

Sun Internet Mail Server 3.5 Advanced 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. 805-4376-10
Revision A, September 1998

Copyright 1997-1998 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, California 94303 U.S.A. All rights reserved.

Copyright 1992-1996 Regents of the University of Michigan. All Rights Reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software or documentation without specific prior written permission.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Solaris, Sun Internet Mail Server, HotJava, Java, Sun Workstation, Solstice, Solstice DiskSuite, OpenWindows, SunExpress, SunDocs, Sun Webserver are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the United States and in other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the United States and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

PostScript is a trademark of Adobe Systems, Incorporated, which may be registered in certain jurisdictions.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a).

THIS PUBLICATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

Copyright 1997-1998 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, Californie 94303 Etatis-Unis. Tous droits réservés.

Copyright 1992-1996 Régents de l'Université de Michigan. Tous droits réservés. La redistribution et l'utilisation sous forme de code source et de code binaire sont autorisées à condition que cette notice soit conservée et qu'il soit fait mention de l'Université de Michigan à Ann Arbor. Le nom de l'Université ne pourra être utilisé pour endosser ou promouvoir des produits dérivés de ce logiciel ou de sa documentation sans autorisation écrite préalable.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie et la décompilation. Aucune partie de ce produit ou de sa documentation associée ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Solaris, Sun Internet Mail Server, HotJava, Java, Sun Workstation, Solstice DiskSuite, OpenWindows, SunExpress, SunDocs, Sun Webserver sont des marques déposées, enregistrées, ou marques de service de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC, utilisées sous licence, sont des marques déposées ou enregistrées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

PostScript est une marque de fabrique d'Adobe Systems, Incorporated, laquelle pourrait être déposée dans certaines juridictions.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



Contents

About This Book	13
Who Should Use This Book	14
Conventions	14
Related Documentation	15
SIMS Documentation	15
Other Related Sun Documentation	15
Shell Prompts in Command Examples	16
Graphical User Interface Conventions	17
1. Overview of SIMS 3.5 Components	19
SIMS 3.5 Core Components	20
SIMS Internet Message Transfer Agent	20
Indexed Message Store	21
Sun Directory Services	21
SIMS 3.5 Optional Components	22
SIMS High Availability	22
Sun Web Access Server	23
Sun Messaging Connectivity Services	23
Remote Administration Console	23
POP3/IMAP4 Proxy	23

2. Server and Client Requirements	25
Platform Requirements	26
CPU Requirements	26
Disk Space Requirements	26
SMCS Storage Requirements	27
Swap Space Requirements	27
Memory Requirements	27
Client Requirements	28
System Configuration Requirements	28
3. What SIMS 3.5 Installs	29
SIMS 3.5 Contents Directories	30
SIMS 3.5 Installed Packages	30
SIMS 3.5 Installed Files	33
Administration Console Files	33
MTA Files	34
Message Store/Proxy Server Files	36
Sun Directory Services Files	37
SMCS Files	38
Web Access Server Files	39
4. Preparing to Configure	41
Software Requirements	42
Administrator's Required Tasks	42
Summary of Files Configurable by Administrator	43
Default Configurations	44
SIMS Configurable Files	45
Startup Scripts	46

Summary of SIMS Default Configurations	47
5. Preparing to Install SIMS 3.5	49
Preparing to Upgrade	50
Upgrading from SIMS 3.x to SIMS 3.5	50
Upgrading from SIMS 2.0	51
Preparing a Clean System	52
Preparing to Install Patches	54
Required Patches	54
Recommended Patches	55
Installing Patches	56
Preparing to Install and Update Licenses	57
Requesting a License Password	57
Determining Server Configurations	58
Installing and Updating Licensing Information	59
Preparing to Install Proxies	61
Preparing to Install SMCS	62
Determining Transport Protocol	62
Specifying Mail Clients Setup	63
Checking Directory Synchronization	63
Meeting SMCS Requirements	64
6. Installing SIMS 3.5	65
Before Installing	66
Installing SIMS 3.5	66
Running the Installation Script	67
Selecting Installation Type	68
Selecting Optional Components	70
Specifying Licenses	71

	Specifying Core Server Configurations	74
	Specifying Optional Configurations	79
	Running the Setup Install	80
	Installing SIMS Add-on Options	81
	Installing SIMS High Availability	83
	Removing SIMS/HA	90
	Installing Stand-Alone Sun™ Web Access	92
	Installing Remote Administration Console	93
	Installing Pure POP3/IMAP Proxy	96
	After Installing SIMS 3.5	98
7.	Post-Installation Configurations	99
	Upgrading SIMS 3.1/3.2 Directory Contents to SIMS 3.5	100
	Modifying the LDAP Directory Server Schema	100
	Configuring Existing Users in the LDAP Directory Database to Use Web Access	102
	Preparing Configuration File for Mail Users Only	104
	HotJava Browser Configuration	105
	Removing sendmail for Pure POP3/IMAP Proxy	106
8.	Post-installation Sun™ Web Access Setup	107
	Starting Sun Web Access	108
	Reference Chapters for Sun Web Access	108
	Configuring Sun Web Access	108
	Restarting the Web Access Server	109
	Changing the port Number	109
	Establishing Secure Service	110
	Extending the Web Access Palette	112
	Using An Alternate JVM for Web Access	112

Changing the LDAP Server	114
Invoking Web Access	115
9. Post-Installation Tasks	117
Overview of SIMS Post-Installation Tasks	118
Checking SIMS Installation Log Files	118
Starting the Mail Server	118
Linking to an Existing Web Server	119
Connecting to the Manual Pages	119
Starting SIMS Administration Console	120
Starting SIMS Administration Console for HA Systems	120
Starting Sun Web Access Server	121
Populating the Directory	121
Migrating Mail Folders	122
Testing Your SIMS 3.5 Server	123
10. Troubleshooting SIMS Server	125
Configuring DNS Setup	126
Diagnosing DNS	126
Configuring Files	128
Reading SIMS Installation Log Files	129
Rebooting after Reinstalling	129
Configuring HotJava Browser	129
Removing sendmail	130
Missing Command Tool	130
Removing Extra Characters in License Password File	130
Cleaning up Corrupted Quota File	131

11. SIMS Asymmetric High Availability	133
Other HA References in this Guide	134
SIMS Asymmetric HA Configuration	135
Fail-over Procedure	138
Linking SIMS Directories to Shared Disks	138
Linking Sun DS Directories to Shared Disks	138
Replacing HA stop and start Scripts	139
Operating System and Platform Support	139
Storage and File System Requirements	139
Directory Services Considerations	140
A. Command-Line Installation	141
Command-Line Utilities	142
Installation Utility	142
The uninstall Utility	144
Example of Command-Line Installation	145
Graphical or Command-Line Installation?	148
B. Planning SIMS System	149
Directory Services Considerations	150
Automatic Directory Information Tree Layout	152
Directory Service Administration	155
Directory Replication	157
Selecting Topologies	158
E-mail System for a Small Organization	158
E-mail System for a Medium Organization	159
Internet Message Transfer Agent Considerations	168
Role of a Mail Server	168
Sample MTA Scenarios	170

Figures

FIGURE 5-1	SIMS Upgrade Configuration Screen	50
FIGURE 6-1	SIMS 3.5 Installation Information Page	67
FIGURE 6-2	SIMS 3.5 Installation Types	68
FIGURE 6-3	SIMS 3.5 Enterprise Edition Core and Optional Components	68
FIGURE 6-4	SIMS 3.5 Departmental Core and Optional Components	69
FIGURE 6-5	SIMS 3.5 Stand-Alone Components	69
FIGURE 6-6	SIMS 3.5 Installation Steps	70
FIGURE 6-7	SIMS Enterprise Optional Components	70
FIGURE 6-8	License Configuration Page	71
FIGURE 6-9	Core Components Configuration Page 1	74
FIGURE 6-10	Core Components Configuration Page 2	76
FIGURE 6-11	Hierarchy of Organizational Units	77
FIGURE 6-12	Core Components Configuration Page 3	78
FIGURE 6-13	Optional Components Configuration Page	79
FIGURE 6-14	SIMS Add-on Features Screen	81
FIGURE 6-15	SIMS Add-on Features Configurations Screen	82
FIGURE 6-16	SIMS/HA Enterprise Option	86
FIGURE 6-17	SIMS/HA Logical Hostname	87
FIGURE 6-18	SIMS/HA Shared File System	87

FIGURE 6-19	SIMS/HA System	89
FIGURE 6-20	Remote Administration Console Option Page	94
FIGURE 6-21	Remote Administration Console Configuration Summary Page	95
FIGURE 6-22	POP3/IMAP4 Pure Proxy Server Option Page	96
FIGURE 10-1	DNS Diagnostic Procedure	127
FIGURE 11-1	SIMS Asymmetric HA Configuration Before Fail-over	135
FIGURE 11-2	SIMS Asymmetric HA Configuration after Fail-over	137
FIGURE B-1	Directory Information Tree for a Small Organization	151
FIGURE B-2	Directory Information Tree for a Medium or Large Organization	151
FIGURE B-3	Partial Configuration Page 1 of 3	152
FIGURE B-4	Partial Configuration Page 2 of 3	153
FIGURE B-5	Automatically Generated Directory Information Tree for a Small Organization	154
FIGURE B-6	Automatically Generated Directory Information Tree for a Large Organization	154
FIGURE B-7	Centralized Directory Information Tree Administration	156
FIGURE B-8	Distributed Directory Information Tree Administration	156
FIGURE B-9	Sample Directory Information Subtree for a Small Organization	158
FIGURE B-10	Sample Topology for a Small Organization	159
FIGURE B-11	Sample Directory Information Tree for a Medium Organization	160
FIGURE B-12	Sample Topology for a Medium Organization	161
FIGURE B-13	Sample Replication Data Flows for a Medium Organization	162
FIGURE B-14	Sample Directory Information Trees for a Large Organization	164
FIGURE B-15	Sample Topology for a Large Organization	165
FIGURE B-16	Sample Replication Data Flows for a Large Organization	166

Tables

TABLE 2-1	Supported Platforms and Operating System Environments	26
TABLE 2-2	SIMS 3.5 Storage Requirements	26
TABLE 2-3	Memory Requirements for IMAP and POP3 Systems	27
TABLE 2-4	Client Requirements	28
TABLE 3-1	SIMS 3.5 Contents Directories	30
TABLE 3-2	SIMS 3.5 Packages	31
TABLE 3-3	Files Installed for Administration Console Component	33
TABLE 3-4	Files Installed for MTA Component	34
TABLE 3-5	Files Installed for Message Store/Proxy Component	36
TABLE 3-6	Files Installed for Directory Services Component	37
TABLE 3-7	Files Installed for SMCS Component	38
TABLE 3-8	Files Installed for Web Access Server Component	39
TABLE 3-9	SDS-Related Files Installed for Web Access Server Component	39
TABLE 4-1	Applications Installed by Default	42
TABLE 4-2	Summary of Files Configurable Through SIMS Administration Console	43
TABLE 4-3	SIMS Components Installed by SIMS Installation	44
TABLE 4-4	Summary of Files Configurable by Administrator	45
TABLE 4-5	Required Scripts Installed by im.server	46
TABLE 4-6	Summary of SIMS Default Configurations along with their Sources	47

TABLE 5-1	The uninstall Command Options	52
TABLE 5-2	SIMS Required Solaris Patches	54
TABLE 5-3	SIMS Additional Recommended Patches	55
TABLE 6-1	Chapters Required Before Installing SIMS 3.5	66
TABLE 6-2	Chapters Required After Installing SIMS 3.5	98
TABLE 8-1	Chapters Containing Sun Web Access Information	108
TABLE 11-1	Chapters Containing High Availability Information	134
TABLE 11-2	SIMS Directories on the Shared Disk between Cluster Nodes	138
TABLE 11-3	Sun DS Directories Mapped to Shared Disk between Cluster Nodes	138
TABLE 11-4	Tested Platform Configurations	139
TABLE A-1	Options for the setup-ty Command	142
TABLE A-2	Options for the uninstall Command	144
TABLE A-3	Main Differences Between the Graphical and the Command-Line Interface	148
TABLE B-1	Directory Information Tree Layers	150
TABLE 11-5	Sample Topology	163

About This Book

The *Sun Internet Mail Server 3.5 Advanced Installation Guide* describes the planning, installing, and configuring the Sun™ Internet Mail Server™ (SIMS) 3.5 software on Solaris™ SPARC and Intel-based x86 systems.

Topics in this chapter include:

- Who Should Use This Book
- Conventions
- Related Documentation
- Ordering Sun Documents
- Shell Prompts in Command Examples
- Graphical User Interface Conventions

Who Should Use This Book

The intended audience for this installation guide is 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 e-mail system also helps to efficiently use this guide.

Conventions

The following table describes the typographic conventions used in this book.

TABLE P-1 Typographic Conventions

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

Related Documentation

SIMS Documentation

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

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

Sun Internet Mail Server Reference Guide—provides detailed information on command-line options, administrator's configurable files, system architecture, supported standards, and locations of software files.

Sun Messaging Connectivity Services Guide—provides information on installing and configuring the cc:Mail, MS-Mail, and IBM/PROFS channels on the server and on the client systems.

Other Related Sun Documentation

For additional product information, refer to the Sun Internet Mail Server 3.5 web site. The URL is <http://www.sun.com/sims>. At this location, you will find the following information:

- Press releases and data sheets
- Technical white papers
- Product documentation
- Product demos
- Product Frequently Asked Questions (FAQs)
- Links to third party client software

Shell Prompts in Command Examples

The following table 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 Administration Console. The following table defines terms used in procedures associated with the installation or the 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 the radio button.
Double-click	Click a mouse button twice quickly without moving the pointer.	Double-click the SMTP channel name from the list of channels to bring up the SMTP property book.

Overview of SIMS 3.5 Components

Sun Internet Mail Server™ software (SIMS) is a highly scalable, complete client/server solution that can be used effectively by enterprises or by Internet Service Provider (ISP) operations. By enabling the deployment of a high-performance and reliable mail system, SIMS delivers key information services within a service-driven network. SIMS 3.5 is based on Internet standards.

Topics in this chapter include

- Overview of SIMS 3.5 Core Components
- Overview of SIMS 3.5 Optional Components

SIMS 3.5 Core Components

The following shows the core components for both SIMS Enterprise and Departmental editions.

Enterprise Edition Core Components

- Full-featured, multi-threaded MTA
- POP3/IMAP4 Server
- Indexed Message Store
- Sun Directory Services
- SIMS 3.5 Administration Console

Departmental Edition Core Components

- Basic MTA
- POP3/IMAP4 Server
- Indexed Message Store
- Sun Directory Services
- SIMS 3.5 Administration Console

See *Sun Internet Messaging Server 3.5 Administrator's Guide* for more information on all SIMS core components.

SIMS Internet Message Transfer Agent

The Internet Message Transfer Agent (IMTA) routes, transports, and delivers Internet Mail (RFC 822) messages within the email system.

The IMTA performs all of its operations on a set of *channels*. There are two types of channels: internal and external. An internal channel is an interface between internal modules of the IMTA. Internal channels include the reprocessing, conversion, and defragmentation channels. These channels are not configurable from the SIMS Administration Console.

An external channel is an interface between the IMTA and another SIMS component (i.e., the Sun Message Store), or another component outside of SIMS (for example, the Internet or a local mail client). The external channels are configurable.

POP3/IMAP4 Protocol

Post Office Protocol Version 3 (POP3) is an implementation of the server side of the POP3 (RFC 1939) access protocol standard. Many popular mail clients currently use POP3.

Internet Mail Access Protocol Version 4 is an implementation of the server side of the standard IMAP4 protocol (RFC 2060). IMAP4 is used by client mail applications to access Internet email messages in distributed, enterprise/Internet-wide message stores.

Note – With `/var/mail` enabled, the server supports only IMAP4. Clients which *require* IMAP4rev1 cannot be used. With `/var/mail` disabled (which is the default), the server supports both IMAP4 revision 1 and IMAP4 access protocols.

Indexed Message Store

Indexed Sun Message Store is a dedicated data store for the delivery, retrieval, and manipulation of Internet email messages. This message store works with the IMAP4 and POP3 servers that ship with SIMS. It saves any message that conforms to RFC 822 specifications, and recognizes the Multipurpose Internet Mail Extensions (MIME) content format.

The main advantage of the Sun Message Store is its ability to save only a single copy of any outgoing message that is sent to a distribution list, provided all recipients are on the same mail server. For example, if a message is sent to 20,000 users on the same server, only one master copy of the source message is saved in the store. In terms of space usage, the Sun Message Store is very conservative.

Sun Directory Services

Sun Directory Services provide a central repository for meta-information: user profiles, distribution lists, and other system resources. SIMS/HA is bundled with a dedicated Lightweight Directory Access Protocol (LDAP) directory service, but is specifically designed to use any directory service compatible with LDAP version 2.

SIMS 3.5 Optional Components

The following shows SIMS optional components. They are optional features for the Enterprise edition, additions to the Departmental edition, and add-on for stand-alone options.

SIMS High Availability

Enterprise Edition Optional Components

- Sun Web Access Server
- Message Transfer Agent SDK
- SMCS Channel for Lotus cc:Mail
- SMCS Channel for Microsoft Mail
- SMCS Channel for IBM OpenVision/PROFS

Departmental Edition Optional Components

- Web Access
- Message Transfer Agent SDK

Stand-Alone Options

- Web Access
- Message Transfer Agent SDK
- Remote Administration Console
- POP3/IMAP4 Proxy

SIMS High Availability

SIMS 3.5 is a high-performance, highly scalable mail delivery and access system. Since mail is critical to enterprises and ISP customers, many SIMS customers wish to run SIMS on a cluster to get higher availability via fail-over to a surviving member of the cluster.

For this reason, SIMS 3.5 provides *Asymmetric* High Availability (HA) configurations. In this configuration, all the SIMS binaries, configuration files, message queues, and message store reside on a shared disk. When a switch-over occurs, the disk is unmounted from the failing system and mounted on the surviving system.

Sun Web Access Server

Sun™ Web Access is an application that gives end users browser-based access to the SIMS 3.5 E-mail and Name Directory services and to the Solaris Calendar server. Sun Web Access is integrated with the SIMS 3.5 server system and centrally administered. See Chapter “Post-Installation Sun Web Access Setup,” for information on configuring this server.

Sun Messaging Connectivity Services

Sun Messaging Connectivity Services (SMCS) provide batch-mode connectivity to proprietary message transfer systems: Lotus cc:Mail, Microsoft Mail, and the mainframe-base IBM OfficeVision (PROFS).

For complete information on SMCS, refer to the *Sun Messaging Connectivity Services Guide*.

Remote Administration Console

This option allows you to remotely access and use the Administration Console on any other Solaris system that is not running SIMS. It allows you to administer the SIMS server from a remote server.

POP3/IMAP4 Proxy

A proxy message access server differs from a typically configured SIMS server in that instead of serving the POP/IMAP requests itself, it forwards the request to the message access server with the requested mail folders. Message access proxies are useful for a number of reasons such as horizontal scalability and internet access to private intranet mail systems.

Server and Client Requirements

This chapter provides information specific to the hardware and software requirements for installing SIMS 3.5, including:

- Platforms Requirements
- Disk Space Requirements
- Memory Requirements
- Client Computer Requirements

Platform Requirements

The SIMS software is available on SPARC and x86 systems running the operating system versions indicated in TABLE 2-1 below:

TABLE 2-1 Supported Platforms and Operating System Environments

Platform	Operating System
SPARCstation 20 or higher	Sun™ Solaris™ SPARC 2.5.1 and 2.6
Intel x86 series	Sun Solaris Intel 2.5.1 and 2.6

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 3.5 core components, and for the SMCS optional component. 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 Sun Web Access or SDK. Use the `df` command to check the free disk space.

TABLE 2-2 SIMS 3.5 Storage Requirements

Directory Path	SIMS Core Requirement	SMCS Requirement
/opt	90 MB	20 MB
/var	20 MB	See Section SMCS Storage Requirements below.
/usr	10.5 MB	

SMCS Storage Requirements

When SIMS connects to another messaging system, the channel might be unavailable and cause queuing the incoming messages. For this reason, the administrator needs to allocate sufficient storage in the directory `/var/opt/SUNWmail`, where all message queues and temporary files are stored.

For example, the administrator needs to allocate 200 megabytes storage to store two days worth of messages for a mail system that transports 100 messages per day (i.e., each message is 1 megabyte).

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 3.5.

TABLE 2-4 Client Requirements

Client	Requirement
Sun Web Access Software	HTML v3.2 compliant Web Browser
MAPI Providers	Microsoft Windows Messaging inbox, Microsoft Outlook 97

System Configuration Requirements

The following are server computer requirements:

- A valid license token
- DNS installed and running

Note – It is highly recommended that this machine be set up as a DNS server. If you already have another DNS server in your organization, set up this machine as a secondary DNS server or a DNS client.

Java Virtual Machine

The SIMS software is compatible with JVM 1.1.3.

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

The Message Store must be installed on a local disk and not on an NFS or other remote file system mounted partition in Solaris.

What SIMS 3.5 Installs

This chapter provides a list of packages along with the files and scripts that SIMS 3.5 installs. Additionally, the sources for configuring and administering each configuration file are identified.

- SIMS 3.5 Contents Directories
- SIMS 3.5 Installed Packages
- SIMS 3.5 Installed Files

SIMS 3.5 Contents Directories

SIMS 3.5 installs packages, configuration, and user files for each SIMS component in the directories listed in TABLE 3-1 below.

TABLE 3-1 SIMS 3.5 Contents Directories

Type	Directory Path
Package	/opt/SUNWmail
Configuration	/etc/opt/SUNWmail
Data	/var/opt/SUNWmail

See Chapter “SIMS 3.5 Components,” for a complete list of SIMS 3.5 core and optional components.

SIMS 3.5 Installed Packages

TABLE 3-2 shows SIMS packages that are installed for the following components:

- Administration Console
- Message Transfer Agent (MTA)
- Message Transfer SDK
- Message Store/Proxy Server
- Sun Directory Services (SDS)
- Sun Messaging Connectivity Services (SMCS)
- Sun Web Access Server
- SIMS High Availability (HA)
- SIMS Documentation

TABLE 3-2 SIMS 3.5 Packages

SIMS Component Name Package Name	Package Description
SIMS Common Package	
SUNWimcom	Sun Internet Mail Common Package
Administration Console	
SUNWimadm	Sun Internet Mail Administration Services
MTA	
SUNWbbmta	Internet MTA, Enterprise edition
SUNWimmta	Internet MTA, Departmental edition
Message Transfer SDK	
SUNWimsdk	Internet MTA, SDK run time library
SUNWimsdh	Internet MTA, SDK header files
SUNWimsdd	Internet MTA, SDK documentation
Message Store/Proxy Server	
SUNWimimu	Sun Internet Mail Message Store utilities
SUNWimims	Sun Internet Mail Indexed Message Store/Access
SUNWimimm	Sun Internet Mail Message Store man pages
SDS	
SUNWsds	Sun Directory Services
SMCS	
SUNWimc	Sun Messaging Connectivity Services core package
SUNWimccc	Sun Messaging Connectivity Services cc:Mail
SUNWimcms	Sun Messaging Connectivity Services MS-Mail
SUNWimcpr	Sun Messaging Connectivity Services PROFS
HA	
SUNWimha	Sun Internet Mail Server High Availability package
SIMS Documentation	
SUNWimdoc	Sun Internet Mail Server on-line documentation

TABLE 3-2 SIMS 3.5 Packages

SIMS Component Name Package Name	Package Description
Web Access Server	
SUNWwa	Sun Web Access classes, images, html files, etc.
SUNWjeev	Java Web Server

SIMS 3.5 Installed Files

This section shows the files that SIMS 3.5 installs for each of the following components:

- Administration Console
- Message Transfer Agent (MTA)
- Message Store/Proxy Server
- Sun Directory Services (SDS)
- Sun Messaging Connectivity Services (SMCS)
- Sun Web Access Server

Each configuration file is identified as being provided either by SIMS or set up by the administrator, as well as being administered through the SIMS Administration Console, where available.

Administration Console Files

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

TABLE 3-3 Files Installed for Administration Console Component

File Name	Configured by Installation	Configurable by Administrator	Configurable via Admin. Console
<code>adminserver.properties</code>	X		X
<code>backupadminserver.properties</code>	X		MTA, MS
<code>defaultadminserver.properties</code>	X		MTA, MS
<code>scheduled.tsk</code>	X		MTA, MS
<code>defaultscheduled.tsk</code>	X		MTA, MS
<code>backupscheduled.tsk</code>	X		MTA, MS
<code>as.pid</code>			
<code>rmi.pid</code>			
<code>directory.adm</code>			
<code>gw.adm</code>			
<code>imap.adm</code>			
<code>ims.adm</code>			

TABLE 3-3 Files Installed for Administration Console Component

File Name	Configured by Installation	Configurable by Administrator	Configurable via Admin. Console
log.adm			
mta.adm			
user.adm			

MTA Files

Files Directory: /etc/opt/SUNWmail/imta

TABLE 3-4 Files Installed for MTA Component

File Name	Configured by Installation	Configurable by Administrator	Configurable through Admin. Console
address_option.sample		X	
aliases	X		
aliases.lock			
aliases.usr			
channel.cat	X		MTA
chardnames.txt			
charsets.txt			
charsets_ps.txt			
charsubs.txt			
countries.txt			
cronjobs	X		
dispatcher.cnf		X	
dl_auth.map			
imta.cnf	X	X	MTA
imta_tailor			
internet.rules			
job_controller.cnf		X	
magic.dat			
mappings		X	MTA

TABLE 3-4 Files Installed for MTA Component

File Name	Configured by Installation	Configurable by Administrator	Configurable through 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/Proxy Server Files

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

TABLE 3-5 Files Installed for Message Store/Proxy Component

File Name	Configured by Installation	Configurable by Administrator	Configurable through Admin. Console
<code>ims.cnf</code>	X	X	MS
<code>ims.cnf.backup</code>	X		
<code>ims.cnf.default</code>			

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 3-6 Files Installed for Directory Services Component

File Name	Configured by Installation	Configurable by Administrator	Configurable through Admin. Console
directory.adm			
ldapfilter.conf			
ldapsearchprefs.conf			
ldapsync.conf	X	X	
ldaptemplates.conf		X	
sdserver.ini			Directory Configuration
slapd.at.conf	X	X	Directory Configuration
slapd.conf	X	X	Directory Configuration
slapd.oc.conf	X	X	Directory Configuration

SMCS Files

Files Directory: /etc/opt/SUNWmail/gtw/cfg

TABLE 3-7 Files Installed for SMCS Component

File Name	Configured by Installation	Configurable by Administrator	Configurable through Admin. Console
ccmail.attrname			
ccmail.attrval			
ccmail.mfin			
ccmail.mfout			
config.dat			
dir_attrs.txt			MTA, SMCS
dirsync.cf			DirSync Manager
doclog_ccmail.dat			MTA, SMCS
doclog_channel.dat			MTA, SMCS
doclog_msmail.dat			MTA, SMCS
initialization.dat			MTA, SMCS
msmail.attrname			
msmail.attrval			
msmail.mfin			
msmail.mfout			
profs.attrname			
profs.attrval			
profs.mfin			
profs.mfout			
std_bodyparts.txt			

Web Access Server Files

Files Directory: `/opt/SUNWwa/properties`

TABLE 3-8 Files Installed for Web Access Server Component

File Name	Configured by Installation	Configurable by Administrator	Monitor through SIMS Admin. Console
<code>realm.sims.properties</code>	X	X	

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

TABLE 3-9 SDS-Related Files Installed for Web Access Server Component

File Name	Configured by Installation	Configurable by Administrator	Configurable through Admin. Console
<code>imldifsync.conf</code>	X	X	X
<code>WebAccess.oc.conf</code>		X	
<code>WebAccess.at.conf</code>		X	

Chapter “Preparing to Install SIMS 3.5” that follows shows the system requirements, configurations, and considerations that you need to know before installing SIMS 3.5.

Preparing to Configure

This chapter provides you with information on files and packages associated with each component of SIMS. It indicates whether each file is installed automatically, or it should be provided by the administrator.

Topics in this chapter include:

- Software Requirements
- Summary of Files Configurable by Administrator
- Default Configurations
- Startup Scripts
- Summary of SIMS Default Configurations

Software Requirements

SIMS 3.5 requires that the software packages listed in TABLE 4-1 be installed. SIMS installation automatically installs these packages if they are not available on your system.

TABLE 4-1 Applications Installed by Default

Component	Required for	Package Name
Sun Web Server 1.0	SIMS Admin Console	SUNWhttpv—HTTP server var package SUNWhttpu—HTTP server user package SUNWhttpr—HTTP server root package
FlexLM License Systems License Installation Tool	licensing	SUNWlicsw SUNWlit
HotJava Browser for Solaris	SIMS	SUNWdthj
Sun High Availability	SIMS/HA system only	SUNWimha
Secure Sockets Layer (SSL)	Secure server	SUNWski—SKI 1.0 Software user SUNWskica—SKI 1.0 Software CA SUNWskicw—SKI 1.0 Software CA licensing SUNWskimc—SKI 1.0 Software CA manual SUNWskimu—SKI 1.0 Software user manual SUNWssl—SSL 1.0 Software global library

Administrator's Required Tasks

Before installing SIMS 3.5, the administrator is required to perform the operations indicated in this section.

SIMS High Availability Option

The following components are required only if you are installing SIMS on a High Availability system.

1. Load Sun Cluster 2.1 for HA.
2. Load Veritas File System (VxFS) 3.2.4 (or later release) for HA.

SIMS SMCS Option Requirement

If you are selecting SIMS SMCS, you need to enable SPX or PC access for the channels.

Summary of Files Configurable by Administrator

TABLE 4-2 below provides a summary of files that the administrator can configure by using the SIMS Administration Console.

TABLE 4-2 Summary of Files Configurable Through SIMS Administration Console

Component Name	File Name	Admin. Console Screen
Admin. Console	adminsrvr.properties	
MTA	channel.cat imta.cnf mappings	MTA MTA MTA
Message Store/Proxy	ims.cnf	Message Store
SDS	sdsrvr.ini slapd.at.conf slapd.conf slapd.oc.confs imldifsys.conf webaccess.at.conf webaccess.oc.conf	Directory Configuration Directory Configuration Directory Configuration Directory Configuration
SMCS	dir_attr.txt dirsync.cf doclog_ccmail.dat doclog_channel.dat doclog_msmail.dat initialization.dat	MTA, SMCS DirSync Manager MTA, SMCS MTA, SMCS MTA, SMCS MTA, SMCS
Sun Web Access	realm.Sims.properties	User Manager

Default Configurations

TABLE 4-3 below provides a list of components along with their associated configuration files that SIMS automatically installs.

TABLE 4-3 SIMS Components Installed by SIMS Installation

Component Name	File Name	Directory Path
Admin. Console	adminserver.properties	/etc/opt/SUNWmail/admin
MTA	aliases channel.cat imta.cnf	/etc/opt/SUNWmail/imta
Message Store/Proxy	ims.cnf ims.cnf.default	/etc/opt/SUNWmail/ims
SDS	ldapsync.conf slapd.at.conf slapd.conf slapd.oc.conf	/etc/opt/SUNWconn/ldap/current
Sun Web Access	realm.Sims.properties imldifsys.conf webaccess.at.conf webaccess.oc.conf	/opt/SUNWwa/properties /etc/opt/SUNWmail/dir_svcs

SIMS Configurable Files

TABLE 4-4 below provides a summary of SIMS 3.5 files that have already been installed by default, but they can be configured by the administrator.

TABLE 4-4 Summary of Files Configurable by Administrator

SIMS Component Name	File Name	Directory Path
MTA	address_option.sample	/etc/opt/SUNWmail/imta
	dispatcher.cnf	
	imta.cnf	
	job_controller.cnf	
	mappings	
	option.dat	
Message Store/Proxy	ims.cnf	/etc/opt/SUNWmail/ims
SDS	ldapsync.conf	/etc/opt/SUNWconn/ldap/current
	slapd.at.conf	
	slapd.conf	
	slapd.oc.confs	
	imldifsyms.conf	/etc/opt/SUNWmail/dir_svc
	webaccess.at.conf	
	webaccess.oc.conf	
Sun Web Access	realm.Sims.properties	/opt/SUNWwa/properties

Startup Scripts

SIMS provides the startup script `/etc/init.d/im.server`, which in turn installs the scripts listed in TABLE 4-5.

After installing SIMS, the administrator has to run this script to startup the SIMS server. See Chapter “Post-Installation Configurations,” for more information on the `im.server` script.

TABLE 4-5 Required Scripts Installed by `im.server`

Script Name	Application Name
<code>mt.scheduler</code>	Message Store/Proxy server
<code>slapd</code>	SDS daemon
<code>httpd</code>	Web Server
<code>lic-mgr</code>	License Manager
<code>web500gw</code>	Web Gateway
<code>smcs</code>	Sun Messaging Connectivity Services (if SMCS option is selected)
<code>imta</code>	SIMS Internet Message Transfer Agent

Summary of SIMS Default Configurations

TABLE 4-6 summarizes the components that SIMS 3.5 installs as well as the tasks that are performed either by default or by the administrator.

TABLE 4-6 Summary of SIMS Default Configurations along with their Sources

Component/Task name	Description of Requirement	Done by Administrator	Done by Install anyway	Done by Install if you don't have
DNS	Setting up these files: /etc/nsswitch.conf /etc/resolv.conf	X		
sendmail	Removing		X	
/etc/init.d/im.server mt.scheduler—Message Store/Proxy server slapd—SDS daemon httpd—Web Server lic_mgr—License Manger web500gw—Web Gateway smcs—Sun Messaging Connectivity Services imta—SIMS Internet Message Transfer Agent	Startup scripts		X	
Sun Cluster 2.1	Required for HA	X		
Veritas File System 3.2.4 (or later release)	Required for HA	X		
Sun Web Server 1.1.5, packages: SUNWhhttpv—HTTP server var package SUNWhhttpu—HTTP server user package SUNWhhttpr—HTTP server root package	Required for SIMS Admin Console			X
SPX or PC access	Required for SMCS	X		
FlexLM License Systems—SUNWlicsw STE License Installation Tool—SUNWlit	Required for licensing			X
HotJava Browser for Solaris - SUNWdthj	Required for SIMS			X
Secure Sockets Layer, packages: SUNWski—SKI 1.0 Software user SUNWskica—SKI 1.0 Software CA SUNWskicw—SKI 1.0 Software CA licensing SUNWskimc—SKI 1.0 Software CA manual SUNWskimu—SKI 1.0 Software user manual SUNWssl—SSL 1.0 Software global library	Required for secure server			X

TABLE 4-6 Summary of SIMS Default Configurations along with their Sources

Component/Task name	Description of Requirement	Done by Administrator	Done by Install anyway	Done by Install if you don't have
Core Java Packages: SUNWjvrt - JavaVM run time environment SUNWjvjit - Java JIT compiler SUNWjvman - JavaVM man pages	Required for SIMS			X
Solaris 2.5.1—Sun Sparc <i>required</i> patches Solaris 2.5.1—Intel 386 <i>required</i> patches Solaris 2.6—Sun Sparc <i>required</i> patches Solaris 2.6—Intel 386 <i>required</i> patches	Required for SIMS			X
Solaris 2.5.1—Sun Sparc <i>recommended</i> patches Solaris 2.5.1—Intel 386 <i>recommended</i> patches Solaris 2.6—Sun Sparc <i>recommended</i> patches Solaris 2.6—Intel 386 <i>recommended</i> patches	Recommended for SIMS	X		

Preparing to Install SIMS 3.5

This chapter covers information on how to prepare and pre-configure your system before installing SIMS 3.5.

- Preparing to Upgrade
- Preparing a Clean System
- Preparing to Install Patches
- Preparing to Install licenses
- Preparing to Install SMCS

Preparing to Upgrade

If you are upgrading from SIMS 3.x or SIMS 2.0 to SIMS 3.5, you need to prepare your system as described in this section.

Upgrading from SIMS 3.x to SIMS 3.5

If you are updating to SIMS 3.5 and already have an older release of SIMS 3.x (3.1, 3.2, or earlier version of 3.5) on your system, you have two options: *Preserve Configuration Files* and *Recreate Configuration files* as shown in FIGURE 5-1. You will see this screen during the installation. See Chapter “Installing SIMS 3.5,” for installation instructions.

Configuration Files Found

Configuration files already exist on your system.

Make a selection:

Preserve configuration files

Recreate configuration files

FIGURE 5-1 SIMS Upgrade Configuration Screen

Preserve Configuration Files—This option allows you to upgrade to SIMS 3.5 by keeping your existing data and configuration files and directory structure.

Recreate Configuration Files—This option is the same as a fresh install, where all of the data and configuration files and directory structure will be removed.

SIMS installation will detect an earlier version of SIMS on your system and then prompt you to make a decision accordingly. That is, whether to install fresh or to keep your data and configuration files. The installation then installs SIMS 3.5 on your system. Simply select one of the upgrade options indicated above.

As an alternative, you may use the `SIMS uninstall` command to remove your files. You may then reinstall SIMS and then restore your system. `uninstall` does not reinstall the software. See Section “Preparing a Clean System,” below for information on how to use the `uninstall` command.

Note – You may backup your entire database and configuration files before upgrading your SIMS system. This enables you to restore your system to its previous state if the upgrade procedure fails for any reason.

See Chapter “Post-Install Configurations,” for detailed information on post-installation configurations.

Note – If you select the “Preserve Configuration File” option, you *must* complete the procedure in Section “Upgrading SIMS 3.1/3.2 Directory Contents to SIMS 3.5,” in Chapter “Post-Install Configurations,” after upgrading.

Upgrading from SIMS 2.0

Before upgrading to SIMS 3.5 from SIMS 2.0, do the following steps:

1. Backup your mail messages under the `/var/mail` directory.
2. Use the `pkgrm` command to remove the existing SIMS 2.0 packages: `SUNWimap`, `SUNWipop`.
3. Decide whether to migrate your existing user mail messages and folders from `/var/mail` to the secured SIMS Message Store or continue to support `/var/mail` users.

Unlike the `imaccessd` daemon that runs as root and delivers mail to `/var/mail`, the daemon that delivers mail to the SIMS Message Store is owned by the postmaster user id, `inetmail` (not root). The SIMS Message Store meets stringent security standards. Migrating to the Sun Message Store ensures that your mail server is secured.

4. Use the `imimportmbox` utility to migrate `/var/mail` to SIMS Message Store. See the *Sun Internet Mail Server 3.5 Administrator's Guide* for more information on using this utility.

Preparing a Clean System

If you are upgrading or reinstalling your SIMS system, you can manually clean up your system by using the `uninstall` command along with appropriate option as shown in TABLE 5-1.

TABLE 5-1 The `uninstall` Command Options

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

You may use the `pkginfo` command to list the packages already installed on your system.

Note – Do not remove individual packages.

▼ 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 – 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 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 a HA cluster, you need to use the `uninstall` command from this directory.

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 5-2 shows a list of patches that are required for SIMS 3.5 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 5-2 SIMS Required Solaris Patches

Patch ID	Operating System	Type of Patch
105266-08 Sparc 105272-08 I386	Solaris 2.5.1/2.6	Sun Directory Services 1.0 patch
103566-18 Sparc 104241-02 I386	Solaris 2.5.1	Xsun Jumbo patch
103640-08 Sparc 103641-08 I386	Solaris 2.5.1	kernel patch
103663-07 Sparc ¹ 103664-07 I386	Solaris 2.5.1	libresolv in.named named-xfer nslookup nstest patches
103594-10 Sparc 103595-10 I386	Solaris 2.5.1	<code>/usr/lib/sendmail</code> fixes
103680-021 Sparc 103681-01 I386	Solaris 2.5.1	nscd/nscd_nischeck/rebuild for BIND 4.9.3
103686-02 Sparc 103687-02 I386	Solaris 2.5.1	<code>rpc.nisd_resolv</code> patches
106514-01 Sparc 106515-01 I386	Solaris 2.6	Sun Internet Mail Server miscellaneous fixes
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	<code>/usr/lib/libthread.so.1</code> patch

TABLE 5-2 SIMS Required Solaris Patches

Patch ID	Operating System	Type of 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 ² 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. These two patches must be installed before starting SIMS installation.

2. Two different versions of the package SUNWcius were shipped with Solaris 2.6. To find out which version you have, run the command `pkginfo -l SUNWcius` 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` on the SIMS CD.

TABLE 5-3 SIMS Additional Recommended Patches

Patch ID	Operating System	Type of Patch
106439-01 Sparc 106440--1 I386	Solaris 2.6	Syslog patch

Note – To locate the recommended patches listed here, go to <http://sunsolve.sun.com> and click on the Public Patches link.

Installing Patches

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 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. Use the following command to verify 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.

Preparing to Install and Update Licenses

To install the license for the components of the SIMS software, you need to do the following:

1. Request a license password.
2. Determine server configurations.
3. Install and update licensing information.

Note – To contact the License Center in your area, refer to <http://www.sun.com/licensing/> for phone numbers and e-mail addresses.

Requesting a License Password

The license password is an alphanumeric code that you must get from the license distribution center. Enter this password into your license page.

1. Gather the following information prior to contacting the license center: Product name, Version number, Serial number (from license card supplied with the product).
2. Specify the following information for each license server: Server hostname, Server's hostid, Number of units, Number of cc:Mail, MS-Mail, or PROFS channels.
3. Specify your contact information: Your name, Phone number, Company name and address.
4. Indicate your preferred method to receive your password information: E-mail address (fill out the form sent to you, and return it via e-mail as well), and Fax number.

When you turn in your form to the License Distribution Center, you will receive licenses that you can use with the SIMS 3.5 software.

Caution – If your license file was saved on a PC and then moved to a Solaris system, you have to make sure that no extra line feed character (^M) exists at the end of each line.

Determining Server Configurations

There are two possible license server configurations: Single and Redundant.

Single Server

The single server configuration suits companies where the license server and the mail server are fairly close together on the network or on the same machine. This configuration is the default and the easiest configuration to install and maintain.

Redundant Servers

A redundant server configuration consists of three servers, acting as one logical server, that manage the same set of license tokens.

In this configuration, one of the redundant servers is the master server that issues license tokens and, thus, has a heavier processing load. If the master server becomes unavailable, then the next available *peer* in the configuration becomes the master server.

Using this configuration should be limited to special situations where its advantages outweigh the increased complexity of installation and maintenance.

Installing and Updating Licensing Information

The generic license file that you have received from the license center is called `license.dat`. If you are installing SIMS 3.5 for the first time, the installation will ask you to enter the directory path to where the file `license.dat` is located.

If you are installing a SIMS/HA system, you will need an additional license for the secondary HA machine.

If you are upgrading from SIMS Departmental edition to the SIMS Enterprise edition, the installation will automatically update your licensing information while upgrading.

If your SIMS license has expired, you need to update the license by following the steps covered in this section. You will be using the License Installation Tool (LIT) to update your license. This tool will extract information from the file `license.dat` and place them into three files, as shown below.

▼ To update the licensing information

1. As root, stop the license manager.

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

2. Stop the SIMS mail server.

This assumes the server is already installed and running on your machine.

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

3. Update the license file using the License Installation Tool (LIT) or LIT-TTY script.

```
# /etc/opt/license/lit
```

4. Enter your license file name along with the directory path where the file is located.
5. Click **Install** to install new licenses.
6. Run the license configuration script.

```
# /etc/opt/licenses/LIC_CONFIG_SCRIPT
```

This tool, in turn, updates the following three files:

```
/opt/SUNWconn/license_dir/slapd1.0.lic,1  
/etc/opt/SUNWmail/license_dir/sims.lic,1  
/etc/opt/licenses/licenses_combined
```

You may use the `lmstat` tool to validate the information contained in these three files, though not required.

7. Edit the file `licenses_combined` to remove the old license information.

```
# /etc/opt/licenses/licenses_combined
```

8. Edit the file `slapd1.0.lic,1`, which contains LDAP information, to remove the old license information.

```
# /opt/SUNWconn/license_dir/slapd1.0.lic,1
```

9. Edit the file `sims.lic,1`, which contains SIMS information, to remove the old license information.

```
# /etc/opt/SUNWmail/license_dir/sims.lic,1
```

Note – before rebooting your system, make sure that you only have *one* file `slapd1.0.lic,1` that contains the SLAPD information that match your license file.

10. Reboot your system.

SIMS server should be up and running now, which results in automatically starting the license manager.

Preparing to Install Proxies

Before installing your proxies, you need to consider the following guidelines. See Chapter “Configuring SIMS as a Proxy Message Store server,” in the *Sun Internet Mail Server 3.5 Administrator’s Guide* for different proxy scenarios, models, and configurations.

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

Typically, each user has a well-defined backend mail server but accesses a random proxy via 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 mailhost.

Once the client is authenticated on the proxy, it will contact the real mailhost and redo the login using the same username 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 mailhost and vice-versa without any interruption on the part of the proxy. Overly large machines should not be required for the proxies.

When configuring for 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 ISP.

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

Preparing to Install SMCS

Before installing SIMS 3.5 optional SMCS software, you need to enable SMCS connections by placing the infrastructure. The criteria includes:

- Determining Transport Protocol
- Checking Mail Clients Setup
- Checking Directory Synchronization
- Meeting SMCS Requirements

Determining Transport Protocol

To ensure that SMCS connections work properly, you need to know if your company is using either the SPX or a file sharing transport for LAN-based e-mail systems.

SPX provides message transport over Ethernet or Token Ring links between LAN clients and the SMCS server. SPX choices include one of the following:

- Sun Solaris SPX stack (Connect/NW 2.0 Protocol Services) and higher
- Syntax TotalNET Advanced Server 5.0 and higher
- Third Party SPX stack

File sharing provides message transport by transparently mapping logical drives from LAN environments to physical disk drives located on the SMCS server. File sharing choices include one of the following:

- Sun's NWServer (Connect/NW 2.0 Protocol Services)
- TotalNet 5.0
- NetWare InternetWare
- Third party NFS software

Specifying Mail Clients Setup

To ensure that e-mail clients are setup and configured correctly, the following requirements must be met.

1. Ensure that you have installed *only one* of the following systems:
 - A dedicated PC running DOS installed on LAN to act as gateway client host or
 - A Windows NT or Windows 95 machine to run the client process in a DOS window.
2. If file sharing is the preferred transport, ensure that it is installed and configured to provide connectivity between the Solaris host and the established LAN.
3. Ensure that the SMCS gateway routing information is added to all LAN e-mail post offices in the network.

For cc:Mail this is called the Gateway Post Office, for MS-Mail it is called the External Post Office.

4. Ensure that directory synchronization between all LAN e-mail post offices is fully operational.

Checking Directory Synchronization

To ensure that e-mail clients are setup and configured correctly, the following requirements must be met.

1. Determine e-mail directories to be synchronized.
2. Check policies on central or distributed data ownership models.

This entails identifying the owner of the data, SMCS, or the individual e-mail directories.

3. Determine how SMCS will access the entries in the gateway post offices and in the sub-post offices.

Meeting SMCS Requirements

The SMCS software packages are provided as features via the SIMS Enterprise edition.

Before installing the SMCS software, you need to make sure that the following SMCS software compatibility requirements are met.

The following is a list of SMCS compatible software for each supported channel.

SMCS Channel for cc:Mail

- cc:Mail Release 5.1 Post Office or higher release
- cc:Mail Router V5.1 or later which includes the cc:Mail Import/Export Facility V5.1 or higher release
- One of the transport options: SPX or File share

SMCS Channel for Microsoft Mail

- MS-Mail for PC or Macintosh Networks, supporting V3.2 or V3.5 post offices/MS Mail Servers that run on DOS or NT
- MS-Mail Gateway Access for SMTP, a subset of the MS-Mail SMTP gateway, Microsoft part number 068-099-127 (one copy for each post office that exchanges mail with SMCS available directly through Microsoft)
- No existing MS SMTP gateway can be installed on post offices that are to exchange mail with SMCS
- One of the transport options, SPX or File share

SMCS Channel for IBM PROFS and OfficeVision/VM

- PROFS Post office configured for SMCS connection
- Dedicated PC, 16 Megabytes 486 or better with Synchronous Communications Card, Ethernet adapter, and 200 Megabytes of disk storage that run OS/2 V2.1 or later, IBM Communications Manager/2

Installing SIMS 3.5

This chapter contains the instructions for installing SIMS 3.5 by using the graphical interface (GUI).

Topics in this chapter include:

- Before Installing
- Installation Overview
- Installing SIMS 3.5 Enterprise Edition
- Installing SIMS Add-on Features
- Installing SIMS High Availability
- Installing Stand-Alone Sun™ Web Access
- Installing Remote Administration Console
- Installing Pure Proxy
- After Installing SIMS 3.5

If you are installing the SMCS software on client machines, see the *Sun Messaging Connectivity Services Guide* for installation details. This document helps you install the client software on cc:Mail, MS-Mail, and PROFS clients.

If you are installing the optional SIMS 3.5/HA software, refer to the Sun Cluster 2.1 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. For detailed information on the Administration Console and its capabilities, refer to the *Sun Internet Mail Server 3.5 Administrator's Guide*.

Note – See Appendix A, "Command-Line Installation," for instructions on a command-line installation sample session.

Before Installing

Before installing SIMS 3.5, make sure that you have already read the following chapters:

TABLE 6-1 Chapters Required Before Installing SIMS 3.5

Chapter Name	To Learn About...
Overview of SIMS 3.5 Components	SIMS 3.5 features, core and optional components.
Server and Client Requirements	Platform, space, memory requirements.
What SIMS 3.5 Installs	Lists of SIMS 3.5 packages and configuration files.
Preparing to Configure	Software requirements, default configurations, startup scripts.
Preparing to Install SIMS 3.5	Upgrade considerations, licenses, patches, SMCS, SIMS removal.

Installing SIMS 3.5

You may use the instructions in this section as a general guideline for all three types of installations: *Enterprise* edition, *Departmental* edition, and *Stand-Alone* options.

To install SIMS add-on features on your existing SIMS system, see Section “Installing SIMS Add-on Features,” that follows this section.

For descriptions of installation types, see Section “Selecting Installation Types,” below. Alternatively, you may select the Enterprise edition installation on an HA system.

1. Run the `setup` installation script.
2. Select the installation type.
3. Select the options.
4. Specify licenses.
5. Specify core server configuration information.
6. Specify optional configuration information.
7. Start the Setup install.

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

Running the Installation Script

1. Ensure that you have already set up the `DISPLAY` variable.

2. Insert the SIMS CD-ROM into the disk drive.

Make sure that your CD is mounted to the `/cdrom/sun_internet_mail_3_5` directory.

3. Change to the SIMS product directory.

```
% cd /cdrom/sun_internet_mail_3_5
```

4. As non-root user, run the `setup` script from the software CD-ROM.

```
% setup
```

This launches a web browser and then displays the first page of the SIMS 3.5 installation interface, as shown in FIGURE 6-1.



FIGURE 6-1 SIMS 3.5 Installation Information Page

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

5. Review the information page and then click Install Main Menu.

6. Make a selection from the main menu as described in the next step.

Selecting Installation Type

The next step after starting the `setup` script is to decide on the type of installation as shown in FIGURE 6-2. If you are upgrading to SIMS 3.5, first see Chapter “Preparing to Install.”



FIGURE 6-2 SIMS 3.5 Installation Types

SIMS 3.5 Enterprise Edition Installation

The Enterprise edition installs SIMS 3.5 core components along with its optional features, including connectivity services as shown in FIGURE 6-3.



FIGURE 6-3 SIMS 3.5 Enterprise Edition Core and Optional Components

See Chapter “Overview of SIMS 3.5,” for more information on SIMS 3.5 Enterprise edition core and optional components.

SIMS 3.5 Departmental Edition Installation

SIMS 3.5 Departmental edition installs the SIMS 3.5 core components and allows you to install SIMS optional components as shown in FIGURE 6-4. SIMS 3.5 Departmental edition is primarily intended for local department environments that perform their own routing and delivery within the local office or workgroup, but hand off interdepartmental mail to a backbone server.



FIGURE 6-4 SIMS 3.5 Departmental Core and Optional Components

See Chapter “Overview of SIMS 3.5,” for more information on SIMS 3.5 Departmental edition core components as well as available optional components.

SIMS 3.5 Stand-Alone Installation

SIMS Stand-alone edition lets you install SIMS optional components on a server that is not running SIMS.



FIGURE 6-5 SIMS 3.5 Stand-Alone Components

7. Click **start** after reviewing the installation procedure displayed in FIGURE 6-6.

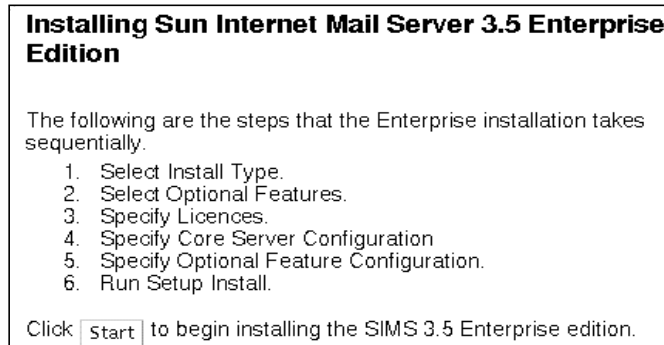


FIGURE 6-6 SIMS 3.5 Installation Steps

Note – If you already have SIMS on your system and now are upgrading to SIMS 3.5, read Section “Preparing to Upgrade,” in Chapter Preparing to Install SIMS 3.5,” to decide on the type of upgrade.

Selecting Optional Components

The next step after specifying the type of installation is to select SIMS optional components. These options are additions to the SIMS Departmental edition and features that are available through SIMS Enterprise edition.



FIGURE 6-7 SIMS Enterprise Optional Components

8. Select SIMS optional components that you wish to add to your SIMS server.
 If you don't select any options, only SIMS core components will be installed.
 If you are installing HA (not shown in FIGURE 6-7) SIMS optional components will not be available. See Section "Installing SIMS High Availability," at the end of this chapter for instructions for installing SIMS/HA.
9. Click **Apply** to go to the License Configuration page.

Specifying Licenses

After selecting the type of installation and options, next you need to specify the information pertaining to licensing as shown in FIGURE 6-8.

If you are installing the optional SMCS software, you need to provide the required licensing information to support the channels that you have purchased—cc:mail, MS-Mail, or PROFS. For HA installation, you need one additional license for the secondary HA machine.

License Configuration Page

Choose one of the options and then enter appropriate parameters.

Note: The software will read the Licensing values from your existing license file and automatically fill in some parameters on this page.

Use existing Licenses

OR Read License from File

(Pathname of File name)

OR Manually enter license information

Single Server

Host name	Host ID
sp11	2289f68

Redundant Servers (Please enter both)

Host name	Host ID
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Feature Name	Feature Version	RTUs	Password	Exp. Date	Vendor String
Enterprise Edition (MTA)	3.108	[1]	[BC1316CBMOCAN42150D1	[08-Sep-1998	[
cc:Mail Gateway Channel	3.108	[1]	[3C2280CB44258A4D5793	[08-Sep-1998	[
Mailboxes	3.108	[100	[7C432018553C86353514	[08-Sep-1998	[
Directory for Intel	1.008	[1]	[CA38008FFANCBD6HE7	[08-Sep-1998	[A

FIGURE 6-8 License Configuration Page

10. Enter the required information on the License Configuration page.

Read License from File—Specify the file containing the license information.

Although your license file can reside in any location, the information you provide is copied into the `license_combined` file in `/etc/opt/licenses`.

If you are upgrading either from the Departmental edition to the Enterprise edition or from an earlier version of the Enterprise edition to the current version of the software, you must either edit the licensing file to register the changed values or provide the information in the Manually Enter License Information section.

Additionally, if you are installing the optional SMCS software, you need to provide the license for the channels that you have purchased—cc:mail, MS-Mail, or PROFS. To update the licensing information, follow the instructions shown in Chapter “Preparing to Install SIMS 3.5,” coupled with information in the *Sun Internet Mail Server 3.5 Administrator's Guide*.

Note – If you enter an invalid license string in the Pathname/File name field, the installation will continue until you invoke the SIMS Administration Console, when you receive an error message indicating that your license is invalid.

Manually Enter License Information—Manually install the licenses, click on this button. Specify the required information. If you choose this option, you do not need to choose the Read License from File button.

Single Server—Indicate the hostname and the host ID of the machine on which SIMS will be installed. You should have already provided this information as part of your preliminary request for license passwords.

Note – When your license server fails, you will not have access to the licenses it manages.

The installation software will automatically recognize the hostname and the host ID of the machine on which you are installing the SIMS software. For redundant servers, you must specify the hostname and host IDs of those systems in the field Redundant Servers.

Redundant Servers—Hostnames and the host IDs of the machines that will serve as the redundant license servers. You should have provided information on the hostnames and the host IDs of all the secondary servers before you were assigned a license key.

A redundant server manages the same set of license tokens. All license servers work as one logical server. Redundant license servers increase the chances of your licenses availability at all times when a majority of servers must be up. For example, if you have 3 redundant servers, at least 2 of them must be operational. If 2 of 3 redundant servers cannot contact each other, none of the license tokens will be available.

Note – Be sure to fill in the information in both fields for the two redundant servers. If you indicate information in *only one* field, your license installation will fail with an error message.

Feature Name—Indicate if you have purchased licenses for the Departmental edition IMTA, Enterprise IMTA, Mailboxes, or the Directory for SPARC and for the optional HA software.

Feature Version—Indicate the version of the feature for which you have purchased licenses.

RTUs—Enter the number of Rights to Use you received from the Sun License Center in the RTU field. You have the ability to split multi-RTU license certificate denominations into multiple passwords. Because of this, you are not required to install all the RTUs on a multipack certificate on a single license server. You can take advantage of the volume discount on these larger denomination as well as the flexibility to install the licenses in the configurations and locations you choose.

Password—Enter the string provided by the Sun License Center.

Exp. Date—Type the date in the *dd-mmm-yyyy* format if your licenses have an expiration date, for example, 15-aug-99 or 15-aug-1999. If you do not have a designated expiration date, leave this field blank.

Vendor String—A vendor string will be provided on your license certificate. If you received a vendor string, fill in the string. If you did not receive a vendor string, leave this field blank.

If your license installation fails, or if you wish to install licenses independently by using the License Installation Tool (LIT), see the *Sun Internet Mail Server 3.5 Administrator's Guide* for instructions. Make sure you install the licenses before installing SIMS 3.5.

If you need to update expired licenses, see Section “Preparing to Update and Install Licenses,” in Chapter “Preparing to Install.”

Specifying Core Server Configurations

After specifying licensing information, you need to configure the SIMS core components. FIGURE 6-9 shows the first page of these configuration pages.

Configuration Page 1 of 3

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

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:

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:

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

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

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.

VA/MAIL Support – Do you want the IMAP4 and POP3 servers to be able to open traditional UNDO/VarMail mailbox files? This is recommended only for sites where users regularly switch back and forth between VarMail clients (like Mailtool) and IMAP4/POP3 clients.
 Yes: I have users that need to switch back and forth between VarMail and IMAP. I am aware that this causes the IMAP4 and POP3 servers to run as root and as such, is a potential security risk.
 No: My users will use IMAP, or they will use VarMail, but do not need to switch back and forth.

FIGURE 6-9 Core Components Configuration Page 1

11. Enter the values in the SIMS core components configuration pages.

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

Mail Server Domain Name Suffix—Enter the fully-qualified domain name of the mail server on which SIMS is being installed. For example, if this server resides in the *eng* domain at *sun*, then specify *eng.sun.com* 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 3.5 checks for a fully-qualified domain name and will display error messages, depending on its finding. See Chapter “Troubleshooting SIMS Server,” for more information on configuring DNS setup.

Organization Top Level Domain Name Suffix—Enter the highest level domain name used within your organization. For example, the top level domain name for Sun Microsystems could be `sun.com`. 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. By default 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.

You will need this postmaster name to administer the mail server after installing SIMS.

Administrator Name—Enter the administrator's name. The default name is `admin`. The administrator's name is needed to configure the mail server using the SIMS Administration Console after the installation is complete. 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.

Administrator Password—Enter the administrator's password. The default password is `secret`. Once the installation is complete, the administrator's password is needed to configure the mail server using the Administration Console. The password you provide in this field is logged in the directory configuration file. By default, this password is stored encrypted.

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 hostname 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`), however, is more secure than `/var/mail` (that runs as `root`). Refer to the *Sun Internet Mail Server 3.5 Administrator's Guide* for migration instructions.

12. Click `Apply` to go to the second page of the core component configuration page.

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

13. Enter information on configuration page 2.

Your input in this form is mandatory. You may choose to accept the default values if they match your configuration plans for your mail server.

The screenshot shows a web form titled "Configuration Page 2 of 3". It contains three main sections:

- Country Name**: A dropdown menu with the instruction "Choose the country name where this mail server resides from the provided drop down list." The selected option is "United States of America". Other visible options are "Afghanistan" and "Albania".
- Organization Name**: A text input field with the instruction "Enter your organization's abbreviated name." Below it, an example states: "For example: If the Mail Server Domain name is 'eng.widget.com', then the Organization Name should be widget." The input field contains "sun".
- Organizational Unit**: A section with the instruction "For each domain name specified below, an organizational unit (OU) name needs to be specified." Below it, an example states: "For example, if the domain name is 'eng.widget.com', then the default OU name would be 'eng'. However, you might want to change it to a more descriptive word, such as 'Engineering'". A table below this section has two columns: "Domain Name" and "Organizational Unit". The first row shows "eng.sun.com" in the "Domain Name" column and "eng" in the "Organizational Unit" column.

At the bottom of the form are two buttons: "Reset" and "Apply".

FIGURE 6-10 Core Components Configuration Page 2

Country Name—Select a country name. The default value is *United States of America*. If you plan to implement multiple mail servers that are geographically distributed in multiple countries, then enter one country only, for example, the location of the organization’s headquarters. Your input in this field should not exceed 2 characters.

Organization Name—Enter your organization's abbreviated name. For example, if your mail server domain name is `eng.sun.com`, your company’s short name is `sun`. Your input in this field should not exceed 64 characters.

Organizational Unit—If your DNS contains sub-domains, enter the name of the division or department name within the specified organization. For instance, if you are referring to the `eng` domain, you may want to fill in `eng` in this field, or retain the defaults provided. Your input in this field should not exceed 64 characters. You can indicate multiple organizational units, up to a maximum of three, but all the organizational units must have a parent-child relationship within the same directory tree.

At installation, you cannot specify two organizational units that exist at the same level. As shown in FIGURE 6-11, for example, only the Quality Assurance (QA) team can report to the Engineering Team; a parallel team called Marketing that may also report into Engineering cannot be specified.

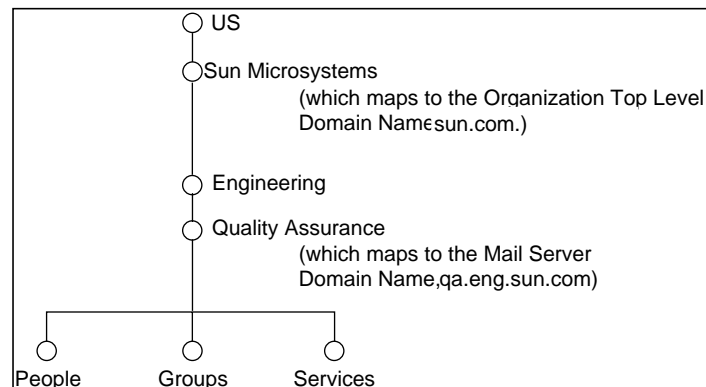


FIGURE 6-11 Hierarchy of Organizational Units

Note – After you have completed the installation of the product software, you can create peer groups at the same level as the Engineering group using the SIMS Administration Console.

The difference between the Mail Server Domain Name and your company’s Organization Top Level Domain Name determines the number of organizational unit listings that are displayed. As shown in FIGURE 6-11, you would see prompts for two

organizational units: Engineering and Quality Assurance. If the mail server domain name and the top level domain name are the same, the Organizational Unit field will not appear.

14. Enter information on configuration page 3.

The screenshot shows a web form titled "Configuration Page 3 of 3". It contains several input fields with labels and instructions:

- Organization Long Name** – Enter the full name for your organization. (ie: Widget Electronics, Inc)
Full Name:
- Postal Address** – The postal address of the system administrator responsible for this server
Postal Address:
- City Name** – The city or town in which this server resides.
City Name:
- State/Province** – The state or province in which this server resides.
State/Province:
- Telephone Number** – The telephone number of the system administrator responsible for this server.
Telephone Number:
- Fax Number** – The fax number of the system administrator responsible for this server.
Fax Number:

At the bottom of the form are two buttons: "Reset" and "Apply".

FIGURE 6-12 Core Components Configuration Page 3

Your input in this form is optional. The configuration information on this page can help the administrator troubleshoot the mail server.

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.

Specifying Optional Configurations

In Step 8 you selected the optional components that you wished to install. Here, you need to enter the configuration information for the options that you selected.

The screenshot shows a web-based configuration page titled "Optional Features Configuration Page". It contains several sections with labels and input fields:

- Directory Services Server Name**: A text box containing "spiffeng-sus.com".
- Directory Services Server Port**: A text box containing "389".
- MMAD Port**: A text box containing "2585".
- Connectivity Services Domain**: A text box containing "spiffeng.com".
- SMTP Port**: A text box containing "25".
- Address Rewrite Format**: A dropdown menu with "CN" selected, and a text box containing "CN".

At the bottom of the page, there are "Reset" and "Apply" buttons.

FIGURE 6-13 Optional Components Configuration Page

15. Enter information about the Optional components on the configuration page.

Directory Services Server Name—Enter the name of the server on which directory services are available. That is, the fully-qualified domain name of the SIMS server.

Directory Services Server Port—Enter the port number that the LDAP server uses.

MMAD Port—Enter the port number to which the SMCS Management Agent daemon will listen.

SMTP Port—Enter the port number that the SMCS software will use to communicate with SIMS MTA.

Address Rewrite Format—Select from one of the available formats, or enter your own format in the space provided. \$g.\$i.\$s.\$q specifies first name, middle initial, last name, and qualifier name (Jr., Sr. etc).

16. Click `Apply` to go to the summary page.

Review the information displayed on this page to verify the accuracy of your input. You may go back to the previous pages and modify any values.

Caution – Do not use the browser’s navigational buttons provided on top of the page to return to the Configuration Summary page to register your revised input.

Running the Setup Install

After selecting SIMS optional components and specifying configurations for both core and optional components, you are now ready to begin installing SIMS 3.5.

17. Click the `Start Install` button 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.

18. Enter the root password at the password prompt.

19. 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.

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

The Installation Summary page displays.

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

You have now successfully installed SIMS 3.5.

22. Reboot your system now as shown in Step 23 if you have installed any patches during installation. Since, however, you still need to complete the post-installation configuration tasks, you may want to reboot at a later time. To do this, go to step 24.

23. If you choose to reboot your system right now, stop the mail server that is automatically started.

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

24. If you choose to reboot your system later, start the directory services daemon:

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


See Section “After Installing,” at the end of this chapter for a roadmap of post-installation configurations and tasks.

Installing SIMS Add-on Options

If you have already installed SIMS 3.5 and would like to add SIMS optional features to your SIMS system, do the following steps:

1. Follow steps 1 through 5 in Section “Running the Installation Script,” under the heading “Installing SIMS 3.5,” in the beginning of this chapter.

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

2. Select **SIMS 3.5 Option** from the SIMS 3.5 installation main menu, as shown in FIGURE 6-2.
3. Click **start**.
4. Select the add-on features that you wish to add to your SIMS server, as shown in FIGURE 6-14.

SIMS Optional Features Add-on

Select the optional features to install

- Web Access
- SIMS Message Transfer Agent SDK
- SIMS Message Transfer Agent SDK Documentation
- SMCS Channel: cc:Mail
- SMCS Channel: Microsoft Mail
- SMCS Channel: IBM OpenVision PROFS

Reset Apply

Previous Step

FIGURE 6-14 SIMS Add-on Features Screen

5. Click **Apply** to go to the License Configuration page, as shown in FIGURE 6-15.

Optional Features Configuration Page

Directory Services Server Name – Enter the name of the directory services server. It is the fully qualified name of the SIMS Server.

LDAP Server Name:

Directory Services Server Port – Enter the port number used by the LDAP server.

LDAP Server Port:

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

Administrator Name:

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

Admin Password:

FIGURE 6-15 SIMS Add-on Features Configurations Screen

6. Specify the information on the configuration page.

Directory Services Server Name—Enter the name of the server on which directory services are available. That is, the fully-qualified domain name of the SIMS server.

Directory Services Server Port—Enter the port number that the LDAP server uses.

Administrator Name—Enter the administrator's name, not exceeding 64 characters. The default name is `admin`. This is needed to configure the mail server by using the SIMS Administration Console after the installation is complete. 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.

Administrator Password—Enter the administrator's password. The default password is `secret`. Once the installation is complete, the administrator's password is needed to configure the mail server using the Administration Console. The password you provide in this field is logged in the directory configuration file. By default, this password is stored encrypted.

7. Click **Apply** to go to the summary page.

8. Run `Setup Install` by following the directions explained in Step 17 in Section "Running the Installation Script," under the heading "Installing SIMS 3.5," in the beginning of this chapter.

Installing SIMS High Availability

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

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

Your SIMS software will be installed in the directory `/opt`. 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 SIMS/HA by using the graphical user interface (GUI). First you will be installing SIMS/HA 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 “SIMS Asymmetric High Availability,” for information on system configuration, and failover 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/HA installation must be fresh and cannot be upgraded.

▼ To prepare before installing SIMS/HA

Before installing SIMS/HA, make sure that you have completed the following steps:

1. **Installed SunOS.**
2. **Installed the Sun Cluster 2.1 software.**
3. **Installed Veritas File System (VxFS) 3.2.4 (or later release).**
4. **Started the cluster.**
5. **Set up a logical hostname for your HA machine.**

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

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

See Section “Removing SIMS/HA,” at the end of this chapter for instructions on how to remove the SIMS/HA system.

7. Ensured 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. Ensured that multiple shared volumes for shared files were not used.

SIMS/HA 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 SIMS/HA

SIMS/HA installation involves installing the software first on the machine where SIMS/HA will be primary used. The next step is to install SIMS/HA on the machine that will be used secondary 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 known to DNS as an *alias*, SIMS/HA will not install.

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 primarily used, for example, *ha-primary*.

ha-logical-hostname is the logical host name assigned to the HA machine, for example *active-ha*.

5. Follow steps 1 through 5 in Section “Running the Installation Script,” under the heading “Installing SIMS 3.5,” in the beginning of this chapter.

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

6. Select SIMS 3.5 Enterprise Edition as the installation type as shown in Figure FIGURE 6-2.

7. Select High Availability from the High Availability Enterprise Installation page as shown in FIGURE 6-16.

Note – SIMS optional components will not be available for SIMS/HA installation.

High Availability Enterprise Edition Installation

Do not install any optional features or services
(Only core SIMS will be installed)

High Availability

Select the optional features to install
(Core SIMS will be installed with the options selected below)
These features are not available on a High Availability installation

- Web Access
- SIMS Message Transfer Agent SDK
- SIMS Message Transfer Agent SDK Documentation
- SMCS Channel: cc:Mail
- SMCS Channel: Microsoft Mail
- SMCS Channel: IBM OpenVision PROFS

Reset
Apply

[Previous Step](#)

FIGURE 6-16 SIMS/HA Enterprise Option

8. Follow steps 9 through 14 from in Section “Running the Installation Script,” under the heading “Installing SIMS 3.5,” in the beginning of this chapter.

This allows you to specify licensing information and server configurations.

9. Select the logical hostname to 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 switchover 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.

Optional Features Configuration Page 1 of 2

Logical Host Name – Select the logical host to install SIMS High Availability from the list of hosts currently mastered on this physical host.

Logical Host Name:

[Previous Step](#)

FIGURE 6-17 SIMS/HA Logical Hostname

10. Specify the shared file system where the SIMS 3.5 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 6-18, select 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.

Optional Features Configuration Page 2 of 2

Shared File System – All relocatable components need to be installed on a file system that is shared by both hosts in the cluster. Select the file system to install relocatable components.

Shared File System:

/active-ha/disk2

[Previous Step](#)

FIGURE 6-18 SIMS/HA Shared File System

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

Note – Record the name of the shared disk that you are selecting here. You will need to use the same name during SIMS/HA installation on the secondary machine.

- 11. Follow steps 16 through 21 in Section "Running the Installation Script," under the heading "Installing SIMS 3.5," in the beginning of this chapter.**

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

You are now done with installing SIMS/HA on the primary machine. Next, you will be installing SIMS/HA on the secondary machine.

- 12. 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*.

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 an example shown in FIGURE 6-18, you may have selected */active-ha/disk1* as the shared disk on which HA and SIMS files were stored.

You also need to provide the licensing information for this secondary machine here.

- 14. Reboot the machine on which you have installed the patches.**

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

- 15. Start up the SIMS services under the HA framework.**

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

You are now done with installing SIMS/HA on both primary and secondary machines.

FIGURE 6-19 illustrates the SIMS/HA system after it is fully installed on both primary and the secondary machines.

Note – SIMS supports failure detection and consequent failover 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 failover.

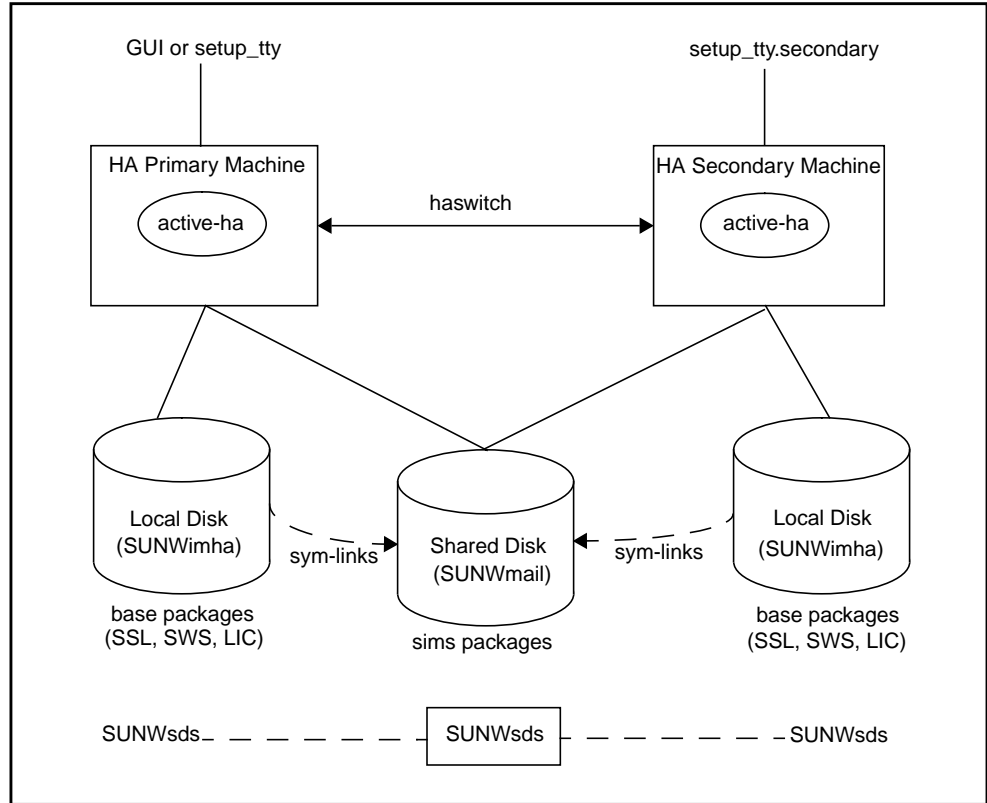


FIGURE 6-19 SIMS/HA System

If you choose to reboot your SIMS/HA system after installing the software, restart your Sun Cluster software by going to steps 16 and 17 below. Otherwise, see Section “Starting SIMS/HA Administration Console,” in Chapter “Post-Installation Task,” for instructions on invoking the SIMS Administration Console.

16. 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/HA machine,

cluster-name is the name of your Sun Cluster.

17. Restart Sun Cluster on the secondary machine.

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

See Section “After Installing,” at the end of this chapter for a roadmap of post-installation configurations and tasks.

Removing SIMS/HA

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 6-19 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 are the steps for completely removing SIMS/HA 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. But 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*.

ha-logical-hostname is the logical name assigned to the HA machine, for example, *active-ha*.

3. Uninstall on the *secondary* machine from either one of the two locations.

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

This removes all files from *both* SUNWmail on the *shared disk* and SUNWimha on the local disk of the secondary machine. See FIGURE 6-19.

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*.

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

Installing Stand-Alone Sun™ Web Access

For optimal performance, it is recommended that you install Web Access as a stand-alone product on a server where SIMS is not installed. The Web Access server, however, will be linked to the SIMS server where Sun Directory Services will be available to the Web Access server.

To accomplish this, do the following steps:

1. Follow steps 1 through 7 given in Section “Running the Installation Script,” under the heading “Installing SIMS 3.5,” in the beginning of this chapter.
2. Select the Web Access option.
3. Specify the server name and the port number for the server where LDAP services for the Web Access server are available as shown in Step 15 in Section “Running the Installation Script.”
4. Enter configuration information about the server on which Web Access is being installed as covered in Step 11 in Section “Running the Installation Script.”
5. Run `Setup Install` by following the directions explained in step 17 through 24 in Section “Running the Installation Script.”

See Chapter “Post-Installation Sun Web Access Setup,” to set up, configure, and start your Web Access server.

Installing Remote 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 3.5 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
```

Running the `setup` script begins the installation program.

▼ To install on Solaris systems

1. Insert the SIMS 3.5 CD-ROM into the CD-ROM drive.

Volume Manager automatically mounts the CD-ROM in the directory.
/cdrom/sun_internet_mail_3_5.

2. Change directories to the SIMS 3.5 product directory.

```
% cd /cdrom/sun_internet_mail_3_5
```

3. As a non-root user, run the setup script to begin the installation program.

```
% ./setup
```

The first page of the SIMS 3.5 installation interface appears as shown in FIGURE 6-1.

4. Click **Install Main Menu** to display the installation main menu, as shown in FIGURE 6-2.

5. Select **SIMS 3.5 Options** from the main menu page.

The SIMS Optional Features for Stand-Alone Machines page displays as shown in FIGURE 6-20.

SIMS Optional Features for Stand Alone Machine

Select the optional features to install
(Core SIMS will NOT be installed with the options selected below)

Web Access

SIMS Message Transfer Agent SDK

SIMS Message Transfer Agent SDK Documentation

Remote Administration Console

POP3/IMAP4 Proxy Server

FIGURE 6-20 Remote Administration Console Option Page

6. Select the Remote Administration Console option.

7. Click the Apply button.

The Summary page displays as shown in FIGURE 6-21.

Configuration Summary	
Please check the information you entered in the previous pages	
General Configuration	
Optional Configuration	
Selected Features/Options	Remote Administration Console

Start Install

FIGURE 6-21 Remote Administration Console Configuration Summary Page

8. Click the Start Install button.

This invokes a command tool.

9. Specify your root password.

SIMS begins installing the necessary software to invoke the SIMS Administration Console.

10. Choose any key in the command tool window to exit when installation completes.

This brings up the installation summary page to indicate that the SIMS Administration Console has been installed and configured.

See Section “After Installing,” at the end of this chapter for a roadmap of post-installation configurations and tasks.

Installing Pure POP3/IMAP Proxy

SIMS 3.5 pure proxy is a stand-alone product that you must install on a server where SIMS is not installed. Pure proxy installs as a replicated *slave* to a remote *master* SIMS server.

Before installing, see Chapter “Preparing to Install SIMS 3.5,” for guidelines regarding proxies installation.

▼ To install pure proxy

1. Follow steps 1 through 5 in Section “Running the Installation Script,” under the heading “Installing SIMS 3.5,” in the beginning of this chapter.

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

2. Select **SIMS 3.5 Option** from the main menu page as shown in FIGURE 6-2.
3. Click **start**.
4. Select the **POP3/IMAP4 Proxy Server** option as shown in FIGURE 6-22.



FIGURE 6-22 POP3/IMAP4 Pure Proxy Server Option Page

5. Click **Apply** to go to the **License Configuration** page.
6. Enter the required information on the **License Configuration** page, as shown in **Step10** in Section “Running the Installation Script.”

7. Specify server configurations, as shown in steps 11 through 14 in Section “Running the Installation Script.”
8. Click **Apply** to go to the summary page.
9. Run **Setup Install** by following the directions explained in steps 17 through 24 in Section “Running the Installation Script.”

To ensure that the directory schema in the slave (pure proxy) LDAP server is synchronized with the master (SIMS) LDAP server, you need to manually copy the schema files from the master (SIMS) server. These schema files are

```
/etc/opt/SUNWconn/ldap/current/slapd.conf  
/etc/opt/SUNWconn/ldap/current/slapd.at.conf  
/etc/opt/SUNWconn/ldap/current/slapd.oc.conf
```

This will ensure that all directories in the slave server will serve the same set of objects that are available on the master server. For procedure to copy the schema configuration files from SIMS master server to the proxy server see *Sun Internet Mail Server 3.5 Administrator's Guide*.

Directory replication ensures that the master and slave servers have the same replication configuration so that the updates work properly. Replication between servers with dissimilar schema may lead to unpredictable results.

To populate users to a proxy-based LDAP directory, see Chapter “Configuring SIMS as a Proxy Mail Access Server,” in the *Sun Internet Mail Server 3.5 Administrator's Guide*.

After Installing SIMS 3.5

After you have completed installing or upgrading to SIMS 3.5, be sure that you read the following chapters:

TABLE 6-2 Chapters Required After Installing SIMS 3.5

Chapter Name	To Learn About...
Post-installation Configurations	Sun Web Access and pure Proxy configurations.
Post-Installation Sun Web Access Setup	Set up, configure, and invoke Web Access server.
Post-Installation Tasks	Starting and testing your SIMS server. You may go directly to this chapter.
Troubleshooting SIMS Server	DNS setup configuration, log files, removing sendmail, rebooting after re-installing

Post-Installation Configurations

After you have installed SIMS 3.5, you may need to further configure your server if you have upgraded, upgraded and selected the Web Access optional client, or installed pure proxy.

Topics in this chapter include:

- Upgrading SIMS 3.1/3.2 Directory Contents to SIMS 3.5
- Preparing Configuration File for Mail Users Only
- HotJava Browser Configuration
- Removing sendmail for Pure Proxy

Upgrading SIMS 3.1/3.2 Directory Contents to SIMS 3.5

SIMS 3.5 requires that new LDAP *object classes* and *attributes* be added to the schema. If you are installing SIMS 3.5 for the first time, it automatically upgrades the schema. If, however, you are upgrading to SIMS 3.5 from SIMS 3.1 or 3.2 and have already populated the LDAP directory, you *must* complete the following two steps:

1. Modify the directory server configuration files to support the new schema.
2. Reprocess the directory contents by using the `imldifsync` program to add instances of the new attributes to each subscriber's LDAP record.

Modifying the LDAP Directory Server Schema

After you have completed upgrading to SIMS 3.5, do the following steps:

1. **Login as root.**

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

2. **Edit the `slapd.at.conf` file.**

```
% /bin/vi /etc/opt/SUNWconn/ldap/current/slapd.at.conf
```

3. **Go to the end of `slapd.at.conf` and include the contents of the following file to specify the new object classes and attributes for the Sun Web Access feature.**

```
/etc/opt/SUNWmail/dir_svc/WebAccess.at.conf
```

4. **Edit the `slapd.oc.conf` file.**

```
/etc/opt/SUNWconn/ldap/current/slapd.oc.conf
```

5. Go to the end of `slapd.oc.conf` and include the contents of the following files to specify the new object classes and attributes for the Sun Web Access feature.

```
/etc/opt/SUNWmail/dir_svc/WebAccess.oc.conf
```

Note – If you use the *include* directive, used elsewhere in `slapd.conf`, to include a file containing the above text, the SunDs admin server will not start successfully. Instead, include the above text lines directly.

6. Save your changes and exit the editor.
7. Stop the LDAP directory server.

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

Note – E-mail users will not be able to login to their mailboxes while the LDAP directory server is down.

8. Regenerate indexes.

```
# /opt/SUNWconn/sbin/idxgen /var/opt/SUNWconn/ldap/dbm
```

If you have changed the location of the datastore, you should run `idxgen` on the server where the datastore is located. The following line defines the location of the datastore in `/etc/opt/SUNWconn/ldap/current/slapd.conf`.

```
directory /var/opt/SUNWconn/ldap/dbm
```

The amount of time required to regenerate the indexes depends on the number of entries in the LDAP Directory. Do not regenerate indexes while `slapd` is running.

Caution – Generating indexes could take several hours for large volume of entries.

9. Restart the LDAP directory server.

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

10. Confirm that the LDAP directory server is running.

```
# /bin/ps -eaf | /bin/grep slapd
root 17254      1  0 15:40:26 ?
0:00 /opt/SUNWconn/ldap/lib/slapd -p 389 -n 256
```

If you have incorrectly configured the `slapd.conf` file and `slapd` does not restart, you may find diagnostic messages displayed on your console or in these log files.

```
/var/adm/messages
/var/opt/SUNWconn/ldap/log/slapd.log
```

See the man page in `slapd.conf(4)` for further details of the required format of `slapd.conf`.

Configuring Existing Users in the LDAP Directory Database to Use Web Access

To perform an initial *bulk load* of the LDAP directory from existing password and mail alias files, you need to use the program `/opt/SUNWmail/sbin/imldifsync`. This command generates LDAP directory data for the Web Access optional client that you have selected during SIMS installation. This configuration file will be used during your post-install, directory population phase.

In SIMS 3.5, the program `/opt/SUNWmail/sbin/imldifsync` replaces the program `/opt/SUNWconn/sbin/ldapsync` that was used in SIMS 3.1 and 3.2. In addition to the functionality similar to `ldapsync`, `imldifsync` allows generating LDAP entries to support the Sun Web Access client.

SIMS Installation procedure will create a configuration file to be used with the program `imldifsync`. The file is located in the following file:

```
/etc/opt/SUNWmail/dir_svc/imldifsync.conf
```

You need to modify the file `imldifsync.conf` before using it with the program `imldifsync`.



Caution – Using the file `imldifsync.conf` without the appropriate modifications as described here can configure the contents of your LDAP directory incorrectly.

Instructions for modifying the file `imldifsync.conf` are explained in Chapter “Sun Directory Services Administration,” Section “Populating the Directory,” sub section titled Converting the Data to LDIF Format Using `imldifsync` in the *Sun Internet Mail Server 3.5 Administrator’s Guide*.

These instructions describe how to configure *existing* users to use the Sun Web Access client, as well as how to add *new* users. `imldifsync.conf` will synchronize changes to the input data files with data in the LDAP Directory.

The directive in the `imldifsync.conf` file, which determines whether generated LDAP directory entries support only e-mail users or it also supports the Sun Web Access client, looks like this:

```
# This example shows e-mail, and WebAccess
# calendaring attribute generation.
option = {"generate=SIMSmail", "generate=IMCalendar"}
```

Note – `imldifsync` cannot automatically detect and remove attributes for the optional software once they are added, that is, if you add support for Web Access and later decide to delete the entry from the configuration file, `imldifsync` cannot remove the related attributes from all LDAP directory entries for the removed *generate* option.

After adding the Sun Web Access directory schema to the `slapd` directory server, you are now ready to modify your existing entries, as explained in Chapter “Sun Directory Services Administration” of the *Sun Internet Mail Server 3.5 Administrator’s Guide*.

Preparing Configuration File for Mail Users Only

Previously after installing SIMS 3.1 or 3.2 for the first time, you needed to populate the LDAP directory that SIMS uses for its mail users only. In SIMS 3.5, the Sun Web Access client requires that you populate the directory for Calendar users in addition to e-mail users.

To support the new client, you need to use `imldifsync` to create the LDIF file. See Section "Configuring Existing Users in the LDAP Directory Database to Use Web Access," for more information about this program.

If you selected this optional client during installation, the file `imldifsync.conf` 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 entry from the `imldifsync.conf` file. The steps are shown below:

▼ To populate the directory for the mail users only

1. Find the following line in the file `/etc/opt/SUNWmail/dir_svc/imldifsync.conf`.

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

2. Remove the following statement from this line.

```
"generate=IMCalendar"
```

3. The result will look like the following.

```
option = {"generate=SIMSmal"}
```

You may now use this modified file `imldifsync.conf` to populate the directory for mail users only. See Chapter "Sun Directory Services Administration," in the *Sun Internet Mail Server 3.5 Administrator's Guide* for detailed instructions on populating the directory.

HotJava Browser Configuration

You need to specify the security level for the HotJava browser as low to further configure the Administration Console.

▼ To specify security level for HotJava browser

1. Change the directory.

```
% cd ~/.hotjava
```

2. Edit the properties file.

3. Add the following statement in the properties file.

```
hotjava.default.security = low
```

4. Save the file.

5. Start the SIMS Administration Console.

See Chapter "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 the console is running from Windows 95 or Windows NT, then the HotJava browser is installed in the directory `.hotjava`.

Removing sendmail for Pure POP3/IMAP Proxy

Full installation of SIMS removes the Sun Solaris `sendmail` and installs SIMS IMTA. Stand-alone (pure) proxy installation, however, leaves `sendmail` configuration intact. This allows `sendmail` to listen for incoming SMTP connections. Since `sendmail` is not a SIMS component, the users or aliases that are defined in the SIMS directory may not be recognized by `sendmail`.

For this reason, it is strongly recommend that you disable `sendmail` from listening for incoming SMTP connections on your proxy server by using the script `/etc/rc2.d/S88sendmail`. You may delete, move, or edit this script.

▼ To stop the sendmail daemon

```
% /etc/init.d/sendmail stop
```

After you have disabled `sendmail`, its binary files will still be available to applications that may use it for outgoing mail.

Note – If your Proxy server is a smarthost in front of the firewall, you do not need to disable your `sendmail`.

Post-installation Sun™ Web Access Setup

After you have installed the Sun Web Access server either as an option along with the SIMS Enterprise or Departmental edition or as a stand-alone product on a server other than the SIMS server, the next step is to configure your Sun Web Access server.

Topics covered in this chapter include:

- What is Sun Web Access?
- Reference Chapters for Sun Web Access
- Configuring Sun Web Access

See the appropriate sections in the *Sun Internet Mail Server 3.5 Client Installation and Configuration Guide* to set up and invoke Sun Web Access for end users.

Starting Sun Web Access

You can invoke and run Web Access from any Internet browser capable of displaying HTML 3.2 compliant documents with frames running on any platform, including Windows, Mac, OS/2, and DOS desktops. Web Access uses Java Web Server (JWS) 1.1 servlet technology from Java Software, and does not require a Java-enabled browser. Web Access does require a browser that supports *cookies*. Cookie functionality must be enabled on any browser that uses Web Access.

Reference Chapters for Sun Web Access

TABLE 8-1 Chapters Containing Sun Web Access Information

Chapter Name	To Learn About...
Overview of SIMS 3.5 Components	Overview of Sun Web Access.
What SIMS 3.5 Installs	List of Web Access packages, configuration files.
Preparing to Configure	Web Access installed packages and configuration files.
Preparing to Install SIMS 3.5	Instructions for installing the Web Access server on Solaris Sparc or Intel systems, including stand-alone Web Access.
Post-installation Configurations	Upgrade configurations for installing Sun Web Access option.

Configuring Sun Web Access

You can perform any of the configuration options discussed here from an administrator-secure computer, the Java Web Server Administration Console, or from any networked computer. For more information about Java Web Server administration, go to <http://<hostname>:9090/system/doc/administration/main.html> or <http://jserv.javasoft.com/products/java-server/documentation/index.html>. This requires that a web server already be running on port 9090.

Configuring Web Access involves several post-installation options and considerations, including:

- Restarting the Web Access Server
- Changing the port number
- Establishing secure service

- Extending Web Access capabilities
- Using an alternate JVM
- Using Web Access with a Netscape for Solaris Browser
- Using Web Access with a HotJava Browser or a JavaStation
- Changing the LDAP server

Note – You cannot monitor Sun Web Access processes by using the SIMS Administration Console.

Restarting the Web Access Server

To restart the Sun Web Access server, enter the following commands:

```
#/etc/rc3.d/K89webaccess stop
#/etc/rc3.d/S89webaccess start
```

Changing the port Number

The port for Web Access is managed through the Java Web Server Administration Console.

▼ To change the port number.

1. Open a Java Web Server Administration Console.
2. Enter the URL to access the Java Web Server.

```
http://<hostname>:9090
```

where *hostname* is the Java Web Server server host name.

3. Login to the Administration Console.

Note – This above procedure is documented in the Java Web Server help pages. To see them, click on the Help button on the Java Web Server Administration Console Login screen.

4. Select Web Service in the scrolling list of services and click on the Manage button.

A dialog appears.

5. Click on Network from the list at the left of the dialog.

The frame to the right should show the Java Web Server port number.

6. Select the port number and change it.

7. Restart the Web Access server.

```
#/etc/rc3.d/K89webaccess stop
#/etc/rc3.d/S89webaccess start
```

Establishing Secure Service

You can quickly and easily provide secure service with Web Access installations. You do so by enabling the Secure Socket Layer (SSL) feature of the Java Web Server. For requirements and a step-by-step procedure, see “Using Secure Sockets Layer (SSL) with Java Web Server,” at the following URL (assuming Sun Web Access 1.0 and the Java Web Server have been installed and are running):

```
http://<hostname>:8080/system/doc/security/ssl.html
```

This procedure shows you how to store server credentials in the key repository. Once server credentials are stored in the key repository, the Java Web Server will prompt the site administrator for a passphrase in order to gain access to the repository. By default, the server attempts to open a dialogue box using an X11 display at ":0". If the server is unable to open this dialogue box, server start-up will fail.

▼ For sites that require hands-off restart ability

1. Edit /etc/rc3.d/S89webaccess to include the line.

```
WA_ARGS=$WA_ARGS "-passfile"
```

2. Create a file in `/opt/SUNWjeev` called `keys.passphrase`, that contains the appropriate passphrase.
3. Perform the following steps.

```
#chown root /opt/SUNWjeev/keys.passphrase
#chmod 600 /opt/SUNWjeev/keys.passphrase
```

Note – You must perform step 3 to protect the passphrase.

▼ For sites that require secure login

You can also configure Web Access services to require that users log in using secure connections only. Web Access provides a simple mechanism for enforcing this policy:

1. Open the following file.

```
/opt/SUNWwa/properties/realm.Sims.properties
```

2. Edit the following line in the affirmative.

```
SimsAuth.sslRequired=<yes|no>
```

3. Restart the Web Access server.

```
#!/etc/rc3.d/K89webaccess stop
#!/etc/rc3.d/S89webaccess start
```

You also can use the SIMS Administration Console to configure the “Document Root Directory” such that the Secure Web Service has exclusive access to the following Web Access directory:

```
/opt/SUNWwa/public_html/WebAccess
```

To do so, see the Java Web Server documentation.

Extending the Web Access Palette

You can extend Web Access functionality by adding site-wide applications to the Web Access application palette. You can add an application by editing `selector.button` statements in the Web Access properties file.

To add an application to Web Access:

1. Open the following file.

```
/opt/SUNWwa/properties/realm.Sims.properties
```

2. Add the following lines of code.

```
selector.button<button-num>.method=<button-class>
selector.button<button-num>.href=<href-definition>
selector.button<button-num>.img=<button-icon-image>
selector.button<button-num>.alt=<button-alt-text-value>
selector.button<button-num>.targ=<button-targ>
```

where *button-class* specifies the Java servlet object class which will be invoked to fetch the appropriate HTML for the button. The remaining configuration items should be sufficiently self-explanatory.

Buttons may be removed from the selector by deleting the appropriate `selector.button` statements. In any case, buttons must be numbered sequentially, 0 through *n*, and will be displayed in a corresponding top to bottom fashion.

Using An Alternate JVM for Web Access

Web Access for SIMS 3.5 ships with a JVM that implements the JDK 1.1.6 level of functionality. If you wish to use another JVM, for example, for performance and scalability, the JVM you specify must implement functionality equivalent to that of JDK 1.1.6.

▼ To configure Web Access to use another JVM

1. Open the following file.

```
/etc/rc3.d/S89webaccess
```

2. Edit the file to include the following line.

```
WA_ARGS=$WA_ARGS -nojre -javahome <java-home>
```

where *java-home* is the location of the new JVM.

3. Restart the Web Access server.

```
#!/etc/rc3.d/K89webaccess stop  
#!/etc/rc3.d/S89webaccess start
```

It is your responsibility to insure that the resulting configuration meets your functional objectives.

Using Web Access with Netscape for Solaris

System administrators should be aware of a potential security risk for users who access Web Access using a Netscape for Solaris browser. The risk scenario involves an authenticated Web Access user who is running the Netscape for Solaris browser. If that user logs out of Web Access and leaves the desktop unattended, it is possible for unauthorized persons to use that instance of the Netscape browser to gain access to the user's Web Access account without presenting a valid username and password. Such users should be advised to

- always exit browsers after logging out of Web Access, and
- properly utilize existing Solaris security mechanisms (screen lock, for example) when leaving their desktops unattended (even after logging out of Web Access).

Note – In extensive testing of Web Access, the Netscape for Solaris browser was the only browser that presented the potential security risk described above.

Using Web Access with HotJava and JavaStations

System administrators that deploy Web Access for use on JavaStations or with the HotJava browser must first edit a Web Access configuration file to alter the Web Access authentication system. To do so, add the following line to the `realm.Sims.properties` file:

```
SimsAuth.checkId=no
```

This allows HotJava browsers and JavaStations to operate with Web Access. Administrators should be aware, however, that such a Web Access configuration faces greater exposure to the limitations of BASIC HTTP authentication.

Changing the LDAP Server

After installing Web Access, you can optionally specify a separate LDAP directory server and also configure the search schema used by Web Access via that server.

▼ To specify a LDAP server

1. Open the following file.

```
/opt/SUNWwa/properties/realm.Sims.properties
```

This file contains entries that determine the LDAP configuration for Web Access.

2. Edit one or more of the following lines.

```
access.LDAPAccess.ldapServiceUrl=ldap://<ldap-host>:<ldap-port>  
access.LDAPAccess.ldapSearchBase=<ldap-search-base>  
access.LDAPAccess.accessDomain=<access-search-base>
```

where,

3. *ldap-host* and *ldap-port* refer to the location from which LDAP service is provided. *ldap-search-base* refers to the base in the LDAP schema used to serve all Sun Web Access requests.

access-search-base is pre-pended to *ldap-search-base* for those LDAP operations that reflect the user state and configuration.

Invoking Web Access

After installing and configuring Web Access on a SIMS 3.5 server, obtain the Web Access URL. Typically, the Web Access URL is as follows:

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

where *hostname* is the name of the server providing Web Access service. The default port number of the Web Access server is 8080, and may be changed by the site administrator using the Java Web Server Administration Console.

From any SIMS 3.5 networked desktop:

- 1. Open an Internet browser.**
- 2. Enter the Web Access URL and press Return.**

This invokes Web Access. There is no user guide for Web Access—see the online help that comes with Web Access.

Post-Installation Tasks

After you have installed SIMS 3.5 or SIMS/HA server, you are now ready to start up you SIMS server. This chapter provides you with steps to start your SIMS server as well as a procedure to test your new server.

- Overview of Post-Installation Tasks
- Procedure to Test Your SIMS 3.5 Server

Overview of SIMS Post-Installation Tasks

The following are the post-installation steps:

1. Checking the SIMS installation log files.
2. Starting the mail server.
3. Linking to the existing web server.
4. Connecting to the manual pages.
5. Starting the SIMS Administration Console.
6. Starting the SIMS Administration Console for HA systems.
7. Starting Sun Web Access Server.
8. Populating the directory.

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 daemons.

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

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

See Section "Startup Scripts," in Chapter "Preparing to Install SIMS 3.5," for a list of components that the `im.server` script starts.

Linking to an Existing 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 (SWS). 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 Web Server to establish this link.

Connecting to the Manual Pages

The SIMS 3.5 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` or `.cshrc` 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`.

Starting SIMS Administration Console

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

1. **Bring up the HotJava browser.**

```
% /usr/dt/bin/hotjava
```

Note – The HotJava Browser is required for running SIMS Administration Console.

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

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

Starting SIMS Administration Console for HA Systems

To start the Administration Console for a SIMS/HA system, do the following steps:

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

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

2. **Restart SIMS.**

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

3. **Bring up the HotJava browser required by SIMS Administration Console as a non-root user.**

```
% /usr/dt/bin/hotjava
```


4. Start the SIMS/HA Administration Console.

```
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 Section "Installing SIMS/HA," in Chapter "Installing SIMS 3.5," for instructions for installing SIMS High Availability.

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

See the *Sun Internet Mail Server 3.5 Administrator's Guide* for information on the SIMS Administration Console.

Starting Sun Web Access Server

To administer Web Access, you can use the Java WebServer administration tool. This is a browser-based, Java administration tool.

▼ To access the Java Web Server tool:

1. Open an Internet browser.
2. Enter the URL to access the Java Web Server Administration tool.

```
http://<hostname>:9090/WebAccess
```

where *hostname* is the name of the SIMS 3.5 server running the Web Access services. 9090 is the default port number for the Java WebServer administration console.

See the online help accompanying Web Access for more information.

Populating the Directory

If you are installing SIMS 3.5 for the first time, you need to populate the LDAP directory that SIMS uses to resolve incoming e-mail 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 “Sun Directory Services Administration,” in the *Sun Internet Mail Server 3.5 Administrator’s Guide* for information about populating the directory.

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 3.5 Administrator’s Guide*, and the *Sun Internet Server 3.5 Reference Manual* for more information on using this utility.

Testing Your SIMS 3.5 Server

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

For detailed instructions on accomplishing these tasks, see the *Sun Internet Mail Server 3.5 Administrator's Guide*.

▼ To test your SIMS server

1. Create a couple of test users by using the SIMS Administration Console, User Management, Create User option.
2. Perform an `imta dirsync -F` to synchronize the directory.
3. Login 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>:9090/webaccess.html
```

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

Troubleshooting SIMS Server

This chapter covers some of the potential issues that you may encounter during the installation of SIMS 3.5, 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 DNS Setup
- SIMS Installation Log Files
- Rebooting after Re-installing
- Configuring HotJava Browser
- Removing sendmail
- Missing Command Tool
- Cleaning up Corrupted Quota File

Configuring DNS Setup

Before installing SIMS 3.5, 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 Section “Configuring Files,” below.

Diagnosing DNS

SIMS 3.5 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 `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 `nsswitch.conf` for the search order for hosts or the `/etc/hosts` files if this file is being used.

FIGURE 10-1 shows the steps that SIMS 3.5 installation takes to check for a fully-qualified domain name.

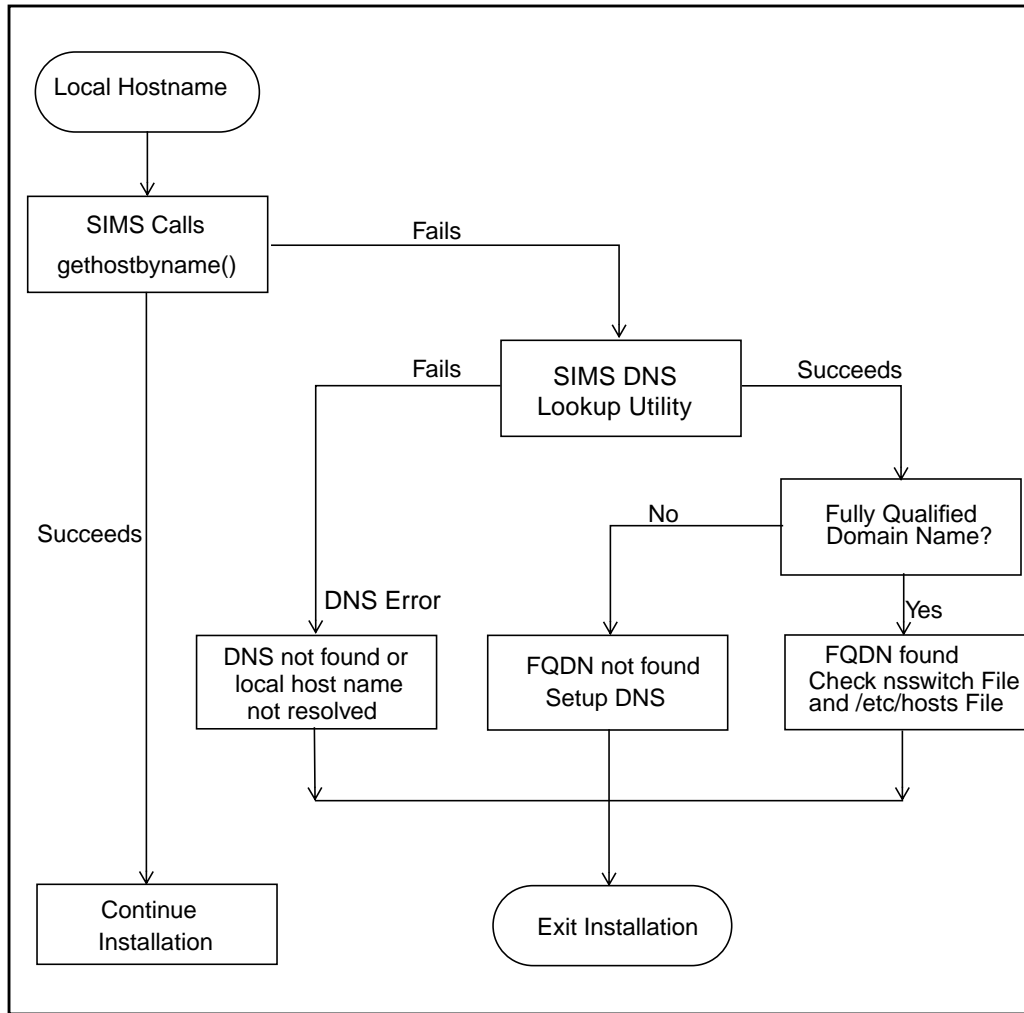


FIGURE 10-1 DNS Diagnostic Procedure

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` file 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,

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 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 may check the log file in `/tmp`.

Rebooting after Reinstalling

If you are reinstalling SIMS 3.5, 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 HotJava Browser

After you have installed SIMS, you need to configure the HotJava property files by setting the default security level to low.

See Section “HotJava Browser Configuration,” in Chapter “Post-Installation Configurations,” for instructions on configuring the “HotJava Browser.”

Removing sendmail

When SIMS 3.5 is fully installed, sendmail is automatically removed from your system. However, if you are installing an stand-alone (pure) proxy, `sendmail` will remain on your system. See Section “Removing sendmail for Pure Proxy” in Chapter “Post-Install Configurations” for information on how to manually remove sendmail from stand-alone proxy servers (not installed on a SIMS server).

Missing 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.

Removing Extra Characters in License Password File

If your license file was saved on a PC and then moved to a Solaris system, you have to make sure that no extra line feed character (^M) exists at the end of each line.

Cleaning up Corrupted Quota File

If you are upgrading to SIMS 3.5 from SIMS 3.2, 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.

After you have upgraded to SIMS 3.5, 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.

```
-----  
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%  
-----
```

See the *Sun Internet Mail Server Administrator's Guide* for instructions on how to set up user quotas.

SIMS Asymmetric High Availability

A major advantage of SIMS 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 e-mail access for an entire user community.

To ensure reliability, SIMS 3.5 enables you to install on a Sun Enterprise Cluster by using the Sun Cluster 2.1 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 HA References in this Chapter
- SIMS Asymmetric HA Configuration
- Fail-over Procedure
- Directory Services Considerations

Other HA References in this Guide

TABLE 11-1 lists out 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 "Installing SIMS 3.5," for instructions on installing SIMS/HA.

TABLE 11-1 Chapters Containing High Availability Information

Chapter Name	To Learn About...
What SIMS 3.5 Installs?	Lists of SIMS 3.5 packages and configuration files, including HA.
Preparing to Configure	Software requirements for SIMS/HA.
Preparing to Install SIMS 3.5	Lists of required and recommended patches.
Installing SIMS 3.5	Instructions for installing SIMS/HA.
Post-Installation Tasks	Instructions to invoke Administration Console.

SIMS Asymmetric HA Configuration

FIGURE 11-1 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.

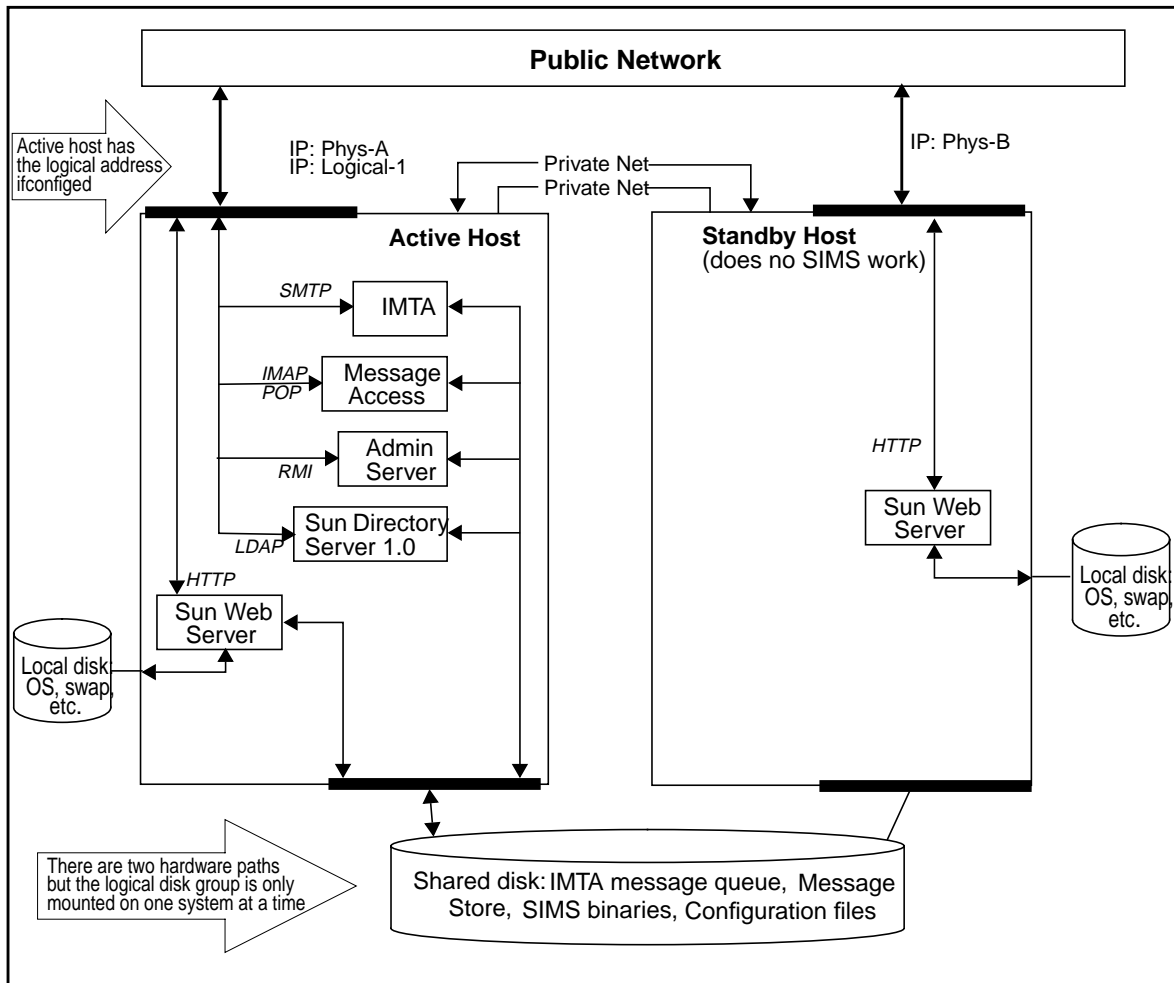


FIGURE 11-1 SIMS Asymmetric HA Configuration Before Fail-over

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 11-1 and subsequent figures in this chapter show this disk cluster as a single logical volume.

Sun Cluster also includes the Sun Enterprise volume manager, which is based on the Veritas VxVM volume manager. 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 11-1, 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 11-2 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, re-connecting 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!

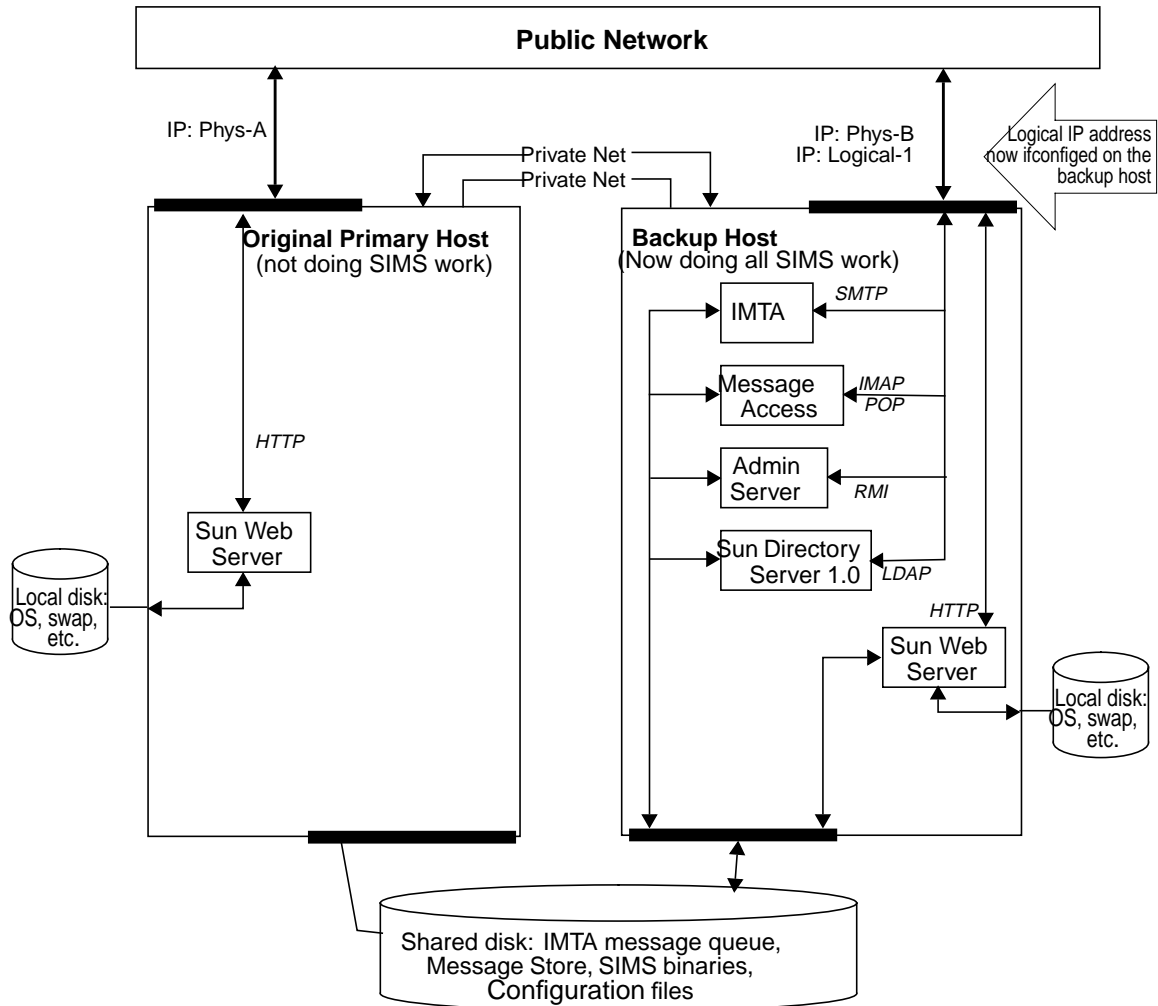


FIGURE 11-2 SIMS Asymmetric HA Configuration after Fail-over

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

- 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 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 11-2.

TABLE 11-2 SIMS Directories on the Shared Disk between Cluster Nodes

Install Creates Links from...	To place on the shared disk
<code>/opt/SUNWmail</code>	<code>/shared-disk-BASEDIR/opt/SUNWmail</code>
<code>/etc/opt/SUNWmail</code>	<code>/shared-disk-BASEDIR/etc/opt/SUNWmail</code>

Linking Sun DS Directories to Shared Disks

The Sun Directory Service 1.0 (SunDS) binaries and data are also normally installed on the shared disk. Since the SunDS packages are not completely relocatable, this is accomplished in the SIMS install script by planting symbolic links from the following locations to the shared disk, as shown in TABLE 11-3.

TABLE 11-3 Sun DS Directories Mapped to Shared Disk between Cluster Nodes

Install Creates Links from...	To place on the shared disk
<code>/opt/SUNWconn/ldap</code>	<code>/shared-disk-BASEDIR/opt/SUNWconn/ldap</code>
<code>/etc/opt/SUNWconn/ldap</code>	<code>/shared-disk-BASEDIR/etc/opt/SUNWconn/ldap</code>

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 optionally the directory) on one machine and start up on the other machine.

Operating System and Platform Support

TABLE 11-4 shows the configurations that are supported in SIMS 3.5.

TABLE 11-4 Tested Platform Configurations

Operating System Release	Cluster Software	Hardware Architecture
Solaris 2.5.1	Sun Cluster 2.1	SPARC
Solaris 2.6	Sun Cluster 2.1	SPARC

Storage and File System Requirements

To ensure system availability by eliminating single points of failure, SIMS, SunDS binaries, configuration files, and data must be *mirrored* on replicated disks. Sun Cluster 2.1 includes the Sun Enterprise Volume Manager, on which SIMS/HA depends to provide redundant storage.

To enable SIMS 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) 3.2.4 to provide a file system with these characteristics.

Note – Since Sun Cluster 2.1 does not include Veritas File System (VxFS) 3.2.4, it must be purchased.

Directory Services Considerations

SIMS 3.5 requires that a SunDS 1.0 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 Sun High Availability configurations in this chapter. You may now follow the instructions covered in Chapter “Installing SIMS 3.5,” to install your SIMS/HA system.

Command-Line Installation

This appendix provides information on commands that you can use to install and uninstall your SIMS server via command-line. It also gives you an example for installing SIMS from command-line. At the end, comparison between graphical user interface (GUI) installation versus command-line installation is provided.

- Command-Line Utilities
- The uninstall Utility
- Example of Command-Line Installation
- Graphical or Command-Line Installation?

Note – Before you begin installing the SIMS 3.5 software by using the command-line installation program, you should have requested and obtained the necessary license passwords. In addition, make sure that you know the location of the `license.dat` file before issuing the installation command.

Command-Line Utilities

This section describes the utilities that are associated with the installation process.

Installation Utility

`setup-tty` is a script that installs SIMS and its related files and packages onto the system.

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:

```
setup-tty [-c install | remove] [-d]
```

The options for this command are:

TABLE A-1 Options for the `setup-tty` Command

Option	Description
<code>-c install</code>	Specifies a standard install of SIMS and related files and packages.
<code>-c remove</code>	Specifies an uninstall of SIMS and related packages and files from the system.
<code>-d</code>	Specifies a non-interactive automated install using the <code>/tmp/sims_setup.dat</code> file, if it exists. If <code>/tmp/sims_setup.dat</code> does not exist, <code>setup-tty</code> will default to the standard interactive install and prompt the user for necessary information. See the <i>Sun Internet Mail Server Reference Guide</i> for the format of the file <code>sims_setup.dat</code> .

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 which 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 dramatic procedure.

Note – `uninstall` 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 A-2 Options for the uninstall Command

Option	Description
<code>-c sims</code>	Specifies a standard <code>uninstall</code> of SIMS and related files and packages.
<code>-d sims</code>	Specifies a dramatic <code>uninstall</code> of SIMS and related files and packages. This option removes all data and configuration files. The dramatic <code>uninstall</code> option is a clean <code>uninstall</code> , 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 <code>uninstall</code> procedure.

The following command performs a standard `uninstall`:

```
% uninstall -c sims
```

The following command performs a dramatic `uninstall`:

```
% uninstall -d sims
```

Example of Command-Line Installation

This section provides an example for installing SIMS through the command-line interface.

1. Login as root.

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

2. Invoke the command-line interface.

```
# /cdrom/sun_internet_mail_3_2/products/sims/setup-tty -c
```

3. Enter the postmaster ID.

```
Postmaster User ID [inetmail]: inetmail
```

4. Enter your license file.

```
License file path [/etc/opt/licenses/licenses_combined#]:  
/tmp/license.dat
```

5. Accept installing patches.

```
Do you want to install these patches? (y): [y,n,?] y
```

6. Enter the mail server's fully-qualified DNS domain name.

```
[eng.sun.com]: eng.alpha.com
```

7. Enter the highest DNS domain name used for your organization.

```
[sun.com]: alpha.com
```

8. Select Yes to accept putting the SIMS server behind a firewall.

Please choose an option from above: 2

9. Enter the administrator's name.

(default=admin): admin

10. Select No to accept receiving mail via SIMS secured message store.

Please choose an option from above: 1

11. Enter the two character country code for your organization.

(default=US): US

12. Enter your organization's abbreviated name.

[: alpha

**13. Enter the division or department name within the organization specified above
[OU=eng,o=alpha,c=US]**

(default=eng): eng

14. Enter the full name of your organization.

Alpha Incorporated

15. Enter the postal address of the system administrator responsible for this installation.

1234 Main Street

16. Enter the city or town in which this server resides.

Anytown

17. Enter the state or province in which this server resides.

CA

18. Enter the postal address of the system administrator responsible for this installation.

555-1234

Graphical or Command-Line Installation?

The graphical and the command-line installations both pose the same set of questions and collect the necessary initial configuration information in a similar manner. TABLE A-3 summarizes the significant differences in the two installation interfaces.

TABLE A-3 Main Differences Between the Graphical and the Command-Line Interface

Type of Difference	Graphical Installation Method	Command Line Installation Method
Invoking	Use the <code>setup</code> 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 <code>setup-tty</code> script. You must invoke this script as <code>root</code> .
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.	As soon as you identify that you want to install the Enterprise or Departmental edition, the installation script proceeds to install 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.

Planning SIMS System

This chapter provides the following types of planning information for setting up your SIMS system:

- Directory Services Considerations
- Selecting Topologies
- Internet Message Transfer Agent Considerations

Directory Services Considerations

The directory service stores information on mail users, distribution lists, and services. This directory information is stored according to the directory information tree (DIT). The DIT is a hierarchical structure that resembles a tree with one major branch at the top and many branches and sub-branches as you work your way down.

TABLE B-1 outlines the layers that the DIT can contain from top to bottom.

TABLE B-1 Directory Information Tree Layers

Layer Name	Attribute	Mandatory Layer?	Maximum Number of Layers	Comments
Country	c	Yes	One level	If an organization has multiple mail servers that are geographically distributed in multiple countries, the country attribute should reflect one country only, for example, the organization headquarters.
Organization	o	Yes	One layer	None
Organizational unit	ou	No	No limit	The existence of this organizational unit layer depends on the size of your organization (number of users) and structure of your organization's Domain Name Service (DNS).
People, Groups, and Services	ou	Yes	One layer	Directory information is stored in the form of user entries, group entries (for distribution lists), and service entries (for example, printer). User entries are stored under People, distributions lists are stored under Groups, and service entries are stored under Services.

As implied in TABLE B-1, the country, organization, and people, groups, and services layers of the DIT are fixed. You can configure names or labels for the country and organization layers but not the people, groups, and services layer. You cannot

remove the country, organization, and people, groups, and services layers or add an additional layer of those categories. The organizational unit layer, however, is not fixed. Your DIT can have zero, one, two, or more organizational unit layers.

The number of organizational units in a DIT is dictated by the size of your organization and the structure of its DNS. For example, if your DNS is composed of only one domain, for example `alpha.com`, then the DIT will have no organizational unit layers. This is shown in FIGURE B-1.

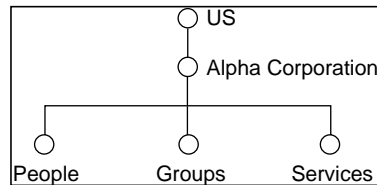


FIGURE B-1 Directory Information Tree for a Small Organization

If your DNS is divided into the subdomains `mkting.bravo.com`, `eng.bravo.com`, `corp.bravo.com`, and `mfg.bravo.com`, then your DIT will have one organizational unit layer with subtrees for each of the four subdomains, as shown in FIGURE B-2.

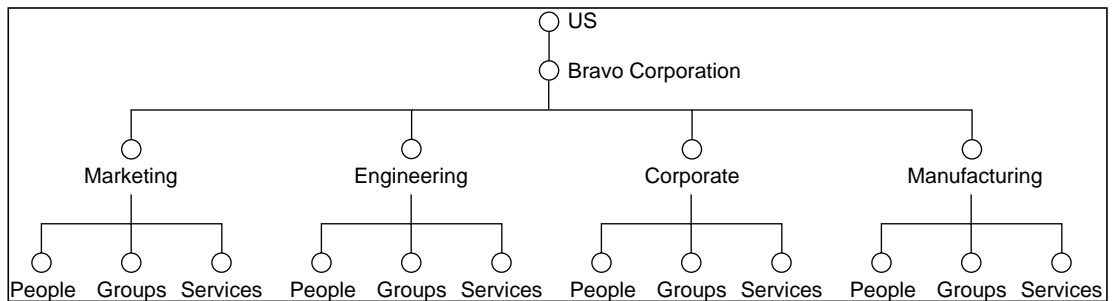


FIGURE B-2 Directory Information Tree for a Medium or Large Organization

If an organization is small (1000 or fewer users and mailboxes) and the DNS is composed of only one domain like the Alpha Corporation, then you can implement the entire DIT on one mail server. If your organization is medium or large, the DNS is divided into subdomains like the Bravo Corporation, and you have decided to implement multiple mail servers, then you can implement portions of the DIT or subtrees on each mail server.

Automatic Directory Information Tree Layout

SIMS provides a mechanism during installation to automatically generate the portion of the directory information tree (DIT) that you plan to implement on a particular mail server. The automatic layout is based on the following assumptions:

- Your organization currently implements the Domain Name Service (DNS).
- The mail server on which you are installing the SIMS software is a valid DNS client.
- If you plan to implement multiple mail servers, you first decide which portions or subtrees of the DIT to implement on each of the mail servers.

During installation, you will be prompted to provide information.

Page 1 of the initial configuration pages asks for your input in these fields:

<p>Mail Server Domain Name Suffix – Enter the mail server's DNS domain suffix. (ie: eng.widget.com)</p> <p>Domain Name Suffix: <input type="text" value="eng.alpha.com"/></p> <p>Organization Top Level Domain Name Suffix – Enter the highest level DNS domain name suffix used for a particular organization. (ie: widget.com)</p> <p>Top Level Domain: <input type="text" value="alpha.com"/></p>
--

FIGURE B-3 Partial Configuration Page 1 of 3

- **Mail Server Domain Name** - if you plan to implement your organization's entire DIT on this mail server, then you can enter, for example, `alpha.com`. If you plan to implement a portions or subtrees of your organization's DIT, then you can enter, for example, `eng.alpha.com` or `mkting.bravo.com`.
- **Organization Top Level Domain Name** - regardless whether you plan to implement your organization's entire DIT or a portions of the DIT on this mail server, you must input your organization domain, for example, `alpha.com` or `bravo.com`

One of the initial configuration pages asks for the following information:

Country Name – Choose the country name where this mail server resides from the provided drop down list.

Country Name:
Afghanistan
Albania

Organization Name – Enter your organization's abbreviated name.

For example: If the Mail Server Domain name is 'eng.widget.com', then the Organization Name should be 'widget'.

Organization Name:

Organizational Unit – For each domain name specified below, an organizational unit (OU) name needs to be specified.

For example, if the domain name is 'eng.widget.com' the default OU name would be 'eng' but, you might want to change it to a more descriptive word like 'Engineering'

Domain Name	Organizational Unit
eng.alpha.com	engineering

FIGURE B-4 Partial Configuration Page 2 of 3

- **Country Name** - If you plan to implement one or more mail servers in the same country, then enter the country in which your mail servers reside. If you plan to implement multiple mail servers that are geographically distributed in multiple countries, then enter one country only, for example, the organization's headquarters.
- **Organization Name** - Enter the name of your organization, for example, Alpha or Bravo.
- **Organizational Unit** - Enter a name or label for each of the organizational units if your DNS contains subdomains, for example, Marketing or Engineering.

The automatic layout of your DIT is based on the structure of your organization's DNS. In fact, the structure of your DIT will mirror the structure of your DNS.

FIGURE B-6 shows one layer of an organizational unit, whereas FIGURE B-5 does not.

For example, if your organization has fewer than 1000 users (mailboxes), you are implementing one mail server, and you provide the following input:

```
mail server domain name = alpha.com  
organization top level domain name = alpha.com  
country = US  
organization = Alpha
```

(when there are no subdomains, there is no prompt for organizational unit name.

Your DIT will look like the one shown in FIGURE B-5.

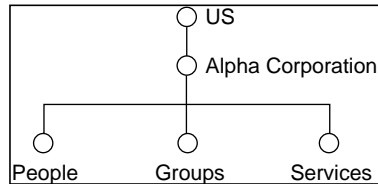


FIGURE B-5 Automatically Generated Directory Information Tree for a Small Organization

If your organization has 100,000 users (mailboxes), you are implementing one subtree per mail server, and you provide the following input for one mail server:

```
mail server domain = eng.bravo.com
top level of organization = bravo.com
country = US
organization = Bravo
organizational unit = engineering
```

The portion of the DIT that will reside on this mail server will be similar to the one shown in FIGURE B-6.

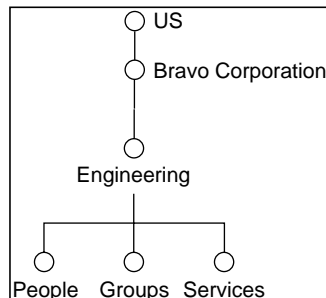


FIGURE B-6 Automatically Generated Directory Information Tree for a Large Organization

In the DITs shown in FIGURE B-5 and FIGURE B-6, a final layer with branches called People, Groups, and Services has been added. The People branch will contain user entries, the Groups branch will contain group entries for distribution lists, and the Services branch will contain services. During installation, you can move users and distribution lists from your existing e-mail system to initially populate the directory service. See Section Populating Directory in Chapter “Post-Installation Tasks,” for more information on populating the directory.

After the installation is complete, you can use the SIMS Administration Console to maintain (add, delete, modify) the user and group entries, to view the structure of the DIT contained on a particular mail server, and to modify the DIT's organizational units (if subdomains are added or deleted). For more information, refer to the *Sun Internet Mail Server 3.5 Administrator's Guide*.

Directory Service Administration

You must decide which directory information tree (DIT) administration scheme works best for your organization: *centralized* or *distributed*. Since the DIT mirrors the DNS layers, if your DNS does not contain subdomains, your DIT structure will not contain organizational units, which implies a centralized DIT administration scheme. Similarly, if your DNS contains multiple subdomains, it implies multiple organizational units and requires a distributed DIT administration scheme.

- You can implement centralized administration, where one authority manages the entire DIT. This type of administration is usually implemented in scenarios where the entire DIT resides on one mail server.
- You can also implement distributed administration, where multiple authorities manage the DIT. This type of administration is usually implemented when your DIT is divided into portions or subtrees and the subtrees reside on different mail servers. Typically in this scenario, it is infeasible for one authority to handle modifications for the entire DIT because of the size of the DIT, and because the mail servers are geographically dispersed. You must assign an authority to manage each subtree of the DIT. It is acceptable for one authority to manage multiple subtrees. An authority can make changes only to the subtree of the DIT that it owns.

FIGURE B-7 shows the DIT of the Alpha Corporation that is administered by one authority. The Alpha Corporation is a small organization with fewer than 1000 users (mailboxes). Alpha's entire DIT resides on one mail server.

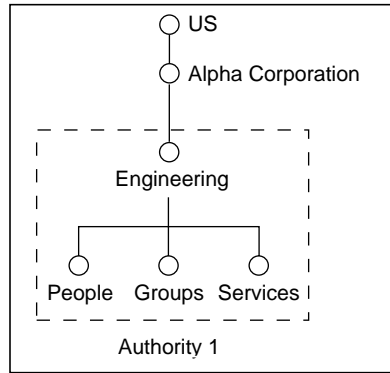


FIGURE B-7 Centralized Directory Information Tree Administration

FIGURE B-8 shows the DIT of the Bravo Corporation that is administered by five authorities. The Bravo Corporation is an organization with 15,000 mailboxes. Bravo's DIT is partitioned into five subtrees and each subtree resides on a different and geographically remote mail server.

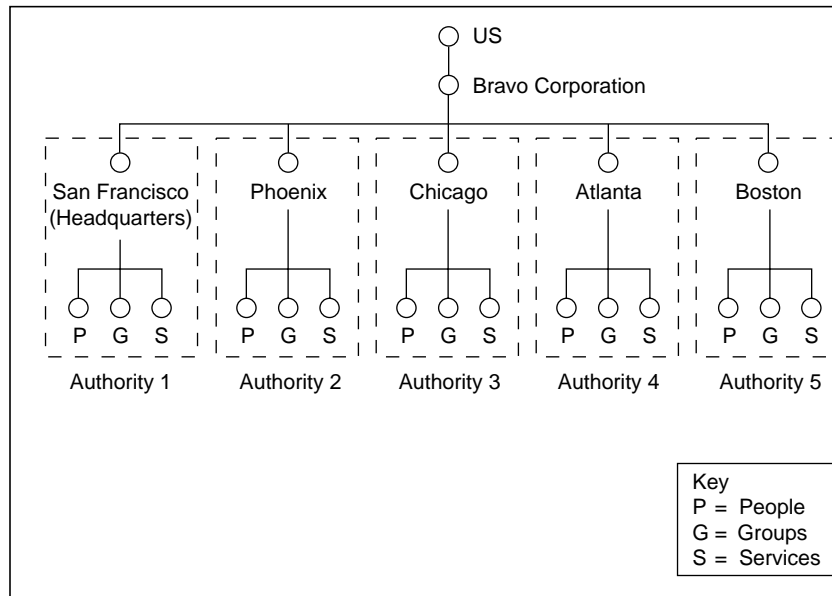


FIGURE B-8 Distributed Directory Information Tree Administration

Directory Replication

If your directory information tree (DIT) is partitioned and you decide to implement the subtrees on different mail servers, you should consider using the replication feature. Replication enables a replica of all or part of the DIT that resides on one mail server (directory server) to be delivered to one or more directory servers.

Benefits of using the replication feature include the following:

- The directory information is more accessible since it is replicated on multiple rather than a single directory server.
- The directory information is cached on a local directory server, saving the effort of accessing the information from a remote directory server and thereby enhancing performance.
- Requests generated by mail clients will be processed faster by multiple directory servers rather than by one mail server.

For complete information on replication, including how to configure the replication feature, see the *Sun Internet Mail Server 3.5 Administrator's Guide*.

Selecting Topologies

This section provides sample topologies for the following scenarios:

- Small organization—1000 or fewer users (mailboxes)
- Medium organization—1000 to 50,000 users
- Large organization—50,000 to 100,000 users

E-mail System for a Small Organization

This section provides a sample topology that illustrates an e-mail system for a small organization of 1000 or fewer mailboxes.

The Engineering workgroup is composed of 300 employees who are part of a larger organization, the Alpha Corporation, which is composed of 600 employees. The Alpha Corporation does not employ a company-wide e-mail system. The Engineering work group is located on the second floor of the Alpha Building.

The Alpha Corporation implements the DNS. Its registered domain name is `alpha.com` and the domain `eng.alpha.com` is used internally to represent the Engineering work group.

FIGURE B-9 shows Alpha's DIT from a high level, with more detail of the Engineering workgroup subtree. The DIT mirrors the DNS. The directory information subtree was generated automatically by the system, thus producing a final layer of organizational units with branches for people, groups, and services.

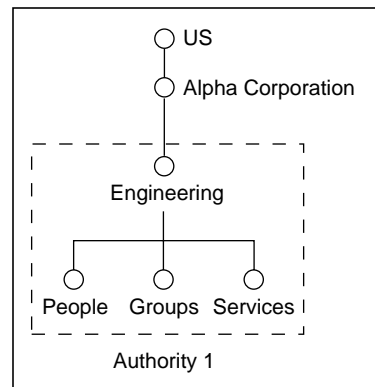


FIGURE B-9 Sample Directory Information Subtree for a Small Organization

One authority administers the Engineering subtree.

The Engineering workgroup implements one mail server, as shown in FIGURE B-10.

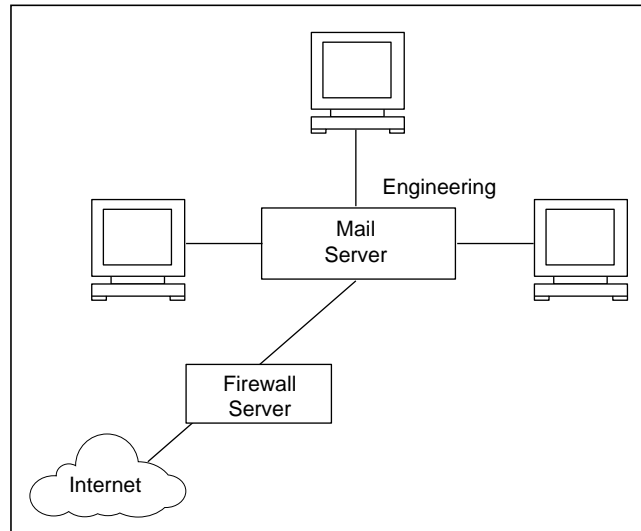


FIGURE B-10 Sample Topology for a Small Organization

E-mail System for a Medium Organization

This section provides a sample topology that illustrates an e-mail system for a medium organization with between 1000 and 50,000 mailboxes.

The Bravo Corporation is a medium organization composed of 15,000 employees. The organization is divided into functional groups that are geographically distributed in San Francisco, Chicago, and New York City; San Francisco is the headquarters.

Bravo implements the DNS. Its registered domain name is `bravo.com` and the following are domains that Bravo uses internally to represent each geographic group:

- `sf.bravo.com`
- `chi.bravo.com`
- `nyc.bravo.com`

Bravo's DIT, which is shown in FIGURE B-11, mirrors the DNS. The DIT was generated automatically by the system; therefore, a final layer of organizational units with branches for people, groups, and services is present.

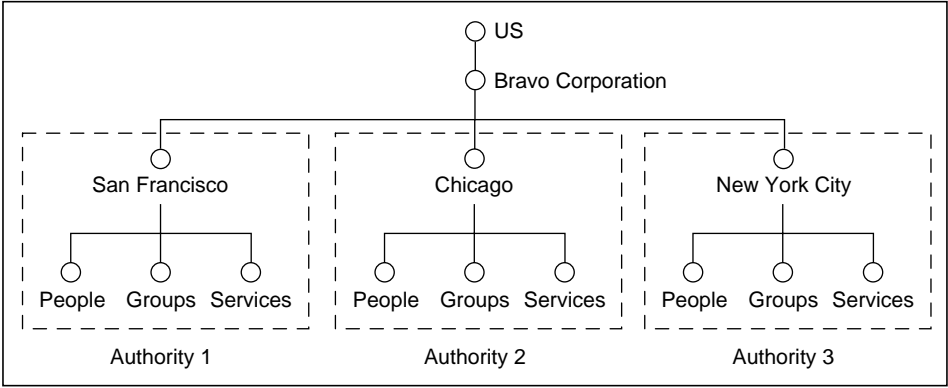


FIGURE B-11 Sample Directory Information Tree for a Medium Organization

The DIT has been partitioned into three subtrees. The partitions are based on the geographic areas that comprise Bravo. One authority manages the San Francisco subtree, another manages the Chicago subtree, and the last one manages the New York City subtree.

Bravo implements one mail server at each of its geographic sites to compose a backbone and a mail server for each of the functional groups at a geographic site, as shown in FIGURE B-12.

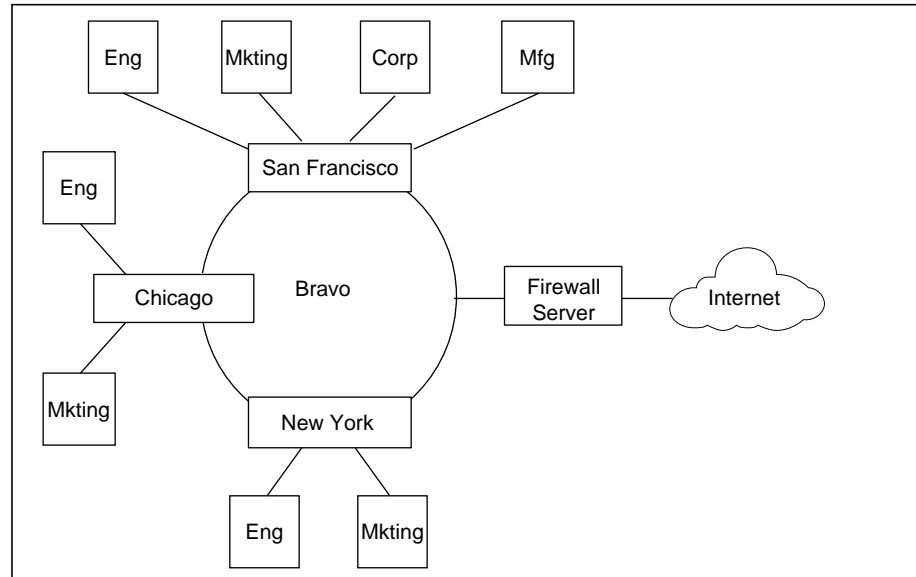


FIGURE B-12 Sample Topology for a Medium Organization

Bravo implements the replication feature in its e-mail system. FIGURE B-13 shows how the replicated directory information flows.

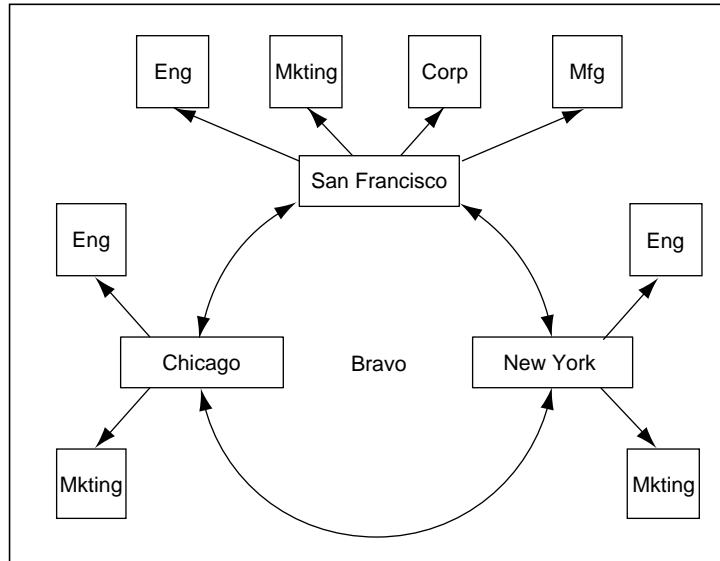


FIGURE B-13 Sample Replication Data Flows for a Medium Organization

As shown in FIGURE B-13, master directory servers have been set up on each of the backbone mail servers (one for San Francisco, one for Chicago, and one for New York City). Each master directory server maintains directory information for the subtree below it. Each master directory server also receives a full replication of information from the other master directory servers, meaning that each master directory server also functions as a replica directory server and contains directory information for the entire DIT.

Replica directory servers have been set up on each of the departmental mail servers (San Francisco has departmental mail servers for Engineering, Marketing, Corporate, and Manufacturing; Chicago has departmental mail servers for Engineering and Marketing; New York City has departmental mail servers for Engineering and Marketing) for a total of eight. Each of the replica directory servers receives only data pertaining to its functional area or subtree. For example, the San Francisco Engineering replica directory server will receive directory information for the San Francisco Engineering subtree. In this sample topology, replicating partial rather than full information to the replica directory servers will help conserve network bandwidth each time synchronization of information between master and replica directory servers occur.

E-mail System for a Large Organization

This section provides a sample topology that illustrates an e-mail system for a large organization of between 50,000 and 100,000 mailboxes.

For example, Net International Corporation is a large organization with 100,000 employees. The organization is divided into functional groups that are geographically distributed in the United States (offices in Los Angeles, St. Louis, and Boston), Europe (offices in London, Paris, and Rome), and Asia (offices in Tokyo, Beijing, and Taipei).

Net implements the DNS. Its registered domain name is `net.com` and the following are domains that Net uses internally to represent each geographic and functional group:

TABLE 11-5 Sample Topology

Domain Name	Valid Sub Domains
<code>la.net.com</code>	<code>corp.la.net.com</code> <code>eng.la.net.com</code> <code>mkting.la.net.com</code> <code>mfg.la.net.com</code>
<code>stlouis.net.com</code>	<code>eng.stlouis.net.com</code> <code>mkting.stlouis.net.com</code>
<code>boston.net.com</code>	<code>eng.boston.net.com</code> <code>mkting.boston.net.com</code>
<code>london.net.com</code>	<code>corp.london.net.com</code> <code>eng.london.net.com</code> <code>mkting.london.net.com</code> <code>mfg.london.net.com</code>
<code>paris.net.com</code>	<code>eng.paris.net.com</code> <code>mkting.paris.net.com</code>
<code>rome.net.com</code>	<code>eng.rome.net.com</code> <code>mkting.rome.net.com</code>

TABLE 11-5 Sample Topology

Domain Name	Valid Sub Domains
tokyo.net.com	corp.tokyo.net.com eng.tokyo.net.com mktng.tokyo.net.com mfg.tokyo.net.com
beijing.net.com	eng.beijing.net.com mktng.beijing.net.com
taipei.net.com	eng.taipei.net.com mktng.taipei.net.com

As shown in FIGURE B-14, Net's DIT mirrors the DNS. The DIT was generated automatically by the system; therefore, a layer of organizational units with branches for people, groups, and services is present.

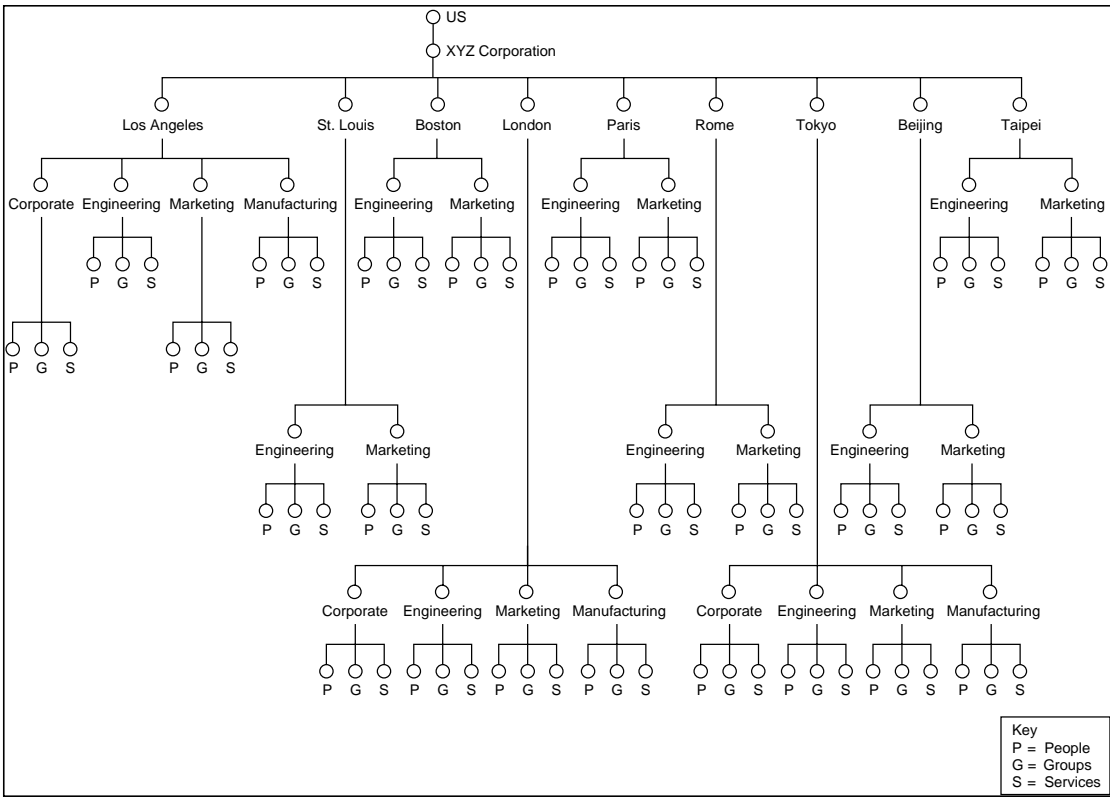


FIGURE B-14 Sample Directory Information Trees for a Large Organization

The DIT has been partitioned into nine subtrees based on geographic location, and subsequently into two to four subtrees, based on function. One authority administers each of the geographic and functional subtrees.

Net implements one mail server at each of its geographic sites, to form an enterprise for each region. In total, the topology consists of three enterprise servers in U.S., Europe, and Asia. Net also implements one mail server for each of the functional groups at a geographic site as shown in FIGURE B-15.

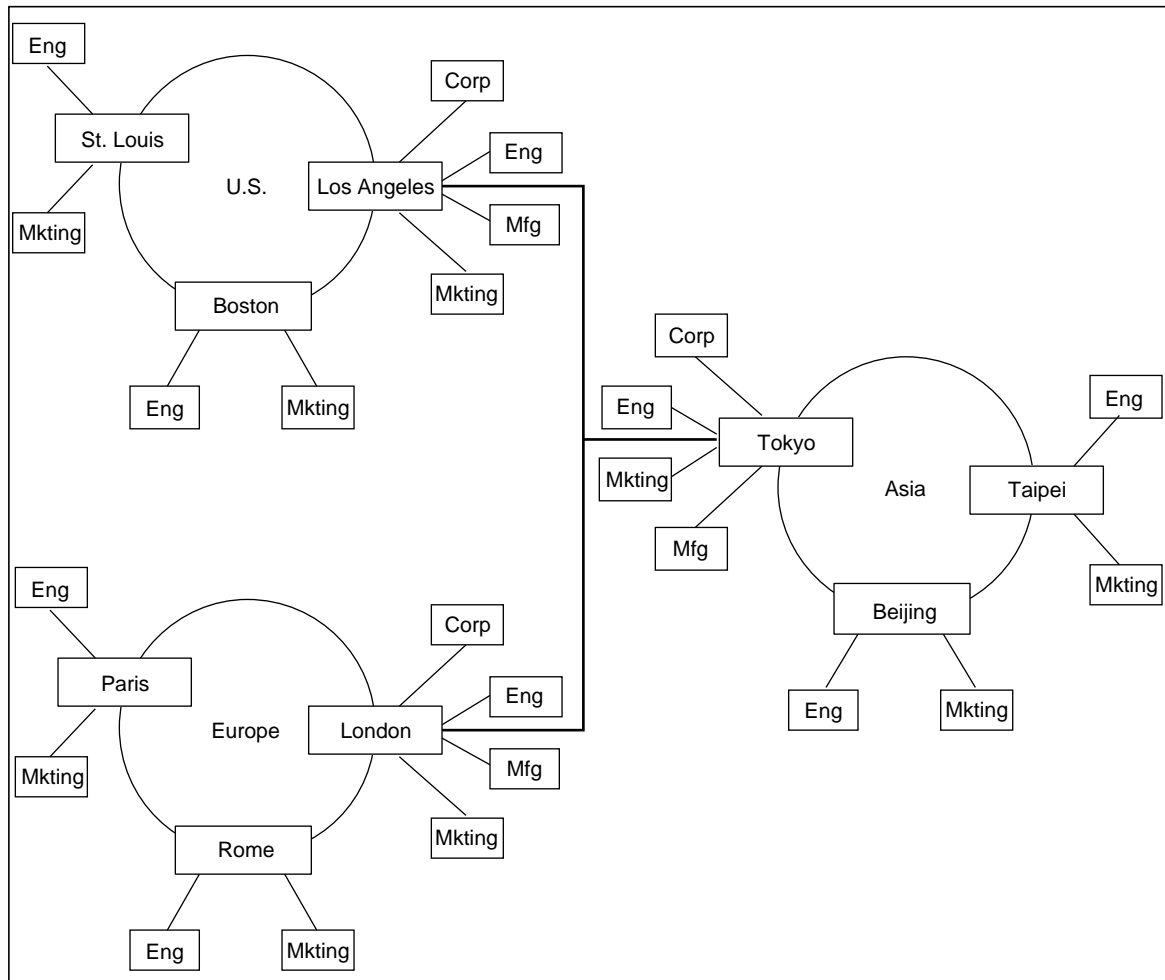


FIGURE B-15 Sample Topology for a Large Organization

Net implements the replication feature in its e-mail system. FIGURE B-16 shows how the replicated directory information flows.

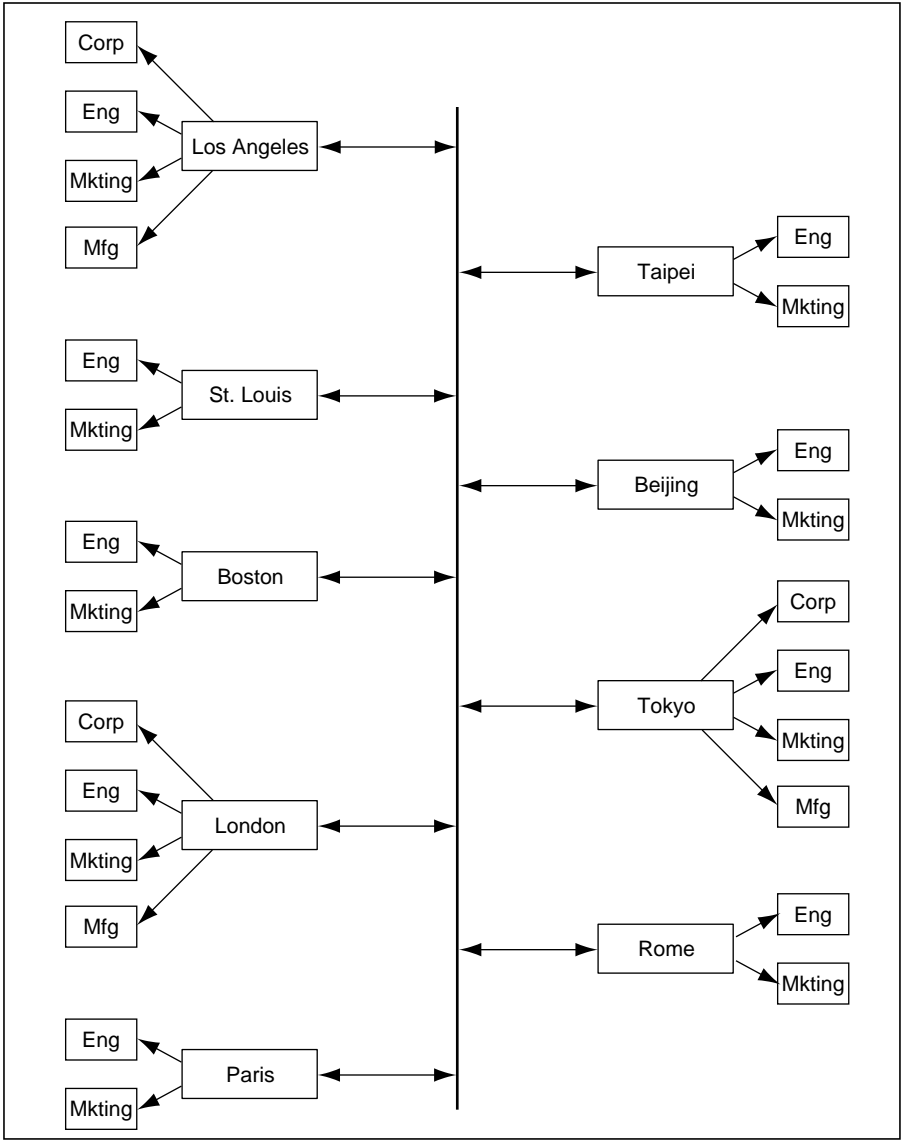


FIGURE B-16 Sample Replication Data Flows for a Large Organization

As shown in FIGURE B-16, master directory servers have been set up on each of the backbone mail servers (one for Los Angeles, St. Louis, Boston, London, Paris, Rome, Tokyo, Beijing, and Taipei). Each master directory server maintains directory information for the subtree below it and provides connections via its backbone servers. Each master directory server also receives a full replication of information from the other master directory servers, meaning that each master directory server also functions as a replica directory server and contains directory information for the entire DIT.

Replica directory servers have been set up on each of the departmental mail servers, for a total of 24. Each of the replica directory servers receives only data pertaining to its functional area or subtree. For example, the Los Angeles Engineering replica directory server will receive directory information for the Los Angeles Engineering subtree. In this sample topology, replicating partial rather than full data to the replica directory servers will help conserve network bandwidth each time synchronization of information between master and replica directory servers occurs.

Internet Message Transfer Agent Considerations

The IMTA component of the SIMS software requires the following information. Be sure to have this information ready before you begin the installation, identifying

1. if the message transfer agent is behind a firewall. If yes, identify which system will be responsible to route messages through the firewall
2. the Mail Server Domain Name
3. the Organization Top Level Domain Name

Role of a Mail Server

Before you install an ensemble of mail servers, you should determine what role you will assign to the message transfer agent for each of them. Two factors can help determine the role of an MTA:

1. The MTA's ability to route messages to a group of e-mail users in one of the following ways:
 - The MTA delivers mail directly to local recipients.
 - The MTA forwards 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:
 - If the mail server is separated from the public Internet by a firewall machine
 - If the mail server is not separated from the public Internet by a firewall machine; your company does not have a machine serving as the firewall, or your mail server also serves as the firewall system.

MTA's Ability to Route Messages

The SIMS product classifies the MTA'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 MTA 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.alpha.com`, the MTA knows to forward this message to `mailhost.eng.alpha.com`. Similarly, it can forward a message addressed to `<user>@qa.eng.alpha.com` to `mailhost.qa.eng.alpha.com`.

2. The MTA can only deliver messages to local users. The MTA cannot deliver to non-local users. If a message arrives that is not addressed to a local user, and 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 MTA forwards it 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 MTA 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.

The MTA'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 MTA. Since your MTA is not a firewall MTA, it also cannot query the public DNS.

This means that each mail server's MTA depends on a smarter MTA (except the firewall machine's MTA) 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 MTA 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, your company, Alpha Corporation, has implemented a firewall. If a user, `joan@eng.alpha.com` sends a message to `pierre@sales.alpha.com`, the message is handled by Joan's mail server. Since Joan's mail server can route only to users within `eng.alpha.com` domain, it forwards the message to its configured smart host, `mailhost.alpha.com`. If `mailhost.alpha.com` has the ability to route messages to `alpha.com`, this mail will be routed directly to Pierre's mail server. However, if `mailhost.alpha.com` serves as a pure backbone MTA, with no ability to route messages directly to users, it will transit the message to a configured MTA (specified in the `mailhost.alpha.com`'s configuration) that can route directly within Pierre's mail domain, `sales.alpha.com`.

In this example, `mailhost.alpha.com` does not necessarily serve as the company's firewall system. So, if a message arrives addressed to `your@net.com`, `mailhost.alpha.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 MTA's location relative to a firewall and how to configure a smart host, see Section "To Configure Position Versus Firewall and Smart Host," in the *Sun Internet Mail Server 3.5 Administrator's Guide*.

Sample MTA Scenarios

Refer to the MTA scenario that best matches your company's mail server set up plans.

Mail Server Supporting Few Users in a Single Domain

Alpha Corporation has 1000 mail users and is part of the `alpha.com` domain. Based on average mail use, Alpha 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 `alpha.com` domain.

If Alpha Corporation has a firewall, locating the corporate mail server and the firewall on different machines is preferable. In this way, the firewall MTA can be responsible for merely forwarding messages to and from the Internet to `mailserver.alpha.com`. The `mailserver.alpha.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 Alpha 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.bravo.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 MTA 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 MTA 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 MTA capable of resolving all addresses in the `xyx.com` domain.

Net Corp 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 MTA can serve as a proxy MTA. 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 MTA must have the ability to resolve these addresses in order to forward messages to the appropriate subdomains. As the router MTA, it also needs information on any additional configured SMTP router channels.

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.alpha.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 3.5 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, Alpha Corporation and Bravo Corporation. Alpha's e-mail 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 Alpha'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 e-mail 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 e-mail administrator can monitor the volume of e-mail 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 Alpha Corporation is composed of the domain `alpha.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`. e-mail 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. If desired, you can implement the same user ID (`hgreen`) for each of these e-mail users since they exist in separate subdomains. Their e-mail addresses respectively would be `hgreen@eng.bravo.com`, `hgreen@corp.bravo.com`, `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 e-mail addresses

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

Sun also recommends that when e-mail users specify addresses for e-mail 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 e-mail, Sun recommends specifying the following:

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

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

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

Glossary

Administration Services	Administers all components of Sun Internet Mail Server 3.5 through a JMAPI-based GUI. See also <i>JMAPI</i> .
Asymmetric configuration	A configuration that contains a single diskset. In an asymmetric configuration, one server acts as the default master of the diskset and the other server acts as a hot standby.
backbone	The primary connectivity mechanism of a hierarchical 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.
configuration file	A file used to set up or configure a specific part of the system because of the information it contains.
data service	A network service that implements read-write access to disk-based data from clients on a network. NFS is an example of a data service. The data service may be composed of multiple processes that work together.
data store	A store that contains directory information, typically for an entire directory information tree.
Default master	The server that is master of a diskset if both servers are rebooted simultaneously. The default master is specified when the system is initially configured.
directory entry	A set of directory attributes and their values. Each entry contains an object class attribute that specifies the kind of object the entry describes and defines the set of attributes it contains.
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 Sun Internet Mail Server 3.5 that stores user, distribution list, and configuration data.

- distinguished name** The fully qualified name of an object in the directory.
- DIT** Directory information tree. A hierarchical structure in which directory data or information (names, email addresses, and so on) is stored.
- DNS** Domain Name Service. The naming facilities of the Internet.
- domain** In the Internet, a part of a naming hierarchy. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by periods (dots), for example, `tundra.mpk.ca.us`.
- Fault detection** Solstice HA programs that detect two types of failures. The first type includes low-level failures such as system panics and hardware faults (that is, failures that cause the entire server to be inoperable). These failures can be detected quickly. The second type of failures are related to data service, such as SIMS 3.2 HA. These types of failures take longer to detect.
- firewall** Router or mail-level hosts that are equipped with special codes to control access between the Internet and the internal network.
- 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.
- Highly available data service** A data service that appears to remain continuously available, despite single-point failures of server hardware or software components.
- Hot standby** In an asymmetric (single diskset) configuration, the machine that is not the current master of the diskset. If both servers reboot simultaneously, the hot standby will not master the diskset and thus will not be running any Solstice HA data services.
- HTML** Hypertext Markup Language.
- HTTP** Hypertext Transfer Protocol.
- 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.
- Internet** A collection of networks interconnected by a set of routers that allow them to function as a single, large virtual network.
- Java** A programming language developed by Sun Microsystems.

JMAPI	Java Management Application Programming Interface. JMAPI is a collection of programming language classes that enable a diverse set of autonomous applications to be brought together under a common look, feel, and behavior everywhere they run.
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.
LDIF	LDAP Data Interchange Format. A data format used to represent LDAP entries in text form.
Logical host	A diskset and its collection of logical host names and their associated IP addresses. Each logical host is mastered by one physical host at a time.
Logical host name	The name assigned to one of the logical network interfaces. A logical host name is used by clients on the network to refer to the location of data and data services. The logical host name is the name for a path to the logical host. Because a host may be on multiple networks, there may be multiple logical host names for a single logical host.
Logical network interface	In the Internet architecture, a host may have one or more IP addresses. HA configures additional logical network interfaces to establish a mapping between several logical network interfaces and a single physical network interface. This allows a single physical network interface to respond to multiple logical network interfaces. This also enables the IP address to move from one HA server to the other in the event of a takeover or <code>haswitch(1M)</code> , without requiring additional hardware interfaces.
Mailtool	A <code>/var/mail</code> client application that runs under the OpenWindows V3 desktop environment.
MIME	Multipurpose Internet Mail Extensions. A format for defining email message content.
Mirroring	Replicating all writes made to a single logical device (the mirror) to multiple devices (the submirrors), while distributing read operations. This provides data redundancy in the event of a failure.
MTA	Message Transfer Agent.
name resolution	The process of mapping a name into the corresponding address. See also <i>DNS</i> .
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." See also <i>gateway</i> .

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.
smart host	The Internet Message Transfer Agent (IMTA) in a particular domain to which other IMTAs acting as routers forward messages if they do not recognize the recipients.
SMCS	Sun Messaging Connectivity Services. Provides batch-mode connectivity to proprietary message transfer systems such as cc:Mail, MS-Mail or PROFS.
Solstice HA	See Solstice High Availability.
Solstice High Availability	A software package that enables two machines to act as read-write data servers while acting as backups for each other.
Solstice DiskSuite	A software product that provides data reliability through disk striping, concatenation, mirroring, UFS logging, dynamic growth of metadevices and file systems, and metadvice state database replicas.
Sun Internet Mail Client	The client end of the Sun Internet Mail Server 3.5 solution that supports online, offline, and disconnected states.
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.
SPARCcluster High Availability	The combination of Solstice HA software with Sun hardware creating a highly available system.
Takeover	The automatic moving of a logical host from one HA server to the other after a failure has been detected. The HA server that has the failure is forced to give up mastery of the logical host.
/var/mail	The UNIX version 7 "From" delimited mailbox as implemented in the Solaris operating system.
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 <i>backbone</i> .

Index

A

- Add-on options
 - installing, 81
- Asymmetric High Availability
 - description of, 133

B

- Before installing
 - configuration files, 43, 45
 - configuring, 41
 - default configuration files, 44
 - preparing a clean system, 52
 - preparing licenses, 57
 - preparing patches, 54
 - preparing proxy configurations, 61
 - preparing SMCS, 62
 - software requirements, 42

C

- cc-Mail
 - channel for, 64
- Command tool
 - troubleshooting, 130
- Command-line installation, 141
 - commands for, 142
 - example of, 145
- Configuration files
 - configurable by administrator, 43, 45
 - list of, 33, 34, 36, 37

- Message Store, 36
- MTA, 34
- Proxy server, 36
 - set by default, 44
- SMCS, 38
 - summary of, 47
- Sun Directory Services, 37
- Sun Web Access, 39

Configurations

- Admin. Console, 33
- core server, 74
- DNS setup, 125
- High Availability, 134
- HotJava browser, 129
- optional components, 79

Core components

- configuring, 74

Corrupted quota file

- troubleshooting, 131

D

- Departmental edition
 - list of components, 22
 - overview of, 69
- Directory Information Tree
 - example of, 153
 - generating, 152
 - models for, 154
 - replication, 157

Directory services
administration, 155
automatically generating DIT, 152
considerations for, 150
models for, 151

DNS setup
configuring, 126
troubleshooting, 125

E

Enterprise edition
list of components, 22
overview of, 68

F

Fail-over
description of, 138

Firewall
MTA's location relative to, 169

Fully Qualified Domain Name
configuring, 126

H

HA primary machine
installing, 84

HA secondary machine
installing, 88

High Availability
configuring, 134
directory services, 140
fail-over, 138
installing HA primary machine, 84
installing HA secondary machine, 88
linking directories to shared disks, 138
overview of, 22
preparing before installing, 83
removing, 90
using uninstall, 53

HotJava browser
configuring, 105, 129

I

IBM PROFS
channel for, 64

im.server
starting, 118
startup script, 46

IMTA
considerations, 168
overview of, 20

Installation
add-on options, 81
clean system, 52
configuring before, 41
core server configurations, 74
High Availability, 83, 88
optional components, 70
optional components configurations, 79
overview of, 65, 66
post configurations, 99
preparing for, 49
preparing licenses, 57
preparing patches, 54
preparing SMCS, 62
proxy configuration, 61
pure proxy server, 96
Remote Admin. Console, 93
removing SIMS, 144
requirements for, 25
script for, 67
specifying licenses, 71
Sun Web Access, 92
types of, 68
upgrading description, 50
upgrading procedure, 100

Internet Message Transfer Agent
considerations, 168

L

Licenses
determining server configuration, 58
preparing to install, 57
removing extra characters, 130
requesting a password, 57
specifying, 71
updating, licence.dat, 59

Log files
description of, 129
overview of, 118

M

Manual pages
connecting to, 119
Message Store
configuration files, 36, 44, 45
overview of, 21
MS-Mail
channel for, 64
MTA
configuration files, 34, 43, 44, 45
scenarios of, 170

O

OfficeVision/VM
channel for, 64
Optional components
add-on, 81
configuring, 79
selecting, 70

P

Packages
list of, 30
Patches
installing, 56
recommended, 55
required, 54
Planning SIMS
directory services considerations, 150
IMTA considerations, 168
topologies, 158
POP3/IMAP4 proxy
overview of, 21, 23
Post installation
configuring for mail users only, 104
configuring HotJava browser, 105
list of tasks, 117
log files, 118

populating directory, 121
removing sendmail, 106
setting up Sun Web Access, 107
starting Admin. Console, 120
starting Sun Web Access, 121
testing your SIMS server, 123
upgrading procedure, 100

Proxy server
configuration files, 44
preparing to install, 61
Pure proxy
installing, 96
removing sendmail, 106

R

Rebooting
description of, 129
Remote Admin. Console
installing on Solaris, 94
installing on Windows, 93
overview of, 23
Requirements
administrator's tasks, 42
client, 28
disk space, 26
file system, 28
Java Virtual machine, 28
memory, 27
naming services, 28
patches, 54
platform, 26
server and client, 25
SIMS/HA, 42
SMCS, 42
SMCS storage, 27
software, 42
swap space, 27
Rewrite rule
versus new channel, 171

S

sendmail
removing, 106, 130

- Setup script
 - running, 67, 80
 - SIMS
 - command-line installation, 141
 - directory contents, 30
 - files of, 33
 - list of components, 20
 - overview of, 19
 - packages, 29, 30
 - planning, 149
 - troubleshooting, 125
 - SIMS Admin. Console
 - list of configuration files, 33
 - starting, 120
 - SIMS components
 - IMTA, 20
 - list of, 20
 - list of options, 22
 - Message Store, 21
 - overview of, 19
 - POP3/IMAP4, 21
 - SMCS, 23
 - Sun Directory Services, 21
 - Sun Web Access Server, 23
 - SIMS options
 - list of, 22
 - SIMS packages
 - list of, 30
 - SMCS
 - checking directory synchronization, 63
 - configuration files, 38, 43
 - overview of, 23
 - preparing to install, 62
 - requirements, 64
 - setting up mail clients, 63
 - transport protocol, 62
 - Stand-alone options
 - list of, 22
 - overview of, 69
 - Startup script
 - contents of, 46
 - starting, 118
 - Sun Directory Services
 - configuration files, 37, 43, 44, 45
 - overview of, 21
 - Sun Messaging Connectivity Services
 - configuration files, 43
 - overview of, 23
 - Sun Web Access
 - changing LDAP server, 114
 - changing port number, 109
 - configuration files, 39, 43, 44, 45
 - configuring, 108
 - configuring for mail users only, 104
 - establishing secure service, 110
 - extending the palette, 112
 - installing stand-alone, 92
 - invoking, 115
 - licensing, 119
 - overview of, 23
 - restarting, 109
 - setting up, 107
 - starting, 108, 121
 - using an alternate JVM, 112
- T**
- Topologies
 - models of, 159
 - Troubleshooting
 - command tool, 125
 - DNS setup, 125
 - HotJava browser, 125
 - log files, 125
 - quota file, 125
 - rebooting, 125
 - removing sendmail, 125
- U**
- uninstall command, 142
 - High Availability, 53
 - instructions for using, 52
 - options for, 52, 144
 - Upgrading
 - post installation procedure, 100
 - preparing for, 50
 - SIMS 2.0 to SIMS 3.5, 51
 - SIMS 3.1/3.2 to SIMS 3.5, 50
 - User ID
 - considerations, 172

W

Web Access
overview of, 23

