Installation Guide for Solaris™ Operating Systems

Sun™ ONE Messaging Server

Version 6.0

816-6735-10
December 2003

Contents

List of Figures

List of Tables

About This Guide

This guide explains how to install and configure the Sun™ ONE Messaging Server 6.0 and its accompanying software components. Sun ONE Messaging Server provides a powerful and flexible cross-platform solution to meet the email needs of enterprises and messaging hosts of all sizes using open Internet standards.

Topics covered in this chapter include:

Who Should Read This Book

You should read this book if you are responsible for installing and deploying Sun ONE Messaging Server at your site.

NOTE You will not be able to directly migrate any existing mailboxes and message queues from Netscape Messaging Server or Sun Internet Mail Server products to Sun ONE Messaging Server.

Refer to the *Sun™ ONE Messaging Server 5.2 Migration Guide* to migrate from Netscape Messaging Server or Sun Internet Mail Server to Sun ONE Messaging Server 5.2. Then, follow the upgrade instructions in Chapter 4, "Upgrading to Sun ONE Messaging Server," to upgrade from Messaging Server 5.2 to Sun ONE Messaging Server 6.0.

What You Need to Know

This book assumes that you are responsible for installing the Messaging Server software and that you have a general understanding of the following:

- The Internet and the World Wide Web
- Messaging Server protocols
- Sun ONE Administration Server
- Sun ONE Identity Server
- Sun ONE Web Server
- Sun ONE Directory Server and LDAP
- Sun ONE Console
- System Administration and Networking on the following platforms:
  - Solaris 8 for Sparc and x86
  - Solaris 9 for Sparc and x86

How This Book is Organized

This book contains the following chapters and appendixes:

- About This Guide (this chapter)
- Chapter 1, “Planning Your Installation”

  This chapter provides much of the information you will need to know before beginning the installation. Some of the topics covered include system requirements, installation and provisioning options.

- Chapter 2, “Installing Messaging Server”

  In this chapter, you will read how to run the Directory Server Setup script (`comm_dssetup.pl`), the questions that make up the Messaging Server initial runtime configuration, and silent installation setup.

- Chapter 3, “Configuring High Availability Solutions”

  This chapter describes how to install and configure high availability models with Messaging Server. High Availability products discussed in this chapter include: Veritas Cluster Server and Sun Cluster Server. In addition, there are instructions for configuring Sun Cluster HAStoragePlus.

- Chapter 4, “Upgrading to Sun ONE Messaging Server”

  This chapter describes how to upgrade from iPlanet Messaging Server to Sun ONE Messaging Server. Server configuration upgrades, store migrations, and MMP upgrades are described.

- Chapter 5, “Performing Post-Installation Procedures”

  This chapter describes post-installation procedures you should perform after installing Messaging Server

- Appendix A, “Installation Worksheets”

  This appendix contains sample installation worksheets to help you plan and record your installation parameters.

Document Conventions

Monospaced Font

`Monospaced font` is used for any text that appears on the computer screen or text that you should type. It is also used for filenames, distinguished names, functions, and examples.

Bold Monospaced Font

`Bold monospaced font` is used to represent text within a code example that you should type. For example, you might see something like this:

```
./installer
```

In this example, **`./installer`** is what you would type at the command line.

Italicized Font

Italicized font is used to represent text that you enter using information that is unique to your installation (for example, variables). It is used for server paths and names.

For example, throughout this document you will see path references of the form:

msg_svr_base`/...`

The Messaging Server Base (*msg_svr_base*) represents the directory path in which you install the server. The default value of the *msg_svr_base* is `/opt/SUNWmsgsr`.

Italicized font is also used for variables within the synopsis of a command line utility. For example, the synopsis for the `commadmin admin remove` command is:

```
commadmin admin remove -D login -l userid -n domain -w password [-d domain]
      [-h] [-i inputfile] [-p port] [-X host] [-s] [-v]
```

In the above example, the italicized words are arguments for their associated option. For example, in the `-w` *password* option, you would substitute the Administrator's password for *password* when you enter the `commadmin admin remove` command.

Square or Straight Brackets

Square (or straight) brackets `[]` are used to enclose optional parameters. For example, in this document you will see the usage for the `configutil` command described as follows:

`./configutil` *[options] [arguments]*

It is possible to run the `configutil` command by itself or to list some or all of the `configutil` parameters and values:

```
./configutil
```

However, the presence of *[options]* and *[arguments]* indicate that there are additional optional parameters that may be added to the `configutil` command. For example, you could use `configutil` command with the `-p` option to list all parameters with the prefix `service.imap`:

```
./configutil -p service.imap
```

Command Line Prompts

Command line prompts (for example, `%` for a C-Shell, or `$` for a Korn or Bourne shell) are not displayed in the examples. Depending on which operating system you are using, you will see a variety of different command line prompts. However, you should enter the command as it appears in the document unless specifically noted otherwise.

Platform-specific Syntax

Note that the examples in this book use the UNIX C shell. If necessary, make appropriate adjustments to your preferred shell.

All paths specified in this manual are in UNIX format. If you are using a Windows 2000-based Sun ONE Messaging Server, you should assume the Windows 2000 equivalent file paths whenever UNIX file paths are shown in this book.

Where to Find Related Information

In addition to this guide, Sun ONE Messaging Server comes with supplementary information for administrators as well as documentation for end users and developers. Use the following URL to see all the Messaging Server documentation:

http://docs.sun.com/db/prod/s1msgsrv

Listed below are the documents that are available:

- *Sun ONE Messaging Server Installation Guide*
- *Sun ONE Messaging Server Release Notes*
- *Sun ONE Messaging Server Administrator's Guide*
- *Sun ONE Messaging Server Reference Manual*
- *Sun ONE Messaging and Collaboration Schema Reference Manual*
- *Sun ONE Messaging Server Provisioning Guide*
- *Sun ONE Messaging and Collaboration Event Notification Service Manual*
- *Sun ONE Messaging Server Messenger Express Customization Guide*
- *Sun ONE Messaging Server MTA SDK Programmer's Reference Manual*

The Sun ONE Messaging Server product suite contains other products such as Sun ONE Console, Directory Server, and Administration Server. Documentation for these and other products can be found at the following URL:

http://docs.sun.com/db/prod/sunone

Also, see the Sun ONE Messaging Server Software Forum for technical help on specific Messaging Server product questions. The forum can be found at the following URL:

http://swforum.sun.com/jive/forum.jsp?forum=15

Where to Find This Book Online

You can find the *Sun ONE Messaging Server 6.0 Installation Guide* online in PDF and HTML formats. This book can be found at the following URL:

http://docs.sun.com/db/prod/s1msgsrv

Chapter 1

Planning Your Installation

This chapter presents an overview for planning your Sun ONE Messaging Server 6.0 installation and configuration. The following topics are covered:

Installation Overview

To install Sun™ ONE Messaging Server 6.0, you will use the Sun Java™ Enterprise System installer. The installer provides a consistent installation interface, common components, and common procedures across the entire Java Enterprise System product set. In addition to Messaging Server, you can also install Sun™ ONE Web Server, Sun™ ONE Directory Server, Sun™ ONE Portal Server, Sun™ ONE Calendar Server, and so on. For more information on the Java Enterprise System installer, review the *Java Enterprise System Installation Guide.*

In addition to the Java Enterprise System installer, the Messaging Server product and documentation provides procedures and tools for completing and upgrading your installation, for configuring your servers, and so on. For more information on these additional installation and configuration steps, read this guide prior to using the Java Enterprise System installer.

Before you install Messaging Server through the Java Enterprise System installer, you should verify that the systems on which you plan to install the software meet the minimum product requirements. In addition, you should have a general understanding of Messaging Server components and the directory schema used by them. It is also a good idea to plan how you want to configure the software components before you begin the installation process.

NOTE Prior to installing Messaging Server, you will need to install Directory Server and Web Server, and optionally Identity Server. The *Java Enterprise System Installation Guide* will describe the installation order in further detail. You should also refer the instructions in the *Sun ONE Directory Server 5.2 Installation Guide* and the *Sun ONE Web Server 6.1 Installation and Migration Guide* for additional installation information.

System Requirements

This section describes the following system requirements and recommendations for Messaging Server:

- Hardware
- Software
- File System
- Physical Memory

- Disk Capacity
- CPU Resources

NOTE Check the *Sun ONE Messaging Server Release Notes* for the latest system requirement updates.

Hardware

The minimum hardware requirements for Messaging Server are:

- Approximately 500 MB of disk space for a standard installation. For production systems, you should plan at least 1 GB to support the product binaries, data, and configuration files.
- 128 MB of RAM. For production systems, you should have a minimum of 256 MB of RAM; be sure to allocate this accordingly, depending on the size of your site and number of users.
- Adequate space for your user mailboxes (message store), database, configuration directory, log files. and message queue directory. These can grow in size dramatically depending on the size of your site, so be sure to allocate space accordingly.

Software

Messaging Server is supported on Sparc and x86 for Solaris 8, and Solaris 9 operating systems.

Read the *Sun ONE Messaging Server 6.0 Release Notes* for required Solaris operating system patches.

A high quality caching DNS server on the local network is a requirement for a production deployment of Messaging Server.

Additionally, ensure in your Solaris setup that DNS is properly configured and that it is clearly specified how to route to hosts that are not on the local subnet:

- The `/etc/defaultrouter` should contain the IP address of the gateway system. This address must be on a local subnet.
- The `/etc/resolv.conf` exists and contains the proper entries for reachable DNS servers and domain suffixes.

- In `/etc/nsswitch.conf`, the `hosts:` line has the `files`, `dns` and `nis` keywords added. The keyword `files` must precede `dns` and `nis`.
- Make sure that the FQDN is the first host name in the `/etc/hosts` file.

  If your Internet host table in your `/etc/hosts` file looks like:

```
123.456.78.910 budgie.west.sesta.com
123.456.78.910 budgie loghost mailhost
```

  change it so that there is only one line for the IP address of the host. Be sure the first host name is a fully qualified domain name. For example:

```
123.456.78.910 budgie.west.sun.com budgie loghost mailhost
```

For Messenger Express access, a JavaScript-enabled browser is required. For optimal performance, Sun ONE recommends using the following browser and platform combinations listed in Table 1-1:

Table 1-1 Messaging Server 6.0 Client Software Recommendations

Browsers	Solaris 8/9 for Sparc and x86	Windows 98	Windows 2000	Windows XP	Red Hat Linux 7.2
Netscape™ Communicator	7	7	7	7	7
Internet Explorer	N/A	5.5, 6.0	5.5, 6.0	6.0	N/A
Mozilla™	1.2	1.2	1.2	1.2	1.2

File System

Messaging Server supports the following file systems:

- **NFS (Network File System).** Though NFS is not supported on machines with message stores, you can use this file system on MTA relay machines, particularly if LMTP is enabled, or for autoreply histories and message defragmentation. (See the *Sun ONE Messaging Server Administrator's Guide* for more information on autoreply). In addition, NFS can be supported on BSD-style mailboxes (`/var/mail/`).

- **LUFS (Logging UFS).**
- **VxFS (Veritas File System).** Veritas File System provides good system performance if configured properly. If you use VxVM, the Veritas Volume Manager, you need to carefully watch that the volumes and the log file for the volumes are set to be regularly striped.
- **Sun Cluster Global File System.**

Physical Memory

Make sure you have an adequate amount of physical memory on each machine in your deployment. Additional physical memory improves performance and enables the server to operate at peak volume. With sufficient memory, Messaging Server can operate efficiently without excessive swapping.

At minimum, be sure to have 1G of memory per CPU.

Disk Capacity

When planning server system disk space, you need to be sure to include space for operating environment software, Messaging Server software, and databases. Be sure to use a robust external disk array, since Messaging Server is typically disk bound.

In addition, user disk space needs to be allocated. This space is usually determined by your site's policy.

CPU Resources

Enable enough CPU for your Message Stores, MTAs, and on systems that are just running multiplexing services (MMP and Messenger Express Multiplexor). In addition, enable enough CPU for any RAID systems that you plan to use.

Understanding Your Messaging Server Provisioning Options

This section outlines your provisioning options with Messaging Server 6.0. Because of the complexity in provisioning Messaging Server 6.0, spend time understanding your options before installing the product.

The following topics are described:

- Messaging Schema Choices
- Messaging Server Provisioning Tools

Messaging Schema Choices

This section describes two schema options that are available and supported with Messaging Server 6.0. This section outlines the following topics:

- Deciding Which Schema to Use
- Sun ONE LDAP Schema, v.1
- Sun ONE LDAP Schema, v.2 (Native Mode)

NOTE In future Messaging Server releases, migration tools and procedures will be available for you to migrate from Sun ONE LDAP Schema, v.1 to Sun ONE LDAP Schema, v.2. In addition, a graphical user interface will be provided for use with Sun ONE LDAP Schema, v.2.

Support for installation and provisioning of Sun ONE LDAP Schema, v.1 will be deprecated and removed from future releases. However, customers with their own provisioning tools may continue to use Sun ONE LDAP Schema, v.1.

Deciding Which Schema to Use

Choosing the schema that's right for your installation depends on your provisioning needs:

- Are you integrating your messaging server with other Java Enterprise System products such as Sun ONE Portal Server?

  If you answer Yes, then you must use Sun ONE LDAP Schema, v.2.

- Are you installing Messaging Server for the first time or are you upgrading from an older version?

  If you are installing Messaging Server for the first time, use Sun ONE LDAP Schema, v.2.

  If you are upgrading from an older version of Messaging Server, you can either use Sun ONE LDAP Schema, v.1 or Sun ONE LDAP Schema, v.2.

- Do you plan to use an interface for your provisioning needs? If so, will it be a graphical interface or a command-line interface?

  If you need to use a graphical user interface or if you need your end users to be able to make modifications to their profiles through a graphical user interface, you should use Sun ONE LDAP Schema, v.1. Note that this option is not available for new installations of Messaging Server. It is only available for existing Messaging Server 5.x installations where Messaging Server 6.0 is now being installed.

  If you are planning on using a command-line interface, you can use Sun ONE LDAP Schema, v.1 (for existing Messaging Server installations) or Sun ONE LDAP Schema, v.2 (for new or for existing Messaging Server installations).

  You can also use your own graphical or command-line interfaces with either schema should you decide not to use the provisioning interfaces that accompany Messaging Server.

Sun ONE LDAP Schema, v.1

Sun ONE LDAP Schema, v.1 is a provisioning schema that consists of both an Organization Tree and a DC Tree. This set of schema was supported in previous Messaging Server 5.x versions (which at the time was simply called “schema”).

When Messaging Server searches for user or group entries, it looks at the user ‘s or group’s domain node in the DC Tree and extracts the value of the `inetDomainBaseDN` attribute. This attribute holds a DN reference to the organization subtree containing the actual user or group entry.

Only users who have installed previous versions of Messaging Server should use Sun ONE LDAP Schema, v.1.

Note that migrating to Sun ONE LDAP Schema, v.2 will be imperative if you plan to install Messaging Server with other Sun ONE products in future releases.

Supported Provisioning Tools: Sun ONE Delegated Administrator for Messaging Graphical User and Command-line Interfaces and LDAP Provisioning Tools for Sun ONE LDAP, Schema v.1. For more information, see Messaging Server Provisioning Tools.

Sun ONE LDAP Schema, v.2 (Native Mode)

Sun ONE LDAP Schema, v.2 is a newly defined set of provisioning definitions that describe the types of information that can be stored as entries using the Directory LDAP.

The native mode uses search templates to search the LDAP directory server; once the domain is found by using the domain search template, the user or group search templates are used to find a specific user or group.

You should use this mode if you are installing Messaging Server for the first time and you don't have other applications on your machine that are dependent on a two tree provisioning model. You should also use this mode if you want to install other products in the Java Enterprise System product suite.

Note that Sun ONE LDAP Schema, v.2 Native Mode is the recommended provisioning model for all Sun ONE products in the Java Enterprise System product suite.

Supported Provisioning Tools: Sun ONE Communication Server Command-line Interface and LDAP Provisioning Tools for Sun ONE LDAP Schema, v.2. For more information, see Messaging Server Provisioning Tools.

Messaging Server Provisioning Tools

Through supported Messaging Server provisioning tools, administrators can query, modify, add, or delete user, group, and domain entry information in their LDAP directory. This section examines these Messaging Server provisioning tools.

In addition to the questions asked in Deciding Which Schema to Use, you should use Table 1-2 to evaluate your schema and provisioning tool options.

NOTE Prior to installing and configuring Messaging Server, you will need to decide upon a schema model and tool or tools for provisioning your Messaging Server entries.

The following sections provide high-level information about the supported provisioning tools:

- Sun ONE Delegated Administrator for Messaging
- LDAP Provisioning Tools
- Sun ONE Communication Server Command-line Utilities
- Comparing Your Provisioning Tool Options

Sun ONE Delegated Administrator for Messaging

Sun ONE Delegated Administrator for Messaging provides both a command-line and a graphical user interface to provision users and groups. Delegated Administrator uses Sun ONE LDAP Schema, v.1, which is the Messaging Server 5.x version of provisioning definitions, that describe the types of information that can be stored as entries in the LDAP Directory Server.

To install Delegated Administrator, you need to download it from the Sun Software page. Contact your Sun ONE representative for information on the download location information.

NOTE Delegated Administrator can only be installed after Messaging Server and Web Server are installed and configured. For more information on installing Delegated Administrator, see the Sun ONE Delegated Administrator documentation.

Delegated Administrator is only available for those customers with existing Messaging Server 5.x installations and who are currently installing Messaging Server 6.0. It is not available to those customers new to the Messaging Server product.

Delegated Administrator must be used with Sun ONE Web Server 6.0 (which is only bundled with the previous Messaging Server 5.2 product). You cannot use Web Server 6.1 (bundled with the Java Enterprise System installer) with Delegated Administrator.

Be sure to read the product limitations in Table 1-2 as well as in the *Sun ONE Messaging Server 6.0 Release Notes*.

Summary of Installation Steps: To install and configure Sun ONE Delegated Administrator for Messaging with Messaging Server 6.0:

NOTE When you install the following products, use the Java Enterprise System installer. Note that some of these products have their own configuration whereas other products' configurators are embedded in the Java Enterprise System installer/configurator. For more information, refer to specific product documentation.

---

1. Be sure that either Sun ONE Directory Server 5.1 or 5.2 is installed and configured.

   For more information, read the *Sun ONE Directory Server Installation Guide.*

2. Install and configure Messaging Server 6.0 with help from this guide.

   Messaging Server will detect that you are using Sun ONE LDAP Schema, v.1 since Sun ONE Identity Server will not be installed.

3. Install Sun ONE Web Server 6.0 from your previous Messaging Server 5.2 bundle.

   Review the Sun ONE Web Server documentation and the Sun ONE Delegated Administrator documentation.

4. Install Sun ONE Delegated Administrator for Messaging 1.2 Patch 2. Contact your Sun support representative to obtain the latest version.

   Refer to the Sun ONE Delegated Administrator documentation.

LDAP Provisioning Tools

You can also provision users and groups through the Directory LDAP. Unlike Sun ONE provisioning graphical and command-line interfaces, you can directly provision users and groups by adding, removing, and modifying the LDIF records through the LDAP without having to use a user interface.

Summary of Installation Steps:

1. If you plan to use Sun ONE LDAP Schema, v.2, install and configure Identity Server. If you plan to use Sun ONE LDAP Schema, v.1, you can skip to Step 2.

   If you install Identity Server, Messaging Server will identify Sun ONE LDAP Schema, v.2 as your schema model. Even though you cannot use the Identity Server GUI to provision your Messaging Server user, group, and domain entries, you need to install Identity Server in order to add the new ACIs and search templates to your organization tree. For more information on installing Identity Server, refer to the *Sun ONE Identity Server 6.1 Installation Guide* and the *Sun ONE Messaging Server 6.0 Provisioning Guide*.

   If you don't install Identity Server, Messaging Server will assume you are using Sun ONE LDAP Schema, v.1.

2. If Directory Server is not already installed, be sure to install and configure it.

   For more information, refer to the *Sun ONE Directory Server Installation Guide.*

3. Configure Identity Server to recognize data in your Directory Server.

   Before Identity Server can recognize the data in your LDAP directory, you must add special object classes to entries for all organizations, groups and users that will be managed by Identity Server. If you have not done this already, do it before you start provisioning new accounts. Sample scripts are bundled in the Identity Server product to help you automatically add these object classes to your directory. For more information on these post-installation steps, see the *Sun ONE Identity Server 6.1 Installation and Migration Guide*.

4. Install and configure Messaging Server 6.0 with help from this guide.

   Messaging Server will detect which Sun ONE LDAP Schema you are using, depending on whether or not Identity Server is installed.

5. Install and configure Sun ONE Web Server 6.1 to enable mail filtering in Messenger Express. For more information on enabling mail filtering, see Configuring Messenger Express Mail Filters. To install Web Server, refer to the *Sun ONE Web Server 6.1 Installation Guide*.

   Though mail filtering is not a provisioning tool, its functionality existed in the previous GUI version of Delegated Administrator for Messaging.

6. Refer to the Sun ONE Messaging Server documentation to perform LDAP provisioning.

   For Sun ONE LDAP Schema, v.2 LDAP provisioning, use the *Sun ONE Messaging Server 6.0 Provisioning Guide* with the *Sun ONE Messaging Server 6.0 Schema Reference Manual*.

   For Sun ONE LDAP Schema, v.1 LDAP provisioning, use the *Messaging Server 5.2 Provisioning Guide* and *Sun ONE Messaging Server 6.0 Schema Reference Manual* (The 6.0 Schema Reference manual contains object classes and attributes for both Sun ONE LDAP Schema, v.1 and v.2).

Sun ONE Communication Server Command-line Utilities

The Sun ONE Identity Server uses Sun ONE LDAP Schema, v.2, the newly defined set of provisioning definitions that describe the types of information that can be stored as entries using the Directory LDAP.

Since the Sun ONE server products in the Java Enterprise System product suite use Sun ONE LDAP Schema, v.2, it is recommended that you use the Sun ONE Communication Server command-line utilities, particularly if you are using more than one Java Enterprise System product or if you are performing a brand new installation of Messaging Server.

NOTE Even though you install Identity Server, there is no graphical user interface compatibility with Messaging Server. Therefore, in order to provision users and groups with an interface, you can only use the user management utility.

Summary of Installation Steps:

1. Install and configure Identity Server.

   Even though you cannot use the Identity Server GUI to provision your Messaging Server user, group, and domain entries, you need to install Identity Server in order to add the new ACIs and search templates to your organization tree. For more information, refer to the *Sun ONE Identity Server Installation Guide* and the *Sun ONE Messaging Server 6.0 Provisioning Guide*.

2. If Directory Server is not already installed, be sure to install and configure it.

   For more information, refer to the *Sun ONE Directory Server Installation Guide*.

3. Configure Identity Server to recognize data in your Directory Server.

   Before Identity Server can recognize the data in your LDAP directory, you must add special object classes to entries for all organizations, groups and users that will be managed by Identity Server. If you have not done this already, do it before you start provisioning new accounts. Sample scripts are bundled in the Identity Server product to help you automatically add these object classes to your directory. For more information on these post-installation steps, see the *Sun ONE Identity Server 6.1 Installation and Migration Guide*.

4. Install and configure Messaging Server 6.0 with help from this guide.

   Messaging Server will detect that you are using Sun ONE LDAP Schema, v.2 because Sun ONE Identity Server is installed.

5. Install and configure Sun ONE Web Server 6.1 to enable mail filtering in Messenger Express. For more information on enabling mail filtering, see Configuring Messenger Express Mail Filters. To install Web Server, refer to the *Sun ONE Web Server 6.1 Installation Guide*.

   Though mail filtering is not a provisioning tool, it is functionality that existed in the previous GUI version of Delegated Administrator for Messaging.

6. Install and configure the User Management Utility for Sun ONE Messaging and Calendar Servers.

   Read the *Sun ONE User Management Utility for Sun ONE Messaging and Calendar Servers Configuration and Reference Manual.*

Comparing Your Provisioning Tool Options

Table 1-2 shows the various supported schema, provisioning tools, provisioning limitations, and recommended documentation for additional information.

Table 1-2 Messaging Server Provisioning Mechanisms

Supported Provisioning Tool	Provisioning Tool Functionality	Provisioning Tool Limitations	For Further Information
Sun ONE Delegated Administrator for Messaging Graphical User Interface Uses: Sun ONE LDAP Schema, v.1	Provides a graphical user interface for administrators to manage users, groups, domains, and mailing lists. End users can manage vacation messages and sieve filters.	• Only available to existing Messaging Server 5.x customers who are now upgrading to Messaging Server 6.0. • Can only be used with Sun ONE Web Server 6.0 (which is only available with the Messaging Server 5.2 bundle). It cannot be used with Sun ONE Web Server 6.1. • Incompatible with Sun ONE Schema, v.2 and with other Java Enterprise System products. • Unable to use mail filters through Sun ONE Messenger Express. Must use filters through Delegated Administrator. • Must use auto reply channel which is only available in Messaging Server 5.2 product.	Read the Sun ONE Delegated Administrator for Messaging 1.3 documentation. Describes how to install and administer the Sun ONE Delegated Administrator interface.

Table 1-2 Messaging Server Provisioning Mechanisms *(Continued)*

Supported Provisioning Tool	Provisioning Tool Functionality	Provisioning Tool Limitations	For Further Information
Sun ONE Delegated Administrator for Messaging Command-line Interface Uses: Sun ONE LDAP Schema, v.1	Provides a command-line interface for administrators to manage users, groups, domains, and mailing lists.	• Incompatible with Sun ONE Schema, v.2 and with other Java Enterprise System products.	Read the Sun ONE Delegated Administrator for Messaging 1.3 documentation. Provides syntax and usage for Sun ONE Delegated Administrator command-line utilities.
LDAP Provisioning Tools Uses: Sun ONE LDAP Schema, v.1	Provides tools to directly modify LDAP entries or for creating custom provisioning tools.	• Incompatible with Sun ONE Schema, v.2 and with other Java Enterprise System products.	Read the *Sun ONE Messaging Server 5.2 Provisioning Guide* and *Sun ONE Messaging and Collaboration 6.0 Schema Reference Manual*. Describes the Sun ONE LDAP Schema, v.1 provisioning model. In addition, these guides explain how to use LDAP provisioning tools and the usage of specific attributes and object classes.
Sun ONE Console Uses: Sun ONE LDAP Schema, v.1	Though provisioning functionality is included in the Sun ONE Console, it is not recommended for provisioning Messaging users and groups. Instead, use Sun ONE Console to administer server configuration such as quotas, log files, and other related Message Store items.	• Incompatible with Sun ONE Schema, v.2 and with other Java Enterprise System products. • Not recommended as a provisioning tool in that the Console is unable to properly add and modify users and groups.	Read the *Sun ONE Messaging Server 6.0 Administrator's Guide* and corresponding Sun ONE Console Online Help.

Table 1-2 Messaging Server Provisioning Mechanisms *(Continued)*

Supported Provisioning Tool	Provisioning Tool Functionality	Provisioning Tool Limitations	For Further Information
Sun ONE Communication Server Command-line Interface Uses: Sun ONE LDAP Schema, v.2	Provides a command-line interface for administrators to manage users, groups, domains, and mailing lists. Compatible with other Java Enterprise System products.	• Not backwards compatible with Sun ONE Schema, v.1. • No GUI provisioning tool to use with Sun ONE Identity Server • Sun ONE Identity Server must be installed in order to enable this command-line interface.	Read the *Sun ONE Communications Server 6.0 Provisioning Tools Configuration and Reference Manual*. Provides syntax and usage for the command-line utility.
LDAP Provisioning Tools Uses: Sun ONE LDAP Schema, v.2	Provides tools to directly modify LDAP entries or for creating custom provisioning tools. Compatible with other Java Enterprise System products.	• Not backwards compatible with Sun ONE Schema, v.1.	Read the *Sun ONE Messaging Server 6.0 Provisioning Guide* and *Sun ONE Messaging and Collaboration 6.0 Schema Reference Manual*. Describes the Sun ONE LDAP Schema, v.2 provisioning model. In addition, these guides explain how to use LDAP provisioning tools and the usage of specific attributes and object classes.

Pre-Installation Procedures

This section describes recommended procedures you should do prior to installing Messaging Server:

- Disabling the sendmail daemon
- Installation Considerations
- Installation Worksheets

Disabling the sendmail daemon

Prior to installing Messaging Server, you should disable the `sendmail` daemon if it is running. To disable, follow these steps:

1. Go to your `/etc/init.d` directory.

```
cd /etc/init.d
```

2. Stop the `sendmail` daemon if it is running.

```
./sendmail stop
```

3. Modify `/etc/default/sendmail` by adding `MODE=""`.

   If the `sendmail` file does not exist, create the file and then add `MODE=""`.

   If a user accidentally runs `sendmail start` or if a patch restarts `sendmail`, then adding this modification will prevent `sendmail` from starting up in daemon mode.

Installation Considerations

This section describes installation considerations to help you prepare for Messaging Server installation.

- **Resource Contention.** To avoid resource contention between the servers, it is recommended that you install the Directory Server on a different machine than where you install Messaging Server.
- **Installation Privileges.** You must install Messaging Server logged in as superuser.
- **Messaging Server Base Directory.** The Messaging Server is installed into a directory referred to as *msg_svr_base* (for example, `/opt/SUNWmsgsr`). This directory provides a known file location structure (file directory path).

Installation Worksheets

While installing Messaging Server, use the installation worksheets in Appendix A, "Installation Worksheets" to record and assist you with the installation process. Note that you can reuse these installation worksheets for multiple installations of Messaging Server, uninstallation, or for Messaging Server upgrades.

TIP It is recommended that you record all of the port numbers you specify during the installation, along with the specific component using that port number.

Chapter 2

Installing Messaging Server

This chapter will describe how to install Sun ONE Messaging Server. It will describe each of the installation screens. Topics covered include:

- Overview of the Installation Process
- Create UNIX System Users and Groups
- Run the Java Enterprise System Installer
- Prepare Directory Server for Messaging Server Configuration
- Create the Initial Messaging Server Runtime Configuration
- Perform Silent Installation
- Install Messaging Server against a Directory Server Replica

To upgrade from Sun ONE Messaging Server 5.2 to Sun ONE Messaging Server 6.0, see Chapter 4, “Upgrading to Sun ONE Messaging Server.”

Overview of the Installation Process

This chapter describes each of the following steps in the installation process.

1. Create UNIX System Users and Groups, with appropriate permissions.
2. Run the Java Enterprise System Installer.
3. Prepare Directory Server for Messaging Server Configuration.
4. Create the Initial Messaging Server Runtime Configuration.

The following optional procedures are also described in this chapter:

- Perform Silent Installation.
- Install Messaging Server against a Directory Server Replica.

NOTE If you are upgrading from a previous version of Messaging Server 5.x, read Chapter 4, "Upgrading to Sun ONE Messaging Server" prior to performing any upgrades or installations.

Create UNIX System Users and Groups

System users run specific server processes. Certain privileges need to be designated for these users to ensure they have appropriate permissions for the processes they are running.

It is recommended that you set up a system user account and group for all Sun ONE servers. You should then set permissions appropriately for the directories and files owned by that user. To do so, follow these steps:

1. Log in as superuser.
2. Create a group to which your system users will belong. In the following example, the `mailsrv` group is created:

```
# groupadd mailsrv
```

3. Create the system user and associate it with the group you just created. In addition, set the password for that user. In the following example, the user `mail` is created and associated with the `mailsrv` group:

```
# useradd -g mailsrv mail
```

   For more information on the `useradd` and `usermod` commands, refer to your UNIX man pages.

4. You might also need to check the `/etc/groups` file to be sure that the user has been added to the system group that you created.

NOTE Should you decide not to set up UNIX system users and groups prior to installing Messaging Server, you will be able to specify them when you the Create the Initial Messaging Server Runtime Configuration.

Run the Java Enterprise System Installer

The Java Enterprise System installation program installs a series of products, shared components, and libraries that cohabit and interoperate with one another. To successfully install and configure Sun ONE Messaging Server, you need to install the following products through the Java Enterprise System installer:

1. Sun ONE Web Server (optional)

   You only need to install Web Server if you are enabling Mail Filtering through Messenger Express — See Configuring Messenger Express Mail Filters.

2. Sun ONE Directory Server

3. Sun ONE Identity Server (optional)

   You only need to install Identity Server if you are enabling Sun ONE LDAP Schema v.2 ¦— See Messaging Schema Choices.

   If you install Identity Server, you do not need to install Directory Server, Administration Server, or Web Server separately. Your Identity Server installation will prompt you to install Directory Server, Administration Server and Web Server.

4. Sun ONE Administration Server
5. Sun ONE Messaging Server

The Java Enterprise System installation program installs the necessary Solaris packages for these products which you will later configure to suit your needs. In other words, the Java Enterprise System installer simply installs (but does not configure) the component product bits that you specify on your machines.

Sun ONE Web Server

If you want to enable mail filtering through the HTTP Messenger Express client, you need to install and configure Web Server 6.1 through the Java Enterprise System installer. For instructions, see the *Sun ONE Web Server 6.1 Installation Guide*. For information on Messenger Express mail filtering, see Configuring Messenger Express Mail Filters and the Messenger Express Online Help.

If you are an existing Messaging Server customer and you want to use Delegated Administrator for Messaging, you need to use Sun ONE Web Server 6.0 SP2 (Service Pack 2), which is only available with the Messaging Server 5.2 product. If you enable mail filters through Delegated Administrator, you cannot enable them through the Messaging Server 6.0 Messenger Express client (and vice versa).

Sun ONE Directory Server

Prior to installing Messaging Server, Sun ONE Directory Server should already be installed and configured. For instructions on installing Directory Server, see the *Sun ONE Directory Server Installation Guide*.

NOTE If you are using the Solaris 9 operating system, you can use the directory server that is bundled in operating system.

Sun ONE Messaging Server can be configured with the following versions of Sun ONE Directory Server:

- Sun ONE Directory Server 5.1 SP1 (Service Pack 1)
- Sun ONE Directory Server 5.1 SP2 (Service Pack 2)
- Sun ONE Directory Server 5.2

You will be able to install Directory Server 5.2 through the Java Enterprise System installer, however, if Directory Server 5.1 SP*x* is already installed and configured, you may continue to use it with Messaging Server.

Use Appendix A, "Installation Worksheets" to record your Directory installation and configuration parameters. You will need these parameters when you install the Administration and Messaging servers.

Sun ONE Identity Server

If you are using Sun ONE LDAP Schema, v.2 to provision your users and groups, you need to install Sun ONE Identity Server before installing Messaging Server.

To do so, be sure to install Identity Server 6.1 through the Java Enterprise System installer. Previous versions of Identity Server are incompatible with Messaging Server.

Note that Identity Server will also automatically install the User Management Utility, the command-line interface for provisioning users and groups with Sun ONE LDAP Schema, v.2. For more information on the User Management Utility, read the *Sun ONE Communications Server 6.0 Provisioning Tools Configuration and Reference Manual.*

If you are an existing customer who wishes to stay with Sun ONE LDAP Schema, v.1 (which is the version of schema included with Messaging Server 5.2), you do not need to install Identity Server.

Additional information on available Messaging Server provisioning tools and schema models is discussed in Understanding Your Messaging Server Provisioning Options in Chapter 1, "Planning Your Installation."

Sun ONE Administration Server

The Administration Server manages operation requests from the Sun ONE Console to all servers installed on a single machine. For example, you can use the Console to start and stop services. The Console sends the request to the appropriate Administration Server. The Administration Server then invokes the programs that actually start or stop Messaging services.

On any machine where you install a Messaging Server, you must also install an Administration Server. There is a single administration server per machine. You use this administration server to manage all the servers installed on that machine.

To install the Administration Server, use the Java Enterprise System installer. Previous versions of Administration Server are incompatible with Messaging Server.

Once the Administration Server is installed, use the Java Enterprise System installer to run the Administration Server initial runtime configuration program. Unlike Messaging Server's configuration program, the Administration Server runtime configuration is built into the Java Enterprise System installer.

Use Appendix A, "Installation Worksheets" to record your Administration Server configuration parameters. You will need these parameters when you install the Messaging server.

Sun ONE Messaging Server

To install Messaging Server through the Java Enterprise System installer, you should use this guide alongside the *Java Enterprise System Installation Guide* in order to properly set up, configure, and perform post-installation tasks.

Table 2-1 lists the specific Messaging Server packages that you will install with the Java Enterprise System installer; some of these packages are shared amongst other products:

Table 2-1 Java Enterprise System Messaging Server Packages

Messaging Server Packages	Description
SUNWmsgwm	Sun ONE Messaging Server Messenger Express
SUNWmsgmp	Sun ONE Messaging Server MMP
SUNWmsgst	Sun ONE Messaging Server Message Store
SUNWmsgmt	Sun ONE Messaging Server MTA
SUNWmsglb	Sun ONE Messaging Server Shared Components
SUNWmsgen	Sun ONE Messaging Server English Localization
SUNWmsgco	Sun ONE Messaging Server Core Libraries
SUNWmsgin	Sun ONE Messaging Server Installation Utilities
SUNWmsgmf	Sun ONE Messaging Server Sieve Filter User Interface

Uninstalling Messaging Server

To uninstall Messaging Server or to uninstall any other products that were installed through the Java Enterprise System installer, use the Java Enterprise System `uninstaller` program. For more information, refer to the *Java Enterprise System Installation Guide.*

Prepare Directory Server for Messaging Server Configuration

This section provides instructions on how to run the Directory Server Setup script (`comm_dssetup.pl`) that configures your LDAP Directory Server to work with your Messaging Server, Calendar Server, or User Management (see Sun ONE Communication Server Command-line Utilities) Utility configurations. The `comm_dssetup.pl` script prepares the Directory Server by setting up new schema, index, and configuration data in your Directory Server.

When the `comm_dssetup.pl` script runs, it automatically detects if you have installed and configured Identity Server and consequently, it will set up Sun ONE LDAP Schema, v.1 or v.2 for your system. For more information on supported schema and provisioning tools, review Understanding Your Messaging Server Provisioning Options.

The following topics are explained:

- comm_dssetup.pl Requirements
- Running the comm_dssetup.pl Script

comm_dssetup.pl Requirements

Before you run the `comm_dssetup.pl` script, be sure to read the following requirements:

- Prior to running the `comm_dssetup.pl` script, your directory server must be installed and configured.
- Run the `comm_dssetup.pl` script as superuser.
- Run `comm_dssetup.pl` prior to running the Messaging Server, Calendar Server, or User Management Utility Initial Runtime Configuration programs.

    - If you run `comm_dssetup.pl` on a directory server for one product (for example, Calendar Server), you don't need to run it again for another product (like Messaging Server), as long as both products are using the same directory server.

- The `comm_dssetup.pl` script must be run on your directory server machine.
- Be sure that your directory server is running prior to running `comm_dssetup.pl`.
- Whenever you install a new version of Messaging Server, you will need to run the new version of `comm_dssetup.pl` on your Directory Server machine. New schema and new indexes may be added to each Messaging Server distribution.
- If the configuration data and user and group data are split into separate directory instances, you will need to run the `comm_dssetup` script on both instances.
- Use the version of Perl that ships with Directory Server to avoid versioning problems: `/var/mps/serverroot/bin/slapd/admin/bin/perl`.
- If you are running `comm_dssetup.pl` on a remote directory server:
    - Copy the `dssetup.zip` file from the *msg_svr_base*`/install` directory to the remote directory server. You may want to copy it to a directory like `/tmp` or `/var/tmp`.
    - Unzip the `dssetup.zip` file (which contains the `comm_dssetup.pl` and required schema).
    - Run the `comm_dssetup.pl` script on the remote directory server.
- If you are running a replicated directory server, you need to make sure you run the `comm_dssetup.pl` script against the master and replica directories. For more information on installing Messaging server against a Directory server, see Install Messaging Server against a Directory Server Replica.

Running the comm_dssetup.pl Script

The `comm_dssetup.pl` script is located in your `msg60/.install/Tools/dssetup` directory.

You can either run `comm_dssetup.pl` in:

- Silent Mode
- Interactive Mode

Use Appendix A, "Installation Worksheets" to record your answers.

Silent Mode

To enable the silent mode, specify all the arguments at one time:

Syntax

```
# perl comm_dssetup.pl -i yes|no -c Directory_Server_Root -d
Directory_instance -r DC_tree -u User_Group_suffix -s yes|no -D
"DirectoryManagerDN" -w password -b yes|no -t 1|1.5|2 -m yes|no [-S
path-to-schema-files]
```

Options

The options for this command are:

Option	Description
`-i yes|no`	Answers the following question: “Do you want to configure new indexes?” Specify `yes` to configure new indexes. Specify `no` if you don’t want to configure new indexes.
`-c` *Directory_Server_Root*	Directory Server Root path name.For example: `/var/mps/serverroot`
`-d` *Directory_instance*	Directory Server instance subdirectory. For example: `slapd-budgie`
`-r` *DC_tree*	DC tree suffix. For example: `o=internet`
`-u` *User_Group_suffix*	User / Group suffix e.g. `o=usergroup`
-s yes | no	Answers the following question: “Do you want to update the schema?” Specify `yes` to update the schema files (Note: you must have configuration directory with schema files). Specify `no` if you don’t want to update the schema files.
`-D` *DirectoryManagerDN*	Directory Manager DN. For example, `"cn=Directory Manager"`
`-w` *password*	Directory Manager password
-b yes | no	Answers the following question: “Will this directory server be used for users and groups?” Specify `yes` if the directory server will be used for configuration and user / groups. Specify `no` if this directory will be only used for configuration data.

Option	Description
`-t 1|1.5|2`	Determines the schema version that you want to use for your Messaging Server: • Choose `1` for Sun ONE LDAP Schema, v.1. • Choose `1.5` for Sun ONE LDAP Schema, v.2 (Compatibility Mode). See the *Sun ONE Messaging Server 6.0 Provisioning Guide for more information.* • Choose `2` for Sun ONE LDAP Schema, v.2 (Native Mode).
`-m yes|no`	Answers the following question: "Do you want to modify the directory server?" Specify `yes` to modify the directory. Specify `no` if you don't want to modify the directory.
`-S` *path-to-schema-files*	Specifies the directory path to schema files. For example: `./schema`.

Example

```
# comm_dssetup.pl -i yes -c /var/mps/serverroot -d slapd-budgie
-r o=internet -u o=usergroup -s yes -D "cn=Directory Manager" -w
password -b yes -t 1 -m yes
```

Once you set all the options for the `comm_dssetup.pl` script, you will see the following summary screen before the script is actually run:

```
Here is a summary of the settings that you chose:
  Server Root                       : /var/mps/serverroot/
  Server Instance                   : slapd-budgie
  Users/Groups Directory            : Yes
  Update Schema                     : yes
  Schema Type                       : 1
  DC Root                           : o=internet
  User/Group Root                   : o=usergroup
  Add New Indexes                   : yes
  Schema Directory                  : ./schema
  Directory Manager DN              : "cn=Directory Manager"
```

Each option is further described in the Interactive Mode section.

Interactive Mode

The following questions will be asked if you specify `comm_dssetup.pl` without any arguments:

1. Introduction

```
# perl comm_dssetup.pl

Welcome to the Directory Server preparation tool for Sun ONE Messaging
Server.
(Version 6.0 Revision 0.004)

This tool prepares your directory server for Sun ONE Messaging Server
install.

The logfile is /var/tmp/dssetup_YYYYMMDDHHSS

Do you want to continue [y]:
```

Press enter to continue. Enter `No` to exit.

2. Installation Root of Directory Server

```
Please enter the full path to the directory where the Sun ONE
Directory Server was installed.

Directory server root [/var/mps/serverroot]
```

Indicate the location of the installation root of the Directory Server on the Directory Server machine.

3. Directory Server Instance

```
Please select a directory server instance from the following
list:

[1]   slapd-varrius

Which instance do you want [1]:
```

If multiple instances of Directory Server reside on the machine, choose the one that will be configured with Messaging Server.

4. Directory Manager Distinguished Name (DN)

```
Please enter the directory manager DN [cn=Directory Manager]:
Password:
```

The Directory Manager DN (`cn=Directory Manager`) is the administrator who is responsible for the user and group data in the Organization Tree. Be sure that the Directory Manager DN you specify in this script is the same DN that you set up in your Directory Server installation as well as your Messaging Server installation.

5. User and Group Directory Server

```
Will this directory server be used for users/groups [Yes]:
```

If you enter `Yes`, you will answer questions on selecting a DC Tree base suffix and a User and Group base suffix for your Organization Tree.

If you enter `No`, it is assumed that this directory instance is only used to store configuration data; you will skip to the question about updating schema files. After you finish running this script against the configuration directory instance, you need to run this script against the directory instance that stores user and group data before moving on in the installation process.

6. User and Group Base Suffix

```
Please enter the Users/Groups base suffix [o=usergroup]:
```

The User and Group base suffix is the top entry in the Organization Tree which holds the namespace for user and group entries. Be sure that the User and Group base suffix you select is the same as what you specified during your Directory Server installation and in your Messaging Server installation.

NOTE If you installed Identity Server, be sure the suffix specified in Identity Server installation is the same as what you specify for this question. If you do not use the same suffix, Messaging Server will not recognize your Identity Server installation.

For more information on the Organization Tree, see the *Sun ONE Messaging Server Provisioning Guide*.

7. Schema Type

```
There are 3 possible schema types:
  1   - schema 1 for systems with iMS 5.x data
  1.5 - schema 2 compatibility for systems with iMS 5.x data
        that has been converted with imsdirmig
  2   - schema 2 native for systems using Identity Server

Please enter the Schema Type (1, 1.5, 2) [1]:
```

Choose Option `1` if you are planning to use Sun ONE LDAP Schema, v.1.

Choose Option `1.5` if you plan to use Sun ONE LDAP Schema, v.2, Compatibility Mode. For more information, see the *Sun ONE Messaging Server 6.0 Provisioning Guide*.

Choose Option `2` if you plan to use Sun ONE LDAP Schema, v.2, Native Mode.

If Identity Server is not installed and configured prior to choosing a Sun ONE LDAP Schema, v.2 option, `comm_dssetup.pl` will terminate. You will be asked to rerun the program once Identity Server is installed.

For more information on your schema options, see Messaging Schema Choices.

8. Domain Component (DC) Tree Base Suffix

```
Please enter the DC Tree base suffix [o=internet]:
```

NOTE In Step 7, if you choose Option 1 or 1.5, you will be asked to provide your DC Tree Base Suffix. If you choose Option 2 - Sun ONE LDAP Schema, v.2 - Native Mode, you will not be asked this question.

The DC Tree mirrors the local DNS structure and is used by the system as an index to the Organization Tree that contain the user and group data entries. The DC Tree base suffix is the name of the top entry on the DC tree. You can either choose the default `o=internet` or another name.

For more information on the DC Tree or the Organization Tree, see the *Sun ONE Messaging Server Provisioning Guide*.

9. Updating Schema Files

```
Do you want to update the schema files [yes]:
```

If you answer `Yes`, new elements will be added to your schema. It is recommended that you update the Directory with the new schema files each time you install newer versions of Messaging Server.

10. Configuring New Indexes

```
Do you want to configure new indexes [yes]:
```

If you answer `Yes` to Step 5 (User and Group Directory Server), you will be asked if you want to configure new indexes, which are used to create caches to improve efficiency of directory searches. It is recommended that you answer `Yes` to this question.

11. Summary of Settings

```
Here is a summary of the settings that you chose:
  Server Root                        : /var/mps/serverroot/
  Server Instance                    : slapd-varrius
  Users/Groups Directory             : Yes
  Update Schema                      : yes
  Schema Type                        : 1
  DC Root                            : o=internet
  User/Group Root                    : o=usergroup
  Add New Indexes                    : yes
  Directory Manager DN               : cn=Directory Manager

Now ready to generate a shell script and ldif file to modify the
Directory.
No changes to the Directory Server will be made this time.
Do you want to continue [y]:
```

A summary of your settings will be displayed before your directory configuration is updated.

NOTE In Step 7, if you choose Option 2: Sun ONE LDAP Schema, v.2 - Native Mode, the DC Root in the Summary of Settings will be the same value that you entered for the User/Group Root.

If you want to change any of your settings, enter `No` and re-run the script.

If you enter `Yes` to continue, the `comm_dssetup.pl` script will create an LDIF file and a shell script that will be used to update the indexes and schema in your directory server:

`/var/tmp/dssetup_`*`YYYYMMDDHHMMSS`*`.sh`
`/var/tmp/dssetup_`*`YYYYMMDDHHMMSS`*`.ldif`

where *YYYYMMDDHHMMSS* indicates the time and date stamps when the files were created.

NOTE You can either choose to run the script now or later. If you choose to run the script now, enter `Yes` when asked if you want to continue. If you want to run the script later, you can invoke the script by using `/var/tmp/dssetup_`*`YYYYMMDDHHMMSS`*`.sh`.

Create the Initial Messaging Server Runtime Configuration

The initial runtime configuration program provides a configuration to get your Messaging Server up and running. The program is only meant to be run once. Subsequent running of this program may result in your configuration being overwritten. To modify your initial runtime configuration, use the configuration utilities described in both the *Sun ONE Messaging Server 6.0 Administrator's Guide* and the *Sun ONE Messaging Server 6.0 Reference Manual*.

The following steps walk you through configuring the Messaging Server initial runtime configuration:

Invoke the Messaging Server initial runtime configuration with the following command:

```
/msg_svr_base/sbin/configure [flag]
```

You might use the `xhost`(1) command if you are configuring Messaging Server on a remote system.

Table 2-2 describes optional flags you can set with the `configure` program:

Table 2-2 Optional Flags for the Messaging Server `configure` Program

Flag	Description
`-nodisplay`	Invokes a command-line configuration program.
`-noconsole`	Invokes a GUI user interface program.
`-state` *[statefile]*	Uses a silent installation file. Must be used with `-nodisplay` and `-noconsole` flags. See Perform Silent Installation.

Once you run the `configure` command, the configuration program will start:

1. Welcome

   The first panel in the configure program is a copyright page. Select Next to continue or Cancel to exit.

2. Software License Agreement

   Read the software license agreement.

   Select Yes to accept the license. Or, select No to exit the program.

3. Select directory to store configuration and data files

   Select the directory where you want to store the Messaging Server configuration and data files. For example, `/var/opt/SUNWmsgsr`. This directory symbolically links with the configuration directories specified in *msg_svr_base*. For more information on these symbolic links, see Post-Installation File Directory Layout in Chapter 5, "Performing Post-Installation Procedures."

   Make sure you have large enough disk space set aside for these files.

4. You will see a small window indicating that components are being loaded.

   This may take a few minutes.

5. Select Components to Configure

   Select the Messaging components that you want to configure.

   - Message Transfer Agent: Handles routing, delivering user mail, and handling SMTP authentication. The MTA provides support for hosted domains, domain aliases, and server-side filters.
   - Message Store: Provides the foundation for unified messaging services through its universal Message Store. Access to the message store is available through multiple protocols (HTTP, POP, IMAP). If you are only configuring a Message Store, you must also select the MTA.
   - Messenger Express: Handles the HTTP protocol retrieval of messages from the Message Store. If you are only configuring Messenger Express, you must also select the Message Store and the MTA.

- Messaging Multiplexor: Acts as a proxy to multiple messaging server machines within an organization. Users connect to the Multiplexor server, which redirects each connection to the appropriate mail server. This component is not enabled by default. If you do check the MMP as well as the Message Store, they will be enabled on the same system; a warning message will appear for you to change your change port numbers after configuration (For instructions on doing so, see Port Numbers).

  To configure the MMP, see the *Sun ONE Messaging Server 6.0 Administrator's Guide* and the *Sun ONE Messaging Server 6.0 Reference Manual*.

Check any components you want to configure, and uncheck those components you do not wish to configure.

6. Enter the system user name and the group that will own the installed files.

   For information on setting up system users and groups, see Create UNIX System Users and Groups.

7. Configuration Directory Server Panel

   Enter your Configuration Directory LDAP URL, Administrator and Password.

   Gather the Configuration Server LDAP URL from your Directory Server installation. See Directory Server Installation in Appendix A, "Installation Worksheets."

   The Directory Manager has overall administrator privileges on the Directory Server and all Sun ONE servers that make use of the Directory Server (for example, the Messaging Server) and has full administration access to all entries in the Directory Server. The default and recommended Distinguished Name (DN) is `cn=Directory Manager`.

   If you are installing against a replicated Directory Server instance, you must you specify the credentials of the replica, not the master directory.

8. User / Group Directory Server Panel

   Enter your Users and Groups Directory LDAP URL, Administrator and Password.

   Gather the User / Group Server LDAP URL information from the host and post number information from your Directory Server installation. See Directory Server Installation in Appendix A, "Installation Worksheets."

   The Directory Manager has overall administrator privileges on the Directory Server and all Sun ONE servers that make use of the Directory Server (for example, the Messaging Server) and has full administration access to all entries in the Directory Server. The default and recommended Distinguished Name (DN) is `cn=Directory Manager`.

   If you are installing against a replicated Directory Server instance, you must specify the credentials of the replica, not the master directory.

9. Postmaster Email Address

   Enter a Postmaster Email Address.

   Select an address that your Administrator will actively monitor. For example, `pma@siroe.com` for a postmaster on the siroe domain. Note that this address cannot begin with "Postmaster."

   Note that the user of the email address is not automatically created. Therefore, you will need create it by using a provisioning tool.

10. Password for administrator accounts

    Enter a universal password that will be used for service administrator, server, user / group administrator, end user administrator privileges as well as PAB administrator and SSL passwords.

    After the initial runtime configuration, you might change this password for individual administrator accounts. For more information, see Modifying Your Configuration in Chapter 5, "Performing Post-Installation Procedures."

11. Default Email Domain

Enter a Default Email Domain.

This email domain is the default that is used if no other domain is specified. For example, if `siroe.com` is the default email domain, then messages that are generated by an internal user will be attempted to be sent to the designated recipient in the `siroe.com` domain if no other domain is specified.

If you are using the User Management Utility, the command-line interface for provisioning users and groups with Sun ONE LDAP Schema, v.2, you will want to specify the same default domain during its configuration. For more information, see the *Sun ONE Communications Server 6.0 Provisioning Tools Configuration and Reference Manual.*

12. Organization DN

Enter an Organization DN.

In the organization tree, you need an organization DN under which your organization will reside.

For example, if your organization DN is `o=Engineering`, all the users in that organization will be placed under the LDAP DN `o=Engineering, o=usergroup` (where `o=usergroup` is your user / group Directory suffix which was specified in Prepare Directory Server for Messaging Server Configuration).

If you choose the same your user / group Directory suffix as your Organization DN, you may have migration problems if you decide to create a hosted domain. If you want to set up a hosted domain during initial runtime configuration, then specify a DN one level below the User / Group suffix.

13. Ready to Configure

The configuration program will check for enough disk space on your machine and then outline the components it is ready to configure.

To configure the Messaging components, select Configure Now. To change any of your configuration variables, select Back. Or to exit from the configuration program, select Cancel.

14. Starting Task Sequence, Sequence Completed, and Installation Summary Panels

    You can read the installation status by selecting Details on the final Installation Summary page. To exit the program, select Close.

    A log file is created in */msg_svr_base*/install/configure_*YYYYMMDDHHMMSS*.log, where *YYYYMMDDHHMMSS* identifies the 4-digit year, month, date, hour, minute, and second of the configuration.

    An initial runtime configuration is now set up for your Messaging Server. To change any configuration parameter, refer to both Modifying Your Configuration in Chapter 5, "Performing Post-Installation Procedures" and the *Sun ONE Messaging Server Administrator's Guide* for instructions on doing so.

To start Messaging Server, use the following command:

```
/opt/SUNWmsgsr/sbin/start-msg
```

Perform Silent Installation

The Messaging Server initial runtime configuration program automatically creates a silent installation *state* file (called saveState) that can be used to quickly configure additional Messaging Server instances in your deployment where the Messaging Server Solaris packages have been installed. All of your responses to the configuration prompts are recorded in that file.

By running the silent installation, you instruct the configure program to read the silent installation *state* file. The configure program uses the responses in this file rather than ask the same installation questions again for subsequent initial runtime configurations of Messaging Server. When you use the *state* file in a new installation, you are not asked any questions. Instead, all of the *state* file responses are automatically applied as the new installation parameters.

The silent installation saveState *state* file is stored in the */msg_svr_base*/install/configure_*YYYYMMDDHHMMSS* directory, where *YYYYMMDDHHMMSS* identifies the 4-digit year, month, date, hour, minute, and second of the saveState file.

To use the silent installation *state* file to configure another Messaging Server instance on another machine in the deployment, follow these steps:

1. Copy the silent installation *state* file to the installation directory on the machine where you are performing the new installation.
2. Review and edit the silent installation *state* file as necessary.

   You will probably want to change some of the parameters and specifications in the *state* file. For example, the default email domain for the new installation may be different than the default email domain recorded in the *state* file. Remember that the parameters listed in the *state* file will be automatically applied to this installation.
3. Run the following command to configure other machines with the silent installation file:

   msg_svr_base/sbin/configure -nodisplay -noconsole -state \
   fullpath/saveState

   where *fullpath* is the full directory path of where the saveState file is located. (See Step 1 of this section).

NOTE After running the silent installation program, a new *state* file is created from the silent installation in directory location: *msg_svr_base*/install/configure_*YYYYMMDDHHMMSS*/saveState, where *YYYYMMDDHHMMSS* identifies the 4-digit year, month, date, hour, minute, and second of the saveState file.

Install Messaging Server against a Directory Server Replica

There might be limitations that prevent you from installing Messaging Server against a Directory Server replica:

- You do not have Directory Server master credentials.
- The Directory Server credentials are unknown.
- Messaging Server cannot communicate directly with the Directory Server master.

To install Messaging Server against a Directory Server replica, follow these steps:

1. Run the comm_dssetup.pl program against all Directory Servers including the the Directory Server replicas as noted in comm_dssetup.pl Requirements.

2. Run the Messaging `configure` program (located in *msg_svr_base*`/sbin/configure`) using the replicated Directory Server credentials as described in Step 7 and Step 8 in Create the Initial Messaging Server Runtime Configuration.

   Because of invalid privileges, the `configure` program will fail in trying to configure the Directory Server Administrators. It will, however, produce the `*.ldif` files that are needed to allow proper privileges to the Directory Server replicas.

3. Move the `*.ldif` files to the Directory Server master.

4. Run the `ldapmodify` command on the `*.ldif` files.

   See the Sun ONE Directory Server documentation for more information on `ldapmodify` or in the */msg_svr_base*`/install/configure_`*YYYYMMDDHHMMSS*`.log`.

5. Re-run the `configure` program.

   Your Directory Server replica (and master) are now configured to work with your Messaging Server.

Chapter 3

Configuring High Availability Solutions

This chapter contains the following sections to help you determine which high availability (HA) model is right for you and how to set up your system to run high availability with Messaging Server. This chapter covers the following topics:

- High Availability Models
- Configuring High Availability
- Unconfiguring High Availability

For more information on High Availability models supported with Messaging Server, the following product documentation is recommended:

- **Sun Cluster Server**
  - *Sun Cluster Concepts Guide*
  - *Sun Cluster Data Services and Planning and Administration Guide*
  - *Sun Cluster System Administration Guide*
  - *Sun Cluster Reference Manual*
- **Veritas Cluster Server**
  - *Veritas Cluster Server User's Guide*

High Availability Models

There are different high availability models that can be used with Messaging Server. Three of the more common ones are:

- Asymmetric (hot standby)
- Symmetric
- N+1 (N Over 1)

Each of these models is described in greater detail in the following subsections. In addition, the following topics are covered:

- Which High Availability Model is Right for you?
- System Down Time Calculations

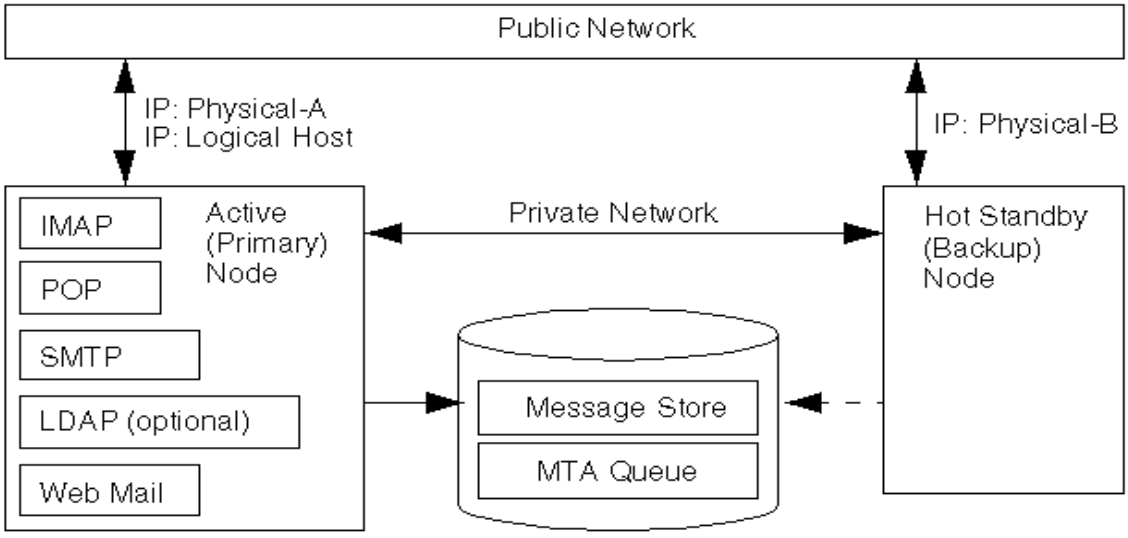
Note that different HA products may or may not support different models. Refer to the HA documentation to determine which models are supported.

Asymmetric

The basic asymmetric or “hot standby” high availability model (Figure 3-1) consists of two clustered host machines or “nodes.” A logical IP address and associated host name are designated to both nodes.

In this model, only one node is active at any given time; the backup or hot standby node remains idle most of the time. A single shared disk array between both nodes is configured and is mastered by the active or “primary” node. The message store partitions and Message Transfer Agent (MTA) queues reside on this shared volume.

Figure 3-1 Asymmetric High Availability Model



Before failover, the active node is Physical-A. Upon failover, Physical-B becomes the active node and the shared volume is switched so that it is mastered by Physical-B. All services are stopped on Physical-A and started on Physical-B.

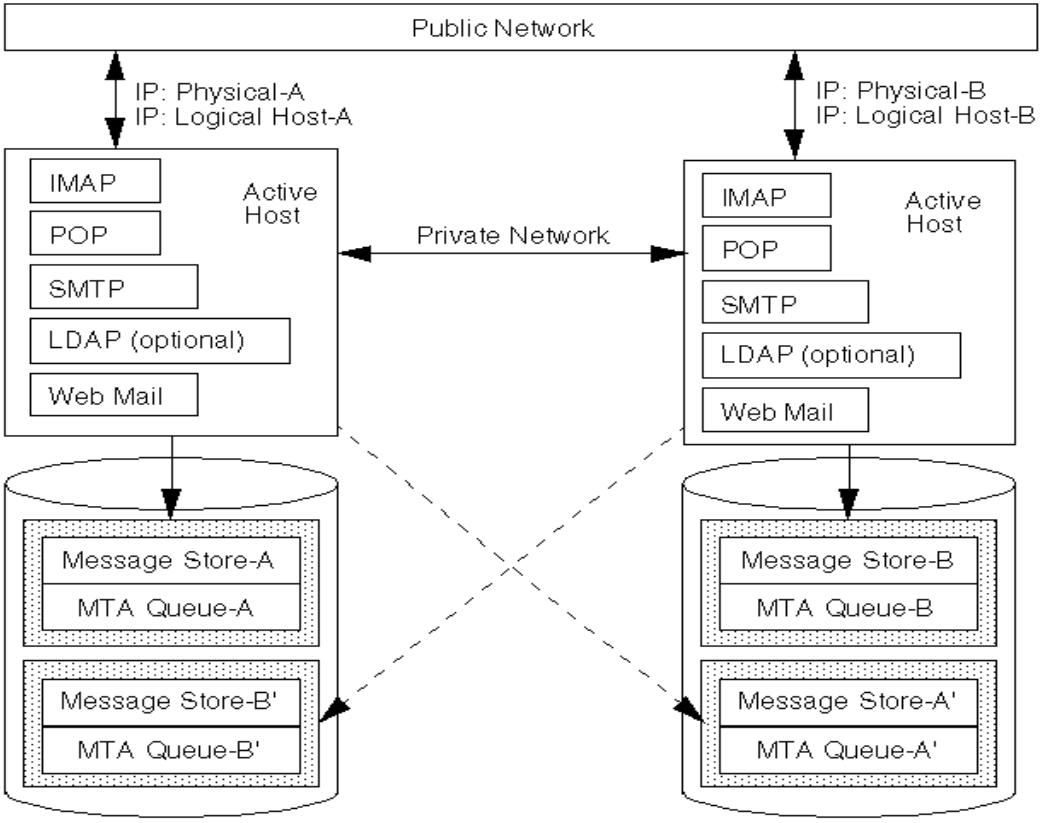
The advantage of this model is that the backup node is dedicated and completely reserved for the primary node; there is no resource contention on the backup node when a failover occurs. However, this model also means that the backup node stays idle most of the time and this resource is therefore under utilized.

Symmetric

The basic symmetric or “dual services” high availability model consists of two hosting machines, each with its own logical IP address. Each logical node is associated with one physical node, and each physical node controls one disk array with two storage volumes. One volume is used for its local message store partitions and MTA queues, and the other is a mirror image of its partner’s message store partitions and MTA queues.

In the symmetric high availability mode (Figure 3-2), both nodes are active concurrently, and each node serves as a backup node for the other. Under normal conditions, each node runs only one instance of the messaging server.

Figure 3-2 Symmetric High Availability Model



Upon failover, the services on the failing node are shut down and restarted on the backup node. At this point, the backup node is running Messaging Server from both nodes and is managing two separate volumes.

The advantage of this model is that both nodes are active simultaneously, thus fully utilizing machine resources. However, during a failure, the backup node will have more resource contention as it runs services for Messaging Server from both nodes. Therefore, you should repair the failed node as quickly as possible and switch the servers back to their dual services state.

This model also provides a backup storage array; in the event of a disk array failure, its mirror image can be picked up by the service on its backup node.

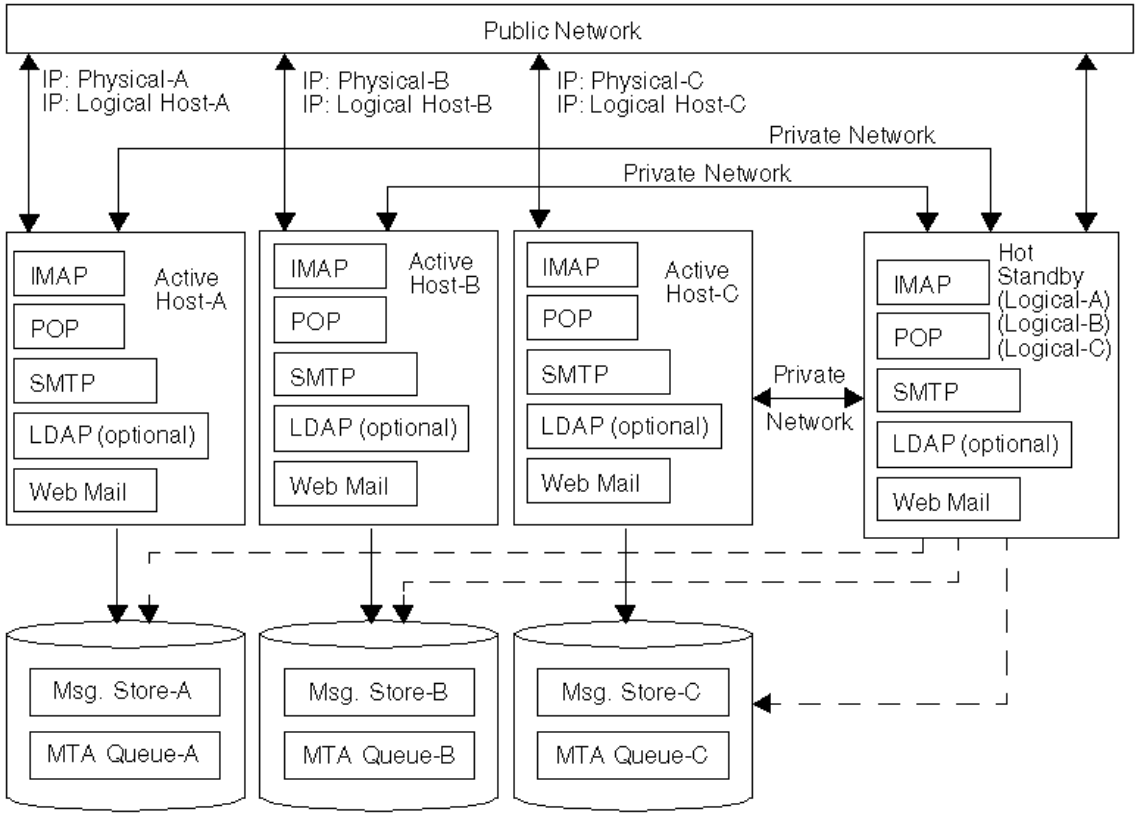
To configure a symmetric model, you need to install shared binaries on your shared disk. Note that doing so may prevent you from performing rolling upgrades, a feature that will allow you to update your system during Messaging Server patch releases (which will be available in future releases).

N+1 (N Over 1)

The N + 1 or “N over 1” model operates in a multi-node asymmetrical configuration. N logical host names and N shared disk arrays are required. A single backup node is reserved as a hot standby for all the other nodes. The backup node is capable of concurrently running Messaging Server from the N nodes.

Figure 3-3 illustrates the basic N + 1 high availability model.

Figure 3-3 N + 1 High Availability Model



Upon failover of one or more active nodes, the backup node picks up the failing node's responsibilities.

The advantages of the N + 1 model are that the server load can be distributed to multiple nodes and that only one backup node is necessary to sustain all the possible node failures. Thus, the machine idle ratio is 1/N as opposed to 1/1, as is the case in a single asymmetric model.

To configure an N+1 model, you need to install shared binaries on your shared disk as with symmetric models. Note that doing so may prevent you from performing rolling upgrades, a feature that will allow you to update your system during Messaging Server patch releases (which will be available in future releases).

Which High Availability Model is Right for you?

Table 3-1 summarizes the advantages and disadvantages of each high availability model. Use this information to help you determine which model is right for you.

Table 3-1 High Availability Model Advantages and Disadvantages

Model	Advantages	Disadvantages	Recommended User
Asymmetric	• Simple Configuration • Backup node is 100 percent reserved	• Machine resources are not fully utilized	A small service provider with plans to expand in the future.
Symmetric	• Better use of system resources • Higher availability	• Resource contention on backup node • Mirrored disks reduce disk write performance	A medium-sized service provider with no expansion plans on their backup systems in the near future.
N + 1	• Load distribution • Easy expansion	• Configuration complexity	A large service provider who requires distribution with no resource constraints.

System Down Time Calculations

Table 3-2 illustrates the probability that on any given day the mail service will be unavailable due to system failure. These calculations assume that on average, each server goes down for one day every three months due to either a system crash or server hang, and that each storage device goes down one day every 12 months. They also ignore the small probability of both nodes being down simultaneously.

Table 3-2 System Down Time Calculations

Model	Server Down Time Probability
Single server (no high availability)	Pr(down) = (4 days of system down + 1 day of storage down) / 365 = 1.37%
Asymmetric	Pr(down) = (0 days of system down + 1 day of storage down) / 365 = 0.27%
Symmetric	Pr(down) = (0 days of system down + 0 days of storage down) / 365 = (near 0)
N + 1	Pr(down) = (0 days of system down + 1 day of storage down) / (365xN) = 0.27% / N

Configuring High Availability

This section provides the information you need to configure the Veritas Cluster Server or Sun Cluster high availability clustering software and prepare it for use with the Messaging Server. (Refer to your Veritas or Sun Cluster Server documentation for detailed installation instructions, required patches, and information as needed.)

Table 3-3 lists the versions of Sun Cluster Server and Veritas Cluster Server that are currently supported with Messaging Server:

Table 3-3 Supported Versions of Sun Cluster Server and Veritas Cluster Server

Cluster	Supported Versions
Sun Cluster Server	Sun Cluster 3.0 Update 3 and Sun Cluster 3.1
Veritas Cluster Server	Veritas Cluster Server 1.3, Veritas Cluster Server 2.0, and Veritas Cluster Server 3.5

For the latest updates on version support, refer to the *Sun ONE Messaging Server 6.0 Release Notes*.

The following topics are covered in this section:

- Cluster Agent Installation

Cluster Agent Installation

A cluster agent is a Messaging Server program that runs under the cluster framework.

The Sun Cluster Messaging Server agent (`SUNWscims`) is installed when you select Sun Cluster 3.1 through the Java Enterprise System installer. The Veritas Cluster Messaging Server agent (`SUNWmsgvc`) can be found in the Messaging Server `Product` subdirectory on the Java Enterprise System CD. (Note that you must use the `pkgadd`(1M) command to install the VCS cluster agent.)

Some items of note regarding the Messaging Server and high availability (applies to both Veritas Cluster, and Sun Cluster) installation:

- High Availability cluster agents for the Messaging Server are not installed by default; be sure to select the appropriate agent package during the Java Enterprise System installation process.
- Before running the Java Enterprise System installer, make sure that the HA logical host names and associated IP address for Messaging Server are active. The reason for this is because portions of the installation will make TCP connections using them. Run the installation on the cluster node currently pointed at by the HA logical host name for Messaging Server.
- When you are asked for the *msg_svr_base* in the Java Enterprise System installer, be sure that the *msg_svr_base* is on the local disk. In other words, you need to install the Messaging Server package locally on each node. However, your configuration and data should be on a disk that is shared between the nodes. Otherwise, if you install your configuration and data on a local disk and one node fails over to the other node, the servers will not see the data accumulated by the server on the failed node.

- After you configure the Administration Server through the Java Enterprise System installer, be sure that the IP address of the Administration Server is associated with the logical IP address for the machine not the IP address of the physical host.

NOTE You can change the IP address from the physical host to the IP address of the logical host for the Administration Server with the `admin_ip.pl` utility. For more information on this utility, consult your Sun ONE Console documentation at:

`http://docs.sun.com/db/prod/s1.ipconsole.2`

- After running the Messaging Server Initial Runtime Configuration (see Create the Initial Messaging Server Runtime Configuration), be sure to manually configure the fully-qualified HA logical host name of the cluster of Messaging Server.

Using the useconfig utility

The `useconfig` utility allows you to share a single configuration between multiple nodes in an HA environment. This utility is not meant to upgrade or update an existing configuration.

For example, if you are upgrading your first node, you will install through the Java Enterprise System installer and then configure Messaging Server (See Chapter 2, “Installing Messaging Server.”). You will then failover to the second node where you will install the Messaging Server package through the Java Enterprise System installer, but you will not have to run the Initial Runtime Configuration Program (`configure`) again. Instead, you can use the `useconfig` utility.

To enable the utility, run `useconfig` utility to point to your previous Messaging Server configuration.

```
msg_svr_base/sbin/useconfig install/configure_YYYYMMDDHHMMSS
```

where `configure_`*YYYYMMDDHHMMSS* is your previous configuration settings file.

On a brand new node, you can find the `configure_`*YYYYMMDDHHMMSS* in the *msg_svr_base*`/data/setup` directory on the shared disk.

NOTE The Messenger Express HTML files are not updated with the `useconfig` command. Therefore, if you have customized your HTML files, you need to manually update these files with the new templates. If you have not customized your HTML files, you can simply copy the new templates to your `config` directory:

```
# cp -rpf msg_svr_base/lib/config-templates/html msg_svr_base/config
```

The following sections on Veritas Cluster Server Agent Installation and Sun Cluster Agent Installation describe when you can use the `useconfig` utility.

Veritas Cluster Server Agent Installation

Messaging Server can be configured with Veritas Cluster Server 1.3, 2.0, and 3.5. The instructions in this section only cover Veritas Cluster 3.5; for Veritas 1.3 and 2.0, review the *Messaging Server 5.2 Installation Guide.*

Be sure to review the Veritas Cluster Server documentation prior to following these procedures.

NOTE

- Veritas Volume Manager (VxVM) has a cluster feature that requires a separate license. This feature provides a global view of the file systems on shared storage, similar to the Sun Cluster 3.0 global file system. See the Veritas Cluster Server documentation for more information.
- `FsckOpt` was optional in pre-3.5 Veritas releases. However, it is required for configuring the `Mount` resource. `FsckOpt` must include a `-y` or `-n`, otherwise the resource will not come online.
- Veritas Cluster Server 2.0 Explorer cannot be used to manage Veritas Cluster Server 3.5.

After installing Messaging Server through the Java Enterprise System installer and configuring HA, be sure to review Binding IP Addresses on a Server for additional steps associated with configuring HA support.

Veritas Cluster Server Requirements

- Veritas Cluster Software is already installed and configured.

- As described in the following instructions (in VCS 3.5 Installation and Configuration Notes), you will install the Veritas Cluster Agent package for Messaging Server along with the Messaging Server software on both nodes.

VCS 3.5 Installation and Configuration Notes

The following instructions describe how to configure Messaging Server as an HA service, by using Veritas Cluster Server 3.5.

The default `main.cf` configuration file sets up a resource group called `ClusterService` that launches the `VCSweb` application. This group includes network logical host IP resources like `csgnic` and `webip`. In addition, the `ntfr` resource is created for event notification.

1. Launch Cluster Explorer from one of the nodes.

   Note that these Veritas Cluster Server instructions assume you are using the graphical user interface to configure Messaging Server as an HA service.

   To launch Cluster Explorer, run the following command:

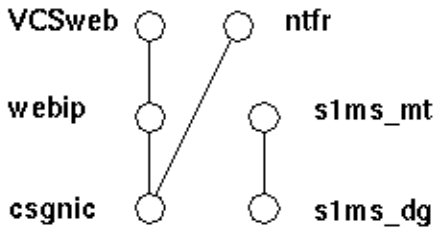
```
# /opt/VRTSvcs/bin/hagui
```

   The `VRTScscm` package must be installed in order to use the GUI.

2. Add `s1ms_dg` disk group resource of type `DiskGroup` and enable it.
3. Add `s1ms_mt` mount resource of type `Mount`.
   a. Unlike in Veritas Cluster Server 2.0, you must add `-y` (or `-n`) to `FsckOpt`. Null options cause `Mount` to hang. See the Solaris Man page for more information on `fsck_vxfs`.
   b. Be sure to click the Link button to enable linking resources, if they are not already enabled.

4. Create a link between `s1ms_mt` and `s1ms_dg`. Enable the resource `s1ms_mt`.

   See the following dependency tree:



5. Run the Java Enterprise System installer, selecting Messaging Server.

   a. Run the Messaging Server Initial Runtime Configuration (see Chapter 2, "Installing Messaging Server") from the primary node (for example, Node_A) to install Messaging Server.

   b. Install the Veritas Cluster Server agent package, `SUNWmsgvc`, (located in the Messaging Server `Product` subdirectory on the Java Enterprise System CD) by using the `pkgadd`(1M) command.

   c. Check to make sure that the logical host name and the logical IP address are specified whenever a host name or an IP address is required during the installation.

      Messaging Server and the Veritas agent are now installed on Node_A.

6. Switch to the backup node (for example, Node_B).

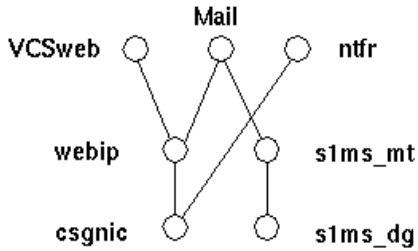
7. Run the Java Enterprise System installer to install Messaging Server on the backup node (Node_B).

8. After installing Messaging Server, you can use the `useconfig` utility to obviate the need for creating an additional initial runtime configuration on the backup node (Node_B). The `useconfig` utility allows you to share a single configuration between multiple nodes in an HA environment. This utility is not meant to upgrade or update an existing configuration. See Using the useconfig utility.

   The Veritas agent is now installed on Node_B.

9. From the Cluster Explorer, Select Import Types... from the File menu which will display a file selection box.

10. Import the `MsgSrvTypes.cf` type from the `/etc/VRTSvcs/conf/config` directory. Import this type file. Note that you need to be on a cluster node to find this file.
11. Now create a resource of type `MsgSrv` (for example, `Mail`). This resource requires the logical host name property to be set.
12. The `Mail` resource depends on `s1ms_mt` and `webip`. Create links between the resources as shown in the following dependency tree:



    a. Enable all resources and bring `Mail` online.
    b. All servers should be started.
13. Switch over to Node_A and check if the High Availability configuration is working.
14. Change the group attribute `OnlineRetryLimit` from `3` to `0`, otherwise the failed-over service might restart on the same node.

MsgSrv Attributes

This section describes `MsgSrv` additional attributes that govern the behavior of the `mail` resource. To configure Messaging Server with Veritas Cluster Server, see Table 3-4.

Table 3-4 Veritas Cluster Server Attributes

Attribute	Description
`FaultOnMonitorTimeouts`	If unset (=0), monitor (probe) time outs are not treated as resource fault. Recommend setting this to 2. If the monitor times out twice, the resource will be restarted or failed over.
`ConfInterval`	Time interval over which faults / restarts are counted. Previous history is erased if the service remains online for this duration. Suggest 600 seconds.

Table 3-4 Veritas Cluster Server Attributes *(Continued)*

Attribute	Description
`ToleranceLimit`	Number of times the monitor should return OFFLINE for declaring the resource FAULTED. Recommend leaving this value at '0' (default).

Sun Cluster Agent Installation

This section describes how to install and configure the Messaging Server as a Sun Cluster Highly Available (HA) Data Service. These installation instructions apply to both Sun Cluster 3.0 Update 3 and Sun Cluster 3.1. The following topics are covered in this section:

- Sun Cluster Requirements
- Configuring Messaging Server HA Support for Sun Cluster
- Enabling HAStoragePlus
- Binding IP Addresses on a Server

Documentation for Sun Cluster 3.0 Update 3 and for Sun Cluster 3.1 can be found at:

`http://docs.sun.com/db/prod/cluster#hic`

Note that Veritas File System (VxFS) is supported with Sun Cluster 3.0 Update 3 and with Sun Cluster 3.1.

Sun Cluster Requirements

This section presumes the following:

- Sun Cluster 3.0 Update 3 or Sun Cluster 3.1 is installed and configured on a Solaris 8 or 9 operating system with required patches.
- The Sun Cluster agent `SUNWscims` is installed on your systems.
- If logical volumes are being created, either Solstice DiskSuite or Veritas Volume Manager is used.

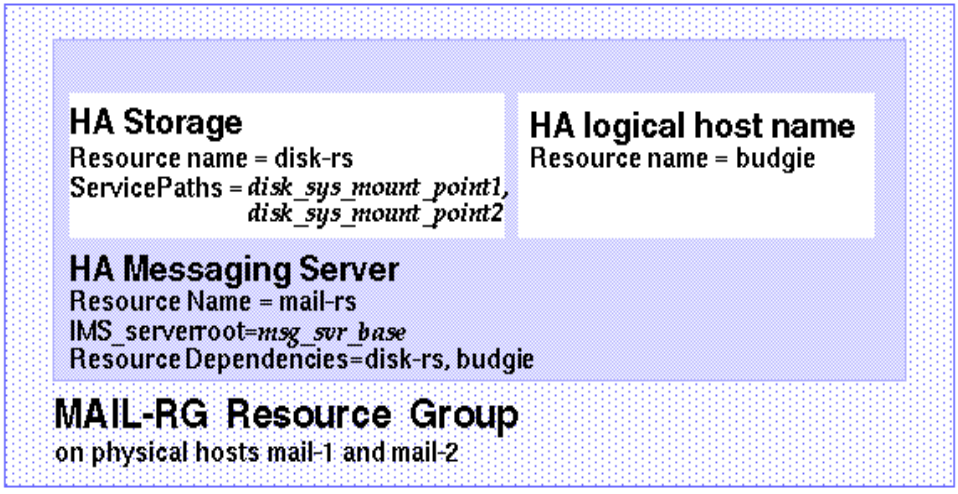
Configuring Messaging Server HA Support for Sun Cluster

This section describes how to configure HA support for Sun ONE Messaging Server for Sun Cluster 3.0 Update 3 and 3.1 through a simple example.

After configuring HA, be sure to review Binding IP Addresses on a Server for additional steps associated with HA support.

The following example assumes that the messaging server has been configured with a HA logical host name and IP address. The physical host names is assumed to be `mail-1` and `mail-2`, with an HA logical host name of `budgie`. Figure 3-4 depicts the nested dependencies of the different HA resources you will create in configuring Messaging Server HA support.

Figure 3-4 A Simple Sun ONE Messaging Server HA configuration



1. Become the superuser and open a console.

   All of the following Sun Cluster commands require that you have logged in as superuser. You will also want to have a console or window for viewing messages output to `/dev/console`.

2. Add required resource types.

   Configure Sun Cluster to know about the resources types we will be using. This is done with the `scrgadm -a -t` command:

   ```
   # scrgadm -a -t SUNW.HAStorage
   # scrgadm -a -t SUNW.ims
   ```

3. Create a resource group for the Messaging Server.

   If you have not done so already, create a resource group and make it visible on the cluster nodes which will run the Messaging Server. The following command creates a resource group named `MAIL-RG`, making it visible on the cluster nodes `mail-1` and `mail-2`:

   ```
   # scrgadm -a -g MAIL-RG -h mail-1,mail-2
   ```

   You may, of course, use whatever name you wish for the resource group.

4. Create an HA logical host name resource and start resource group.

   If you have not done so already, create and enable a resource for the HA logical host name, placing it in the resource group. The following command does so using the logical host name `budgie`. Since the `-j` switch is omitted, the name of the resource created will also be `budgie`.

   ```
   # scrgadm -a -L -g MAIL-RG -l budgie
   # scswitch -Z -g MAIL-RG
   ```

5. Create an HA storage resource.

   Next, you need to create an HA storage resource type for the file systems on which Messaging Server is dependent. The following command creates an HA storage resource named `disk-rs` and the file system *disk_sys_mount_point* is placed under its control:

   ```
   # scrgadm -a -j disk-rs -g MAIL-RG \
   -t SUNW.HAStorage \
   -x ServicePaths=disk_sys_mount_point-1, disk_sys_mount_point-2
   ```

   The comma-separated list of `ServicePaths` are the mount points of the cluster file systems on which Messaging Server is dependent. In the above example, only two mount points, *disk_sys_mount_point-1* and *disk_sys_mount_point-2*, are specified. If one of the servers has additional file systems on which it is dependent, then you can create an additional HA storage resource and in Step 8 to indicate that additional dependency.

6. Install and configure Messaging Server (Chapter 2, "Installing Messaging Server"); be sure to use the HA logical host name created in Step 4.

   a. In the Initial Runtime Configuration, you are asked to specify a configuration directory in Step 3 of Create the Initial Messaging Server Runtime Configuration. Be sure to use the shared disk directory path of your HA Storage resource (or HAStoragePlus resource, described in Enabling HAStoragePlus).

b. Be sure to run the following command to enable the watcher process under Sun Cluster:

```
configutil -o local.autorestart -v 1
```

For more information on the watcher process, refer to the *Sun ONE Messaging Server 6.0 Administrator's Guide*.

7. Run the `ha_ip_config` script to set `service.listenaddr` and `service.http.smtphost` and to configure the `dispatcher.cnf` and `job_controller.cnf` files for high availability. The script will ensure that the logical IP address is set for these parameters and files, rather than the physical IP address.

For instructions on running the script, see Binding IP Addresses on a Server.

The `ha_ip_config` script should only be run once on the machine with the shared disk (for configuration and data).

8. Create an HA Messaging Server resource.

It's now time to create the HA Messaging Server resource and add it to the resource group. This resource is dependent upon the HA logical host name and HA disk resource.

In creating the HA Messaging Server resource, we need to indicate the path to the Messaging Server top-level directory—the *msg_svr_base* path. These are done with the `IMS_serverroot` extension properties as shown in the following command.

```
# scrgadm -a -j mail-rs -t SUNW.ims -g MAIL-RG \
          -x IMS_serverroot=msg_svr_base \
          -y Resource_dependencies=disk-rs,budgie
```

The above command, creates an HA Messaging Server resource named `mail-rs` for the Messaging Server which is installed on `IMS_serverroot` in the *msg_svr_base* directory. The HA Messaging Server resource is dependent upon the HA disk resource `disk-rs` as well as the HA logical host name `budgie`.

If the Messaging Server has additional file system dependencies, then you can create an additional HA storage resource for those file systems. Be sure to include that additional HA storage resource name in the `Resource_dependencies` option of the above command.

9. Enable the Messaging Server resource.

   It's now time to activate the HA Messaging Server resource, thereby bringing the messaging server online. To do this, use the command

   ```
   # scswitch -e -j mail-rs
   ```

   The above command enables the `mail-rs` resource of the MAIL-RG resource group. Since the MAIL-RG resource was previously brought online, the above command also brings `mail-rs` online.

10. Verify that things are working.

    Use the `scstat` command to see if the MAIL-RG resource group is online. You may want to look at the output directed to the console device for any diagnostic information. Also look in the `syslog` file, `/var/adm/messages`.

11. Fail the resource group over to another cluster node in order to make sure failover properly works.

    Manually fail the resource group over to another cluster node. Use the `scstat` command to see what node the resource group is currently running on ("online" on). For instance, if it is online on mail-1, then fail it over to mail-2 with the command:

    ```
    # scswitch -z -g MAIL-RG -h mail-2
    ```

Enabling HAStoragePlus

`SUNW.HAStoragePlus` is a resource type that can be used to make locally mounted file systems highly available within a Sun Cluster environment. Any file system resident on a Sun Cluster global device group can be used with `HAStoragePlus`. Unlike a globally mounted filesystem like HAStorage, HAStoragePlus is available only on one cluster node at any given point of time. These locally mounted file systems can only be used in failover mode and in failover resource groups. `HAStoragePlus` offers FFS (failover file system), in contrast to HAStorage's GFS (global file system).

HAStoragePlus has a number of benefits:

- HAStoragePlus bypasses the global file service layer completely. For disk-IO intensive data services, this leads to a significant performance increase.
- HAStoragePlus can work with any file system (like UFS,VxFS, and so forth), even those that might not work with the global file service layer. If a file system is supported by the Solaris operating system, it will work with HAStoragePlus.

For more information on HAStoragePlus, read the *Sun Cluster 3.1 Data Service Planning and Administration Guide.*

To enable HAStoragePlus on your cluster:

1. Disable your messaging and storage resources.

```
# scwitch -n -j mail-rs
# scwitch -n -j disk-rs
```

2. Remove your messaging and storage resources.

```
# scrgadm -r -j mail-rs
# scrgadm -r -j disk-rs
```

3. Create the disk type `SUNW.HAStoragePlus`.

```
# scrgadm -a -t SUNW.HAStoragePlus
```

4. Create your disk resource and resource dependencies with HAStoragePlus.

HA Storage Resource

```
# scrgadm -a -j disk-rs -g MAIL-RG \
          -t SUNW.HAStoragePlus \
         -x FileSystemMountPoints=file_sys_mount_point-1
```

Messaging Server Resource

```
# scrgadm -a -j mail-rs -g MAIL-RG \
          -x IMS_serverroot=msg_svr_base
         -y Resource_dependencies=disk-rs,budgie
```

5. Remove the term `global` from the `/etc/vfstab` file. At bootup, `/etc/vbstab` must be set to 'no.' For more information, refer to your Sun Cluster 3.1 documentation.

   Before the `vfstab` file is enabled with HAStoragePlus, you might first `umount` the file systems that are currently global file systems. You can then enable the `vfstab` file with HAStoragePlus and remount the file systems.

6. Start your cluster server.

```
# scswitch -Z -g MAIL-RG
```

Binding IP Addresses on a Server

If you are using the Symmetric or N + 1 high availability models, there are some additional things you should be aware of during configuration in order to prepare the Sun Cluster Server for Messaging Server.

Messaging Server running on a server requires that the correct IP address binds it. This is required for proper configuration of Messaging in an HA environment.

Part of configuring Messaging Server for HA involves configuring the interface address on which the Messaging Servers bind and listen for connections. By default, the servers bind to all available interface addresses. However, in an HA environment, you want the servers to bind specifically to the interface address associated with an HA logical host name.

A script is therefore provided to configure the interface address used by the servers belonging to a given Messaging Server instance. Note that the script identifies the interface address by means of the IP address which you have or will be associating with the HA logical host name used by the servers.

The script effects the configuration changes by modifying or creating the following configuration files. For the file

msg_svr_base/config/dispatcher.cnf

it adds or changes INTERFACE_ADDRESS option for the SMTP and SMTP Submit servers. For the file

msg_svr_base/config/job_controller.cnf

it adds or changes the INTERFACE_ADDRESS option for the Job Controller.

Finally it sets the configutil service.listenaddr and service.http.smtphost parameters used by the POP, IMAP, and Messenger Express HTTP servers.

Note that the original configuration files, if any, are renamed to *.pre-ha.

Run the script as follows:

1. Become superuser.
2. Execute *msg_svr_base*/sbin/ha_ip_config
3. The script presents the questions described below. The script may be aborted by typing control-d in response to any of the questions. Default answers to the questions will appear within square brackets, [ ]. To accept the default answer, simply press the RETURN key.
    a. Logical IP address: Specify the IP address assigned to the logical host name which the Messaging Server will be using. The IP address must be specified in dotted decimal form, for example, 123.456.78.90.

        The logical IP address is automatically set in the configutil parameter service.http.smtphost which allows you to see which machine is running your messaging system in a cluster. For example, if you are using Messenger Express, your server will be able to determine from which mail host to send outgoing mail.

b. Messaging Server Base (*msg_svr_base*): Specify the absolute path to the top-level directory in which Messaging Server is installed.

c. Do you wish to change any of the above choices: answer “no” to accept your answers and effect the configuration change. Answer “yes” if you wish to alter your answers.

NOTE In addition, the `ha_ip_config` script automatically enables two new processes `watcher` and `msprobe` with the following parameters: `local.autorestart` and `local.watcher.enable`. These new parameters help to monitor the health of the messaging server. Process failures and unresponsive services result in log messages indicating specific failures. The cluster agents now monitor the `watcher` process and failover whenever it exits. Note that the parameters must be enabled in order for Sun Cluster to function properly.

For more information on the `watcher` and `msprobe` processes, see the *Sun ONE Messaging Server 6.0 Release Notes*.

Unconfiguring High Availability

This section describes how to unconfigure high availability. To uninstall high availability, follow the instructions in your Veritas or Sun Cluster documentation.

The High Availability unconfiguration instructions differ depending on whether you are removing Veritas Cluster Server or Sun Cluster.

The following topics are covered in this section:

- Unconfiguring Veritas Cluster Server
- Unconfiguring Messaging Server HA Support for Sun Cluster 3.x

Unconfiguring Veritas Cluster Server

To unconfigure the high availability components for Veritas Cluster Server:

1. Bring the `iMS5` service group offline and disable its resources.
2. Remove the dependencies between the `mail` resource, the `logical_IP` resource, and the `mountshared` resource.
3. Bring the `iMS5` service group back online so the `sharedg` resource is available.

4. Delete all of the Veritas Cluster Server resources created during installation.
5. Stop the Veritas Cluster Server and remove following files on both nodes:

   ```
   /etc/VRTSvcs/conf/config/MsgSrvTypes.cf
   /opt/VRTSvcs/bin/MsgSrv/online
   /opt/VRTSvcs/bin/MsgSrv/offline
   /opt/VRTSvcs/bin/MsgSrv/clean
   /opt/VRTSvcs/bin/MsgSrv/monitor
   /opt/VRTSvcs/bin/MsgSrv/sub.pl
   ```

6. Remove the Messaging Server entries from the `/etc/VRTSvcs/conf/config/main.cf` file on both nodes.
7. Remove the `/opt/VRTSvcs/bin/MsgSrv/` directory from both nodes.

Unconfiguring Messaging Server HA Support for Sun Cluster 3.x

This section describes how to undo the HA configuration for Sun Cluster. This section assumes the simple example configuration (described in the Sun Cluster Agent Installation). For other configurations, the specific commands (for example, Step 3) may be different but will otherwise follow the same logical order.

1. Become the superuser.

   All of the following Sun Cluster commands require that you be running as user superuser.

2. Bring the resource group offline.

   To shut down all of the resources in the resource group, issue the command

   ```
   # scswitch -F -g MAIL-RG
   ```

   This shuts down all resources within the resource group (for example, the Messaging Server and the HA logical host name).

3. Disable the individual resources.

   Next, remove the resources one-by-one from the resource group with the commands:

   ```
   # scswitch -n -j mail-rs
   # scswitch -n -j disk-rs
   # scswitch -n -j budgie
   ```

4. Remove the individual resources from the resource group.

   Once the resources have been disabled, you may remove them one-by-one from the resource group with the commands:

   ```
   # scrgadm -r -j mail-rs
   # scrgadm -r -j disk-rs
   # scrgadm -r -j budgie
   ```

5. Remove the resource group.

   Once the all the resources have been removed from the resource group, the resource group itself may be removed with the command:

   ```
   # scrgadm -r -g MAIL-RG
   ```

6. Remove the resource types (optional).

   Should you need to remove the resource types from the cluster, issue the commands:

   ```
   # scrgadm -r -t SUNW.ims
   # scrgadm -r -t SUNW.HAStoragePlus
   ```

Chapter 4

Upgrading to Sun ONE Messaging Server

This chapter describes how to upgrade from Messaging Server 5.2 to 6.0.

NOTE You must first upgrade or migrate to Messaging Server 5.2 prior to upgrading to Sun ONE Messaging Server 6.0. You will not be able to directly upgrade or migrate to Messaging Server 6.0 from versions prior to 5.2. See the *iPlanet Messaging Server 5.2 Migration Guide* and *Installation Guide* for more information on migrating to Messaging Server 5.2.

There are three steps to upgrading from Messaging Server 5.2 to Messaging Server 6.0. following topics outline the process:

1. Creating Upgrade Files to Update your Configuration (`UpgradeMsg5toMsg6.pl`)
2. Running the Upgrade Utility (`do_the_upgrade.sh`)
   - MTA Configuration (`make_mta_config_changes.sh`)
   - configutil Parameters (`make_configutil_changes.sh`)
   - Backup Configuration (`make_backup_config_changes.sh`)
   - mboxlist Database (`make_mboxlistdb_changes.sh`)
3. Migrating User Mailboxes (optional)

NOTE Prior to performing the upgrade:

- Messaging Server 6.0 is installed and configured (with the instructions in Chapter 2, "Installing Messaging Server.") on either the same or a different system from the Messaging Server 5.2 system.
- Existing Messaging Server 5.2 installations are configured with MTA Direct LDAP Lookup not with `imsimta dirsync`. For more information, see the *Sun ONE Messaging Server 6.0 Administrator's Guide.*

Creating Upgrade Files to Update your Configuration

This section describes how special upgrade files are created in order to update your configuration on your Messaging Server 6.0 system:

Overview

Prior to running an upgrade utility to move from Messaging Server 5.2 to 6.0, you first need to run the `UpgradeMsg5toMsg6.pl` Perl script (located in *msg_svr_base*`/sbin`).

`UpgradeMsg5toMsg6.pl` compares your 5.2 configuration files with your 6.0 configuration files and creates to sets of files for each configuration file: `*.CHANGES` files and `*.MERGED` files.

The `*.CHANGES` files and `*.MERGED` files are generated in the workspace directory, `/var/tmp/UpgradeMsg5toMsg6.ScratchDir`.

The *.CHANGES files show critical configuration file differences between Messaging Server 5.2 and Messaging Server 6.0. These files highlight the configuration entities that are only found in Messaging Server 6.0, the configuration entities from Messaging Server 5.2 that are obsolete in Messaging Server 6.0, and the configuration entities that are only found in the Messaging Server 5.2. Note that not all *.CHANGES files will show differences between the versions of configuration files, and not all configuration files will generate *.CHANGES files.

The *.MERGED files are a consolidation of Messaging Server 5.2 and 6.0 configuration values and settings. In general, configuration parameter values from Messaging Server 5.2 are retained over the Messaging Server 6.0 version if:

- There is no default value in the Messaging Server 6.0 version, or
- The value specified in your 5.2 configuration is not a default setting.

Table 4-1 lists the configuration files that generate *.MERGED or *.CHANGES files:

Table 4-1 Messaging Server Configuration Files that Generate *.MERGED or *.CHANGES files

Configuration Information	Description	Generates *.MERGED File	Generates *.CHANGES File
job_controller.cnf	Job Controller File	**X**	**X**
conversions	Conversions File	**X**	
*channel*_option, where *channel* is an SMTP channel	SMTP channel option files	**X**	
native_option	Native channel option file (exception to *channel*_option)	**X**	**X**
*channel*_headers.opt, where *channel* is an SMTP channel	Header option files	**X**	
dispatcher.cnf	Dispatcher File	**X**	**X**
imta_tailor	Tailor File	**X**	**X**
option.dat	Global MTA Option File	**X**	**X**
aliases	Aliases File	**X**	

Table 4-1 Messaging Server Configuration Files that Generate `*.MERGED` or `*.CHANGES` files *(Continued)*

Configuration Information	Description	Generates *.MERGED File	Generates *.CHANGES File
`imta.cnf`	MTA Configuration File; only the include references (like file directory locations) are changed. Rewrite rule and channel settings are retained from your 5.2 configuration. To include LMTP in your imta.cnf, copy the LMTP information from your 6.0 imta.cnf file.	**X**	In some instances, a `*.CHANGES` file may be generated.
`mappings`	Mappings File	**X**	
`mappings.locale`	Localized Mappings File	**X**	
`internet.rules`	Internet Rule Configuration File	**X**	
`backup-groups.conf`	Backup Group Definitions	**X**	**X**
`configutil`	Changes of configuration parameters in `local.conf` and `msg.conf` configuration files.		**X**

Running the UpgradeMsg5toMsg6.pl Perl Script

To run the `UpgradeMsg5toMsg6.pl` to create sets of files by which you'll be able to update your configuration, follow these steps:

1. If your Messaging Server 5.2 and 6.0 versions are not on the same machine, transfer, extract and copy the Messaging Server 5.2 *server-root* directory to the Messaging Server 6.0 system. If your server versions are installed on the same machine, you can skip this step.

a. If your Message Store is too large to transfer from one system to another, you can unmount the disks from the 5.2 system and mount them onto the 6.0 system by using the `umount` (1M) and `mount` (1M) commands.

NOTE You don't have to copy the Messaging Server 5.2 store data to the Messaging Server 6.0 system, however, you must ensure that the Messaging Server 5.2 store data is accessible during the upgrade process.

b. Both your 5.2 and 6.0 systems can be running at this point.

2. Run the `UpgradeMsg5toMsg6.pl` upgrade script (located in *msg_svr_base*`/sbin`) against the `msg-`*instance* of 5.2 version and the *msg_svr_base* of the 6.0 version. For example:

```
perl UpgradeMsg5toMsg6.pl /usr/sunone/server5/msg-budgie \
  /opt/SUNWmsgsr
```

where `/usr/sunone/server5/msg-budgie` is the `msg-`*instance* of the 5.2 Messaging Server and `/opt/SUNWmsgsr` is the *msg_svr_base* of the 6.0 Messaging Server.

NOTE Messaging Server 6.0 does not support multiple instances. If you have multiple instances of Messaging Server version 5.2, you may only choose one instance to upgrade to Messaging Server 6.0. Furthermore, running the upgrade utility more than once in an attempt to migrate multiple instances will only result in you overwriting your configuration.

`*.MERGED` and `*.CHANGES` files (as described in Table 4-1) will be created.

3. Carefully review the `*.MERGED` files; if you don't want to use the suggested recommendations, you must manually adjust the settings.

This utility does not update the Messenger Express customization files. Therefore, you need to manually change these files in order to keep the relevant information from Messaging Server 5.2 and add any new information from the Messaging Server 6.0 installation.

Running the Upgrade Utility

This section describes the `do_the_upgrade.sh` utility (located in `/var/tmp/UpgradeMsg5toMsg6.ScratchDir`), a shell script that is made up of four sub-scripts. The following topics are covered in this section:

- Overview (`do_the_upgrade.sh`)
- MTA Configuration (`make_mta_config_changes.sh`)
- configutil Parameters (`make_configutil_changes.sh`)
- Backup Configuration (`make_backup_config_changes.sh`)
- mboxlist Database (`make_mboxlistdb_changes.sh`)

Overview

The `do_the_upgrade.sh` utility is made up of four shell scripts that, with your `*.MERGED` files, update the configuration and file directory locations of your MTA configuration, your configutil parameters, backup parameters, and your `mboxlist` database in your Messaging Server 6.0 system.

You can either run the `do_the_upgrade.sh` utility, or you can individually run one or more of the scripts that make up the `do_the_upgrade.sh` utility (`make_mta_config_changes.sh`, `make_configutil_changes.sh`, `make_backup_config_changes.sh`, and `make_mboxlistdb_changes.sh`).

To run the `do_the_upgrade.sh` utility:

```
# sh /var/tmp/UpgradeMsg5toMsg6.ScratchDir/do_the_upgrade.sh
```

NOTE When executing either the `do_the_upgrade.sh` utility or any of the sub-scripts, be sure that neither Messaging Server 5.2 nor 6.0 is up and running.

After running the do_the_upgrade.sh script, you can either continue to reference your 5.2 partition paths (though you will not be able to remove your Messaging Server 5.2 *server-root* directory) or you can manually move the 5.2 store partitions to the appropriate Messaging Server 6.0 directory location. You should perform this step prior to restarting Messaging Server.

MTA Configuration

The MTA upgrade configuration sub-script that makes up of part of the do_the_upgrade.sh utility is called make_mta_config_changes.sh (located in /var/tmp/UpgradeMsg5toMsg6.ScratchDir).

The make_mta_config_changes.sh script backs up, renames, and moves the *.MERGED server configuration files to their original names and locations within the Messaging Server 6.0 file directory structure.

Once the script has finished renaming and moving the files, it automatically runs the imsimta cnbuild command to recompile the MTA configuration.

NOTE If you want to upgrade an MTA relay machine from Messaging Server 5.2 to Messaging Server 6.0, you only need to run the make_mta_config_changes.sh and the make_backup_config_changes.sh (described in Backup Configuration).

configutil Parameters

The configutil upgrade configuration sub-script that makes up part of the do_the_upgrade.sh utility is called make_configutil_changes.sh script (located in /var/tmp/UpgradeMsg5toMsg6.ScratchDir).

The make_configutil_changes.sh script incorporates new or updated parameters in the msg.conf and local.conf files. If default values are not specified in configutil parameters in Messaging Server 6.0, any Messaging Server 5.2 values are carried forward to the Messaging Server 6.0 version.

Backup Configuration

The backup upgrade configuration sub-script that makes up part of the do_the_upgrade.sh utility is called make_backup_config_changes.sh script (located in /var/tmp/UpgradeMsg5toMsg6.ScratchDir).

The `make_backup_config_changes.sh` script upgrades the configuration of your backup services such as those in your `backup-groups.conf` file.

mboxlist Database

The `mboxlist` database upgrade configuration sub-script that makes up part of the `do_the_upgrade.sh` utility is called `make_mboxlistdb_changes.sh` script (located in `/var/tmp/UpgradeMsg5toMsg6.ScratchDir`).

The `make_mboxlistdb_changes.sh` script transfers and upgrades your 5.2 `mboxlist` database and upgrades it to the Messaging Server 6.0 directory structure. The script copies the four `*.db` files (`folder.db`, `quota.db`, `peruser.db`, and `subscr.db`) from *server-root*`/msg-`*instance*`/store/mboxlist` on your Messaging Server 5.2 system to *msg_svr_base*`/data/store/mboxlist` on your Messaging Server 6.0 system.

Migrating User Mailboxes

This section describes how to optionally migrate user mailboxes from your Messaging Server 5.2 system to your Messaging Server 6.0 system. If you have Messaging Server 5.2 and 6.0 installed on the same machine, you should not have to migrate your user mailboxes. Furthermore, if you are able to continue accessing the 5.2 machine where your user mailboxes are stored, you are not required to migrate your user mailboxes to your 6.0 machine. You only need to migrate your user mailboxes if you are no longer going to have access to your Messaging Server 5.2 machine.

To move user mailbox data from Messaging Server 5.2 to 6.0 in an online method, follow the steps described in this section. You should not need to bring the Messaging Server down while you move data.

The following topics are outlined:

Requirements

The only requirement for migration is stored running on both the old and new messaging servers.

Migration Instructions

To migrate your user mailboxes from your 5.2 system to your 6.0 system:

1. Notify users in advance that until data move process is completed, they do not have access to their mailboxes. Be sure that users log out of their mail systems before the data move takes place.

2. Change the `mailUserStatus` user LDAP attribute on all user entries on the 5.2 message store from `active` to `hold` in order to hold incoming users' messages in the hold queue and to prevent access to the mailboxes over IMAP, POP, and HTTP.

   For more information on `mailUserStatus`, see the *Sun ONE Messaging Server Schema Reference Manual*.

3. Be sure that both your 5.2 and 6.0 Messaging Servers are up and running during this process.

4. Change the `mailHost` attribute in all user entries from the old mail server to the new mail server.

   To do so, use the following `ldapsearch` command to find the user entries where the `mailHost` attribute needs to be modified:

```
ldapsearch -h ldap.siroe.com -b "o=internet" \
   "(&(objectclass=maildomain)(mailHost=oldmail.siroe.com))"
```

   Then, use the `ldapmodify` command to appropriately change the entries to the new mail server.

   For more information on `mailhost`, see the *Sun ONE Messaging Server Schema Reference Manual*.

5. On the old system (`oldmail.siroe.com`), split your user entries into equal groups (one user name per line) and place into user files

6. Move the user data from the Messaging 5.2 message store to the Messaging Server 6.0 message store. You only need to perform this step if:

   - you are migrating from windows to unix or from unix to windows.
   - you do not want to migrate the entire message store all at once.

- you need to rename your users, including uids, domain names, and default domain changes.

This step is accomplished by backing up the Messaging Server 5.2 message store with the `imsbackup` utility and restoring the message store to Messaging Server 6.0 with `imsrestore` utility.

If migration using the `imsbackup` and `imsrestore` utilities is the chosen method to transfer the store data, then the partition paths should not be mapped to the Messaging Server 5.2 partitions and the `mboxlist` upgrade step should not be performed. The `make_configutil_changes.sh` script generated by the upgrade script automatically sets the partition path to map to the Messaging Server 5.2 partitions. This need to be altered manually. In addition, you should not run the `make_mboxlistdb_changes.sh` script. The `do_the_upgrade.sh` script runs it automatically by default, so you must remove it manually.

See the *Sun ONE Messaging Server Reference Manual* for more information on syntax and usage of the `imsbackup` and `imsrestore` utilities.

Run this command on `newmail.siroe.com`:

```
rsh "ipaddress_of_oldmail.siroe.com  /server-root/bin/msg/store/bin/imsbackup \
  -f- -u user_file" | /opt/SUNWmsgsr/sbin/imsrestore -f- -cy -n -v1
```

where *user_file* is the user file described in Step 5 containing user mailbox names.

7. Using the user files, run multiple concurrent backup and restore sessions (between 10-15) to maximize the restore speed into the new message store.

8. Set Messaging Server 6.0 to be the new default messaging server for the system.

   Change the A record of `oldmail.siroe.com` to point to `newmail.siroe.com` (the server responsible for domain(s) previously hosted on `oldmail.siroe.com`).

9. Release the messages in the hold queue on your Messaging Server 5.2 system by issuing the following command:

```
imsimta process_held -uid=user -domain=domain
```

   where *user* is the user ID and *domain* is the domain where the user resides.

10. Ensure that the user clients are pointing to the new mail server.

    After the upgrade finishes, have the users point to the new server through their mail client program (in this example, have it point to `newmail.siroe.com` from `oldmail.siroe.com`).

    An alternative is to use an MMP which obviates the need to have users point their clients directly at the new mail server; the MMP will get that information from the `mailHost` attribute which is stored in the LDAP user entries and will automatically re-direct them to the new server.

Chapter 5

Performing Post-Installation Procedures

This chapter describes post-installation procedures you need to perform prior to starting Messaging Server. The following topics are described:

Post-Installation File Directory Layout

After you install Sun ONE Messaging Server, its directories and files are arranged in the organization depicted in Table 5-1. The table is not exhaustive; it shows only those directories and files of most interest for typical server administration tasks.

Table 5-1 Post-Installation Directories and Files

Directory	Default Location and Description
Messaging Server Base (*msg_svr_base*)	`/opt/SUNWmsgsr/` (default location)
	The directory on the Messaging Server machine dedicated to holding the server program, configuration, maintenance, and information files.
	Note that only one Messaging Server Base directory per machine is permitted.
Configuration `config`	*msg_svr_base*`/config/` (required location)
	Contains all of the Messaging Server configuration files such as the `imta.cnf` and the `msg.conf` files.
	On UNIX platforms only: This directory is symbolically linked to the `config` sub-directory of the data and configuration directory (default: `/var/opt/SUNWmsgsr/`) that you specified in the initial runtime configuration.
Log `log`	*msg_svr_base*`/log/`
	Contains the Messaging Server log files like the `mail.log_current` file.
	On UNIX platforms only: This directory is symbolically linked to the `log` sub-directory of the data and configuration directory (default: `/var/opt/SUNWmsgsr/`) that you specified in the initial runtime configuration.
Data `data`	*msg_svr_base*`/data/` (required location)
	Contains databases, configuration, log files, site-programs, queues, store and message files.
	The `data` directory includes the `config` and `log` directories.
	On UNIX platforms only: This directory is symbolically linked to the data and configuration directory (default: `/var/opt/SUNWmsgsr/`) that you specified in the initial runtime configuration.

Table 5-1 Post-Installation Directories and Files *(Continued)*

Directory	Default Location and Description
System Administrator Programs `sbin`	*msg_svr_base*`/sbin/` (required location) Contains the Messaging Server system administrator executable programs and scripts such as `imsimta`, `configutil`, `stop-msg`, `start-msg`, and `uninstaller`.
Library `lib`	*msg_svr_base*`/lib/` (required location) Contains shared libraries, private executable programs and scripts, daemons, and non-customizable content data files. For example: `imapd` and `qm_maint.hlp`.
SDK Include Files `include`	*msg_svr_base*`/include/` (required location) Contains Messaging header files for SDKs.
Examples `examples`	*msg_svr_base*`/examples/` (required location) Contains the examples for various SDKs, such as Messenger Express AUTH SDK.
Installation Data `install`	*msg_svr_base*`/install/` (required location) Contains installation-related data files such as installation log files, silent installation files, factory default configuration files, and the initial runtime configuration log files.

Modifying Your Configuration

After the Messaging Server installation and initial runtime configuration, you may choose to make some additional modifications to your configuration. For detailed information, see the *Sun ONE Messaging Server Administrator's Guide*.

Passwords

Because you set up a number of administrators with the same password in Step 10 Password for administrator accounts (See Create the Initial Messaging Server Runtime Configuration), you might want to change the passwords of those administrators.

Refer to Table 5-2, which shows the parameters where default passwords are set up during initial runtime configuration and the utilities you can use to change them. For those parameters that use the `configutil` utility to change passwords, see the *Sun ONE Messaging Server Reference Manual* for complete syntax and usage.

Table 5-2 Passwords Set in Messaging Server Initial Runtime Configuration

Parameter	Description
`local.ugldapbindcred`	Password for the user / group administrator set through the `configutil` utility.
`local.service.pab.ldappasswd`	Password for user specified by Bind DN for PAB searches set through the `configutil` utility.
SSL passwords for keyfiles	Passwords that are directly set in the `sslpassword.conf` file.
Service Administrator Credentials	These are credentials that are directly set in your LDAP Directory (with the `ldapmodify` command).
Service Administrator for Sun ONE Delegated Administrator	You will only need to change the password of this administrator if you have enabled Sun ONE LDAP Schema, v.1 and you are using the Sun ONE Delegated Administrator utility. To change the password of the Delegated Administrator Service Administrator, you can do so in the Sun ONE Console, your LDAP Directory (with the `ldapmodify` command), or the Delegated Administrator UI.
Store Administrator	To change the password of the Store Administrator, you can do so in either the Sun ONE Console or in your LDAP Directory (with the `ldapmodify` command).

The following example uses the `local.enduseradmincred configutil` parameter to change the password of the end user administrator.

```
configutil -o local.enduseradmincred -v newpassword
```

Port Numbers

In the installation and initial runtime configuration programs, port numbers will be chosen for various services. These port numbers can be any number from 1 to 65535.

Table 5-3 lists the port numbers that are designated after installation:

Table 5-3 Port Numbers Designated During Installation

Port Number	Service
389	Standard Directory Server LDAP Port on the machine where you install Directory Server. (This port is specified in the Directory Server installation program)
110	Standard POP3 Port (This port may conflict with the MMP port if installed on the same machine)
143	Standard IMAP4 Port (This port may conflict with the MMP port if installed on the same machine)
25	Standard SMTP Port
80	Messenger Express HTTP Port (This port may conflict with the Web Server port if installed on the same machine.)
992	POP3 over SSL port (For encrypted communications)
993	IMAP over SSL Port (For encrypted communications) (This port may conflict with the MMP port if installed on the same machine)
443	HTTP over SSL Port (For encrypted communications)
7997	Messaging and Collaboration ENS (Event Notification Service) Port
27442	Port that is used Job Controller for internal product communication.

Table 5-3 Port Numbers Designated During Installation *(Continued)*

Port Number	Service
49994	Port that is used by the Watcher for internal product communication. See the *Sun ONE Messaging Server 6.0 Administrator's Guide* for more information on the Watcher.
user-specified	Administration Server HTTP Port (For listening to Sun ONE Console requests)

If certain products are installed on the same machine, you will encounter port number conflicts. Table 5-4 shows potential port number conflicts:

Table 5-4 Potential Port Number Conflicts

Conflicting Port Number	Port	Port
143	IMAP Server	MMP IMAP Proxy
110	POP3 Server	MMP POP3 Proxy
993	IMAP over SSL	MMP IMAP Proxy with SSL
80	Identity Server (Web Server port)	Messenger Express

If possible, it is recommended that you install products with conflicting port numbers on separate machines. If you are unable to do so, then you will need to change the port number of one of conflicting products.

To change port numbers, use the `configutil` utility. See the *Sun ONE Messaging Server Reference Manual* for complete syntax and usage.

The following example uses the `service.http.port configutil` parameter to change the Messenger Express HTTP port number to `8080`.

```
configutil -o service.http.port -v 8080
```

Managing Messaging Server with Sun ONE Console

When the messaging server installation process and initial runtime configuration program completes, you can start your Messaging server through the Sun ONE Console. If your directory and messaging server reside on a single machine, you can use the Console interface to manage both servers.

To invoke the console, run the `/usr/sbin/mpsconsole` command.

For more information on running Messaging Server through the Console, see the *Sun ONE Messaging Server Administrator's Guide* and the *Sun ONE Messaging Server Administrator's Online Help* which can be invoked through the Console.

SMTP Blocking

By default, Messaging Server is configured to block attempted SMTP relays; that is, it rejects attempted message submissions to external addresses from unauthenticated external sources (external systems are any other system than the host on which the server itself resides). This default configuration is quite aggressive in blocking SMTP relaying in that it considers all other systems to be external systems.

After installation, it is important to manually modify your configuration to match the needs of your site. Specifically, your messaging server should recognize its own internal systems and subnets from which SMTP relaying should always be accepted. If you do not update this configuration, you might encounter problems when testing your MTA configuration.

IMAP and POP clients that attempt to submit messages via the Messaging Server system's SMTP server destined for external addresses, and who do not authenticate using SMTP AUTH (SASL), will find their submission attempts rejected. Which systems and subnets are recognized as internal is typically controlled by the INTERNAL_IP mapping table, which may be found in the file *msg_svr_base*`/config/mappings`.

For instance, on a Messaging Server system whose IP address is `192.45.67.89`, the default INTERNAL_IP mapping table would appear as follows:

```
INTERNAL_IP

  $(192.45.67.89/24)  $Y
  127.0.0.1  $Y
  *  $N
```

The initial entry, using the `$(IP-pattern/significant-prefix-bits)` syntax, is specifying that any IP address that matches the first 24 bits of `192.45.67.89` should match and be considered internal. The second entry recognizes the loopback IP address `127.0.0.1` as internal. The final entry specifies that all other IP addresses should not be considered internal.

You may add additional entries by specifying additional IP addresses or subnets before the final $N entry. These entries must specify an IP address or subnet (using the $(.../...) syntax to specify a subnet) on the left side and $Y on the right side. Or you may modify the existing $(.../...) entry to accept a more general subnet.

For instance, if this same sample site has a class-C network, that is, it owns all of the `192.45.67.0` subnet, then the site would want to modify the initial entry so that the mapping table appears as follows:

```
INTERNAL_IP

  $(192.45.67.89/24)  $Y
  127.0.0.1  $Y
  *  $N
```

Or if the site owns only those IP addresses in the range 192.45.67.80-192.45.67.99, then the site would want to use:

```
INTERNAL_IP

  ! Match IP addresses in the range 192.45.67.80-192.45.67.95
  $(192.45.67.80/28)  $Y
  ! Match IP addresses in the range 192.45.67.96-192.45.67.99
  $(192.45.67.96/30)  $Y
  127.0.0.1  $Y
  *  $N
```

Note that the *msg_svr_base*/sbin/imsimta test -match utility can be useful for checking whether an IP address matches a particular $(.../...) test condition. The imsimta test -mapping utility can be more generally useful in checking that your INTERNAL_IP mapping table returns the desired results for various IP address inputs.

After modifying your INTERNAL_IP mapping table, be sure to issue the *msg_svr_base*/sbin/imsimta cnbuild and the *msg_svr_base*/sbin/imsimta restart utilities so that the changes take effect.

Further information on the mapping file and general mapping table format, as well as information on imsimta command line utilities, can be found in the *Sun ONE Messaging Server Reference Manual*. In addition, information on the INTERNAL_IP mapping table can be found in the *Sun ONE Messaging Server Administrator's Guide*.

Enabling Start-up Across Reboots

You can enable Messaging Server start-up across system reboots by using the bootup script: *msg_svr_base*/lib/SunONE_MsgSvr. In addition, this script can start up your MMP, if enabled.

To enable SunONE_MsgSvr:

1. Copy the SunONE_MsgSvr script into the /etc/init.d directory.

2. Change the following ownerships and access modes of the SunONE_MsgSvr script:

Table 5-5 Ownership and Access Mode Changes to SunONE_MsgSvr

Ownership (chown(1M))	Group Ownership (chgrp(1M))	Access Mode (chmod(1M))
root (superuser)	sys	744

3. Go to the /etc/init.d/rc2.d and create the following symbolic link:

```
ln /etc/init.d/SunONE_MsgSvr S92SunONE_MsgSvr
```

4. Go to the /etc/init.d/rc0.d directory and create the following symbolic link:

```
ln /etc/init.d/SunONE_MsgSvr K08SunONE_MsgSvr
```

Handling sendmail Clients

If end users send messages through sendmail clients, you can configure Messaging Server to work with those clients over protocol. Users can continue to use the UNIX sendmail client.

To create compatibility between sendmail clients and Messaging Server, you can create and modify a sendmail configuration file.

NOTE Each time a new sendmail patch is applied to your system, you will need to modify the submit.cf file as described in the following instructions for Solaris 8 and Solaris 9.

Solaris 8

On Solaris 8 operating systems, follow these steps:

1. Find the file main-v7sun.mc file in directory /usr/lib/mail/cf and create a copy of this file.

   In the example in this section, a copy called sunone-msg.mc is created.

2. In the sunone-msg.mc file, add the following lines before the MAILER macros:

```
FEATURE('nullclient', 'smtp:rhino.west.sesta.com')dnl
MASQUERADE_AS('west.sesta.com')dnl
define('confDOMAIN_NAME', 'west.sesta.com')dnl
```

Note that rhino.west.sesta.com is the localhost name and west.sesta.com is the default email domain as described in Step 11 Default Email Domain in Create the Initial Messaging Server Runtime Configuration. In an HA environment, use the logical host name. See Chapter 3, "Configuring High Availability Solutions" for more information about logical host names for High Availability.

3. Compile the sunone-msg.mc file:

```
/usr/ccs/bin/make sunone-msg.cf
```

The sunone-msg.mc will output sunone-msg.cf.

4. Make a backup copy of the existing sendmail.cf file located in the /etc/mail directory.

   a. Copy and rename /usr/lib/mail/cf/sunone-msg.cf to sendmail.cf file.

   b. Move the new sendmail.cf file to /etc/mail directory.

Solaris 9

On Solaris 9 platforms, sendmail is no longer a setuid program. Instead, it is a a setgid program.

To create the sendmail configuration file on Solaris 9 platforms:

1. Find the file submit.mc file in directory /usr/lib/mail/cf and create a copy of this file.

   In the example in this section, a copy called sunone-submit.mc is created.

2. Change the following line in the file `sunone-submit.mc`:

```
FEATURE('msp')dn
```

to

```
FEATURE('msp', 'rhino.west.sesta.com')dnl
```

where `rhino.west.sesta.com` is the localhost name.

Note that `rhino.west.sesta.com` is the localhost name and `west.sesta.com` is the default email domain as described in Step 11 Default Email Domain in Create the Initial Messaging Server Runtime Configuration. In an HA environment, use the logical host name. See Chapter 3, "Configuring High Availability Solutions" for more information about logical host names for High Availability.

3. Compile the `sunone-submit.mc` file:

```
/usr/ccs/bin/make sunone-submit.cf
```

The `sunone-submit.mc` will output `sunone-submit.cf`.

4. Make a backup copy of the existing `submit.cf` file in `/etc/mail` directory.
   a. Copy and rename `/usr/lib/mail/cf/sunone-submit.cf` file to `submit.cf` file.
   b. Move the new `submit.cf` file to the `/etc/mail` directory.

Configuring Messenger Express Mail Filters

To install the mail filters, follow these steps:

1. When you installed Messaging Server (using the directions in Chapter 2, "Installing Messaging Server"), the mail filter package (`SUNWmsgmf`) was one of many Messaging Server packages that you installed.

   Verify that the `MailFilter.war` file, which implements management of sieve filters, is in the *msg_svr_base*`/SUNWmsgmf` directory.

2. Be sure that Sun ONE Web Server 6.1 is already installed and configured through the Java Enterprise System installer.

NOTE Web Server needs to be installed on the same system where Messenger Express is configured.

3. Set the environment variable `IWS_SERVER_HOME` to the Web Server installation root directory. For example:

```
setenv IWS_SERVER_HOME webserver_install_root
```

4. Issue the following Web Server command:

```
web_svr_base/bin/https/httpadmin/bin/wdeploy deploy -u /MailFilter -i \
     https-vs_id -v https-vs_id msg_svr_base/SUNWmsgmf/MailFilter.war
```

   where *web_svr_base* is the web server root directory, *vs_id* is the virtual server ID of the web server, and *msg_svr_base* is the messaging root directory.

   Refer to the Web Server documentation for detailed information on the `wdeploy` command.

   When you have completed installing the mail filters, a `MailFilter` directory will be placed in the Web Server's `docs` directory.

5. Use the `configutil` utility to set the following option:

   `local.webmail.sieve.port` = *port*

   where *port* is the Web Server port number.

6. Stop and restart the HTTP daemon:

```
# msg_svr_base/sbin/stop-msg http
# msg_svr_base/sbin/start-msg http
```

Refer to the *Sun ONE Messenger Express Customization Guide* for mail filter usage information.

7. If you want to delete the `*.war` file in order to install a new version of it, use the following command:

```
web_svr_base/bin/https/httpadmin/bin/wdeploy delete -u /MailFilter -i https-vs_id
-v https-vs_id -n hard
```

where *web_svr_base* is the web server root directory and *vs_id* is the virtual server ID of the web server.

NOTE With the `-n` option, you have the choice of specifying a `hard` or `soft` value. If you use the `hard` value, it denotes a hard delete and the mail filter is physically removed. The `hard` value should only be used when the new `*.war` file is available.

Refer to the Web Server documentation for detailed information on the `wdeploy` command.

Appendix A

Installation Worksheets

This appendix provides worksheets by which you can plan your installation. The following worksheets are included:

- Directory Server Installation
- Administration Server Initial Runtime Configuration
- Directory Server Setup Script (comm_dssetup.pl)
- Messaging Server Initial Runtime Configuration

Directory Server Installation

You installed Directory Server through the Java Enterprise System installer or through a previous installation. Record your Directory Server installation and configuration parameters in Table A-1. You will need these parameters when you install and configure the Administration and Messaging servers.

Table A-1 Directory Server Installation Parameters

Parameter:	Description:	Example:	Used in:	Your Answers:
Directory Installation Root	A directory on the directory server machine dedicated to holding the server program, configuration, maintenance, and information files.	`/var/mps/serverroot/`	`comm_dssetup.pl` Perl script See Prepare Directory Server for Messaging Server Configuration.	
Host	The host name is the IP host name, which might be either a “short-form” host name (for example, `fiddle`) or a fully qualified host name. The fully qualified host name consists of two parts: the host name and the domain name.	`fiddle.west.sesta.com`	Administration Server Configuration See Prepare Directory Server for Messaging Server Configuration.	
LDAP Directory Port Number	The default for and LDAP directory server is 389.	389	Administration Server Configuration and Messaging Server Configuration See Prepare Directory Server for Messaging Server Configuration and Create the Initial Messaging Server Runtime Configuration	

Parameter:	Description:	Example:	Used in:	Your Answers:
Administrator ID and Password	Administrator in charge or responsible for configuration information. Password for the Administrator	`Admin` `PaSsWoRd`	Administration Server Configuration See Prepare Directory Server for Messaging Server Configuration.	
User and Group Tree Suffix	The distinguished name of the LDAP entry at the top of the directory tree, below which user and group data is stored.	`o=usergroup`	`comm_dssetup.pl` Perl script See Prepare Directory Server for Messaging Server Configuration.	
Directory Manager DN and Password	The privileged directory administrator, comparable to the superuser user in UNIX. Typically, this administrator is responsible for user and group data. Password for the Directory Manager.	`cn=Directory Manager` `pAsSwOrD`	`comm_dssetup.pl` Perl script and Messaging Server Configuration See Prepare Directory Server for Messaging Server Configuration and Create the Initial Messaging Server Runtime Configuration.	
Administration Domain	A region of administrative control.	`System Lab`	Administration Server Configuration See Prepare Directory Server for Messaging Server Configuration.	

Administration Server Initial Runtime Configuration

When you run the Administration Server initial runtime configuration program through the Java Enterprise System installer, record your installation parameters in Table A-2. You will need some of these parameters for the Messaging Server initial runtime configuration. You might also refer to your Directory Server Installation checklist to answer certain questions.

Table A-2 Administration Server Initial Runtime Configuration Program Parameters

Parameter	Description	Example	Your Answers:
Fully Qualified Domain Name	Fully Qualified domain for the host machine.	`fiddle.west.sesta.com`	
Server Root Definition	Installation Root of the Administration Server dedicated to holding the server program, configuration, maintenance, and information files.	`/var/mps/serverroot`	
UNIX System User	Certain privileges designated to system users to ensure they have appropriate permissions for the processes they are running.	`inetuser`	
UNIX System Group	The group to which certain UNIX System users belong.	`inetgroup`	
Configuration Directory Server	Host and Port specified during Directory Server Installation.	Host `fiddle.west.sesta.com` Port 389	
Configuration Directory Server Administrator and Password	Administrator ID specified during Directory Server Installation. Password of Administrator ID	`Admin` PaSsWoRd	

Table A-2 Administration Server Initial Runtime Configuration Program Parameters

Parameter	Description	Example	Your Answers:
Administration Domain	A region of administrative control. If you have installed Messaging Server and Directory Server on the same machine, then you should choose the same Administration Domain in Directory Server Installation.	System Lab2	
Administrative Server Port	A unique port number dedicated to the Administration Server.	5555	

Directory Server Setup Script (comm_dssetup.pl)

When you run the Directory Server Setup script (`comm_dssetup.pl`) to prepare Directory Server for Messaging Server configuration, record your installation parameters in Table A-3. You will need some of these parameters for the Messaging Server initial runtime configuration.

Table A-3 `comm_dssetup.pl` Script Parameters

Parameter	Description	Example	Your Answers:
Server Root	Installation Root of the Directory Server dedicated to holding the server program, configuration, maintenance, and information files.	`/var/mps/serverroot/`	
Server Instance	LDAP Directory Server daemon or service that is responsible for most functions. In certain deployments, you might dedicate an instance for maintaining users and groups and maintain a separate instance for configuration.	`slapd-varrius`	
DC Root	If you want to have a two-tree DIT provisioning model (Sun ONE LDAP Schema, v.1 or Sun ONE LDAP Schema, v.2 (compatibility mode), the DC Tree mirrors the local DNS structure and is used by the system as an index to the Organization Tree that contain the user and group data entries.	`o=internet`	
User and Group Base Suffix	Top entry in the Organization Tree which holds the namespace for user and group entries.	`o=usergroup`	

Table A-3 `comm_dssetup.pl` Script Parameters *(Continued)*

Parameter	Description	Example	Your Answers:
Directory Manager DN and Password	Administrator who is responsible for the user and group data in the Organization Tree. Should be the same as what was specified in Run the Java Enterprise System Installer and Sun ONE Messaging Server. Password of Directory Manager DN	`cn=Directory Manager` pAsSwOrD	

Messaging Server Initial Runtime Configuration

When you run the Messaging Server initial runtime configuration program, record your installation parameters in Table A-4. You might also refer to your Directory Server Installation checklist to answer certain questions.

Table A-4 Messaging Server Initial Runtime Configuration Program Parameters

Parameter	Description	Example	Your Answers:
Configuration and Data Directory	Contains all of the Messaging Server configuration files. The *msg_svr_base*/data directory is symbolically linked to this directory.	/var/opt/SUNWmsgsr	
UNIX System User	Certain privileges designated to system users to ensure they have appropriate permissions for the processes they are running. This system user should not be the same user that you specified in the Administration Server Initial Runtime Configuration.	mailsrv	
UNIX System Group	The group to which certain UNIX System users belong.This system group should not be the same group that you specified in the Administration Server Initial Runtime Configuration.	mail	
Configuration Directory LDAP URL, Directory Manager, and Password	Configuration Directory Server, LDAP URL, Bind DN, and Password	ldap://fiddle.west.sesta.com:389 cn=Directory Manager PaSsWoRd	
User and Group Directory LDAP URL, Directory Manager, and Password	User and Group Directory Server, LDAP URL, Bind DN, and Password. It is recommended that you have a separate User and Group directory from your Configuration directory.	ldap://fiddle.west.sesta.com:389 cn=Directory Manager PaSsWoRd	

Table A-4 Messaging Server Initial Runtime Configuration Program Parameters

Parameter	Description	Example	Your Answers:
Postmaster Email Address	Email address of the administrator who will monitor postmaster mail. Address must be a fully qualified address, and must be valid, in that there is a mailbox associated with the address.	`pma@siroe.com`	
Password for Administrator Accounts	Password that will be used for service administrator, user/group administrator, end user administrator privileges as well as PAB administrator and SSL passwords.	`paSSwoRD`	
Default Email Domain	The email default that is used if no domain is specified	`siroe.com`	
Organization Name for Default Email Domain	An organization name under which your organization will reside and is used to construct the organization tree.	For example if your organization name is `Engineering`, all the users for `siroe.com` (your default email domain) will be placed under the LDAP DN `o=Engineering, o=usergroup` Your user and group directory suffix was specified in `comm_dssetup.pl`.	

Glossary

A record A type of DNS record containing a host name and its associated IP address. A records are used by messaging servers on the Internet to route email. See also **Domain Name System (DNS)**, **MX record**.

access control A method for controlling access to a server or to folders and files on a server.

access control entry (ACE) A single item of information from an access control list. Also called access control information

access control information (ACI) Information from an access control entry. See also **access control entry**.

access control list (ACL) A set of data associated with a directory that defines the permissions that users and / or groups have for accessing it. ACLs are comprised of one or more ACEs.

access control rules Rules specifying user permissions for a given set of directory entries or attributes.

access domain Limits access to certain Messaging Server operations from within a specified domain. For example, an access domain can be used to limit where mail for an account can be collected.

account Information that defines a specific user or user group. This information includes the user or group name, valid email address or addresses, and how and where email is delivered.

address Information in an email message that determines where and how the message must be sent. Addresses are found both in message headers and in message envelopes. Envelope addresses determine how the message gets routed and delivered; header addresses are present merely for display purposes.

address handling The actions performed by the MTA to detect errors in addressing, to rewrite addresses if necessary, and to match addresses to recipients.

addressing protocol The addressing rules that make email possible. RFC 822 is the most widely used protocol on the Internet and the protocol supported by Messaging Server. Other protocols include X.400 and UUCP (UNIX to UNIX Copy Protocol).

address token The address element of a rewrite rule pattern.

administration console See **Console**.

administration domain A region of administrative control. See also **domain**.

administration privileges A set of privileges that define a users administrative role.

administration server administrator User who has administrative privileges to start or stop a server even when there is no Directory Server connection. The administration server administrator has restricted server tasks (typically only Restart Server and Stop Server) for all servers in a local server group. When an administration server is installed, this administrator's entry is automatically created locally (this administrator is not a user in the user directory).

administrator A user with a defined set of administrative privileges. See also **configuration administrator**, **Directory Manager**, **administration server administrator**, **server administrator**, **message store administrator**, **top-level administrator**, **domain administrator**, **organization administrator**, **family group administrator**, **mail list owner**.

alias An alternate name of an email address.

alias file A file used to set aliases not set in a directory, such as the postmaster alias.

Allow filter A Messaging Server access-control rule that identifies clients that are to be allowed access to one or more of the following services: POP, IMAP, or HTTP. See also **Deny filter**.

allowed attributes The attributes that optionally can be present in entries using a particular object class, but are not required to be present. See also **attributes**, **required attributes**.

alternate address A secondary address for an account, generally a variation on the primary address. In some cases it is convenient to have more than one address for a single account.

APOP Authenticated Post Office Protocol. Similar to the Post Office Protocol (POP), but instead of using a plaintext password for authentication, it uses an encoding of the password together with a challenge string.

attributes LDAP data is represented as attribute-value pairs. Any specific piece of information is associated with a descriptive attribute. See also **allowed attributes**, **required attributes**.

AUTH An SMTP command enabling an SMTP client to specify an authentication method to the server, perform an authentication protocol exchange, and, if necessary, negotiate a security layer for subsequent protocol interactions.

authentication (1) The process of proving the identity of a client user to Messaging Server. (2) The process of proving the identity of Messaging Server to a client or another server.

authentication certificate A digital file sent from server to client or client to server to verify and authenticate the other party. The certificate ensures the authenticity of its holder (the client or server). Certificates are not transferable.

autoreply option file A file used for setting options for autoreply, such as vacation notices.

AutoReply utility A utility that automatically responds to messages sent to accounts with the AutoReply feature activated. Every account in Messaging Server can be configured to automatically reply to incoming messages.

backbone The primary connectivity mechanism of a distributed system. All systems that have connectivity to an intermediate system on the backbone are connected to each other. This does not prevent you from setting up systems to bypass the backbone for reasons of cost, performance, or security.

backend server An email server whose only function is to store and retrieve email messages. Also called a message store server.

backup The process of backing up the contents of folders from the message store to a backup device. See also **restore**.

banner A text string displayed by a service such as IMAP when a client first connects to it.

base DN A distinguished name entry in the directory from which searches will occur. Also known as a search base. For example, `ou=people, o=siroe.com`.

Berkeley DB A transactional database store intended for high-concurrency read-write workloads, and for applications that require transactions and recoverability. Messaging Server uses Berkeley databases for numerous purposes.

bind DN A distinguished name used to authenticate to the Directory Server when performing an operation.

body One part of an email message. Although headers and envelopes must follow a standard format, the body of the message has a content determined by the sender—the body can contain text, graphics, or even multimedia. Structured bodies follow the MIME standard.

class path A path to directories and `.jar` files needed to run the servlet engine and servlet templates.

capability A string, provided to clients, that defines the functionality available in a given IMAP service.

CA Certificate Authority. An organization that issues digital certificates (digital identification) and makes its public key widely available to its intended audience.

Certificate Authority See **CA**.

certificate-based authentication Identification of a user from a digital certificate submitted by the client. See also **password authentication**.

certificate database A file that contains a server's digital certificate(s). Also called a certificate file.

certificate name The name that identifies a certificate and its owner.

channel The fundamental MTA component that processes a message. A channel represents a connection with another computer system or group of systems. Each channel consists of one or more channel programs and an outgoing message queue for storing messages that are destined to be sent to one or more of the systems associated with the channel. See also **channel block**, **channel host table, channel program**.

channel block A single channel definition. See also **channel host table**.

channel host table The collective set of channel definitions.

channel program Part of a channel that performs the following functions: (1) transmits messages to remote systems and deletes messages from the queue after they are sent and (2) accepts messages from remote systems placing them in the appropriate channel queues. See also **master channel program**, **slave channel program**.

cipher An algorithm used in encryption.

ciphertext Text that has been encrypted. Opposite of **cleartext**.

client A software entity that requests services or information from a server.

CNAME record A type of DNS record that maps a domain name alias to a domain name.

cleartext Unencrypted text.

CLI See **command line interface**.

client-server model A computing model in which networked computers provide specific services to other client computers. Examples include the name-server / name-resolver paradigm of the DNS and file-server / file-client relationships such as NFS and diskless hosts.

cn LDAP alias for common name.

command line interface Command that can be executed from the command-line. Also called utility.

comm_dssetup.pl A Directory Server preparation tool that makes an existing Directory Server ready for use by an Messaging Server.

comment character A character that, when placed at the beginning of a line, turns the line into a nonexecutable comment.

configuration administrator Person who has administrative privileges to manage servers and configuration directory data in the entire topology. The configuration administrator has unrestricted access to all resources in the topology. This is the only administrator who can assign server access to other administrators. The configuration administrator initially manages administrative configuration until the administrators group and its members are in place.

Configuration Directory Server A Directory Server that maintains configuration information for a server or set of servers.

configuration file A file that contains the configuration parameters for a specific component of the Messaging system.

congestion thresholds A disk space limit that can be set by the system administrator that prevents the database from becoming overloaded by restricting new operations when system resources are insufficient.

Console A GUI (graphical user interface) that enables you to configure, monitor, maintain, and troubleshoot many components.

cookie Text-only strings entered into the browser's memory automatically when you visit specific web sites. Cookies are programmed by the web page author. Users can either accept or deny cookies. Accepting the cookies allows the web page to load more quickly and is not a threat to the security of your machine.

CRAM-MD5 A lightweight standards track authentication mechanism documented in RFC 2195. It provides a fast (albeit somewhat weaker) alternative to TLS (SSL) when only the user's login password needs to be protected from network eavesdroppers.

cronjob UNIX only. A task that is executed automatically by the cron daemon at a configured time. See also **crontab file**.

crontab file UNIX only. A list of commands, one per line, that executes automatically at a given time.

daemon A UNIX program that runs in the background, independent of a terminal, and performs a function whenever necessary. Common examples of daemon programs are mail handlers, license servers, and print daemons. On Windows NT machines, this type of program is called a service. See also **service**.

data store A store that contains directory information, typically for an entire directory information tree.

DC Tree Domain Component tree. A directory information tree that mirrors the DNS network syntax. An example of a distinguished name in a DC Tree would be `cn=billbob,dc=bridge,dc=net,o=internet`.

defragmentation The Multipurpose Internet Mail Extensions (MIME) feature that enables a large message that has been broken down into smaller messages or fragments to be reassembled. A Message Partial Content-Type header field that appears in each of the fragments contains information that helps reassemble the fragments into one message. See also **fragmentation**.

Delegated Administrator Console A web browser-based software console that allows domain administrators to add and modify users and groups to a hosted domain. Also allows end users to change their password, set message forwarding rules, set vacation rules, and list mail list subscriptions.

Delegated Administrator for Messaging and Collaboration. A set of interfaces (GUI and utilities) that allow domain administrators to add and modify users and groups to a hosted domain.

delegated administrator server A daemon program that handles access control to the directory by hosted domains.

delete message The act of marking a message for deletion. The deleted message is not removed from the message store until it is expunged or purged in a separate action by the user. See also **purge message**, **expunge message**.

delivery See **message delivery**.

delivery status notification A message giving status information about a message in route to a recipient. For example, a message indicating that delivery has been delayed because of network outages.

denial of service attack A situation where an individual intentionally or inadvertently overwhelms your mail server by flooding it with messages. Your server's throughput could be significantly impacted or the server itself could become overloaded and nonfunctional.

Deny filter A Messaging Server access-control rule that identifies clients that are to be denied access to one or more of the following services: POP, IMAP, or HTTP. See also **Allow filter**.

dereferencing an alias Specifying, in a bind or search operation, that a directory service translate an alias distinguished name to the actual distinguished name of an entry.

DIGEST-MD5 A lightweight standards track authentication mechanism that is more secure then CRAM-MD5. Documented in RFC 2831 which also provides an option to protect the entire connection without the setup overhead of TLS (SSL).

directory context The point in the directory tree information at which a search begins for entries used to authenticate a user and password for message store access. See also **base DN**.

directory entry A set of directory attributes and their values identified by its distinguished name. Each entry contains an object class attribute that specifies the kind of object the entry describes and defines the set of attributes it contains.

directory information tree The tree-like hierarchical structure in which directory entries are organized. Also called a DIT. DITs can be organized along the DNS (DC Trees) or Open Systems Interconnect networks (OSI trees).

directory lookup The process of searching the directory for information on a given user or resource, based on that user or resource's name or other characteristic.

Directory Manager User who has administrative privileges to the directory server database. Access control does not apply to this user (think of the directory manager as the directory's superuser).

directory schema The set of rules that defines the data that can be stored in the directory.

Directory Server The directory service based on LDAP. See also **directory service**, **Lightweight Directory Access Protocol**, **Configuration Directory Server**, **User/Groups Directory Server**.

directory service A logically centralized repository of information about people and resources within an organization. See also **Lightweight Directory Access Protocol**.

directory synchronization The process of updating—that is, synchronizing—the MTA directory cache with the current directory information stored in the directory service. See also **MTA directory cache**.

disconnected state The mail client connects to the server, makes a cache copy of selected messages, then disconnects from the server.

Dispatcher The MTA component that handles connection requests for defined TCP ports. The Dispatcher is a multi-threaded connection dispatching agent that permits multiple multi-threaded servers to share responsibility for a given service. When using the Dispatcher, it is possible to have several multi-threaded SMTP server processes running concurrently.

distinguished name The comma-separated sequence of attributes and values that specify the unique location of an entry within the directory information tree. Often abbreviated as DN.

distribution list See **mail list**.

distribution list owner See **mail list owner**.

DIT See **directory information tree**.

DN See **distinguished name**.

dn LDAP alias for distinguished name. See also **distinguished name**.

DNS See **Domain Name System**.

DNS alias A host name that the DNS server recognizes as pointing to a different host—specifically a DNS CNAME record. Machines always have one real name, but they can have one or more aliases. For example, `www.siroe.domain` might be an alias that points to a real machine called `realthing.siroe.domain` where the server currently exists.

DNS database A database of domain names (host names) and their corresponding IP addresses.

DNS domain A group of computers whose host names share a common suffix, the domain name. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by periods (dots), for example, `corp.mktng.siroe.com`. See also **domain**.

DNS spoofing A form of network attack in which a DNS server has been subverted to provide false information.

document root A directory on the server machine that contains files, images, and data that will be displayed to users accessing Web Server.

domain Resources under control of a single computer system. See also **administration domain**, **DNS domain**, **hosted domain**, **virtual domain**.

domain administrator User who has administrative privileges to create, modify, and delete mail users, mail lists, and family accounts in a hosted domain by using the Delegated Administrator for Messaging and Collaboration GUI or CLIs. By default, this user can act as a message store administrator for all messaging servers in the topology.

domain alias A domain entry that points to another domain. By using aliases, hosted domains can have several domain names.

domain hosting The ability to host one or more domains on a shared messaging server. For example, the domains `siroe.com` and `sesta.org` might both be hosted on the `siroe.net` mail server. Users send mail to and receive mail from the hosted domain—the name of the mail server does not appear in the email address.

domain name (1) A host name used in an email address. (2) A unique name that defines an administrative organization. Domains can contain other domains. Domain names are interpreted from right to left. For example, `siroe.com` is both the domain name of the Siroe Company and a subdomain of the top-level `com` domain. The `siroe.com` domain can be further divided into subdomains such as `corp.siroe.com`, and so on. See also **host name**, **fully-qualified domain name**.

Domain Name System (DNS) A distributed name resolution software that allows computers to locate other computers on a network or the Internet by domain name. The system associates standard IP addresses with host names (such as `www.siroe.com`). Machines normally get this information from a DNS server. DNS servers provide a distributed, replicated, data query service for translating hostnames into Internet addresses. See also **A record**, **MX record**, **CNAME record**.

domain organization A sub-domain below a hosted domain in the Organization Tree. Domain organizations are useful for companies that wish to organize their user and group entries along departmental lines. (Used in Delegated Administrator for Messaging and Collaboration). See also **suborganization.**

domain part The part of an email address to the right of the @ sign. For example, `siroe.com` is the domain part of the email address `dan@siroe.com`.

domain quota The amount of space, configured by the system administrator, allocated to a domain for email messages.

domain rewrite rules See **rewrite rules**.

domain template The part of a rewrite rule that defines how the host/domain portion of an address is rewritten. It can include either a full static host/domain address or a single field substitution string, or both.

DSN See **Delivery Status Notification**.

dsservd A daemon that accesses the database files that hold the directory information, and communicates with directory clients using the LDAP protocol.

dynamic group A mail group defined by an LDAP search URL. Users usually join the group by setting an LDAP attribute in their directory entry.

EHLO command An SMTP command that queries a server to find out if the server supports extended SMTP commands. Defined in RFC 1869.

encryption The process of disguising information so that it cannot be deciphered (decrypted) by anyone but the intended recipient who has the code key.

enterprise network A network that consists of collections of networks connected to each other over a geographically dispersed area. The enterprise network serves the needs of a widely distributed company and is used by the company's mission-critical applications.

envelope A container for transport information about the sender and the recipient of an email message. This information is not part of the message header. Envelopes are used by various email programs as messages are moved from place to place. Users see only the header and body of a message.

envelope field A named item of information, such as `RCPT TO`, in a message envelope.

error handler A program that handles errors. In Messaging Server, issues error messages and processes error action forms after the postmaster fills them out.

Error-Handler Action form A form sent to the postmaster account that accompanies a received message that Messaging Server cannot handle. The postmaster fills out the form to instruct the server how to process the message.

error message A message reporting an error or other situation. Messaging Server generates messages in a number of situations, notably when it gets an email message that it can't handle. Others messages, called notification errors, are for informational purposes only.

ESMTP See **Extended Simple Mail Transfer Protocol**.

ESP Enterprise Service Provider.

ETRN An SMTP command enabling a client to request that the server start the processing of its mail queues for messages that are waiting at the server for the client machine. Defined in RFC 1985.

expander Part of an electronic mail delivery system that allows a message to be delivered to a list of addressees. Mail expanders are used to implement mail lists. Users send messages to a single address (for example, `hacks@somehost.edu`) and the mail expander takes care of delivery to the mailboxes in the list. Also called mail exploders. See also **EXPN**.

expansion This term applies to the MTA processing of mail lists. The act of converting a message addressed to a mail list into enough copies for each mail list member.

EXPN An SMTP command for expanding a mail list. Defined in RFC 821.

expunge message The act of marking a message for deletion and then permanently removing it from the INBOX. See also **delete message**, **purge message**.

Extended Simple Mail Transfer Protocol (ESMTP) An Internet message transport protocol. ESMTP adds optional commands to the SMTP command set for enhanced functionality, including the ability for ESMTP servers to discover which commands are implemented by the remote site.

extranet The part of a company intranet that customers and suppliers can access. See also **intranet**.

facility In a Messaging Server log-file entry, a designation of the software subsystem (such as Network or Account) that generated the log entry.

failover The automatic transfer of a computer service from one system to another to provide redundant backup.

family group administrator User who has administrative privileges to add and remove family members in a family group. This user can grant family group administrative access to other members of group.

firewall A network configuration, usually both hardware and software, that forms a barrier between networked computers within an organization and those outside the organization. A firewall is commonly used to protect information such as a network's email, discussion groups, and data files within a physical building or organization site.

folder A named collection of messages. Folders can contain other folders. Also called a mailbox. See also **personal folder**, **public folder**, **shared folder, INBOX**.

forwarding See **message forwarding**.

FQDN See **fully-qualified domain name**.

fragmentation The Multipurpose Internet Mail Extensions (MIME) feature that allows the breaking up of a large message into smaller messages. See also **defragmentation**.

fully-qualified domain name (FQDN) The unique name that identifies a specific Internet host. See also **domain name**.

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.

greeting form A message usually sent to users when an account is created for them. This form acts as confirmation of the new account and verification of its contents.

group A group of LDAP mail entries that are organized under a distinguished name. Usually used as a mail list, but may also be used to grant certain administrative privileges to members of the group. See also **dynamic group**, **static group**.

group folders These contain folders for shared and group folders. See also **public folder**, **shared folder**.

GUI Graphical User Interface

HA See **High Availability**.

hashdir A command-line utility for determining which directory contains the message store for a particular user.

header The portion of an email message that precedes the body of the message. The header is composed of field names followed by a colon and then values. Headers contain information useful to email programs and to users trying to make sense of the message. For example, headers include delivery information, summaries of contents, tracing, and MIME information; they tell whom the message is for, who sent it, when it was sent, and what it is about. Headers must be written according to RFC 822 so that email programs can read them.

header field A named item of information, such as From: or To:, in a message header. Often referred to as a “header line”.

High Availability Enables the detection of a service interruption and provides recovery mechanisms in the event of a system failure or process fault. In addition, it allows a backup system to take over the services in the event of a primary system failure.

hop A transmission between two computers.

host The machine on which one or more servers reside.

hosted domain An email domain that is outsourced by an ISP. That is, the ISP provides email domain hosting for an organization by operating and maintaining the email services for that organization. A hosted domain shares the same Messaging Server host with other hosted domains. In earlier LDAP-based email systems, a domain was supported by one or more email server hosts. With Messaging Server, many domains can be hosted on a single server. For each hosted domain, there is an LDAP entry that points to the user and group container for the domain. Hosted domains are also called virtual hosted domains or virtual domains. See also **domain**, **virtual domain**.

host name The name of a particular machine within a domain. The host name is the IP host name, which might be either a "short-form" host name (for example, mail) or a fully qualified host name. The fully qualified host name consists of two parts: the host name and the domain name. For example, `mail.siroe.com` is the machine `mail` in the domain `siroe.com`. Host names must be unique within their domains. Your organization can have multiple machines named `mail`, as long as the machines reside in different subdomains; for example, `mail.corp.siroe.com` and `mail.field.siroe.com`. Host names always map to a specific IP address. See also **domain name**, **fully-qualified domain name**, **IP address**.

host name hiding The practice of having domain-based email addresses that do not contain the name of a particular internal host.

HTTP See **HyperText Transfer Protocol**.

hub A host that acts as the single point of contact for the system. When two networks are separated by a firewall, for example, the firewall computer often acts as a mail hub.

HyperText Transfer Protocol A standard protocol that allows the transfer of hypertext documents over the Web. Messaging Server provides an HTTP service to support web-based email. See also **Messenger Express**.

iCalendar Message-Based Interoperability Protocol (iMIP) This protocol specifies a binding from the **iCalendar Transport-independent Interoperability Protocol (iTIP)** to Internet email-based transports. iMIP is defined in RFC 2447.

iCalendar Transport-Independent Interoperability Protocol (iTIP) An Internet protocol based on the iCalendar object specification that provides scheduling interoperability between different calendar systems. iTIP is defined in RFC 2446.

IDENT See **Identification Protocol**.

Identification Protocol A protocol that provides a means to determine the identity of a remote process responsible for the remote end of a particular TCP connection. Defined in RFC 1413.

IMAP4 See **Internet Message Access Protocol Version 4**.

iMIP See **iCalendar Message-Based Interoperability Protocol**.

imsadmin commands A set of command line utilities for managing domain administrators, users, and groups.

imsimta commands A set of command line utilities for performing various maintenance, testing, and management tasks for the Message Transfer Agent (MTA).

INBOX The name reserved for a user's default mailbox for mail delivery. INBOX is the only folder name that is case-insensitive. For example: INBOX, Inbox, and inbox are all valid names for a users default mailbox.

installation directory The directory into which the binary (executable) files of a server are installed. For example: *msg_svr_base*/ Se also **messaging server base directory**.

Internet The name given to the worldwide network of networks that uses TCP/IP protocols.

Internet Message Access Protocol Version 4 (IMAP4) A standard protocol that allows users to be disconnected from the main messaging system and still be able to process their mail. The IMAP specification allows for administrative control for these disconnected users and for the synchronization of the users' message store once they reconnect to the messaging system.

Internet Protocol (IP) The basic network-layer protocol on which the Internet and intranets are based.

internet protocol address See **IP address**.

intranet A network of TCP/IP networks within a company or organization. Intranets enable companies to employ the same types of servers and client software used for the World Wide Web for internal applications distributed over the corporate LAN. Sensitive information on an intranet that communicates with the Internet is usually protected by a firewall. See also **firewall**, **extranet**.

invalid user An error condition that occurs during message handling. When this occurs, the message store sends a communication to the MTA, the message store deletes its copy of the message. The MTA bounces the message back to the sender and deletes its copy of the message.

IP See **Internet Protocol**.

IP address A set of numbers, separated by dots, such as `198.93.93.10`, that specifies the actual location of a machine on an intranet or the Internet. A 32-bit address assigned to hosts using TCP/IP.

ISP Internet Service Provider. A company that provides Internet services to its customers including email, electronic calendaring, access to the world wide web, and web hosting.

iTIP See **iCalendar Transport-Independent Interoperability Protocol**.

Job Controller The MTA component responsible for scheduling and executing tasks upon request by various other MTA components.

key database A file that contains the key pair(s) for a server's certificate(s). Also called a key file.

knowledge information Part of the directory service infrastructure information. The directory server uses knowledge information to pass requests for information to other servers.

LDAP See **Lightweight Directory Access Protocol**.

LDAP Data Interchange Format (LDIF) The format used to represent Directory Server entries in text form.

LDAP filter A method of specifying a set of entries, based on the presence of a particular attribute or attribute value.

LDAP referrals An LDAP entry that consists of a symbolic link (referral) to another LDAP entry. An LDAP referral consists of an LDAP host and a distinguished name. LDAP referrals are often used to reference existing LDAP data so that this data does not have to be replicated. They are also used to maintain compatibility for programs that depend on a particular entry that may have been moved.

LDAP search string A string with replaceable parameters that defines the attributes used for directory searches. For example, an LDAP search string of "uid=%s" means that searches are based on the user ID attribute.

LDAP Server A software server that maintains an LDAP directory and services queries to the directory. The Directory Services are implementations of an LDAP Server.

LDAP server failover A backup feature for LDAP servers. If one LDAP server fails, the system can switch over to another LDAP server.

LDBM LDAP Data Base Manager.

LDIF See **LDAP Data Interchange Format**.

LMTP See **Local Mail Transfer Protocol**.

Legato Networker. A third-party backup utility distributed by Legato®.

level A designation of logging verbosity, meaning the relative number of types of events that are recorded in log files. At a level of Emergency, for example, very few events are logged; at a level of Informational, on the other hand, very many events are logged.

Lightweight Directory Access Protocol (LDAP) Directory service protocol designed to run over TCP/IP and across multiple platforms. A simplification of the X.500 Directory Access Protocol (DAP) that allows a single point of management for storage, retrieval, and distribution of information, including user profiles, mail lists, and configuration data across servers. The Directory Server uses the LDAP protocol.

listen port The port that a server uses to communicate with clients and other servers.

Local Mail Transfer Protocol (LMTP) Defined in RFC 2033, LMTP is similar to SMTP but does not require management of a mail delivery queue. In addition, LMTP provides a status code for each recipient of a message whereas SMTP provides only one status code for the message. See also S**imple Mail Transfer Protocol**.

local part The part of an email address that identifies the recipient. See also **domain part**.

log directory The directory in which all of a service's log files are kept.

log expiration Deletion of a log file from the log directory after it has reached its maximum permitted age.

log rotation Creation of a new log file to be the current log file. All subsequent logged events are to be written to the new current file. The log file that was the previous current file is no longer written to, but remains in the log directory.

lookup Same as a search, using the specified parameters for sorting data.

mailbox A place where messages are stored and viewed. See also **folder**.

mail client The programs that help users send and receive email. This is the part of the various networks and mail programs that users have the most contact with. Mail clients create and submit messages for delivery, check for new incoming mail, and accept and organize incoming mail.

mail exchange record See **MX record**.

mail list A list of email addresses to which a message can be sent by way of a mail list address. Sometimes called a group.

mail list owner A user who has administrative privileges to add members to and delete members from the mail list.

mail relay A mail server that accepts mail from a MUA or MTA and relays it to the mail recipient's message store or another router.

mail router See **mail relay**.

mailing list See **mail list**.

mailing list owner See **mail list owner.**

managed object A collection of configurable attributes, for example, a collection of attributes for the directory service.

master channel program A channel program that typically initiates a transfer to a remote system. See also **slave channel program**.

master directory server The directory server that contains the data that will be replicated.

MD5 A message digest algorithm by RSA Data Security. MD5 can be used to produce a short digest of data that is unique with high probability. It is mathematically extremely hard to produce a piece of data that produces the same message digest email.

member A user or group who receives a copy of an email addressed to a mail list. See also mail list, expansion, moderator, and owner.

message The fundamental unit of email, a message consists of a header and a body and is often contained in an envelope while it is in transit from the sender to the recipient.

message access services The protocol servers, software drivers, and libraries that support client access to the Messaging Server message store.

message delivery The act that occurs when an MTA delivers a message to a local recipient (a mail folder or a program).

message forwarding The act that occurs when an MTA sends a message delivered to a particular account to one or more new destinations as specified by the account's attributes. Forwarding may be configurable by the user. See also **message delivery**, **message routing**.

Message Handling System (MHS) A group of connected MTAs, their user agents, and message stores.

message routing The act of transferring a message from one MTA to another when the first MTA determines that the recipient is not a local account, but might exist elsewhere. Routing is normally configurable only by a network administrator. See also **message forwarding**.

message queue The directory where messages accepted from clients and other mail servers are queued for delivery (immediate or deferred).

message quota A limit defining how much disk space a particular folder can consume.

message store The database of all locally delivered messages for a Messaging server. Messages can be stored on a single physical disk or stored across multiple physical disks.

message store administrator User who has administrative privileges to manage the message store for a Messaging Server installation. This user can view and monitor mailboxes, and specify access control to the store. Using proxy authorization rights, this user can run certain utilities for managing the store.

message store partition A message store or subset of a message store residing on a single physical file system partition.

message submission The client User Agent (UA) transfers a message to the mail server and requests delivery.

Message Transfer Agent (MTA) A specialized program for routing and delivering messages. MTAs work together to transfer messages and deliver them to the intended recipient. The MTA determines whether a message is delivered to the local message store or routed to another MTA for remote delivery.

Messaging Multiplexor A specialized Messaging Server that acts as a single point of connection to multiple mail servers, facilitating the distribution of a large user base across multiple mailbox hosts.

Messaging Server administrator The administrator whose privileges include installation and administration of an Messaging Server.

messaging server base directory The directory into which all servers associated with a given Administration Server on a given host are installed. Typically designated *msg_svr_base*. See also **installation directory**.

Messenger Express A mail client that enables users to access their mailboxes through a browser-based (HTTP) interface. Messages, folders, and other mailbox information are displayed in HTML in a browser window. See also **webmail**.

Messenger Express Multiplexor A proxy messaging server that acts as a Multiplexor; it allows you to connect to the HTTP service of Messaging Server (Messenger Express). The Messenger Express Multiplexor facilitates distributing mail users across multiple server machines.

MHS See **Message Handling System**.

MIME See **Multipurpose Internet Mail Extension**.

MMP See **Messaging Multiplexor**.

moderator A person who first receives all email addressed to a mail list before (A) forwarding the message to the mail list, (B) editing the message and then forwarding it to the mail list, or (C) not forwarding the message to the mail list. See also **mail list**, **expansion**, **member**.

MTA See **Message Transfer Agent**.

MTA configuration file The file (`imta.cnf`) that contains all channel definitions for the Messaging Server as well as the rewrite rules that determine how addresses are rewritten for routing. See also **channel**, **rewrite rules**.

MTA directory cache a snapshot of the directory service information about users and groups required by the MTA to process messages. See also **directory synchronization**.

MTA hop The act of routing a message from one MTA to another.

MUA See **user agent**.

Multiplexor See **Messaging Multiplexor**.

Multipurpose Internet Mail Extension (MIME) A protocol you can use to include multimedia in email messages by appending the multimedia file in the message.

MX record Mail Exchange Record. A type of DNS record that maps one host name to another.

name resolution The process of mapping an IP address to the corresponding name. See also **DNS**.

namespace The tree structure of an LDAP directory. See also **directory information tree**.

naming attribute The final attribute in a directory information tree distinguished name. See also **relative distinguished name**.

naming context A specific suffix of a directory information tree that is identified by its DN. In Directory Server, specific types of directory information are stored in naming contexts. For example, a naming context which stores all entries for marketing employees in the Siroe Corporation at the Boston office might be called `ou=mktg, ou=Boston, o=siroe, c=US`.

NDN See **nondelivery notification**.

network manager A program that reads, formats, and displays SNMP data. Also called an SNMP client.

next-hop list A list of adjacent systems a mail route uses to determine where to transfer a message. The order of the systems in the next-hop list determines the order in which the mail route transfers messages to those systems.

node An entry in the DIT.

nondelivery notification During message transmission, if the MTA does not find a match between the address pattern and a rewrite rule, the MTA sends a nondelivery report back to the sender with the original message.

notary messages Nondelivery notifications (NDNs) and delivery status notifications (DSNs) that conform to the NOTARY specifications RFC 1892.

notification message A type of message, sent by the Messaging Server providing the status of message delivery processing, as well as the reasons for any delivery problems or outright failures. It is for information al purposes and requires no action from the postmaster. See also **delivery status notifications**.

object class A template specifying the kind of object the entry describes and the set of attributes it contains. For example, Directory Server specifies an `emailPerson` object class which has attributes such as `commonname`, `mail` (email address), `mailHost`, and `mailQuota`.

off-line state A state in which the mail client downloads messages from a server system to a client system where they can be viewed and answered. The messages might or might not be deleted from the server.

online state A state in which messages remain on the server and are remotely responded to by the mail client.

organization administrator User who has administrative privileges to create, modify, and delete mail users and mail lists in an organization or suborganization by using the Delegated Administrator for Messaging and Collaboration GUI or CLIs.

OSI tree A directory information tree that mirrors the Open Systems Interconnect network syntax. An example of a distinguished name in an OSI tree would be `cn=billt,o=bridge,c=us`.

partition See **message store partition**.

password authentication Identification of a user through user name and password. See also **certificate-based authentication**.

pattern A string expression used for matching purposes, such as in Allow and Deny filters.

permanent failure An error condition that occurs during message handling. When this occurs, the message store deletes its copy of an email message. The MTA bounces the message back to the sender and deletes its copy of the message.

personal folder A folder that can be read only by the owner. See also **shared folder**.

plaintext Refers to a method for transmitting data. The definition depends on the context. For example, with SSL plaintext passwords are encrypted and are therefore not sent as cleartext. With SASL, plaintext passwords are hashed, and only a hash of the password is sent as text. See also **SSL** and **SASL**.

plaintext authentication See **password authentication**.

POP3 See **Post Office Protocol Version 3**.

port number A number that specifies an individual TCP/IP application on a host machine, providing a destination for transmitted data.

postmaster account An alias for the email group and email addresses who receive system-generated messages from the Messaging Server. The postmaster account must point to a valid mailbox or mailboxes.

Post Office Protocol Version 3 (POP3) A protocol that provides a standard delivery method and that does not require the message transfer agent to have access to the user's mail folders. Not requiring access is an advantage in a networked environment, where often the mail client and the message transfer agent are on different computers.

process A self-contained, fully functional execution environment set up by an operating system. See also **thread**.

protocol A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.

provisioning The process of adding, modifying or deleting entries in the Directory Server. These entries include users and groups and domain information.

proxy The mechanism whereby one system "fronts for" another system in responding to protocol requests. Proxy systems are used in network management to avoid having to implement full protocol stacks in simple devices, such as modems.

public folder Folder that does not have any one owner and is shared by multiple people who may access it. Depending on the ACLs set for the folder, more than one person may update or administer the folder.

public key encryption A cryptographic method that uses a two-part key (code) that is made up of public and private components. To encrypt messages, the published public keys of the recipients are used. To decrypt the messages, the recipients use their unpublished private keys known only to them.

purge message The process of permanently removing messages that have been deleted and are no longer referenced in user and group folders and returning the space to the message store file system. See also **delete message**, **expunge message**.

queue See **message queue**.

RC2 A variable key-size block cipher by RSA Data Security.

RC4 A stream cipher by RSA Data Security. Faster than RC2.

RDN Relative distinguished name. The name of the actual entry itself, before the entry's ancestors have been appended to the string to form the full distinguished name.

referral A process by which the directory server returns an information request to the client that submitted it, with information about the Directory Service Agent (DSA) that the client should contact with the request. See also **knowledge information**.

regular expression A text string that uses special characters to represent ranges or classes of characters for the purpose of pattern matching.

relative distinguished name See **RDN**.

relaying The process of passing a message from one messaging server to another messaging server.

replica directory server The directory that will receive a copy of all or part of the data.

required attributes Attributes that must be present in entries using a particular object class. See also **allowed attributes**, **attributes**.

restore The process of restoring the contents of folders from a backup device to the message store. See also **backup**.

reverse DNS lookup The process of querying the DNS to resolve a numeric IP address into the equivalent fully qualified domain name.

rewrite rules Also known as domain rewrite rules. A tool that the MTA uses to route messages to the correct host for delivery. Rewrite rules perform the following functions: (1) extract the host / domain specification from an address of an incoming message, (2) match the host / domain specification with a rewrite rule pattern, (3) rewrite the host / domain specification based on the domain template, and (4) decide which channel queue the message should be placed in.

RFC Request For Comments. The document series, begun in 1969, describes the Internet suite of protocols and related experiments. Not all (in fact very few) RFCs describe Internet standards, but all Internet standards are published as RFCs. See http://www.imc.org/rfcs.html.

root entry The top-level 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 matrix.” In OSI terminology, a router is a Network Layer intermediate system. See also **gateway**.

routing See **message routing**.

routing tables The internal databases that hold the information about message originators and recipients. See also SMTP mail routing table.

safe file system A file system performs logging such that if a system crashes it is possible to rollback the data to a pre-crash state and restore all data. An example of a safe file system is Veritas File System, VxFS.

SASL See **Simple Authentication and Security Layer**.

schema Definitions—including structure and syntax—of the types of information that can be stored as entries in Directory Server. When information that does not match the schema is stored in the directory, clients attempting to access the directory might be unable to display the proper results.

SCM See **Service Control Manager**.

search base See **base DN**.

Secure Sockets Layer (SSL) A software library establishing a secure connection between two parties (client and server).

security-module database A file that contains information describing hardware accelerators for SSL ciphers. Also called `secmod`.

sendmail A common MTA used on UNIX machines. In most applications, Messaging Server can be used as a drop-in replacement for sendmail.

server administrator Person who performs server management tasks. The server administrator provides restricted access to tasks for a particular server, depending upon task ACIs. The configuration administrator must assign user access to a server. Once a user has server access permissions, that user is a server administrator who can provide server access permissions to users.

server side rules (SSR) A set of rules for enabling server-side filtering of mail. Based on the Sieve mail filtering language.

service (1) A function provided by a server. For example, Messaging Server provides SMTP, POP, IMAP, and HTTP services. (2) A background process on Windows 2000 that does not have a user interface. Sun ONE servers on Windows 2000 platforms run as services. Equivalent to **daemon** on UNIX platforms.

Service Control Manager Windows NT administrative program for managing services.

servlet server-side Java programs that Web servers run to generate content in response to a client request. Servlets are similar to applets in that they run on the server-side but do not use a user interface.

session An instance of a client-server connection.

shared folder A folder that can be read by more than one person. Shared folders have an owner who can specify read access to the folder and who can delete messages from the shared folder. The shared folder can also have a moderator who can edit, block, or forward incoming messages. Only IMAP folders can be shared. See also **personal folder, public folder**.

Sieve A proposed language for filtering mail.

Simple Authentication and Security Layer (SASL) A means for controlling the mechanisms by which POP, IMAP or SMTP clients identify themselves to the server. Messaging Server support for SMTP SASL use complies with RFC 2554 (ESMTP AUTH). SASL is defined in RFC 2222.

Simple Mail Transfer Protocol (SMTP) The email protocol most commonly used by the Internet and the protocol supported by the Messaging Server. Defined in RFC 821, with associated message format descriptions in RFC 822.

SIMS Sun Internet Mail Server.

single field substitution string In a rewrite rule, part of the domain template that dynamically rewrites the specified address token of the host / domain address. See also **domain template**.

single sign-on The ability for a user to authenticate once and gain access to multiple services (mail, directory, file services, and so on).

SIZE An SMTP extension enabling a client to declare the size of a particular message to a server. The server may indicate to the client that it is or is not willing to accept the message based on the declared message size; the server can declare the maximum message size it is willing to accept to a client. Defined in RFC 1870.

slave channel program A channel program that accepts transfers initiated by a remote system. See also **master channel program**.

smart host The mail server in a domain to which other mail servers forward messages if they do not recognize the recipients.

SMTP See **Simple Mail Transfer Protocol**.

SMTP AUTH See **AUTH**.

sn Aliased directory attribute for surname.

spoofing A form of network attack in which a client attempting to access or send a message to a server misrepresents its host name.

SSL See **Secure Sockets Layer**.

SSR See **Server Side Rules**.

static group A mail group defined statically by enumerating each group member. See also **dynamic group**.

subdomain A portion of a domain. For example, in the domain name `corp.siroe.com`, `corp` is a subdomain of the domain `siroe.com`. See also **host name**, **fully-qualified domain name**.

subnet The portion of an IP address that identifies a block of host IDs.

subordinate reference The naming context that is a child of the naming context held by your directory server. See also **knowledge information**.

suborganization A sub-domain below a hosted domain in the Organization Tree. Domain organizations are useful for companies that wish to organize their user and group entries along departmental lines. (Used in Identity Server). See also **domain organization**.

synchronization (1) The update of data by a master directory server to a replica directory server. (2) The update of the MTA directory cache.

TCP See **Transmission Control Protocol**.

TCP/IP See **Transmission Control Protocol/Internet Protocol**.

thread A lightweight execution instance within a process.

TLS See **Transport Layer Security**.

top-level administrator User who has administrative privileges to create, modify, and delete mail users, mail lists, family accounts, and domains in an entire Messaging Server namespace by using the Delegated Administrator for Messaging and Collaboration GUI or CLIs. By default, this user can act as a message store administrator for all messaging servers in the topology.

transient failure An error condition that occurs during message handling. The remote MTA is unable to handle the message when it's delivered, but may be able to later. The local MTA returns the message to the queue and schedules it for retransmission at a later time.

Transmission Control Protocol (TCP) The basic transport protocol in the Internet protocol suite that provides reliable, connection-oriented stream service between two hosts.

Transmission Control Protocol/Internet Protocol (TCP/IP) The name given to the collection of network protocols used by the Internet protocol suite. The name refers to the two primary network protocols of the suite: TCP (Transmission Control Protocol), the transport layer protocol, and IP (Internet Protocol), the network layer protocol.

Transport Layer Security (TLS). The standardized form of SSL. See also **Secure Sockets Layer**.

transport protocols Provides the means to transfer messages between MTAs, for example SMTP and X.400.

UA See **user agent**.

UBE See **Unsolicited Bulk Email**.

UID (1) User identification. A unique string identifying a user to a system. Also referred to as a userID. (2) Aliased directory attribute for userID (login name).

unified messaging The concept of using a single message store for email, voicemail, fax, and other forms of communication. Messaging Server provides the basis for a complete unified messaging solution.

Unsolicited Bulk Email (UBE) Unrequested and unwanted email, sent from bulk distributors, usually for commercial purposes.

upper reference Indicates the directory server that holds the naming context above your directory server's naming context in the directory information tree (DIT).

user account An account for accessing a server, maintained as an entry on a directory server.

user agent (UA) The client component, such as suborganization Communicator, that allows users to create, send, and receive mail messages.

User/Groups Directory Server A Directory Server that maintains information about users and groups in an organization.

user entry or user profile Fields that describe information about each user, required and optional, examples are: distinguished name, full name, title, telephone number, pager number, login name, password, home directory, and so on.

user folders A user's email mailboxes.

user quota The amount of space, configured by the system administrator, allocated to a user for email messages.

UUCP UNIX to UNIX Copy Program. A protocol used for communication between consenting UNIX systems.

vanity domain A domain name associated with an individual user—not with a specific server or hosted domain. A vanity domain is specified by using the `MailAlternateAddress` attribute. The vanity domain does not have an LDAP entry for the domain name. Vanity domains are useful for individuals or small organizations desiring a customized domain name, without the administration overhead of supporting their own hosted domain. Also called custom domain.

/var/mail A name often used to refer to Berkeley-style inboxes in which new mail messages are stored sequentially in a single, flat text file.

Veritas Cluster Server High availability clustering software from Veritas Software with which Messaging Server can integrate.

virtual domain (1) An ISP hosted domain. (2) A domain name added by the Messaging Multiplexor to a client's user ID for LDAP searching and for logging into a mailbox server. See also **domain**, **hosted domain**.

VRFY An SMTP command for verifying a user name. Defined in RFC 821.

Web server A software program or server computer equipped to offer World Wide Web access. A Web server accommodates requests from users, retrieves requested files or applications, and issues error messages.

webmail A generic term for browser-based email services. A browser-based client—known as a "thin" client because more processing is done on the server—accesses mail that is always stored on a server. See also **Messenger Express**.

wildcard A special character in a search string that can represent one or more other characters or ranges of characters.

workgroup Local workgroup environment, where the server performs its own routing and delivery within a local office or workgroup. Interdepartmental mail is routed to a backbone server. See also **backbone**.

X.400 A message handling system standard.

Index

E

F

H

I

J

L

M

N

O

P

R

S

T

U

V

W