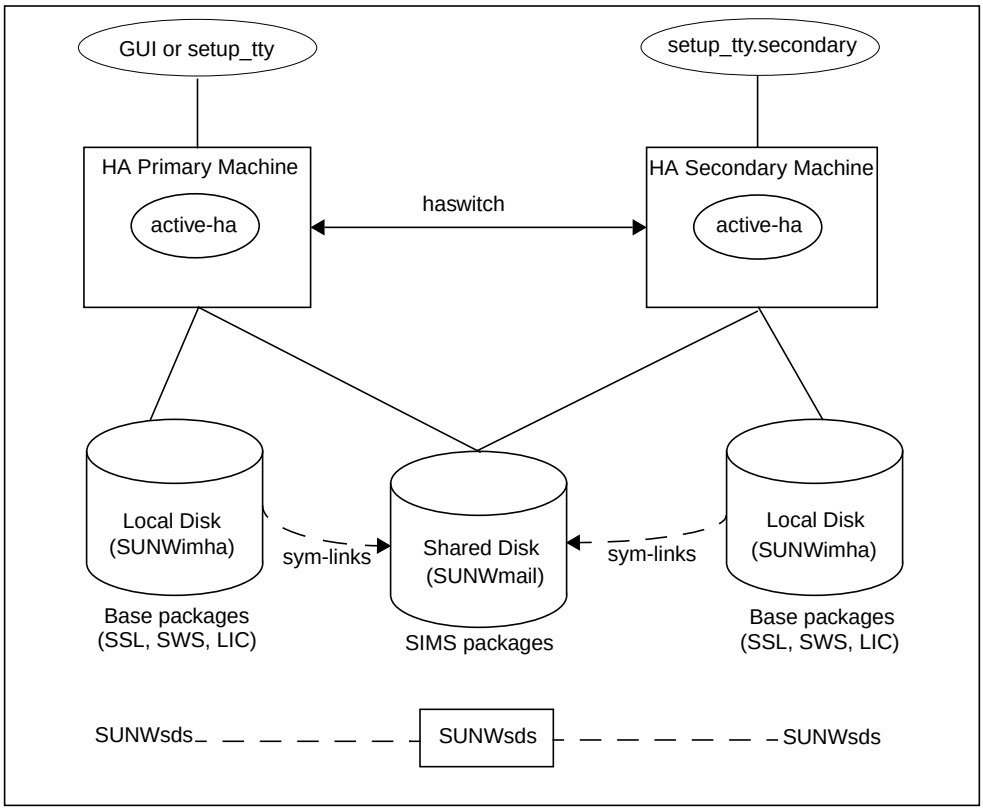


FIGURE 7-13 SIMS / HA System

If you choose to reboot your SIMS / HA system after installing the software, restart your Sun Cluster software by going to steps 17 and 18 below. Otherwise, see “Starting SIMS Administration Console for High Availability Systems” on page 77 in Chapter 9, “Post Installation Tasks," for instructions on invoking the SIMS Administration Console.

17. Restart Sun Cluster on the primary SIMS/HA machine.

```
# /opt/SUNWcluster/bin/scadmin startcluster
<local-machine> <cluster-name>
```

Where,

local-machine is the name of the primary SIMS High Availability machine, and *cluster-name* is the name of your Sun Cluster.

18. **Restart Sun Cluster on the secondary machine.**

```
# /opt/SUNWcluster/bin/scadmin startnode <cluster-name>
```

See “After Installing SIMS 4.0” on page 68 for a roadmap of post-installation configurations and tasks.

Note – After you have installed the SIMS High Availability, you need to configure the Netscape browser property files by setting the default security level to low. See “Netscape Browser Configuration” on page 70 in Chapter 9, “Post Installation Tasks," for instructions on configuring the Netscape browser.

Removing the SIMS High Availability System

SIMS installs files on the shared file disk as well as on the local disks for the primary and secondary SIMS/HA machines as shown in FIGURE 7-13 above. To completely remove SIMS/HA software, you need to delete files from all three locations.

To accomplish this, use the `uninstall` command that is available from both `SUNWmail` and `SUNWimha` directories.

The first time `uninstall` is used, it is available on both `/opt/SUNWmail/sbin` and `/opt/SUNWimha/sbin` directories. However, once it is removed from the shared disk, the `uninstall` command for the secondary machine is available on the other local disk only in the `/opt/SUNWimha/sbin` directory.

The following steps completely remove the SIMS High Availability from the shared disk and the two local disks.

1. **Check to see if you are already on the master machine.**

```
# ./haget -f mastered
```

If this command returns a logical host name, you are already on the master machine and can skip to Step 3. If you are not on the master machine, it returns nothing.‘

2. **Switch over to the secondary HA machine.**

```
# ./haswitch <local-machine> <ha-logical-hostname>
```

Where,
local-machine is the machine on which SIMS/HA will be used secondary, for example, *ha-secondary*, and
ha-logical-hostname is the logical name assigned to the HA machine, for example, *active-ha*.

3. **Uninstall on the** *secondary* **machine from the following location.**

```
# /opt/SUNWmail/sbin/uninstall -d sims
or
# /opt/SUNWimha/sbin/uninstall -d sims
```

This removes all files from both the `SUNWmail` on the shared disk and `SUNWimha` on the local disk of the secondary machine. See FIGURE 7-13.

4. **Switch over to the primary HA machine.**

```
# ./haswitch <local-machine> <ha-logical-hostname>
```

Where,
local-machine is the logical name for the machine on which SIMS/HA will be primary used, for example, *ha-primary*, and
ha-logical-hostname is the logical host name assigned to the HA machine, for example *active-ha*.

5. **Uninstall on the primary machine from the following location.**

```
# /opt/SUNWimha/sbin/uninstall -d sims
```

This removes all files from `SUNWimha` on the local disk of the primary machine.

After Installing SIMS 4.0

After you have completed installing or upgrading to SIMS 4.0, be sure that you read the following chapters:

Note – After you have installed SIMS, be sure to configure the Netscape browser property files by setting the default security level to low. See “Netscape Browser Configuration” on page 70 in Chapter 8, “Post Installation Configurations," to configure the Netscape browser.

TABLE 7-2 Chapters Required after Installing SIMS 4.0

Chapter Number, Name	To Learn About...
8, Post Installation Configurations	Netscape browsers and SIMS as a proxy configurations
9, Post Installation Tasks	Starting and testing your SIMS server. Starting SIMS Administration and Delegated Management consoles, Web Access, directories. You may go directly to this chapter
11, Troubleshooting SIMS Server	DNS setup configuration, log files, removing sendmail, rebooting after re-installing
App A, Installing NSDS for SIMS	Instructions to install NSDS 4.1 and configure it for SIMS 4.0
App B, Installing NSDS for SIMS/HA	Instructions to install NSDS 4.1 and configure it for SIMS/HA 4.0
Sun Internet Mail Server 4.0 Web Access Guide	Set up, configure, and administer the Sun Web Access.

CHAPTER 8

Post Installation Configurations

After you have installed Sun™ Internet Mail Server™ 4.0, you need to configure the Netscape browser that you will be using to run the SIMS Administration Console. You may also need to further configure your server if you have selected the Sun Web Access optional feature.

Topics in this chapter include:

- Netscape browser configuration
- Preparing configuration file for mail users only

Netscape Browser Configuration

If you are using the Netscape browser to start the SIMS Administration Console, you need to configure the preferences file as shown below.

▼ To specify the security level for Netscape browser

1. **Close all Netscape browser windows.**
2. **Change the directory.**

```
% cd ~/.netscape
```

3. **Edit the `preferences.js` file.**
4. **Add the following statement to the `preferences.js` file.**

```
user_pref("signed.applets.codebase_principal_support",true);
```

5. **Save the file.**
6. **Start the Netscape browser and then the SIMS Administration Console.**

   See Chapter 9, “Post Installation Tasks" for instructions on how to start the SIMS Administration Console.

   If you are installing the console from the SIMS CD on Windows 95 or Windows NT, the security is automatically set in the `properties` file.

   If you are running the console from Windows 95 or Windows NT, then the Netscape Browser is installed in the directory `.netscape`

Preparing the Configuration Files for Mail Users Only

If you selected the Sun Web Access optional feature during the installation, the `imldifsync.groups.conf` and `imldifsync.users.conf` configuration files will contain entries that supports both Calendar users and SIMS mail users. If, however, you wish to populate the directory for the mail users only, you need to remove the Web Access entries from the `imldifsync.groups.conf` and `imldifsync.users.conf` files. The steps are shown below:

▼ To populate the directory for mail users only

1. **Login as root.**

```
% su
Password: <Enter your root password>
```

2. **Edit the configuration files.**

```
# /usr/bin/vi /etc/opt/SUNmail/dir_svc/imldifsync.groups.conf
# /usr/bin/vi /etc/opt/SUNmail/dir_svc/imldifsync.users.conf
```

3. **Find the following line in these configuration files.**

```
option = {"generate=SIMSmail", "generate=IMCalendar"}
```

4. **Remove the following statement from this line.**

```
"generate=IMCalendar"
```

5. **The result will look like the following.**

```
option = {"generate=SIMSmail"}
```

6. **Save your changes and exit the editor.**

   You may now use these modified files `imldifsync.groups.conf` and `imldifsync.users.conf` to populate the directory for mail users only. See Chapter 9, “Sun Directory Services Administration” in the *Sun Internet Mail Server 4.0 Administrator’s Guide* for detailed instructions on populating the directory.

CHAPTER 9

Post Installation Tasks

After you have installed Sun™ Internet Mail Server™ 4.0 or the SIMS High Availability system, you are now ready to start up you server. This chapter provides you with steps to start your SIMS server as well as a procedure to test your new server.

- Overview SIMS post installation tasks
- Adjusting the IMTA dirsync and impurge schedules
- Building the IMTA table
- Configuring dirsync and impurge
- Checking SIMS installation log files
- Starting the mail server
- Linking to an existing Sun Web Server
- Accessing the manual pages
- Accessing the online documentation
- Starting the SIMS Administration Console
- Starting SIMS Administration Console for HA Systems
- Starting the Sun Web Access server
- Starting the Sun Directory Services
- Starting the Delegated Management server
- Populating the directory
- Starting the Delegated Management Console
- Migrating mail folders
- Testing your SIMS 4.0 server

Overview of SIMS Post Installation Tasks

The following are the steps that you need to take after you have installed SIMS:

1. Adjust the IMTA dirsync and impurge schedules.
2. Build the IMTA table.
3. Configure dirsync and impurge
4. Check the SIMS installation log files.
5. Start the mail server.
6. Link to an existing Web Server.
7. Access the manual pages.
8. Accessing the online documentation
9. Start the SIMS Administration Console.
10. Start the SIMS Administration Console for High Availability systems.
11. Start the Sun Web Access server.
12. Start the Sun Directory Services.
13. Start the Delegated Management server.
14. Populate the directory.
15. Start the Delegated Management Console.
16. Migrate mail folders.
17. Testing your SIMS 4.0 server.

Checking SIMS Installation Log Files

SIMS records installation activities in log files located in `/var/opt/SUNWmail/log/SIMS_installation_log.`*n*, where *n* is the date and time stamp of the form *YYMMDD.HR:MM*. This number is generated automatically. For example, `SIMS_installation_log.97112012:40`.

Note – During installation, the log file is created in the `/tmp` directory. It is then moved to the directory `/var/opt/SUNWmail/log` after installation is completed.

Starting the Mail Server

After checking the log file, the next step is to start the mail server daemon `im.server`. This script invokes several startup scripts, including Message Store, IMTA, and Sun Directory Services daemons.

To activate `im.server`, run the following command as root.

```
# /etc/init.d/im.server start
```

The `im.server` script is provided by SIMS, which in turn executes other scripts. After installing SIMS, the administrator needs to run this script to startup the SIMS server.

See “Startup Scripts” on page 39 in Chapter 6, “What SIMS 4.0 Installs," for a list of components that the `im.server` script starts.

Linking to an Existing Sun Web Server

If while installing SIMS an HTTP server is not already running on port 80 of the mail server, SIMS will install the Sun Web Server. SIMS then automatically connects the `http://`<*machinename*>`/sims` URL to the SIMS main page, which is located on `/opt/SUNWmail/html/index.html`.

However, if your HTTP server is already running on the mail server, you need to manually link the `index.html` SIMS main page to the server where your SIMS server resides. Use the documentation for your Sun WebServer to establish this link.

Accessing the Manual Pages

The SIMS 4.0 manual pages that are accessible via the `man` command reside in the `/opt/SUNWmail/man` directory. Optionally, you may want to add this directory to your `$MANPATH` variable in your `.login`, `.cshrc`, or `.profile` file by entering the following command:

```
% setenv MANPATH $MANPATH\:/opt/SUNWmail/man
```

The man pages for the LDAP directory server are in `/opt/SUNWconn/man` and should also be added to your `$MANPATH`.

Accessing the Online Documentation

If you installed the SIMS 4.0 documentation set from the product CD, use the following URL to access the online documentation:

```
http://<machinename>/sims/en/DocSet.html
```

where, <*machinename*> is the machine on which SIMS is installed.

Starting the SIMS Administration Console

To start the SIMS Administration Console, do the steps in this section.

Note – Be sure to have configured your Netscape browser as described in Chapter 8, "Post Installation Configurations."

---

1. **Bring up the Netscape browser.**

```
% netscape
```

2. **Start the SIMS Administration Console from the browser.**

```
http://<sims-machinename>/sims/
```

where <*sims-machinename*> is the name of the server on which SIMS is installed.

Starting SIMS Administration Console for High Availability Systems

To start the Administration Console for a SIMS High Availability system, follow the steps in this section:

1. **Stop the HTTP daemon as a root user.**

```
# /etc/init.d/httpd stop
```

2. **Restart the HTTP daemon.**

```
# /etc/init.d/httpd start
```

Note – Be sure to have already configured the Netscape browser as described in Chapter 8, "Post Installation Configurations."

---

3. **Bring up the Netscape browser.**

```
% netscape
```

4. **Start the SIMS Administration Console for the High Availability system.**

```
http://<ha-logical-hostname>/sims/
```

Where *ha-logical-hostname* is the logical name assigned to the HA machine that you used during installing SIMS/HA, for example, *relo-up*.

See “Installing the SIMS High Availability System” on page 59 in Chapter 7, “Installing SIMS 4.0," for instructions for installing the SIMS High Availability system.

See Chapter 12, “SIMS Asymmetric High Availability System," for HA configuration information.

See the *Sun Internet Mail Server 4.0 Concepts Guide* and the *Sun Internet Mail Server 4.0 Administrator’s Guide* for information on the SIMS Administration Console.

Adjusting IMTA dirsync and impurge schedules

After you install SIMS, use the SIMS Administration Console to adjust the IMTA dirsync and impurge schedules within `crontab`. impurge has no default `crontab` entry and will not run until it is configured in `crontab`.

To configure the Purge schedule see "Message Purge" in Chapter 7, Message Store Administration" in the *Sun Internet Mail Server Administrator’s Guide*.

To reconfigure the alias synchronization schedule see "Alias Synchronization Schedule" in Chapter 5, "Internet Mail Transport Agent (IMTA) Administration" in the *Internet Mail Server Administrator’s Guide*.

Building the IMTA Table

Enter the following command to build your initial IMTA table:

```
# /opt/SUNWmail/imta/sbin/imta dirsync -F
```

Configuring dirsync and impurge

Use the SIMS Administration Console to adjust the IMTA `dirsync` and `impurge` schedules within crontab. After SIMS is installed, `impurge` has no default `crontab` entry and will not run until it is configured `in crontab`.

Starting the Sun Web Access Server

To administer the Sun Web Access server, you can use the Sun Web Server 2.1 administration tool.

▼ To access the Sun Web Server 2.1 tool:

1. **Open an Internet browser.**
2. **Enter the URL to access the Sun Web Server administration tool.**

```
http://<hostname>:2380/admin/server_admin.html
```

Where,

hostname is the name of the SIMS 4.0 server running the Web Access services, and 2380 is the default port number for the Sun Web Server administration console.

See the *Sun Internet Mail Server 4.0 Web Access Online Help* for more information on the Sun Web Access Client user interface.

▼ To access the Sun Web Access:

1. **Open an Internet browser.**

2. **Enter the URL to access the Sun Web Access directly.**

```
http://<hostname>:8080/WebAccess
```

Where,

hostname is the name of the SIMS 4.0 server with the Web Access services enabled, and 8080 is the default port number on which the Sun Web Access is running.

Starting the Sun Directory Services

You may start the Sun Directory Services (SDS) 3.1 by entering the following command:

```
/etc/init.d/dsserv start
```

Starting the Delegated Management Server

To start the Delegated Management Server:

1. **Login as root.**
2. **Start the `dm.server`.**

```
# /opt/SUNWmail/spm/sbin/dm.server start
```

Populating the Directory

If you are installing SIMS 4.0 for the first time, you need to populate the LDAP directory that SIMS uses to resolve incoming email addresses and logins to mailboxes stored in SIMS.

Note – Messages sent to the SIMS system will not be routed until you populate the directory.

Populating the directory is a multi-phase operation which may require significant manipulation of data from NIS/NIS+ files for successful population.

You need to populate the directory with entries for mail users, calendar users, user aliases, and distribution lists. The entries are created either from the `/etc/passwd` file and the mail `/etc/mail/aliases` file, or from the NIS/NIS+ equivalents.

See Chapter 9, “Sun Directory Services Administration,” in the *Sun Internet Mail Server 4.0 Administrator’s Guide* for information about populating the directory.

Starting the Delegated Management Console

To start the Delegated Management Console, do the steps in this section.

1. **Bring up the Netscape browser.**

Note – The Netscape Browser is required for running Delegated Administration Console.

2. **Start the Delegated Administration Console from the browser.**

```
http://<sims-machinename>/sims/en/login.html
```

where <*sims-machinename*> is the name of the server on which SIMS is installed.

3. **Login as the Site Administrator, Delegated Administrator, or the end-user.**

Depending on the type of login you entered, different sets of functionality will be available.

See Chapter 10, "Delegated Management Administration," in the *Sun Internet Mail Server 4.0 Concepts Guide* for different lists of tasks that can be accomplished by the Site Administrator, Delegated Administration, and the end-user.

Migrating Mail Folders

To migrate your existing user mail messages and folders from `/var/mail` to the secured SIMS Message Store, use the `imimportmbox` utility.

See the *Sun Internet Mail Server 4.0 Administrator's Guide* and the *Sun Internet Server 4.0 Reference Manual* for more information on using this utility.

Testing Your SIMS 4.0 Server

This section provides you with steps to test the ability of your SIMS server to send and receive mail to and from SIMS.

For detailed instructions on accomplishing these tasks, see the *Sun Internet Mail Server 4.0 Administrator's Guide.*

▼ To test your SIMS server

1. Create a couple of test users by using the SIMS Administration Console, User Management, User from Create option.
2. Perform an `/opt/SUNWmail/sbin/imta dirsync -F` to synchronize the directory.
3. Log in as one of the users that you have just created with an IMAP or POP3 client.
4. If you have installed Web Access, use any Web browser and then log into mail via Web Access. Use the following URL:

```
% http://<sims-system>:8080/WebAccess
```

5. Send a couple of email messages to another SIMS user or another user on a different system.
6. Verify that the user on the other end has received your email.

CHAPTER 10

Configuration Files

This chapter provides a list of configuration files that Sun™ Internet Mail Server™ 4.0 installs for each of the following components:

- SIMS Administration console
- Delegated Administration console
- Internet Message Transfer Agent
- Message Transfer Agent SDK
- Message Store / Message Access
- Sun Directory Services
- Sun Web Access server
- SIMS documentation

Each configuration file is identified as being configured by default during the installation, by the SIMS administrator through a text editor, via the Administration CLIs, or through the SIMS Administration Console, where available.

Configuration files are located in the `/etc/opt/SUNWmail` directory.

You may use the `imedit` tool to manually edit the configuration files.

Common Configuration Files

Files Directory: `/etc/opt/SUNWmail`

TABLE 10-1 Configuration Files Common to All SIMS Components

File Name	Configured by Installation	Configurable via Text Editor	Configurable via Administrative CLIs	Configurable via SIMS Admin. Console
`sims.cnf`	X	X	X	X
`simsr.cnf`	X		X	

SIMS Administration Console Files

Files Directory: `/etc/opt/SUNWmail/admin`

TABLE 10-2 Configuration Files for the SIMS Administration Console

File Name	Configured by Installation	Configurable via Administration CLIs	Configurable via SIMS Admin. Console
`adminserver.properties`	X	X	X
`adminserver.properties.backup`	X		MTA, MS
`defaultadminserver.properties`	X		MTA, MS
`scheduled.tsk`	X		MTA, MS
`defaultscheduled.tsk`	X		MTA, MS
`backupscheduled.tsk`	X		MTA, MS
`as.pid`			
`rmi.pid`			
`directory.adm`			
`gw.adm`			
`imap.adm`			
`ims.adm`			

TABLE 10-2 Configuration Files for the SIMS Administration Console *(Continued)*

File Name	Configured by Installation	Configurable via Administration CLIs	Configurable via SIMS Admin. Console
log.adm			
mta.adm			
user.adm			

Delegated Management Console Files

Files Directory: /etc/opt/SUNWmail/spm and /etc/opt/SUNWmail

TABLE 10-3 Configuration Files for Delegated Management Console

File Name	Configured by Installation	Configurable via Text Editor	Configurable via SIMS Admin. Console
imdmc.cnf	X	X	
simsr.cnf	X		
sims.cnf			

Internet Message Transfer Agent Files

Files Directory: `/etc/opt/SUNWmail/imta`

TABLE 10-4 Configuration Files for MTA Component

File Name	Configured by Installation	Configurable via Text Editor	Configurable via Administration CLIs	Configurable via SIMS Admin. Console
address_option.sample	X			
aliases	X			
aliases.dl	X			MTA
aliases.usr	X			MTA
channel.cat	X			MTA
charnames.txt				User Manager
charsets.txt				User Manager
charsets_ps.txt				User Manager
charsubs.txt				User Manager
countries.txt				User Manager
cronjobs				User Manager
dispatcher.cnf				User Manager
dl_auth.map				User Manager
imta.cnf	X		X	MTA
imta_tailor				MTA
internet.rules				MTA
job_controller.cnf				MTA
magic.dat				MTA
mappings		X		MTA

TABLE 10-4 Configuration Files for MTA Component *(Continued)*

File Name	Configured by Installation	Configurable via Text Editor	Configurable via Administration CLIs	Configurable via SIMS Admin. Console
maximum.dat				
maximum_command.dat				
name_content.dat				
option.dat		X		
option_charset.dat				
locale/C/LC_MESSAGES/ return_bounced.txt				
locale/C/LC_MESSAGES/ return_deferred.txt				
locale/C/LC_MESSAGES/ return_delayed.txt				
locale/C/LC_MESSAGES/ return_delivered.txt				
locale/C/LC_MESSAGES/ return_failed.txt				
locale/C/LC_MESSAGES/ return_forwarded.txt				
locale/C/LC_MESSAGES/ return_header.opt				
locale/C/LC_MESSAGES/ return_prefix.txt				
locale/C/LC_MESSAGES/ return_suffix.txt				
locale/C/LC_MESSAGES/ return_timeout.txt				

Message Store / Message Access Files

Files Directory: `/etc/opt/SUNWmail/ims`

TABLE 10-5 Configuration Files for Message Store / Proxy Component

File Name	Configured by Installation	Configurable via Text Editor	Configurable via SIMS Admin. Console
`ims.cnf`	X	X	MS
`ims.cnf.backup`	X		MS
`ims.cnf.default`	X		MS

The following is a list of the commands and scripts that use the `ims.cnf` file:

- `imcheck`
- `imdeluser`
- `imimportmbox`
- `iminitquota`
- `impurge`
- `imrestore`
- `imsinit`
- `imexpire`
- `imquotacheck`
- `ims_master`
- `imexportmbox`
- `mkbackupdir`

Sun Directory Services Files

Files Directory: `/etc/opt/SUNWconn/ldap/current`

TABLE 10-6 Configuration Files for the Directory Services

File Name	Configured by Installation	Configurable by Administrator	Configurable through SIMS Admin. Console
`directory.adm`			
`ldapfilter.cnf`			
`ldapsearchprefs.cnf`			
`ldapsync.cnf`		X	
`ldaptemplates.cnf`		X	
`sdserv.ini`			Directory Configuration
`dsserv.at.cnf`		X	Directory Configuration
`dsserv.cnf`	X	X	Directory Configuration
`dsserv.oc.cnf`		X	Directory Configuration
`webldapfilter.cnf`			
`sims-sisp.at.cnf`			
`sims-sisp.oc.cnf`			
`sims.at.cnf`			
`sims.oc.cnf`			
`webldapfriendly`			

Web Access Server Files

Files Directory: `/opt/SUNWwa/properties`

TABLE 10-7 Configuration Files for Web Access Server Component

File Name	Configured by Installation	Configurable by Administrator	Monitor through SIMS Admin. Console
`realm.Sims.properties`	X	X	

Files Directory: `/etc/opt/SUNWmail/dir_svc`

TABLE 10-8 Directory Configuration Files for Web Access Server Component

File Name	Configured by Installation	Configurable by Administrator	Configurable through SIMS Admin. Console
`imldifsync.users.cnf`	X	X	X
`imldifsync.groups.cnf`	X	X	X

CHAPTER 11

Troubleshooting the Sun Internet Mail Server

This chapter covers some of the potential issues that you may encounter during the installation of SIMS 4.0, including diagnosing and then properly configuring your DNS setup. It also gives you information about the log file, where installation activities and error messages are recorded.

- Configuring the DNS setup
- Reading the SIMS installation log files
- Rebooting after reinstalling
- Configuring the Netscape browser
- Missing the command tool
- LDAP libraries not being removed
- Cleaning up the corrupted quota file

Configuring the DNS Setup

Before installing SIMS 4.0, installation looks up the host name of your local machine. If this host name is *not* a fully qualified domain name, installation exits. You will then need to correctly configure your DNS setup before installing SIMS, as explained in "Diagnosing DNS," below.

What is a Fully Qualified Domain Name?

Fully Qualified Domain Name (FQDN) is the full name of a system, consisting of its local host name along with its domain name. Recall that a host name is the logical name assigned to a computer. For example, *class* is a host name and `eng.stream.com` is an FQDN.

A FQDN should be sufficient to determine a unique Internet address for any host on the Internet. The same naming scheme is also used for some hosts that are not on the Internet, but share the same name-space for electronic mail addressing. A host which does not have a FQDN must be addressed using a bang path.

A *bang path* is an address for sending e-mail via UUCP that specifies the entire route to the destination computer. It separates each host name with an exclamation point, which is known as a *bang*. For example, the bang path `midearth!shire!eng!jsmith` would go to the *jsmith* user account on the *eng* host, which is reached by first going to *midearth* and then *shire*.

Diagnosing DNS

SIMS 4.0 installation automatically diagnoses the host name to determine whether the name returned is a fully qualified domain name, but somehow cannot be accessed.

The following are the steps that SIMS installation takes:

1. The procedure makes a function call to `gethostbyname()`, which in turn uses the file `nsswitch.conf` to check the host name.
2. If the lookup results in a fully qualified domain name, the installation proceeds; otherwise, it runs the SIMS DNS lookup utility. This utility directly accesses the Internet Domain Name Server.
3. The SIMS DNS lookup utility, in turn, uses the file `etc/resolv.conf` and directly queries the Internet Domain Name Servers.

4. If the SIMS DNS lookup utility cannot find the DNS name in the system, it displays an error message and exits.

5. If, however, the SIMS DNS lookup utility *finds* the DNS name in the system, it further searches to check whether the name is a fully qualified domain name.

6. If the SIMS DNS lookup utility *finds* a DNS name that is *not* a fully qualified name, it displays a message indicating that the Administrator needs to configure the DNS on the machine correctly before installing.

7. If the SIMS DNS lookup utility concludes that the name it found *is* a fully qualified domain name, it displays a message indicating that the name is good, but cannot be accessed. It then suggests that you check the file `/etc/nsswitch.conf` for the search order for hosts or the `/etc/hosts` files if this file is being used.

FIGURE 11-1 shows the steps that SIMS 4.0 installation takes to check for a fully qualified domain name.

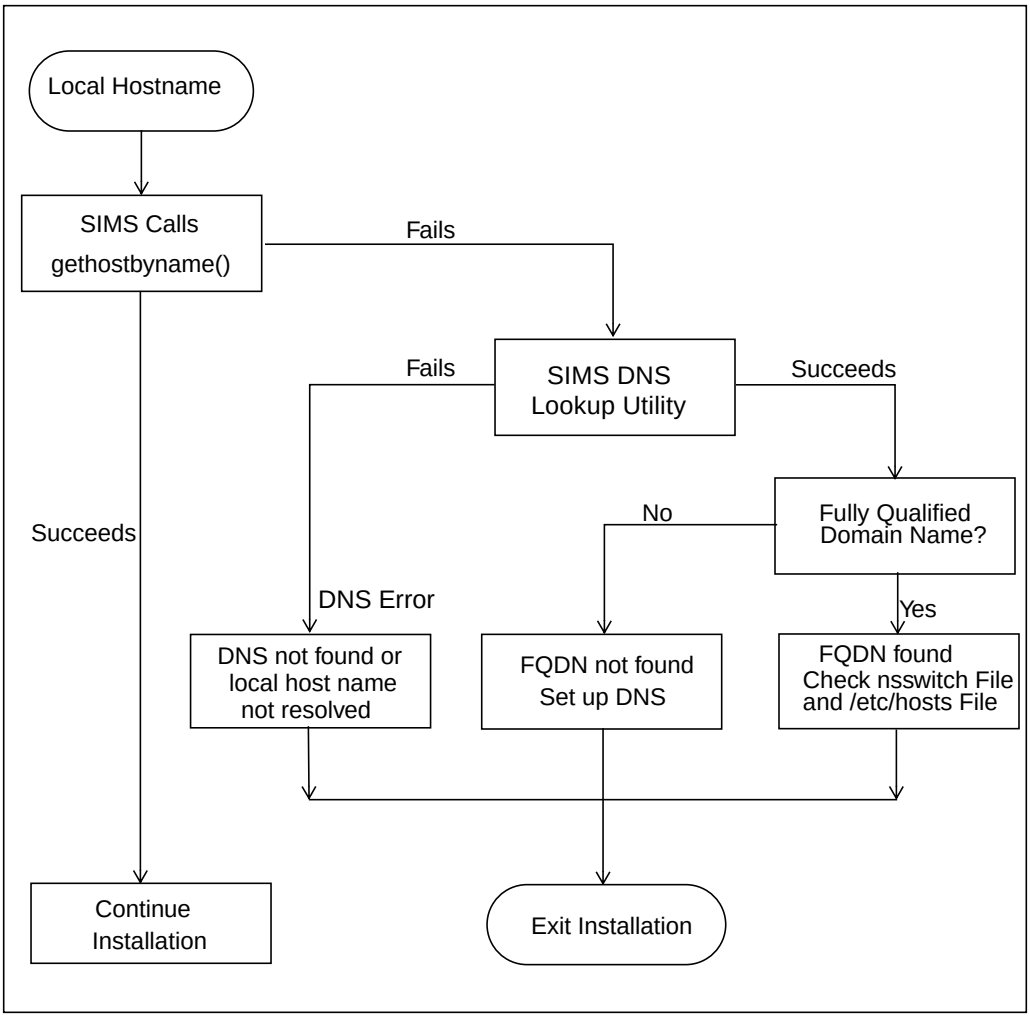


FIGURE 11-1 DNS Diagnostic Procedure

Configuring Files

Once the SIMS installation determines that the DNS setup you are using is in fact good, the next step for you is to configure your `resolv.conf` and `nsswitch.conf` files.

Recall that the order in which `gethostbyname()` consults the sources DNS, NIS, and `/etc/hosts` is configured in the file `/etc/nsswitch.conf`.

This section provides you with the steps that help you configure the order in which the sources are consulted.

1. Configure the `/etc/nsswitch.conf` to specify the DNS source and the order in which it is looked up, for example:

```
hosts: dns files
```

Note – If you have placed *files* before *dns*, make sure that your */etc/hosts* files contains fully qualified domain names for all hosts. Also, make sure that the fully qualified domain name for the local machine appears in `/etc/nodename` and `/etc/hostname.*`.

---

2. Configure the `/etc/resolv.conf` file to specify how to access the Internet Domain Name System.

```
domain <domain-name>
nameserver <name-server-IP-address>
```

Where,

domain-name specifies a local domain name that is used as the default domain, and

name-server-IP-address specifies the Internet address of one name server to which the resolver should direct any queries.

Note – *name-server-IP-server* cannot be the same as the IP of the local host name.

Example:

The following is an example of the contents of the `/etc/resolv.conf` file:

```
domain sun.com
nameserver 129.155.121
nameserver 129.155.125
```

The `nslookup` data for the *marketing* host name will then be:

```
nslookup marketing
Name: marketing.eng.sun.com
```

Reading the SIMS Installation Log Files

SIMS records installation activities in log files located in `/var/opt/SUNWmail/log/SIMS_installation_log.`*n*, where *n* is the date and time stamp of the form *YYMMDD.HR:MM*. This number is generated automatically. For example, `SIMS_installation_log.97112012:40` is the log file for the install which was started at 12:40 on November 20, 1997.

Note – During installation, the log file is created in the `/tmp` directory. It is then moved to the directory `/var/opt/SUNWmail/log` after installation is completed. If the installation exits before it is completed, you can check the log file in `/tmp`.

Rebooting after Reinstalling

If you are reinstalling SIMS 4.0, make sure that you reboot your system after the installation of the new server. If you do not reboot, you may encounter errors while creating new calendar or mail users.

If you cannot create new users, check if you have rebooted the system after you have reinstalled the SIMS server.

Configuring the Netscape Browser

After you installed SIMS or SIMS/HA, you need to configure the Netscape property files by setting the defeat security level to low.

See “Netscape Browser Configuration” on page 70 in Chapter 8, “Post Installation Configurations," for instructions on configuring the Netscape browser.

Missing the Command Tool

The next step after you have selected the installation type and specified configurations for your selection is to run the `setup` install script. This will invoke the command tool to continue the installation. If, however, this command tool is not available, an error message will be displayed. You may check the path where the command tool should reside or check your operating system setup.

LDAP Libraries Not Being Removed

The `uninstall -d` command does not remove the `SUNWlldap` LDAP library packages or any associated patches which is part of Solaris 2.7.

Cleaning Up the Corrupted Quota File

If you are upgrading to SIMS 4.0 from SIMS 3.5, you need to initialize all the user quota files. The purpose for doing this procedure is to clean up the potential by corrupted message store user quota files. See the *Sun Internet Mail Server 4.0 Administrator's Guide* for instructions on how to set up user quotas.

After you have upgraded to SIMS 4.0, do the following steps:

1. **Change the directory.**

```
# cd /opt/SUNWmail/ims/sbin
```

2. **Initialize all the user quota files.**

```
# ./iminitquota -a
```

3. **Print a user quota report.**

```
# ./imquotacheck -v -n
```

4. **Verify that the information on a user quota report is correct.**

TABLE 11-1 User Quota Report Sample

Username	Quota (Byte)	Total (Byte)	% used
u1	NO LIMIT	16840	NA
u2	NO LIMIT	250	NA
u3	NO LIMIT	500	NA
u4	20000000	750	<1%
u5	20000000	14750	<1%
u6	20000000	3000	<1%
u7	10000000	515650	<6%
u8	10000000	2343950	<24%
u9	10000000	3000	<1%
u10	10000000	753	<1%

CHAPTER 12

SIMS Asymmetric High Availability System

A major advantage of Sun™ Internet Mail Server™ 4.0 over competitors is its superior scalability, which enables populating large number of users on just one server. Although this provides excellent price versus performance advantages, it results in a *single point of failure*, where one failing machine could interrupt email access for an entire user community.

To ensure reliability, SIMS 4.0 enables you to install on a Sun Enterprise Cluster by using the Sun Cluster 2.2 software. This capability provides automatic *fail over* when a failure occurs.

See `http://www.sun.com/clusters` for information on Sun Cluster.

Topics in this chapter include:

- Other High Availability references in this guide
- SIMS asymmetric High Availability configuration
- Fail over procedure

Other HA References in this Guide

TABLE 12-1 lists other chapters in this guide that contain information on SIMS/HA. After you read this chapter and are familiar with the design of SIMS/HA, you may proceed with Chapter 7, “Installing SIMS 4.0," for instructions on installing the SIMS High Availability system.

TABLE 12-1 Chapters Containing High Availability Information

Chapter Number, Name	To Learn About...
4, Preparing to Install SIMS	Prepare a clean system, and lists of required and recommended patches.
5, Preparing to Configure	Software requirements for the SIMS High Availability system.
6, What SIMS 4.0 Installs	Lists of SIMS 4.0 packages.
7, Installing SIMS 4.0	Instructions for installing the SIMS High Availability system.
9, Post Installation Tasks	Instructions to start Administration Console.

SIMS Asymmetric HA Configuration

FIGURE 12-1 illustrates SIMS running on a cluster. Each node in the cluster is a complete Solaris system with its own private disk that contains the operating system and the Sun Cluster software.

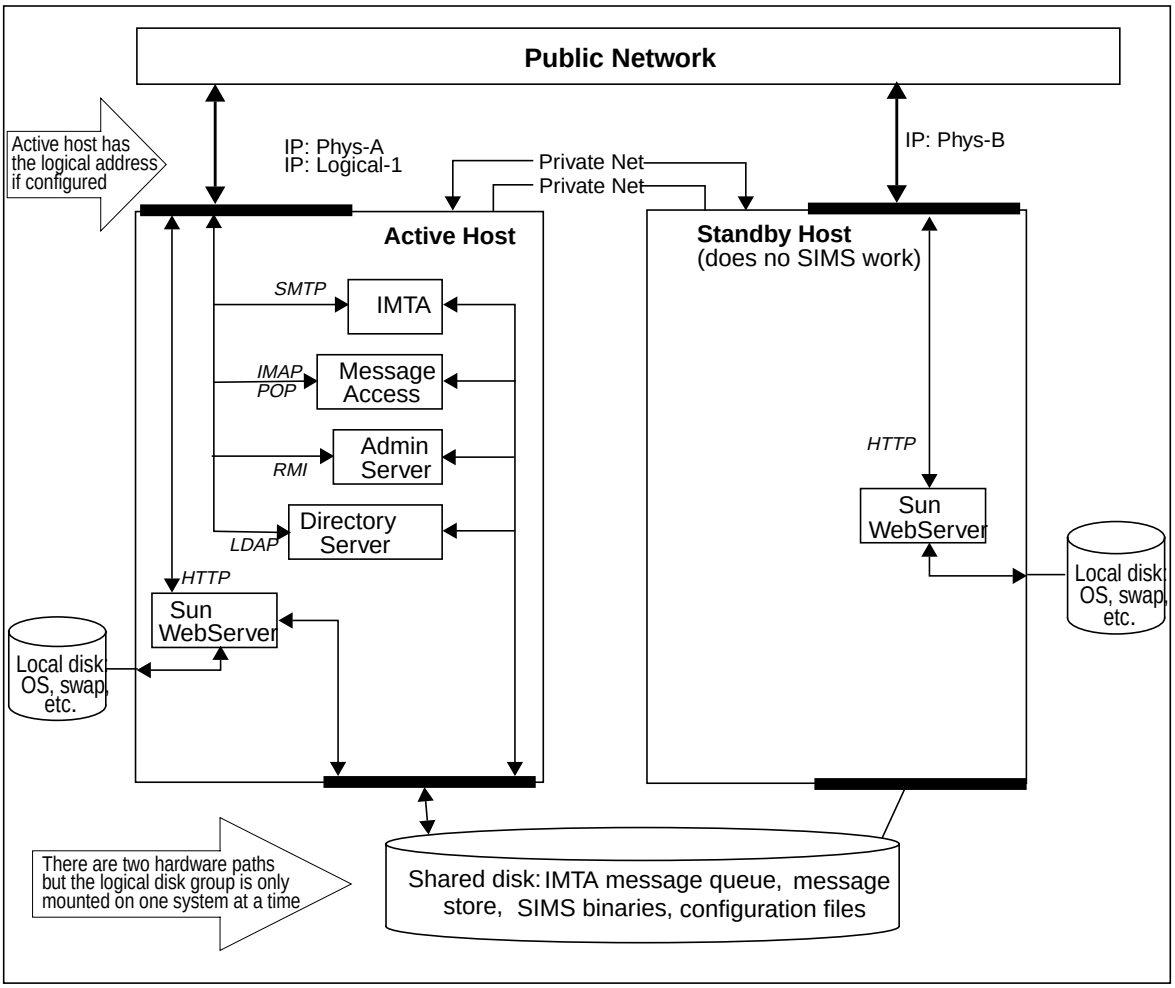


FIGURE 12-1 SIMS Asymmetric HA Configuration before Fail Over

Since each node has at least one network interface connected to the public network, users can connect through this interface to read their mail messages. Each node has at least two additional *private* network interfaces, which connect to corresponding private network interfaces on the other members of the cluster. These are used by the Sun Cluster software on each node for system status monitoring and cluster configuration data sharing. Only one pair of private network interfaces is in use at any given time; the other is a redundant interface so that there is not a single point of failure.

Each node has a connection to the disk cluster that contains the message store, message queues, directory contents, configuration files, and SIMS binaries. While both nodes are connected to the disk cluster continuously, the volumes in the disk cluster are mounted on only one of the nodes at any given time. FIGURE 12-1 and subsequent figures in this chapter show this disk cluster as a single logical volume.

In SIMS 4.0, both the Veritas and the DiskSuite volume managers are supported for Sun Cluster. The volume manager allows a logical volume to be mirrored across multiple physical volumes, providing uninterrupted service even if a physical disk fails.

As shown in FIGURE 12-1, only one of the nodes in the cluster runs SIMS at any time. This represents an *Asymmetric High Availability* (HA) configuration. In this configuration, all the SIMS binaries, configuration files, message queues, and message store reside on a *shared disk*. As a result, when a fail-over occurs the disk is unmounted from the failing system and mounted on the surviving system. FIGURE 12-2 shows the cluster after a fail-over.

The *logical* IP address is now configured on the public network interface of the other system. Users and mail agents on the public network always connect using the logical IP address. Thus, reconnecting after a failure automatically connects to the other system. A fail-over, will then, appear to be a very quick crash and reboot of a single system!

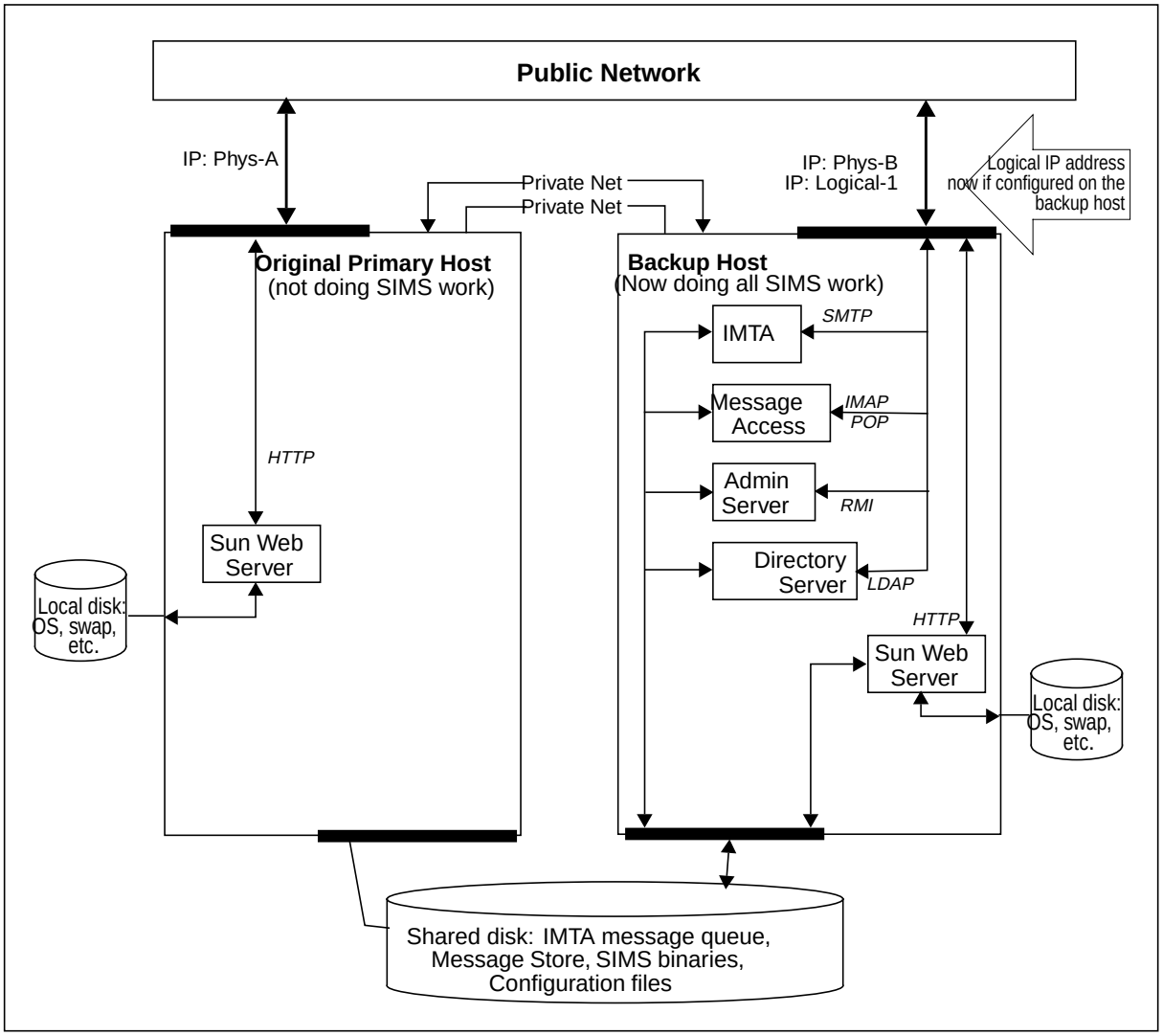


FIGURE 12-2 SIMS Asymmetric HA Configuration after Fail Over

In the SIMS Asymmetric HA configuration, the other node in the cluster is idle as far as SIMS usage is concerned. This node, however, remains a fully-functional Solaris system and is available for other work, as long as procedures to terminate or limit the other work after a fail-over are in place.

As long as the CPU speed and memory size of the two nodes in the cluster are alike (recommended) in this Asymmetric HA configuration, the performance does not suffer during a fail-over. The stand-by node, however, is unused much of the time.

Fail Over Procedure

The fail over procedure in the SIMS High Availability environment involves the following:

- Linking SIMS directories to shared disks between cluster nodes
- Linking Sun DS directories to shared disks between cluster nodes
- Replacing stop and start scripts with HA scripts

Linking SIMS Directories to Shared Disks

Although the basic SIMS architecture remains unchanged by the SIMS/HA configuration during normal execution, SIMS/HA functions and performs similar to SIMS. The SIMS binaries, configuration files, IMTA spools, message store, and logs are all placed on disks shared between the cluster nodes. The installation process plants symbolic links from the following locations to the corresponding places on the shared disk, as shown in TABLE 12-2.

TABLE 12-2 SIMS Directories on Shared Disk between Cluster Nodes

Install Creates Links from...	To place on the shared disk
`/opt/SUNWmail`	`/`*`shared-disk-BASEDIR`*`/opt/SUNWmail`
`/etc/opt/SUNWmail`	`/`*`shared-disk-BASEDIR`*`/etc/opt/SUNWmail`
`/var/opt/SUNWmail`	`/`*`shared-disk-BASEDIR`*`/var/opt/SUNWmail`

Linking Sun Directory Services to Shared Disks

The Sun Directory Service 3.1 (SunDS) binaries and data are also normally installed on the shared disk. Since the SunDS packages are not completely re locatable, this is accomplished in the SIMS install script by planting symbolic links from the following locations to the shared disk, as shown in TABLE 12-3.

TABLE 12-3 Sun DS Directories Mapped to Shared Disk between Cluster Nodes

Install Creates Links from...	To place on the shared disk
`/opt/SUNWconn`	`/shared-disk-BASEDIR/opt/SUNWconn`
`/etc/opt/SUNWconn`	`/shared-disk-BASEDIR/etc/opt/SUNWconn`
`/usr/opt/SUNWconn`	`/shared-disk-BASEDIR/usr/opt/SUNWconn`

Replacing HA `stop` and `start` Scripts

To ensure that SIMS and directory `start` and `stop` can be controlled through the HA framework, the normal `/etc/rc?.d` hard links to the `start` and `stop` scripts in `/etc/init.d` are removed. In return, these scripts are replaced with specialized HA `start` and `stop` scripts.

These HA scripts are packaged in SUNWimha and located by default in `/opt/SUNWimha/clust_progs` (This path is similar to those used by other HA services.)

SIMS installation uses the `hareg` command to register these scripts with the HA framework and associates them with the HA *service name* `Sun_Internet_Mail`.

While a fail over can occur either at a system administrator's request or after a failure is detected, it proceeds by calling these HA scripts to shut down SIMS and the directory server on one machine and start up on the other machine.

Operating System and Platform Support

TABLE 12-4 shows the configurations that are supported in SIMS 4.0.

TABLE 12-4 Tested Platform Configurations

Operating System Release	Cluster Software	Hardware Architecture
Solaris 2.6	Sun Cluster 2.2	SPARC
Solaris 2.7	Sun Cluster 2.2	SPARC

Storage and File System Requirements

To ensure system availability by eliminating single points of failure, SIMS, SunDS, or Netscape Directory Services (NSDS) binaries, configuration files, and data must be *mirrored* on replicated disks. Sun Cluster 2.2 includes the Sun Enterprise Volume Manager, on which SIMS/HA depends to provide redundant storage.

To enable SIMS to back up quickly after a fail-over, it's important that the file systems holding the SIMS writable data recover quickly and be restored to a consistent state.

Because the base Solaris UNIX File System (UFS) does not synchronously write file meta-data at `fsync()` time, `fsck` times can be large and the file system state may not be completely recovered. For example, small files that were created right before a crash might not exist after `fsck` and remount. SIMS/HA depends on the Veritas File System (VxFS) 3.3.2 to provide a file system with these characteristics.

Note – Since Sun Cluster 2.2 does not include the Veritas File System (VxFS) 3.3.2 or the Solaris UFS, either file system of your choice must be purchased separately.

Directory Services Considerations

SIMS 4.0 requires that a directory service server with the proper schema run on the same host. This means that the SunDS server must also have the High Availability capability. Since SunDS 1.0 does not support the High Availability capability, SIMS/HA has incorporated a mechanism to have SunDS highly available. To accomplish this by default, SIMS installs SunDS on a shared disk. It then changes the `/etc/rc?.d` links so that `start` and `stop` operations are under the control of the SIMS/HA scripts.

As an alternative, you may consider another method for installing SIMS/HA. That is, rather than considering SunDS as part of the `Sun_Internet_Mail` service and switching it back and forth between the two hosts in the cluster, you could install SunDS on each host, and set up SunDS replication to keep the two hosts in synchronization. To implement this configuration, you could make the SunDS on one of the hosts as the *primary* and the other host as the *secondary*.

A more symmetrical approach, however, would be to make both hosts secondaries of the primary that is not part of the cluster. In this configuration, however, a SIMS fail-over may cause the *cached* copy of the directory that SIMS not to match the directory on the new node (since there is no synchronization between SunDS and its replications).

To avoid this, installations should see that a full `dirsync` be run soon after a fail-over occurs. To restore the services as quickly as possible, however, the SIMS/HA interface scripts will not run a full `dirsync` automatically.

To allow installations to create directory configurations like this, SIMS/HA follows the same practice established in earlier releases of SIMS. That is, if SunDS is already installed when SIMS/HA installation is started, SIMS installation leaves the SunDS installation alone.

You have learned about the SIMS High Availability configurations in this chapter. You can now follow the instructions covered in Chapter 7, “Installing SIMS 4.0," to install your SIMS High Availability system.

See Appendix B, “Installing Netscape Directory Services for SIMS High Availability," for instructions to install NSDS 4.1 and configure it for the SIMS High Availability system.

APPENDIX **A**

Installing Netscape Directory Services for SIMS

SIMS 4.0 supports both the Netscape Directory Services (NSDS) 4.1 and the Sun Directory Services 3.1. The NSDS is the preferred directory server to use with SIMS 4.0 in the SPARC/Solaris operating environment.

This chapter provides you with step-by-step instructions that you can use to install NSDS 4.1 and configure it for SIMS 4.0. It also gives you the guidelines to install SIMS 4.0 with NSDS 4.1 and shows the post installation configuration that you may need to perform if you have installed SIMS *befor*e installing NSDS.

Topics in this chapter include:

- Overview of the Netscape Directory installation
- Installing Netscape Directory Services 4.1
- Configuring Netscape Directory Services 4.1
- Disabling the Netscape Directory Services uid uniqueness
- Guidelines for installing SIMS with the Netscape Directory
- Post SIMS installation configuration

Overview of the Netscape Directory Services Installation

To install Netscape Directory Services 4.1 with SIMS 4.0:

1. **Install Netscape Directory Services 4.1.**
2. **Configure Netscape Directory Services 4.1.**
3. **Disable the NSDS uid Uniqueness.**

Note – You are required to install NSDS *before* installing SIMS 4.0.

After you install NSDS, read "Guidelines for Installing SIMS with the Netscape Directory" on page 115 for the specific information for which you will be asked by the SIMS installation GUI while installing SIMS with the Netscape Directory.

If, however, you install NSDS *after* you installed SIMS 4.0, read "Post SIMS Installation Configuration" on page 118 for instructions that you can use to manually configure the Netscape configuration.

Installing Netscape Directory Services 4.1

To install NSDS 4.1, you must first display the Netscape Directory Server Installation page. While installing NSDS, you may need to accept the default values for all fields, except the following, which you will be using during the SIMS installation:

- Installation Location
- Computer Name
- Directory Server Network Port
- Directory Server Identifier
- Administrator ID
- Suffix
- Directory Manager

To install NSDS:

1. **Ensure that you have set the `DISPLAY` variable.**
2. **To install NSDS 4.1, insert the NSDS 4.1 CD-ROM (included in the SIMS 4.0 packaging) into the disk drive.**
3. **Untar the `directry.tar` file on the NSDS CD into a temporary directory.**

```
% tar -xvf /cdrom/directry_41ue/solaris/directry/directry.tar
```

4. **Change to this temporary directory.**
5. **At the command line, execute the `setup` command as root.**

```
# ./setup
```

This displays the NSDS installation page.

6. **Accept the default values to all the questions asked:**

Note – You need to record the information to the following six questions so that you can use the answers while installing SIMS with NSDS. You may either accept the default values or enter different information. In either case, you *must* record this data.

---

a. **Installation Location [***/usr/netscape/server4***] –** The directory path to which the NSDS files will be copied. You may change this path, otherwise `/usr/netscape/server4` will be the default directory where the NSDS files will be installed.

b. **Computer Name [<***hostname***>.<***domainname***>] –** The fully qualified domain name of the directory server on which you are installing the Netscape Directory Services software. Make a note of this name.

c. **Directory Server Network Port [***portnumber***] –** The port number on which the Netscape Directory server will be running. By default, the LDAP directory should run on port 389. If this port is being used by another directory server, you will see a different port number assigned. Make a note of this number.

   Directory Server Network Port is the same as the LDAP Port field on the Directory Services Information page of the SIMS installation GUI.

d. Directory Server Identifier [*hostname***] –** By default, the host name of the machine on which you are installing NSDS is appended to the word `slapd` (`slapd-<`*`hostname`*`>`) to create a sub-directory under the Installation Location directory path (specified in 5.a above), where the NSDS files will be installed. For example, `/usr/netscape/server/slapd-<`*`hostname`*`>` will be an instance name of this directory path. You may change *hostname* to any name.

e. Administrator ID (admin) – Either accept the default (admin) or enter another name. Enter a password for this administrator as well. You will be using the Administrator ID later to log into the Netscape Console that will be explained later in this chapter.

f. Suffix – The Directory Component (DC) tree root. Enter **o=internet** instead of accepting the default value if you are using the SIMS DC tree with the default value *internet*. Suffix is the same as the Domain Component Tree Root field that appears on the first configuration page of the SIMS installation GUI. Make a note of this entry.

g. Directory Manager – The directory administrator name. Either accept the default value or change to another name. Enter a password for this administrator. This password must be at least eight characters. For example, you may enter **`nssecret`**. Make a note of this entry.

Directory Manger is the same as Directory Administrator Name that appears on the first configuration page of the SIMS installation GUI.

You have now installed NSDS 4.1. The next step is to configure your Netscape configuration files.

Configuring Netscape Directory Services 4.1

To configure your Netscape Directory, you need to:

- Copy the SIMS configurations files to the NSDS configuration directory.
- Append the SIMS indexes to the NSDS configuration file.

To configure NSDS:

1. **Copy the SIMS 4.0 schema files to the NSDS configuration directory.**

```
# cp /cdrom/sun_internet_mail_4_0/nsschema/sims*.conf
     /usr/netscape/server4/slapd-<hostname>/config
```

Where

`/usr/netscape/server4` is the directory in which you have installed your NSDS files as entered in step 5.a in "Installing Netscape Directory Services 4.1" on page 110.

<*hostname*> is the name of the machine on which you have installed your NSDS files, as you entered in step 5.d in "Installing Netscape Directory Services 4.1" on page 110.

`slapd-`<*hostname*> is an instance name assigned to this directory name.

2. **Stop the Netscape Directory Server.**

```
# /usr/netscape/server4/slapd-<hostname>/stop-slapd
```

3. **Open the NSDS' `slapd.conf` configuration file using an editor of your choice.**

```
# vi /usr/netscape/server4/slapd-<hostname>/config/slapd.conf
```

4. **Include the SIMS 4.1 schema files into the `slapd.conf` file.**

Find the last *include* statement and then insert the following four lines after that line.

```
include "/usr/netscape/server4/slapd-<hostname>/config/
         sims-sisp.at.conf"
include "/usr/netscape/server4/slapd-<hostname>/config/
         sims-sisp.oc.conf"
include "/usr/netscape/server4/slapd-<hostname>/config/
         sims.at.conf"
include "/usr/netscape/server4/slapd-<hostname>/config/
         sims.oc.conf"
```

Note – The sequence of the include statements are important. The `at.conf` files *must* precede the `oc.conf` files.

---

5. **Save the `slapd.conf` file and exit.**

6. **Append the SIMS indexes to the NSDS configuration files.**

```
# cat /cdrom/sun_internet_mail_4_0/nsschema/nsds.index.conf >>
/usr/netscape/server4/slapd-<hostname>/config/slapd.ldbm.conf
```

7. **Start the Netscape Directory Server if you would like to start the server now, otherwise, proceed to the next section and then start the server.**

```
# /usr/netscape/server4/slapd-<hostname>/start-slapd
```

Disabling the Netscape Directory Services uid Uniqueness

After installing and configuring NSDS, the next step is to disable the uid uniqueness feature in the NSDS configuration.

By default, NSDS enforces unique user IDs throughout its entire directory tree (that is, from the root tree at the `o=internet` node down).

Since SIMS 4.0 provides domain hosting, it must be able to use the same user ID within different domains. For this reason, you need to disable the uid uniqueness settings here.

Note – If you are going to use SIMS within one domain and will not be using it for domain hosting or with multiple domains, you may bypass the instructions in this section.

To disable NSDS uid uniqueness:

1. **Start the Netscape Console.**

```
# /usr/netscape/server4/start-admin
# /usr/netscape/server4/startconsole &
```

2. **Log into the Netscape Console.**

The login uid and password are the same as the Administrator ID that you entered in step 5.e in “Installing Netscape Directory Services 4.1” on page 110.

3. **Expand <*hostname*>.<*domainame*> on the Netscape Console screen.**

   Where <*hostname*>.<*domainame*> is the domain name in which the host name is located.

4. **Expand `Server Group`.**
5. **Double click `Directory Server`.**
6. **Select the `Configuration` tab.**
7. **Expand `Plugins`.**
8. **Click `uid uniqueness`.**
9. **Uncheck `Enable Plugin`.**
10. **Click `Save`.**
11. **Select `Console->Exit`.**
12. **Restart the Netscape Directory Server.**

```
# /usr/netscape/server4/slapd-<hostname>/stop-slapd
# /usr/netscape/server4/slapd-<hostname>/start-slapd
```

Guidelines for Installing SIMS with the Netscape Directory

Since Netscape Directory Services software is installed separately, the specific information about the setup of NSDS is not available to SIMS. This section lists the criteria specific to Netscape Directory Services that you will need to enter during the installation of SIMS.

Use the notes in this section in accordance with Chapter 7, “Installing SIMS 4.0," which covers the instructions for installing SIMS with the Netscape Directory.

The following is a summary of the questions that you will be asked by the SIMS installation GUI while installing SIMS with NSDS. The instructions cover the specific fields on the Directory Services Information and Configuration Page 1 of the SIMS installation GUI, which is shown in FIGURE A-1.

To install SIMS with the Netscape Directory:

1. **Make sure that the LDAP Server Name assigned to the Directory Services Server Name on the Directory Services Information page is where your NSDS software is located.**

   This is shown in FIGURE A-1.

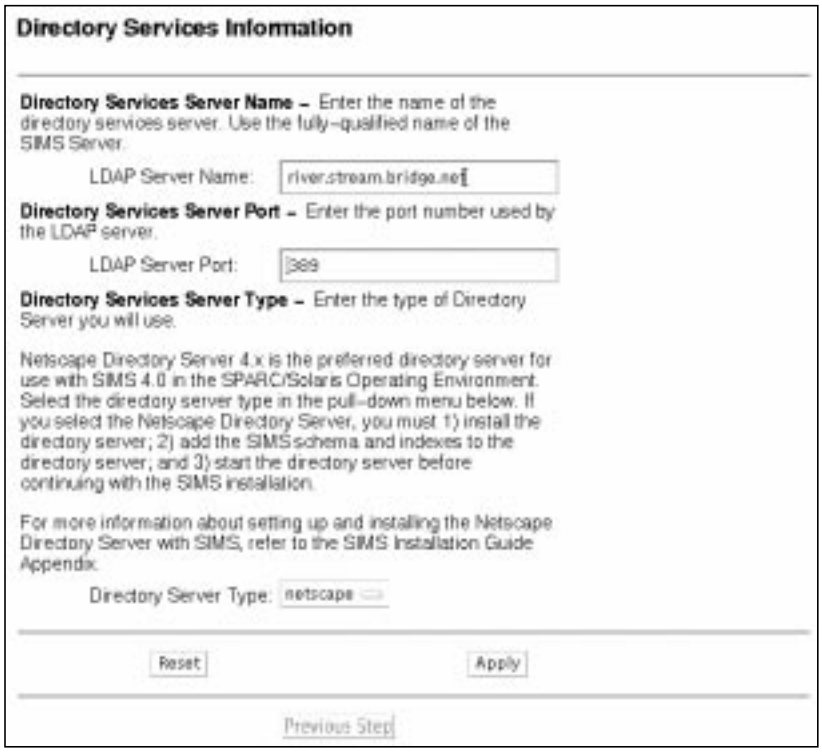


FIGURE A-1 SIMS Installation Directory Services Information Page

By default, SIMS assumes that you have installed your NSDS software on the same machine that you are installing SIMS. If you have installed NSDS on a remote machine, you need to enter the fully qualified name of the server where NSDS resides.

2. **Type the Directory Services Server Port, which is the port number that you used during the NSDS installation.**

   NSDS should have been installed on port 389, unless the port was busy. In this case, you would have needed to use a different port number that you specified as Directory Server Network Port in step 5.c in “Installing Netscape Directory Services 4.1” on page 110.

3. **Select `netscape` as the Directory Services Server Type that appears on the Directory Services Information page of the SIMS 4.0 Installation GUI.**

4. **Make sure that the name assigned to the Directory Administrator Name on the Configuration Page 1 is specified as Directory Manager, as shown in** FIGURE A-2**.**

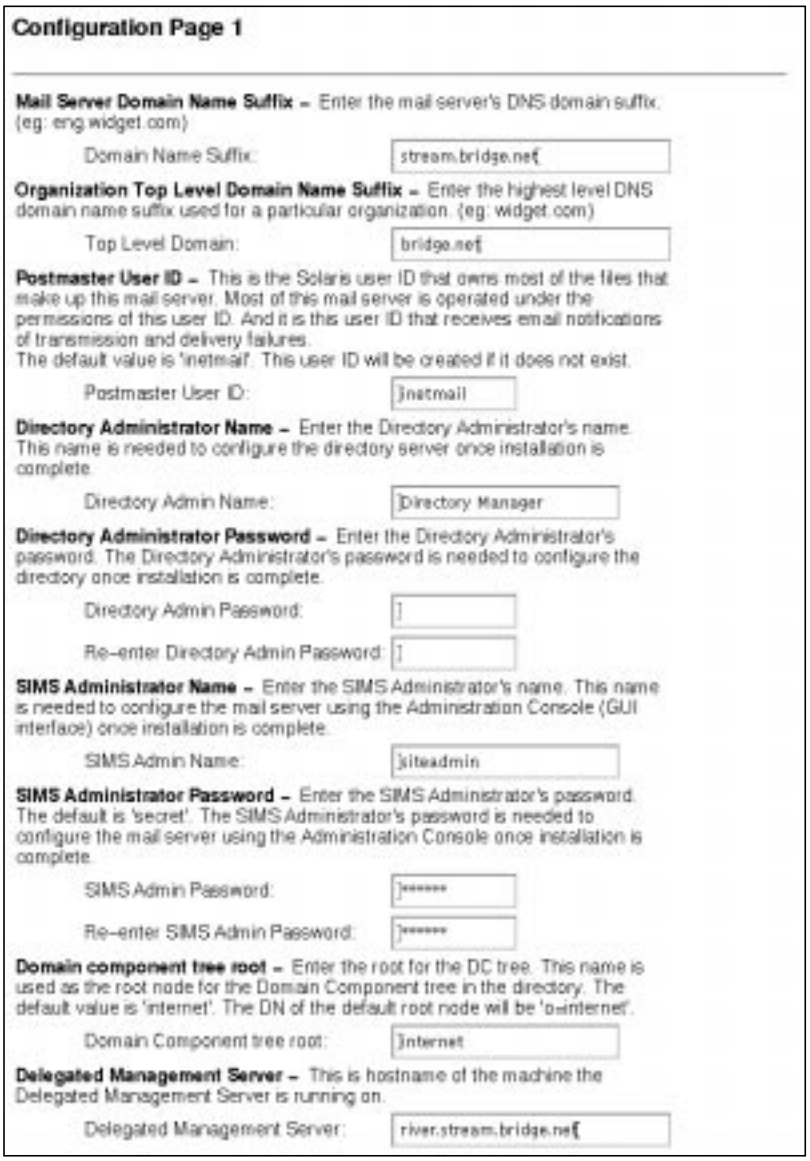


FIGURE A-2 SIMS Installation Configuration Page 1

This is the name you entered while installing NSDS in step 5.g in “Installing Netscape Directory Services 4.1” on page 110.

5. **Type the password for the Directory Administrator Password.**

   This password is the one you entered for Directory Manger in step 5.g. in “Installing Netscape Directory Services 4.1” on page 110.

6. **Make sure that the Domain Component tree root is specified as `internet`, if you are using the SIMS DC tree with the default value** *internet*.

   This is the same Suffix that you entered in step 5.f in “Installing Netscape Directory Services 4.1” on page 110.

Note – If you need to enter this name, do not use the `o=internet` syntax. Instead, type `internet`, because `o=` is automatically prepended to the entry.

Post SIMS Installation Configuration

The SIMS installation procedure automatically creates the Directory Information Tree (DIT) that SIMS supports and adds the access control instructions (ACIs) to your NSDS configuration files.

If you installed SIMS *before* installing NSDS, the SIMS installation will be unable to create this DIT and add the ACIs to the NSDS configuration.

This section describes the commands that you can type manually to:

- Add the SIMS Directory Information Tree (DIT)
- Add the Access Control Instructions (ACIs)

Note – The steps covered in this section are only applicable if for any reason SIMS installation has not added the DIT and ACIs.

Adding the SIMS Directory Information Tree (DIT)

Type the following command to create the DIT for your directory:

```
# /opt/SUNWconn/bin/ldapadd -c -h <hostname>
  -p <portnumber> -D “cn=<Directory Manager>” -w <passwd>
  -f /etc/opt/SUNWmail/slapd.ldif
```

See Chapter 6, “Domain Hosting with SIMS,” in the *Sun Internet Mail Server 4.0 Concepts Guide* for a definition of the DIT and how the information is mapped out.

Adding the Access Control Instructions

Access control is the mechanism by which you can set permissions for the entire directory, a subset of the directory, specific entries in the directory, a specific set of entry attributes, or configuration tasks for any 4.x Netscape Server. When the server evaluates an incoming request, it determines the access type based on the access control instructions (ACIs) that you define. The collection of ACIs within a single suffix (The DC tree root) is called an access control list (ACL). See the Netscape documentation for more information about ACIs.

To add the ACIs to your Netscape Directory configuration:

```
# /usr/netscape/server4/shared/bin/ldapmodify -h <hostname>
  -p <portnumber> -D “cn=<Directory Manager>” -w <passwd>
  -f /etc/opt/SUNWmail/nsds.acl.ldif
```

APPENDIX **B**

Installing Netscape Directory Services for SIMS High Availability

SIMS 4.0 supports both the Netscape Directory Services (NSDS) 4.1 and the Sun Directory Services 3.1. The NSDS is the preferred directory server to use with the SIMS High Availability 4.0 in the SPARC/Solaris operating environment.

This chapter provides you with step-by-step instructions to install NSDS 4.1 and configure it for the SIMS High Availability system. It also gives you the guidelines to install SIMS/HA 4.0 with NSDS 4.1 and shows the post installation configuration that you may need to perform if you installed SIMS/HA *befor*e installing NSDS.

Topics in this chapter include:

- Overview of the Netscape Directory installation
- Installing Netscape Directory Services 4.1
- Configuring Netscape Directory Services 4.1
- Disabling the Netscape Directory Services uid uniqueness
- Guidelines for installing SIMS/HA with the Netscape Directory
- Post SIMS/HA installation configuration

Overview of the Netscape Directory Services Installation for SIMS / HA

To install Netscape Directory Services 4.1 with SIMS / HA 4.0:

1. **Install Netscape Directory Services 4.1.**
2. **Configure Netscape Directory Services 4.1.**
3. **Disable the NSDS uid Uniqueness.**

Note – You are required to install NSDS *before* installing SIMS 4.0.

After you install NSDS, read "Guidelines for Installing SIMS / HA with the Netscape Directory" on page 132 for the specific information for which you will be asked by the SIMS installation GUI while installing SIMS / HA with the Netscape Directory.

If, however, you install NSDS *after* you installed SIMS / HA 4.0, read "Post SIMS Installation Configuration for High Availability" on page 136 for instructions that you can use to manually configure the Netscape configuration.

Caution – If you have Sun Directory Services installed, please remove it prior to installing NSDS. To uninstall, type `pkgrm SUNWsds` and `SUNWsdsc` at the command prompt.

Installing Netscape Directory Services 4.1 for SIMS / HA

To install NSDS 4.1, you must first display the Netscape Directory Server Installation page. While installing NSDS, you may need to accept the default values for all fields, except the following, which you will be using during the SIMS / HA installation:

- Installation Location
- Computer Name
- Directory Server Network Port
- Directory Server Identifier

- Administrator ID
- Suffix
- Directory Manager

To install NSDS for SIMS/HA:

1. **Ensure that you have set the `DISPLAY` variable.**
2. **To install NSDS 4.1, insert the NSDS 4.1 CD-ROM (included in the SIMS 4.0 packaging) into the disk drive.**
3. **Untar the `directry.tar` file on the NSDS CD into a temporary directory.**

```
% tar -xvf /cdrom/directry_41ue/solaris/directory/directry.tar
```

4. **Change to this temporary directory.**
5. **At the command line, execute the `setup` command as root.**

```
# ./setup
```

This displays the NSDS installation page.

6. **Enter the values to all the questions asked:**

Note – You need to record the information to the following six questions so that you can use the answers while installing SIMS/HA with NSDS. You may either accept the default values or enter different information. In either case, you *must* record this data.

---

a. **Installation Location [<***shared-file-system***>/NSDS] –** The directory path to which the NSDS files will be copied. You need to change this path, otherwise `/usr/netscape/server4` will be the default directory where the NSDS files will be installed. *Shared-file-system* is the shared disk where your information will be stored.

b. **Computer Name [<***ha-logical-hostname***>.<***domainame***>] –** The combination of the logical hostname and the domain comprises a fully qualified domain name (FQDN) of the directory server on which you are installing the Netscape Directory Services software. Make a note of this name.

c. **Directory Server Network Port [***portnumber***] –** The port number on which the Netscape Directory server will be running. By default, the LDAP directory should run on port 389. If this port is being used by another directory server, you will see a different port number assigned. Make a note of this number.

   Directory Server Network Port is the same as the LDAP Port field on the Directory Services Information page of the SIMS / HA installation GUI.

d. **Directory Server Identifier [**<*ha-logical-hostname*>.<*domainame*>**] –** By default, the host name of the machine on which you are installing NSDS is appended to the word `slapd` (`slapd-<`*`ha-logical-hostname`*`>`) to create a sub-directory under the Installation Location directory path (specified in 5.a above), where the NSDS files will be installed. For example, <`shared-file-system`> / NSDS/ `slapd-<`*`ha-logical-hostname`*`>` will be an instance name of this directory path.

e. **Administrator ID (admin) –** Either accept the default (admin) or enter another name. Enter a password for this administrator as well. You will be using the Administrator ID later to log into the Netscape Console that will be explained later in this chapter.

f. **Suffix –** The Directory Component (DC) tree root. Enter **o=internet** instead of accepting the default value if you are using the SIMS DC tree with the default value *internet*. Suffix is the same as the Domain Component Tree Root field that appears on the first configuration page of the SIMS / HA installation GUI. Make a note of this entry.

g. **Directory Manager –** The directory administrator name. Either accept the default value or change to another name. Enter a password for this administrator. This password must be at least eight characters. For example, you may enter **`nssecret`**. Make a note of this entry.

   Directory Manager is the same as Directory Administrator Name that appears on the first configuration page of the SIMS / HA installation GUI.

You have now installed NSDS 4.1. The next step is to configure your Netscape configuration files.

Configuring Netscape Directory Services 4.1 for SIMS / HA

To configure your Netscape Directory you need to:

- Copy the SIMS / HA configurations files to the NSDS configuration directory.
- Append the SIMS / HA indexes to the NSDS configuration file.

To configure NSDS:

1. **Copy the SIMS/HA 4.1 schema files to the NSDS configuration directory.**

```
# cp /cdrom/sun_internet_mail_4_0/nsschema/sims*.conf
     <shared-file-system>/NSDS/slapd-<ha-logical-hostname>/config
```

Where

<*shared-file-system*>/NSDS is the directory in which you have installed your NSDS files as entered in step 5.a in "Installing Netscape Directory Services 4.1 for SIMS / HA" on page 122.

<*ha-logical-hostname*> is the name of the machine on which you have installed your NSDS files, as you entered in step 5.d in "Installing Netscape Directory Services 4.1 for SIMS / HA" on page 122.

slapd-<*ha-logical-hostname*> is an instance name assigned to this directory name.

2. **Stop the Netscape Directory Server.**

```
# <shared-file-system>/NSDS/slapd-<ha-logical-hostname>/stop-slapd
```

3. **Open the NSDS' `slapd.conf` configuration file using an editor of your choice.**

```
# vi <shared-file-system>/NSDS/slapd-<ha-logical-hostname>/
config/slapd.conf
```

4. **Include the SIMS/HA 4.1 schema files into the `slapd.conf` file.**

   Find the last *include* statement and then insert the following four lines after that line.

```
include "<shared-file-system>/NSDS/slapd-<ha-logical-hostname>/
config/sims-sisp.at.conf"
include "<shared-file-system>/NSDS/slapd-<ha-logical-hostname>/
config/sims-sisp.oc.conf"
include "<shared-file-system>/NSDS/slapd-<ha-logical-hostname>/
config/sims.at.conf"
include "<shared-file-system>/NSDS/slapd-<ha-logical-hostname>/
config/sims.oc.conf"
```

Note – The sequence of the include statements are important. The `at.conf` files *must* precede the `oc.conf` files.

---

5. **Save the `slapd.conf` file and exit.**

6. **Append the SIMS/HA indexes to the NSDS configuration files.**

```
# cat /cdrom/sun_internet_mail_4_0/nsschema/nsds.index.conf >>
<shared-file-system>/NSDS/slapd-<hostname>/config/
slapd.ldbm.conf
```

7. **Start the Netscape Directory Server.**

```
# <shared-file-system>/NSDS/slapd-<ha-logical-hostname>/start-slapd
```

Setting up the Netscape Directory Services Administration Server for SIMS / HA

Once you have completed configuring the Directory Services you will need to set up the Netscape Directory Services Administration server.

To set up the NSDS Administration server:

1. **Look up the Netscape server IP address.**

```
# <shared-file-system>/NSDS/shared/bin/ldapsearch -p <portnumber>
-b “o=NetscapeRoot” -D “cn=<Directory Manager>” -w <PASSWD>
“(&(cn=configuration) (objectclass=nsConfig))”
```

Check for the current **nsserveraddress** attribute. If this attribute is the physical address, continue on to step 2; otherwise, skip to step 4.

Make sure that your `LD_LIBRARY_PATH` includes `<shared-file-system>NSDS/lib`.

2. **Change the nsserveraddress to the logical address for the system.**

```
# <shared-file-system>/NSDS/shared/bin/ldapmodify -p <portnumber>
-D “cn=<Directory Manager>” -w <PASSWD>

dn: cn=configuration, cn=admin-serv-<ha-logical-hostname>,
cn=Netscape Administration Server, cn=Server Group, cn=<ha-
logical-hostname>, ou=<root domain name>, o=NetscapeRoot
```

Where <*root domain name*> is the root domain name for the server.

After pressing **Return**, enter the following information pressing **Return** after each entry.

```
changetype: modify
replace: nsserveraddress
nsserveraddress: <ha-logical-host-ipaddress>
```

3. **Once you have completed the modification, press Control+C to exit the command**

You will now be presented with a shell prompt.

4. **Restart the Netscape Directory Server.**

```
# <shared-file-system>/NSDS/slapd-<ha-logical-hostname>/stop-
slapd
# <shared-file-system>/NSDS/slapd-<ha-logical-hostname>/start-
slapd
```

5. **Restart the Administration server. Look up the Netscape server address.**

```
# <shared-file-system>/NSDS/stop-admin
# <shared-file-system>/NSDS/start-admin
```

Disabling the Netscape Directory Services uid Uniqueness for SIMS / HA

After installing and configuring NSDS, the next step is to disable the uid uniqueness feature in the NSDS configuration.

By default, NSDS enforces unique user IDs throughout its entire directory tree (that is, from the root tree at the `o=internet` node down).

Since SIMS / HA 4.0 provides domain hosting, it must be able to use the same user ID within different domains. For this reason, you need to disable the uid uniqueness settings here.

Note – If you are going to use SIMS / HA within one domain and will not be using it for domain hosting or with multiple domains, you may bypass the instructions in this section.

To disable NSDS uid uniqueness:

1. **Start the Netscape Console.**

```
# <shared-file-system>/NSDS/startconsole &
```

2. **Log into the Netscape Console.**

   The login uid and password are the same as the Administrator ID that you entered in step 5.e in “Installing Netscape Directory Services 4.1 for SIMS / HA” on page 122.

   To choose the logical host at the Console, replace the URL physical host name with the logical host name.

3. **Expand `<ha-logical-hostname>.<domainame>` on the Netscape Console screen.**

   Where <*ha-logical-hostname*>.<*domainame*> is the domain name in which the host name is located**.**

4. **Expand `Server Group`.**

5. **Double click `Directory Server`.**

6. **Select the `Configuration` tab.**

7. **Expand `Plugins`.**

8. **Click `uid uniqueness`.**
9. **Uncheck `Enable Plugin`.**
10. **Click `Save`.**
11. **Select `Console->Exit`.**
12. **Restart the Netscape Directory Server.**

```
# <shared-file-system>/NSDS/slapd-<ha-logical-hostname>/stop-slapd
# <shared-file-system>/NSDS/slapd-<ha-logical-hostname>/start-slapd
```

Guidelines for Installing and Configuring Sun Cluster and High Availability

1. **Install the following three SunCluster HA-NSDS packages on both nodes using `pkgadd`.**

   SUNWscpro

   SUNWscds

   SUNWscnsl

   Note – These packages are available on the Sun Cluster CD-Rom.

2. **Enter the following command.**

```
# /opt/SUNWcluster/bin/hadsconfig
```

   This begins the configuration process.

3. **Select option 1 from the configuration menu. Where option 1 is:**

   nsldap - HA-LDAP for Netscape

4. **Select option 1 from the next screen. Where option 1 is:**

   Create a new instance

5. **In the screens that follow, enter the information outlined here.**

Note – The above listed items may be altered to suit your needs.

Name of the instance: NSDS

Logical host: <*ha-logical-hostname*>

Base directory of product installation: <*shared-file-system*> / NSDS

Server Port Number: [389]

Time between probes (sec): [60]

Time out value for the probe (sec): [30]

Add this instance to configuration (yes / no): [yes]

Update configuration from workfile (yes / no): [yes]

Note – If you receive the following prompt; “Please manually copy the file `/etc/opt/SUNWscnsl/hadsconf` to <mcm-up>,” it simply means that <mcm-up> is the other physical node. All that needs to be done is to follow the instruction, and copy the file to the same directory on that node. The most convenient way of copying these files is by using FTP.

6. **You now need to edit the `/SUNWcluster/ha/nsldap_svc_stop` script on both nodes.**

   Make the following change to the `method_timeout` line.

   ```
   method_timeout=’hareg -q nsldap -T stop’
   ```

   Change to:

   ```
   method_timeout=’hareg -q NSDS -T stop’
   ```

7. **Create the appropriate links using the following commands.**

```
# ln -s <shared-file-system>/NSDS/slapd-<ha-logical-hostname>/
start-slapd <shared-file-system>/NSDS/start

# ln -s <shared-file-system>/NSDS/slapd-<ha-logical-hostname>/
stop-slapd <shared-file-system>/NSDS/stop
```

Guidelines for Installing SIMS / HA with the Netscape Directory

Since Netscape Directory Services software is installed separately, the specific information about the setup of NSDS is not available to SIMS / HA. This section lists the criteria specific to Netscape Directory Services that you will need to enter during the installation of SIMS / HA.

Use the notes in this section in accordance with Chapter 7, “Installing SIMS 4.0," which covers the instructions for installing SIMS.

The following is a summary of the questions that you will be asked by the SIMS installation GUI while installing SIMS with NSDS. The instructions cover the specific fields on the Directory Services Information and Configuration Page 1 of the SIMS installation GUI, which is shown in FIGURE B-1.

To install SIMS with the Netscape Directory:

1. **Make sure that the LDAP Server Name assigned to the Directory Services Server Name on the Directory Services Information page is where your NSDS software is located.**

   This is shown in FIGURE B-1.

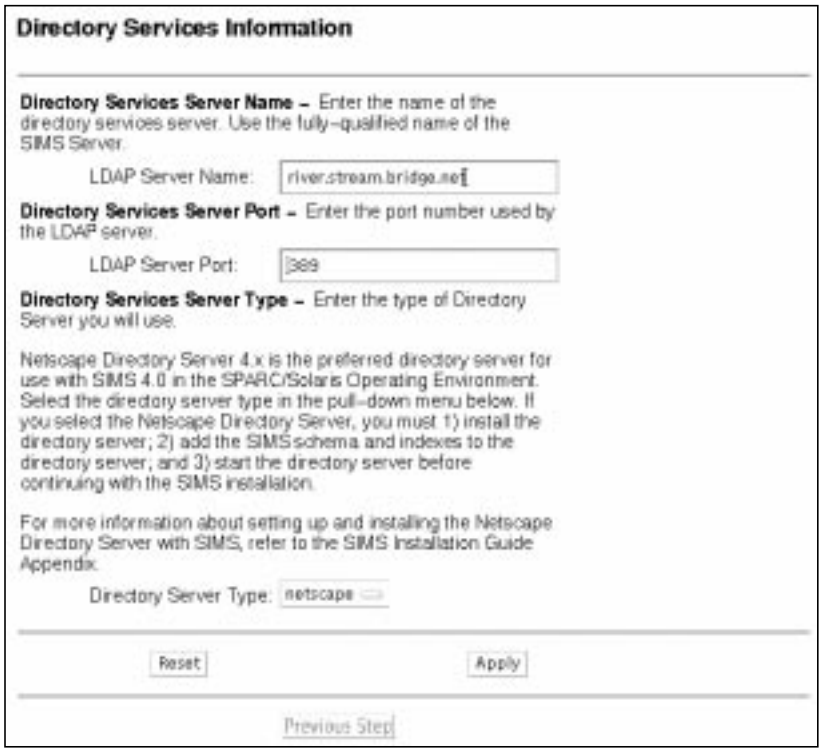


FIGURE B-1 SIMS Installation Directory Services Information Page

   By default, SIMS assumes that you have installed your NSDS software on the same machine that you are installing SIMS. If you have installed NSDS on a remote machine, you need to enter the fully qualified name of the server where NSDS resides.

2. **Type the Directory Services Server Port, which is the port number that you used during the NSDS installation.**

   NSDS should have been installed on port 389, unless the port was busy. In this case, you would have needed to use a different port number that you specified as Directory Server Network Port in step 5.c in “Overview of the Netscape Directory Services Installation for SIMS / HA” on page 122.

3. **Select `netscape` as the Directory Services Server Type that appears on the Directory Services Information page of the SIMS 4.0 Installation GUI.**

4. **Make sure that the name assigned to the Directory Administrator Name on the Configuration Page 1 is specified as Directory Manager, as shown in** FIGURE B-2**.**

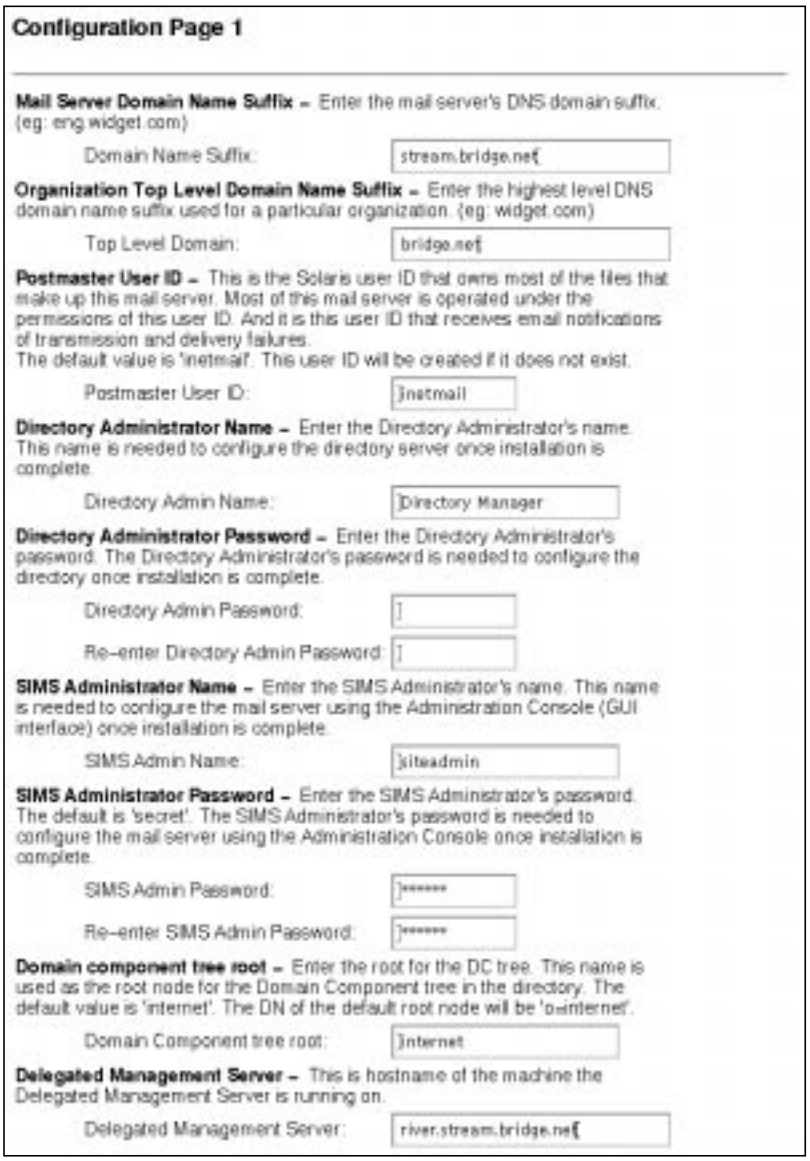


FIGURE B-2 SIMS Installation Configuration Page 1

This is the name you entered while installing NSDS in step 5.g in “Installing Netscape Directory Services 4.1 for SIMS/HA” on page 122.

5. **Type the password for the Directory Administrator Password.**

   This password is the one you entered for Directory Manger in step 5.g. in “Installing Netscape Directory Services 4.1 for SIMS/HA” on page 122.

6. **Make sure that the Domain Component tree root is specified as `internet`, if you are using the SIMS DC tree with the default value** *internet*.

   This is the same Suffix that you entered in step 5.f in “Installing Netscape Directory Services 4.1 for SIMS/HA” on page 122.

Note – If you need to enter this name, do not use the `o=internet` syntax. Instead, type `internet`, because `o=` is automatically prepended to the entry.

Registering the Netscape Directory Service with the High Availability Framework

The following steps take you through the process of registering NSDS with the HA framework.

1. **Stop the SIMS/HA service.**

```
# /opt/SUNWhadf/bin/hareg -n Sun_Internet_Mail
```

2. **Unregister the SIMS/HA service.**

```
# /opt/SUNWhadf/bin/hareg -u Sun_Internet_Mail
```

3. **Register the NSDS/HA service.**

```
# /opt/SUNWhadf/bin/hareg -r NSDS -b /opt/SUNWcluster/ha/nsldap -
m START=nsldap_svc_start,STOP=nsldap_svc_stop -t
START=120,STOP=90
```

4. **Start the NSDS/HA service.**

```
# /opt/SUNWhadf/bin/hareg -y NSDS
```

5. **Re-register the SIMS/HA service.**

```
# /opt/SUNWhadf/bin/hareg -r Sun_Internet_Mail -b /opt/SUNWimha/
clust_proga -m START_NET=imha_start_net, STOP_NET=imha_stop_net -
t START_NET=120,STOP_NET=30 -v 4.0 -d NSDS
```

6. **Start the SIMS/HA service.**

```
# /opt/SUNWhadf/bin/hareg -y Sun_Internet_Mail
```

Note – The NSDS Admin server needs to be manually started after a failover.

Post SIMS Installation Configuration for High Availability

The SIMS installation procedure automatically creates the Directory Information Tree (DIT) that SIMS supports and adds the access control instructions (ACIs) to your NSDS configuration files.

If you have installed SIMS *before* installing NSDS, the SIMS installation will be unable to create this DIT and add the ACIs to the NSDS configuration.

This section describes the commands that you can type manually to:

- Add the SIMS Directory Information Tree (DIT)
- Add the Access Control Instructions (ACIs)

Note – The steps covered in this section are only applicable if for any reason SIMS installation has not added the DIT and ACIs.

Adding the SIMS Directory Information Tree (DIT) for High Availability

Type the following command to create the DIT for your directory:

```
# <shared-file-system>/NSDS/shared/bin/ldapmodify -a -c -h
  <ha-logical-hostname> -p <portnumber> -D “cn=<Directory
  Manager>” -w <passwd> -f /etc/opt/SUNWmail/slapd.ldif
```

where *<dcroot>* is the Directory Component (DC) tree root that you entered in step 5.f in “Installing Netscape Directory Services 4.1 for SIMS/HA” on page 122.

See Chapter 6, “Domain Hosting with SIMS,” in the *Sun Internet Mail Server 4.0 Concepts Guide* for a definition of the DIT and how the information is mapped out.

Adding the Access Control Instructions for High Availability

Access control is the mechanism by which you can set permissions for the entire directory, a subset of the directory, specific entries in the directory, a specific set of entry attributes, or configuration tasks for any 4.x Netscape Server. When the server evaluates an incoming request, it determines the access type based on the access control instructions (ACIs) that you define. The collection of ACIs within a single suffix (The DC tree root) is called an access control list (ACL). See the Netscape documentation for more information about ACIs.

To add the ACIs to your Netscape Directory configuration:

1. **Add the ACIs.**

```
# <shared-file-system>/NSDS/shared/bin/ldapmodify -h <ha-logical-
hostname>
  -p <portnumber> -D “cn=<Directory Manager>” -w <passwd>
  -f /etc/opt/SUNWmail/nsds.acl.ldif
```

Procedure for Removing the NSDS Data Service

It is recommended that you remove the NSDS Data Service prior to uninstalling SIMS from your system.

To remove the NSDS Data Service:

1. **Stop the SIMS/HA service.**

```
# /opt/SUNWhadf/bin/hareg -n Sun_Internet_Mail
```

2. **Unregister the SIMS/HA service.**

```
# /opt/SUNWhadf/bin/hareg -u Sun_Internet_Mail
```

3. **Stop the NSDS/HA service.**

```
# /opt/SUNWhadf/bin/hareg -n NSDS
```

4. **Unregister the NSDS/HA service.**

```
# /opt/SUNWhadf/bin/hareg -u NSDS
```

Once you have completed these steps, you may now use the uninstall command.

APPENDIX **C**

Commandline Installation

This appendix provides information on commands that you can use to install and uninstall your SIMS server using the commandline. It also gives you an example for installing SIMS from commandline. At the end, comparison between graphical user interface (GUI) installation versus commandline installation is provided.

- Command line utilities
- SIMS Administration commandline interface
- Delegated Administration commandline interface
- The uninstall utility
- Graphical or commandline installation

Commandline Utilities

This section describes the utilities that are associated with the installation process.

Installation Utility

The `setup-tty` script installs SIMS and its related files and packages onto the system. `setup-tty` should be run as root.

Note – Because `setup-tty` is not installed on the target system, you must retrieve the `setup-tty` program from the distribution image and not from the system.

The syntax for using this command is:

```
/cdrom/sun_internet_mail_4_0/products/sims/setup-tty [-c install
| remove | removeall] [-d]
```

The options for this command are:

TABLE C-1 Options for the setup-tty Command

Option	Description
`-c install`	Specifies a standard install of SIMS and related files and packages.
`-c remove`	Specifies an uninstall of SIMS and related packages and files from the system.
`-c removeall`	Specifies an uninstall of SIMS and related packages and files plus all configuration files and data.
`-d`	Specifies a non interactive automated install using the `/tmp/sims_setup.dat` file, if it exists. If `/tmp/sims_setup.dat` does not exist, `setup-tty` will default to the standard interactive install and prompt the user for necessary information. See the *Sun Internet Mail Server 4.0 Reference Manual* for the format of the file `sims_setup.dat`.

The following command performs a standard interactive installation:

```
# setup-tty -c install
```

If you do not specify any arguments while invoking this command, by default `setup-tty` will perform a `-c install` operation.

Execute the following to uninstall SIMS and related packages and files from the system:

```
# setup-tty -c remove
```

The following command

```
# setup-tty -d
```

performs a non interactive install that uses the file `/tmp/sims_setup.dat` if it exists. It will gather all necessary configuration data from the `/tmp/sims_setup.dat` file. If the file does not exist, `setup-tty` reverts to the interactive install, which prompts the user for necessary information. If `/tmp/sims_setup.dat` exists and `setup-tty` is executed without the `-d` option specified, the `/tmp/sims_setup.dat` file is removed and the interactive install continues.

The `uninstall` Utility

The `uninstall` utility removes SIMS and other related files and packages from your system. You can specify `uninstall` to perform a standard or a comprehensive procedure. `uninstall` should be done as root.

Note – The `uninstall` utility may not remove certain packages that are likely to have been installed by a separate application and may be used by that application. This is the case even if SIMS has installed that package upon setup.

The syntax for using this command is:

```
uninstall [-c sims] | [-d sims]
```

The options for this command are:

TABLE C-2 Options for the `uninstall` Command

Option	Description
`-c sims`	Specifies a standard `uninstall` of SIMS and related files and packages.
`-d sims`	Specifies a comprehensive `uninstall` of SIMS and related files and packages. This option removes all data and configuration files. The dramatic `uninstall` option is a clean `uninstall`, removing all files installed by the SIMS installation process and created by SIMS during operation, with the exception of packages that may have already been present before the `uninstall` procedure.

The following command performs a standard `uninstall`:

```
# uninstall -c sims
```

The following command performs a dramatic `uninstall`:

```
# uninstall -d sims
```

Graphical or Commandline Installation

The graphical and the commandline installations both pose the same set of questions and collect the necessary initial configuration information in a similar manner. TABLE C-3 summarizes the significant differences in the two installation interfaces.

TABLE C-3 Main Differences between the Graphical and Commandline Interfaces

Type of Difference	Graphical Installation Method	Command Line Installation Method
Invoking	Use the `setup` command. Initially, you must invoke this browser as user (non-root). Before the installation begins, you must provide your root password in the command tool window that appears after the initial configuration information is collected.	Use the `setup-tty` script. You must invoke this script as `root`.
Order of installing packages	The installation script installs the software packages that comprise the Enterprise or Departmental edition only after you have walked through all of the initial configuration pages.	The installation script installs the software packages that comprise that edition of the software. Once done, it asks for your input in the configuration fields.
Validating syntax	Each time you click on the Go to Next Page button, all the fields on that page are validated for syntax conformance. If accurate, you are allowed to proceed to the next page.	Each time you provide input in a field, your input is validated for syntax conformance. If your input is inaccurate, you will not be allowed to proceed to the next field.
Modifying fields	When the confirmation page appears, you can use the hypertext links to access the field you want to change.	When the confirmation page appears, type the number of the field you want to modify to access the field.
Remotely administering	You can remotely administer the SIMS mail server from Solaris, Windows 95, and Windows NT 4.0 systems.	The TTY session offers no remote administration capabilities.
Licensing	You have a choice of providing your license information manually in each license component field or by providing a path to your license file.	You can only provide license information by indicating a path to your license file. You cannot provide license information in each licensed component field.

Glossary

ACAP Application Configuration Access Protocol. A protocol which enhances IMAP by allowing the user to set up address books, user options, and other data for universal access.

access control rules Rules specifying user permissions for a given set of directory entries or attributes.

access control list (ACL) A set of data associated with a directory that defines the permissions that users and/or groups have for accessing it.

Administration Console or Admin Console A GUI (graphical user interface) which enables you to configure, monitor, maintain, and troubleshoot the SIMS components.

address mapping See forward address mapping or reverse address mapping.

address token The address element of a rewrite rule pattern.

Administration Services A service daemon that administers components of SIMS through a GUI.

agent In the client-server model, the part of the system that performs information preparation and exchange on behalf of a client or server application. See also *MTA*.

alias An alternate name of an email address.

alias file A file used to set aliases not set in a directory, such as the postmaster alias.

APOP Authenticated Post Office Protocol. Similar to the Post Office Protocol (POP), but instead of using a plaintext password for authentication, it uses an encoding of the password together with a challenge string.

attribute The form of information stored and retrieved by the directory service. Directory information consists of entries, each containing one or more attributes. Each attribute consists of a type identifier together with one or more values. Each directory read operation can retrieve some or all attributes from a designated entry.

attribute index An index, or list, of entries which contains a given attribute or attribute value.

autoreply option file A file used for setting options for autoreply, such as vacation notices.

backbone The primary connectivity mechanism of a distributed system. All systems that have connectivity to an intermediate system on the backbone are connected to each other. This does not prevent you from setting up systems to bypass the backbone for reasons of cost, performance, or security.

bang path An address for sending e-mail via UUCP that specifies the entire route to the destination computer. It separates each host name with an exclamation point, which is also known as a bang. For example, the bang path `midearth!shire!bilbo!jsmith` would go to the `jsmith` user account on the `bilbo` host, which is reached by first going to `midearth` and then `shire`.

CA Certificate Authority. An organization that issues digital certificates (digital identification) and makes its public key widely available to its intended audience.

directory cache A temporary storage of information that has been retrieved from the directory.

Certificate Authority See CA.

channel An interface with another SIMS component, another email system, or a mail user agent.

character set labels A name or label for a character set.

client-server model A computing model in which powerful networked computers provide specific services to other client computers. Examples include the name-server/name-resolver paradigm of the DNS and fileserver/file-client relationships such as NFS and diskless hosts.

composition The process of constructing a message by the Mail User Agent (MUA). See also *MUA*.

configuration file A file that contains the configuration parameters for a specific component of the SIMS system.

congestion thresholds A disk space limit that can be set by the system administrator that prevents the database from becoming overloaded by restricting new operations when system resources are insufficient.

conversion channel Converts body of messages from one form to another.

cookie Cookies are text-only strings entered into the browser's memory automatically when you visit specific web sites. Cookies are programmed by the web page author. Users can either accept or deny cookies. Accepting the cookies allows the web page to load more quickly and is not a threat to the security of your machine.

ciphertext Text which has been encrypted. Opposite of plaintext.

daemon A UNIX program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The instigator of the condition need not be aware that a daemon is lurking (though often a program will commit an action only because it knows that it will implicitly invoke a daemon). Typical daemons are print spoolers, e-mail handlers, and schedulers that start up another process at a designated time or condition.

data store A store that contains directory information, typically for an entire directory information tree.

DC tree Domain Component tree. A directory information tree that mirrors the DNS network syntax. An example of a distinguished name in an DC tree would be `cn=billbob,dc=bridge,dc=net,o=internet`

defragmentation The Multiple Internet Mail Extensions (MIME) feature that enables a large message that has been broken down into smaller messages or fragments to be reassembled. A Message Partial Content-Type header field that appears in each of the fragments contains information that helps reassemble the fragments into one message. See also *fragmentation*.

delegated administrator A person who has the privileges to add, modify, delete, and search for group or user entries at a specified hosted domain.

Delegated Management Console A web browser-based software console that allows delegated administrators to add and modify users and groups to a hosted domain. Also allows end users to change their password, set message forwarding rules, set vacation rules, and list distribution list subscriptions.

delegated management server A daemon program that handles access control to the directory by hosted domains.

denial of service attack A situation where an individual intentionally or inadvertently overwhelms your mail server by flooding it with messages. Your server's throughput could be significantly impacted or the server itself could become overloaded and nonfunctional.

dereferencing an alias Specifying, in a bind or search operation, that a directory service translate an alias distinguished name to the actual distinguished name of an entry.

destination channel The last element of a host/domain rewrite rule, in whose queue a message should be placed in for delivery.

directory cache A cache containing the directory information used by the IMTA to deliver mail.

directory context The point in the directory tree information at which a search begins for entries used to authenticate a user and password for Sun Message Store access.

directory entry A set of directory attributes and their values identified by its distinguished name. Each entry contains an object class attribute that specifies the kind of object the entry describes and defines the set of attributes it contains. Also called the *IMTA directory cache.*

directory information tree The tree-like hierarchical structure in which directory entries are organized. Also called a DIT. DITs can be organized along the DNS (DC trees) or Open Systems Interconnect networks (OSI trees).

directory schema The set of rules that defines the data that can be stored in the directory.

directory service A logically centralized repository of information. The component in SIMS that stores user, distribution list, and configuration data.

directory synchronization Because information stored in the directory service is updated as new entries are added, modified and deleted, the information in the IMTA directory cache must be periodically updated with the current information in the directory service. This process is called directory synchronization. Sometimes called a dirsync in reference to the `imta dirsync` command.

dirsync option file A file used to set options for the `dirsync` program which cannot be set through the command line.

disconnected state The mail client connects to the server, makes a cache copy of selected messages, then disconnects from the server.

distinguished name The comma-separated sequence of attributes and values that specify the unique location of an entry within the directory information tree. Often abbreviated as DN.

distribution list A list of email addresses (users) that can be sent a message by specifying one email address. Also called a group. See also *expansion*, *member*, *moderator*, *owner,* and *alias*.

distribution list owner An individual who is responsible for a distribution list. An owner can add or delete distribution list members. See also *distribution list*, *expansion*, *member,* and *moderator.*

DIT See *directory information tree*.

DN Distinguished name.

DNS Domain Name System. A distributed name resolution software that allows computers to locate other computers on a UNIX network or the Internet by domain name. DNS servers provide a distributed, replicated, data query service for translating host names into Internet addresses.

DNS database A database of domain names (host names) and their corresponding IP addresses.

domain A group of computers whose host names share a common suffix, the *domain name*. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by periods (dots), for example, `tundra.mpk.ca.us`.

domain quota The amount of space, configured by the system administrator, allocated to a domain for email messages.

domain rewriting rules See also *rewrite rules*.

domain template The part of a rewrite rule that defines how the host/domain portion of an address is rewritten. It can include either a full static host/domain address or a single field substitution string, or both.

dsservd A daemon that operates that accesses the database files that hold the directory information, and communicates with directory clients using the LDAP protocol.

EMAPI Extended MAPI Service Provider. Transparently turns Microsoft Exchange client into an Internet standard IMAP/LDAP client. See also *IMAP*, *LDAP*.

encryption Scrambling the contents of a message so that its contents cannot be read without the encryption, or code key.

entries User, group, or organizational data used to configure message accounts.

envelope The part of an Internet mail message that contains the delivery information. The envelope contains the originator and recipient information associated with a message.

ESMTP Extended Simple Mail Transfer Protocol. An Internet message transport protocol.

expander Part of an electronic mail delivery system which allows a message to be delivered to a list of addressees. Mail expanders are used to implement mailing lists. Users send messages to a single address (e.g., hacks@somehost.edu) and the mail expander takes care of delivery to the mailboxes in the list. Also called *mail exploders*.

expansion This term applies to the IMTA processing of distribution lists. The act of converting a message addressed to a distribution list into enough copies for each distribution list member.

expunge The act of marking a message for deletion and then permanently removing it from you INBOX.

external channel An interface between the IMTA and either another SIMS component or another component outside the SIMS email system.

failover The automatic transfer of a computer service from one system to another to provide redundant backup.

Filesharing Transport This type of transport moves messages between the UNIX operating system and the PC running a client through a shared file system available to both platforms. When a channel is configured to use filesharing transport, the shared directory to use for the file exchange must be specified.

firewall A dedicated gateway machine with special security precautions used to service outside network, especially Internet, connections and dial-in lines. The idea is to protect a cluster of more loosely administered machines hidden behind the firewall from unwanted entry from outside the firewall.

folder Named place where mail is stored. Also called a *mailbox*. Inbox is a folder that stores new mail. Users can also have folders where mail can be stored. A folder can contain other folders in a hierarchical tree. Folders owned by a user are called *private folders*. See also *shared folders*.

Folder Check A utility which checks the accessibility of messages and folders and verifies links. This utility is used as part of the regular maintenance of SIMS.

forward address mapping Message envelopes, TO:address, are processed to a mapping table. The result of the mapping is tested. If necessary, the exact form of the envelope is exchanged for another which can then be processed by a different, and perhaps non-compliant RFC 822, mail system.

FQDN See fully qualified domain name.

fragmentation The Multiple Internet Mail Extensions (MIME) feature that allows the breaking up of a large message into smaller messages. See also *defragmentation*.

full static host/domain address The portion of a host/domain address elements set off by decimals as part of the domain template. See also *domain template*.

fully qualified domain name The full name of a system, consisting of its local host name and its domain name. For example, *class* is a host name and *class.sun.edu* is an fully qualified domain name. A fully qualified domain name should be sufficient to determine a unique Internet address for any host on the Internet. The same naming scheme is also used for some hosts that are not on the Internet, but share the same name-space for electronic mail addressing. A host which does not have a fully qualified domain name must be addressed using a bang path.

gateway The terms *gateway* and *application gateway* refer to systems that do translation from one native format to another. Examples include X.400 to/from RFC 822 electronic mail gateways. A machine that connects two or more electronic mail systems (especially dissimilar mail systems on two different networks) and transfers messages between them. Sometimes the mapping and translation can be complex, and it generally requires a store-and-forward scheme whereby the message is received from one system completely before it is transmitted to the next system after suitable translations.

global log manager A utility that handles log information from each Sun Internet Mail Server component.

group Same as a distribution list.

group folders These contain folders for shared and group folders. See *shared folder.*

header The part of an Internet mail message that is composed of a field name followed by a colon and then a value. Headers include delivery information, summaries of contents, tracing, and MIME information.

hosted domain An email domain that is outsourced by an ISP. That is, the ISP provides email domain hosting for an organization by operating and maintaining the email services for that organization. A hosted domain shares the same SIMS host with other hosted domains. In earlier LDAP-based email systems, a domain was supported one or more email server hosts. With SIMS, many domains can be hosted on a single server. Hosted domains are also called *virtual hosted domains* or *virtual domains.*

host name The logical name assigned to a computer. On the Web, most hosts are named `www`; for example, `www.mycompany.com`. If a site is composed of several hosts, they might be given different names such as `support.mycompany.com` and `sales.mycompany.com`. `support` and `sales` are the host names, `mycompany` is the subdomain name, and `com` is the top-level domain name.

IMAP4 Internet Message Access Protocol. IMAP4 provides advanced disconnected mode client access.

IMTA Internet Message Transfer Agent. IMTA routes, transports, and delivers Internet Mail messages within the email system.

internal channel An interface between internal modules of the IMTA. Internal channels include the reprocessing, conversion, and defragmentation channels. These channels are not configurable.

Internet A collection of networks interconnected by a set of routers that allow them to function as the largest single world-wide virtual network.

internet protocol address A 32-bit address assigned to hosts using TCP/IP. Also called the *IP address* and *internet address.*

invalid user An error condition that occurs during message handling. When this occurs, the message store sends a communication to the Internet Message Transport Agent (IMTA), the message store deletes its copy of the message. The IMTA bounces the message back to the sender and deletes its copy of the message.

ISP Internet Service Provider. A company that provides internet services to its customers including email, electronic calendaring, access to the world wide web, and web hosting.

job controller An IMTA daemon responsible for scheduling message delivery. Job controller also controls channel queues and determines the order of processing. Requests are processed in the order in which they are received by the system.

knowledge information Part of the directory service infrastructure information. The directory server uses knowledge information to pass requests for information to other servers.

LDAP Lightweight Directory Access Protocol. LDAP is a protocol used for the storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data.

LDAP referrals An LDAP entry that consists of a symbolic link (referral) to another LDAP entry. An LDAP referral consists of an LDAP host and a distinguished name. LDAP referrals are often used to reference existing LDAP data so that this data does not have to be replicated. They are also used to maintain compatibility for programs that depend on a particular entry that may have been moved.

LDAP Server A software server that maintains an LDAP directory and services queries to the directory. The Sun Directory Services and the Netscape Directory Services are implementations of an LDAP Server.

LDAP server failover A backup feature for LDAP servers. If one LDAP server fails, the system can switch over to another LDAP server.

LDAP filter A way of specifying a set of entries, based on the presence of a particular attribute or attribute value.

LDBM LDAP Data Base Manager.

LDIF LDAP Data Interchange Format. A data format used to represent LDAP entries in text form.

local channel A channel that allows you to determine delivery options of local users and delivers mail to Solaris Operating Environment mailboxes.

lookup Same as a search, using the specified parameters for sorting data.

mailbox A place where messages are stored and viewed. See *folder*.

managed object A collection of configurable attributes, for example, a collection of attributes for the directory service.

mapping tables Two column tables which transform, map, an input string into an output string.

master directory server The directory server that contains the data that will be replicated.

master message catalog Contains message catalogs for the SIMS components.

master program A channel program that initiates a message transfer to another interface on its own.

member A user or group who receives a copy of an email addressed to a distribution list. See also *distribution list*, *expansion*, *moderator*, and *owner*.

Message Access and Store The SIMS components which store user messages and allow for retrieval and processing of messages.

Message Access Services Consists of protocol servers, software drivers, and libraries which support client access to the message store.

message access services The drivers and libraries that support client access to the SIMS message store.

message catalogs The log messages, command line responses, and graphical user interface screen text contained in the SIMS components.

message submission The client Mail User Agent (MUA) transfers a message to the mail server and requests delivery.

MIB Management Information Base. A collection of objects that can be accessed via a network management protocol. See also *SMI*.

MIME Multipurpose Internet Mail Extensions. A format for defining email message content.

moderator A person who first receives all email addressed to a distribution list before A) forwarding the message to the distribution list, B) editing the message and then forwarding it to the distribution list, or C) not forwarding the message to the distribution list. See also *distribution list*, *expansion*, *member*, and *owner*.

MTA Message Transfer Agent. An OSI application process used to store and forward messages in the X.400 Message Handling System. Equivalent to Internet mail agent. See *IMTA*.

MUA Mail User Agent. The client applications invoked by end users to read, submit, and organize their electronic mail.

mx record Mail Exchange Record. A DNS resource record stating a host that can handle electronic mail for a particular domain.

name resolution The process of mapping an IP address to the corresponding name. See also *DNS*.

namespace The space from which an object name is derived and understood. Files are named within the file namespace, domain components are named within the domain namespace.

naming attribute The final attribute in a directory information tree distinguished name. See also *relative distinguished name*.

naming context A specific subtree of a directory information tree that is identified by its DN. In SIMS, specific types of directory information are stored in naming contexts. For example, a naming context which stores all entries for marketing employees in the XYZ Corporation at the Boston office might be called ou=mktg, ou=Boston, o=XYZ, c=US.

NIS A distributed network information service containing key information about the systems and the users on the network. The NIS database is stored on the master server and all the replica or slave servers.

NIS+ A distributed network information service containing hierarchical information about the systems and the users on the network. The NIS+ database is stored on the master server and all the replica servers.

nondelivery report During message transmission, if the IMTA does not find a match between the address pattern and a rewrite rule, the IMTA sends a nondelivery report back to the sender with the original message.

notary messages Text messages sent by the MTA to an email sender indicating delivery or non-delivery status of a sent message.

object class A template specifying the kind of object the entry describes and the set of attributes it contains. For example, SIMS specifies an `emailPerson` object class which has attributes such as `commonname`, `mail` (email address), `mailHost`, and `mailQuota`.

off-line state The mail client fetches messages from a server system to a client system, which may be a desktop or portable system and may delete them from the server. The mail client downloads the messages where they can be viewed and answered.

on-line state A state in which messages remain on the server and are remotely responded to by the mail client.

option files IMTA option files contain global parameters used to override default values of parameters which apply to IMTA as a whole, such as sizes for various tables into which various configuration and alias files are read.

OSI tree A directory information tree that mirrors the Open Systems Interconnect network syntax. An example of a distinguished name in an OSI tree would be `cn=billt,o=bridge,c=us`

permanent failure An error condition that occurs during message handling. When this occurs, the message store deletes its copy of an email message. The Internet Message Transport Agent (IMTA) bounces the message back to the sender and deletes its copy of the message.

pipe channel A channel which performs delivery of messages via a per-user-site-supplied program. These programs must be registered in SIMS by the system administrator, and thus do not pose a security risk.

plaintext Unencrypted readable text. The opposite of cypher text

plaintext authentication Authentication that occurs by sending passwords over the network in plaintext. Considered a security problem since plaintext passwords can be easily captured over a network.

POP Post Office Protocol. POP provides remote access support for older mail clients.

populating the directory Entering information for users and distribution lists to the SIMS directory service.

protocol A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.

provisioning The process of adding, modifying or deleting entries in the SIMS directory service. These entries include users and groups.

provisioning commands SIMS commands that provide provisioning functions. These commands are prefaced with `imadmin`.

proxy The mechanism whereby one system "fronts for" another system in responding to protocol requests. Proxy systems are used in network management to avoid having to implement full protocol stacks in simple devices, such as modems.

public key encryption A cryptographic method that uses a two-part key (code) that is made up of public and private components. To encrypt messages, the published public keys of the recipients are used. To decrypt the messages, the recipients use their unpublished private keys known only to them.

purge The process of permanently removing messages that have been deleted and are no longer referenced in user and group folders and returning the space to the Sun Message Store file system. See also *backup* and *restore*.

quota See user quota.

referral A process by which the directory server returns an information request to the client that submitted it, with information about the Directory Service Agent (DSA) that the client should contact with the request. See also *knowledge information*.

relaying A message is passed from one mail server to another mail server.

relative distinguished name The final attribute and its value in the attribute and value sequence of the distinguished name. See also *distinguished name*.

replica directory server The directory that will receive a copy of all or part of the data.

reprocessing channel Performs deferred processing. The reprocessing channel is the intersection of all other channel programs. It performs only the operations that are shared with other channels.

restore The process of restoring the contents of folders from a backup device to the Sun Message Store. See also *backup* and *purge*.

reverse address mapping Addresses are processed to a mapping table, with a reversal database, generally substituting a generic address, possibly on a central machine, for an address on a remote or transitory system.

rewrite rules Also known as domain rewriting rules. A tool that the Internet Mail Transport Agent (IMTA) uses to route messages to the correct host for delivery. Rewrite rules perform the following functions: (1) extract the host / domain specification from an address of an incoming message, (2) match the host / domain specification with a rewrite rule pattern, (3) rewrite the host / domain specification based on the domain template, and (4) decide which IMTA channel queue the message should be placed in.

RFC Request For Comments. The document series, begun in 1969, describes the Internet suite of protocols and related experiments. Not all (in fact very few) RFCs describe Internet standards, but all Internet standards are published as RFCs. See `http://www.imc.org/rfcs.html`.

root entry The first entry of the directory information tree (DIT) hierarchy.

router A system responsible for determining which of several paths network traffic will follow. It uses a routing protocol to gain information about the network, and algorithms to choose the best route based on several criteria known as “routing metrics.” In OSI terminology, a router is a Network Layer intermediate system. See also *gateway*.

routability scope Specifications which enable the IMTA to send messages by the most direct route, either to a specific user's folder, a group of folders, or to a mail host.

routing In an email system, the act of delivering a message based on addressing information extracted from the body of the message. The Internet Message Transfer Agent (IMTA) is the component responsible for routing messages.

safe file system A file system performs logging such that if a system crashes it is possible to rollback the data to a pre-crash state and restore all data. An example of a safe file system is Veritas File System, VxFS.

schema A set of rules which sets the parameters of the data stored in a directory. It defines the type of entries, their structure and their syntax.

sendmail This program acts as a mail transport agent for Solaris software. It is responsible for routing mail and resolution of mail addresses.

shared folder or shared mailbox *A* mailbox that can be viewed by members of a *distribution list*. Shared folders have an *owner* who can add or delete members to the group and can delete messages from a the shared folder. The can also have a moderator who can edit, block, or forward incoming messages.

SIMS administrator An individual who has a valid log in and password for the SIMS Admin Console. This person can also use this log in and password to execute the provisioning CLIs.

single field substitution string Part of the domain template that dynamically rewrites the specified address token of the host/domain address. See also *domain template.*

SKIP Simple Key management for IP. A security system that encrypts or scrambles the text of a message so only the receiving mail client or message server can decrypt or unscramble the text.

slave program A channel program that accepts transfers initiated by another interface.

smart host The mail server in a domain to which other mail servers, forward messages if they do not recognize the recipients.

SMTP Simple Mail Transfer Protocol. The Internet electronic mail protocol. Defined in RFC 821, with associated message format descriptions in RFC 822.

SMTP Dispatcher A multithreaded connection dispatching agent which allows multiple multithreaded servers to share responsibility for a given service, thus allowing several multithreaded SMTP servers to run concurrently and handle one or more active connections.

SMTP intranet or internet channel A channel dedicated to relaying messages between the IMTA and a group of SMTP hosts within, or outside of, your mail network.

SMTP router channel SMTP channel that handles messages between the IMTA and firewall host.

SNMP Simple Network Management Protocol. The network management protocol of choice for TCP/IP-based internets.

subordinate reference The naming context that is a child of the naming context held by your directory server. See also *knowledge information*.

Sun Directory Services Sun Microsystems' implementation of an LDAP directory server. Provides storage of, and access to, user profiles, distribution lists, and other SIMS information. The Sun Directory Services is one of the three main SIMS components along with the IMTA and MS/MA.

Sun Internet Mail Server An enterprise-wide, open-standards based, scalable electronic message-handling system.

Sun Message Store The server from which mail clients retrieve and submit messages.

SSL Secure Sockets Layer is an open, non-proprietary security protocol for authenticated and encrypted communication between clients and servers.

synchronization The update of data by a master directory server to a replica directory server.

table lookup With a table consisting of two columns of data, an input string is compared with the data within the table and transformed to an output string.

tailor file An option file used to set the location of various IMTA components.

transient failure An error condition that occurs during message handling. The remote Internet Message Transport Agent (IMTA) is unable to handle the message when it's delivered, but may be able to later. The local IMTA returns the message to the channel queue and schedules it for retransmission at a later time.

transport protocols Provides the means to transfer messages between message stores.

uid User identification. A unique string identifying a user to a system. Also referred to as a userid.

unsafe file system A file system that does not perform logging. If the system crashes, the state cannot be recreated and some data may be lost. You must also perform `imcheck` before activating message access to these files.

upper reference Indicates the directory server that holds the naming context above your directory server's naming context in the directory information tree (DIT).

user entry or user profile Fields that describe information about each user, required and optional, examples are: distinguished name, full name, title, telephone number, pager number, login name, password, home directory, etc.

user folders A user's email mailboxes.

user quota The amount of space, configured by the system administrator, allocated to a user for email messages.

user redirection The remote Internet Message Transport Agent (IMTA) cannot accept mail for the recipient, but can reroute the mail to a mail server that can accept it.

UUCP UNIX to UNIX Copy Program. A protocol used for communication between consenting UNIX systems.

valid user A condition that occurs during message handling. After the message store sends a communication to the Internet Message Transport Agent (IMTA), the IMTA deletes its copy of the message and it is now the message store's responsibility.

`/var/mail` The UNIX version 7 "`From`" delimited mailbox as implemented in the Solaris operating system.

virtual hosted domains or virtual domains See *hosted domains*.

workgroup Local workgroup environment, where the server performs its own routing and delivery within a local office or workgroup. Interdepartmental mail is routed to a backbone server. See also *backbone*.

X.400 A message handling system standard.

Index

H

I

L

M

N

P

R

S

T

U