Mac OS X Server Mail Service Administration

For Version 10.3 or Later

Apple Computer, Inc.

034-2349/8/22/03

Contents

How to Use This Guide

What's Included in This Guide

This guide explains how to administer Mac OS X Server mail services.

Using This Guide

The first chapter provides an overview of how the mail service works, what it can do for you, strategies for using it, how to set it up for the first time, and how to administer it over time.

Also take a look at any chapter that describes a service with which you're unfamiliar. You may find that some of the services you haven't used before can help you run your network more efficiently and improve performance for your users.

Most chapters end with a section called "Where to Find More Information." This section points you to web sites and other reference material containing more information about the service.

Setting Up Mac OS X Server for the First Time

If you haven't installed and set up Mac OS X Server, do so now.

- Refer to *Mac OS X Server Getting Started For Version 10.3 or Later,* the document that came with your software, for instructions on server installation and setup. For many environments, this document provides all the information you need to get your server up, running, and available for initial use.
- Read specific sections to learn how to continue setting up individual features of mail service. Pay particular attention to the information in these sections: "Setup Overview," "Before You Begin," and "Setting Up for the First Time."

Getting Help for Everyday Management Tasks

If you want to change settings, monitor services, view service logs, or do any other day-to-day administration task, you can find step-by-step procedures by using the on-screen help available with server administration programs. While all the administration tasks are also documented in the second chapter of this guide, sometimes it's more convenient to retrieve information in on-screen help form while using your server.

Getting Additional Information

In addition to this document, you'll find information about Mac OS X Server in:

- *Mac OS X Server Getting Started For Version 10.3 or Later,* which tells you how to install and set up your server initially
- *Mac OS X Server Migration to Version 10.3 or Later,* which provides instructions for migrating data to Mac OS X Server from existing Macintosh computers
- on-screen help on your server
- Read Me files on your server CD
- and at www.apple.com/server

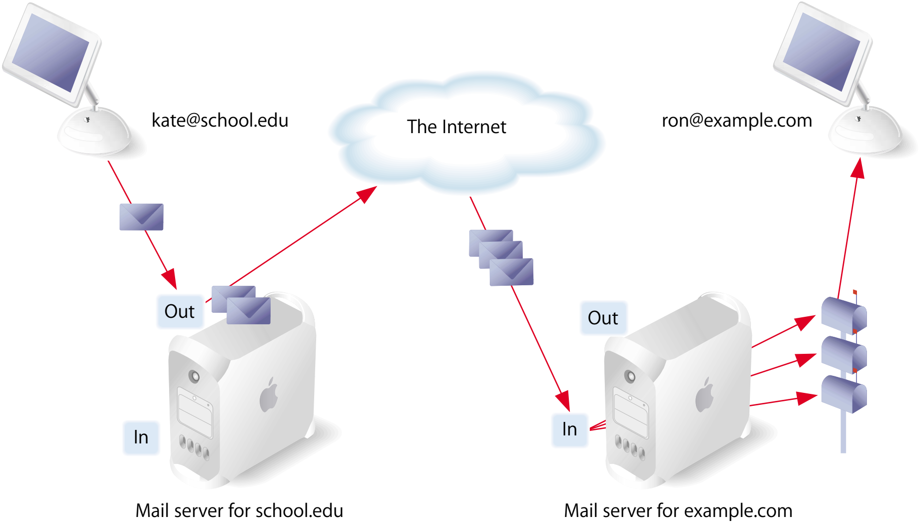
Mail Service Setup

1

Mail service in Mac OS X Server allows network users to send and receive email over your network or across the Internet. Mail service sends and receives email using the standard Internet mail protocols: Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP). Mail service also uses a Domain Name System (DNS) service to determine the destination IP address of outgoing mail.

This chapter begins with a look at the standard protocols used for sending and receiving email. Then it explains how mail service works, summarizes the aspects of mail service setup, and tells you how to:

- Set up mail service for incoming and outgoing mail
- Support mail users
- Limit junk mail



Mail Service Protocols

A standard mail client setup uses SMTP to send outgoing email and POP and IMAP to receive incoming email. Mac OS X Server includes an SMTP service and a combined POP and IMAP service. You may find it helpful to take a closer look at the three email protocols.

Outgoing Mail

Outgoing mail service is the means by which your users can send mail out to the Internet. Subject to restrictions that you control, the SMTP service also transfers mail to and from mail service on other servers. If your mail users send messages to another Internet domain, your SMTP service delivers the outgoing messages to the other domain's mail service.

Simple Mail Transfer Protocol (SMTP)

SMTP is a protocol used to send and transfer mail. SMTP queues outgoing mail messages from the user These messages are transferred along the Internet to their destinations, to be picked up by the incoming mail protocols.

Mac OS X Server uses Postfix (www.postfix.org) as its *mail transfer agent (MTA)*. Postfix fully supports the Internet standard SMTP protocol. Your email users will set their email applications's outgoing mail server to your Mac OS X Server running Postfix, and access their own incoming mail from a Mac OS X Server running incoming mail service.

If you choose to use another MTA (such as Sendmail), you won't be able to configure your mail service with Mac OS X Server administration tools.

If you want to use the Sendmail program instead of Postfix, you must disable current SMTP service through Postfix, and then install and configure Sendmail. For more information about Sendmail, see the web site www.sendmail.org.

Incoming Mail

Mail is transferred from incoming mail storage to the email recipient's inbox by a *local delivery agent (LDA)*. The LDA is responsible for handling local delivery, making mail accessible by the user's email application. There are two different protocols available from Mac OS X Server's mail access agent: POP and IMAP.

Mac OS X Server uses Cyrus (asg.web.cmu.edu/cyrus) to provide POP and IMAP service.

Post Office Protocol (POP)

POP is used only for receiving mail, not for sending mail. The mail service of Mac OS X Server stores incoming POP mail until users have their computers connect to the mail service and download their waiting mail. After a user's computer downloads POP mail, the mail is stored only on the user's computer. The user's computer disconnects from the mail service, and the user can read, organize, and reply to the received POP mail. The POP service is like a post office, storing mail and delivering it to a specific address.

An advantage of using POP is that your server doesn't need to store mail that users have downloaded. Therefore, your server doesn't need as much storage space as it would using the IMAP protocol. However, because the mail is removed from the server, if any client computers sustain hard disk damage and lose their mail files, there is no way to recover these files without using data backups.

Another advantage of POP is that POP connections are transitory. Once the mail is transferred, the connection is dropped and the load on both the network and the mail server is removed.

POP is not the best choice for users who access mail from more than one computer, such as a home computer, an office computer, and a laptop while on the road. When a user fetches mail via POP, the mail is downloaded to the user's computer and is usually completely removed from the server. If the user logs in later from a different computer, he or she won't be able to see previously downloaded mail.

Internet Message Access Protocol (IMAP)

IMAP is the solution for people who need to use more than one computer to receive mail. IMAP is a client-server mail protocol that allows users to access their mail from anywhere on the Internet. Users can send and read mail with a number of IMAP-compliant email clients.

With IMAP, a user's mail is delivered to the server and stored in a remote mailbox on the server; to users, mail appears as if it were on the local computer. A key difference between IMAP and POP is that with IMAP the mail is not removed from the server until the user deletes it.

The IMAP user's computer can ask the server for message headers, ask for the bodies of specified messages, or search for messages that meet certain criteria. These messages are downloaded as the user opens them. IMAP connections are persistent and remain open, maintaining load on the server and possibly the network as well.

User Interaction With Mail Service

Mail is delivered to its final recipient using a *mail user agent (MUA)*. MUAs are usually referred to as "email clients" or "email applications." These email clients often run on each user's local computer. Each user's email application must be configured to send messages to the correct outgoing server and receive messages from the incoming server. These configurations can affect your server's processing load and available storage space.

Where Mail Is Stored

Mail is stored in either an outgoing queue awaiting transfer to a remote server or in a local mail store accessible by local mail users.

Outgoing Mail Location

Outgoing mail messages are stored, by default, in the following spool directory on the startup disk:
/var/spool/postfix

This location is temporary, and the mail is stored until it's successfully transferred out to the Internet. These locations can be moved to any accessible volume (either local or NFS mounted) and symlinked to by the mail administrator.

Incoming Mail Location

The mail service keeps track of incoming email messages with a small database (BerekeleyDB.4.1), but the database doesn't contain the messages themselves. The mail service stores each message as a separate file in a mail folder for each user. Incoming mail is stored on the startup disk in the following directory:
/var/spool/imap/[user name]

Cyrus puts a database index file in the folder of user messages. You can change the location of any or all of the mail folders and database indexes to another folder, disk, or disk partition. You can even specify a shared volume on another server as the location of the mail folder and database, although using a shared volume incurs performance penalties. The incoming mail remains on the server until deleted by an MUA.

Maximum Number of Mail Messages per Volume

Because the mail service stores each email message in a separate file, the number of messages that can be stored on a volume is determined by the total number of files that can be stored on the volume.

The total number of files that can be stored on a volume that uses Mac OS Extended format (sometimes referred to as *HFS Plus format*) depends on the following factors:

- The size of the volume
- The sizes of the files
- The minimum size of a file, which by default is one 4K block

For example, a 4 GB HFS Plus volume with the default block size of 4KB has one million available blocks. This volume could hold up to a million 4KB files, which means a million email messages that were 4KB or less apiece. If some email messages were larger than 4KB, this volume could hold fewer of them. A larger volume with the same default block size could hold proportionately more files.

What Mail Service Doesn't Do

Mac OS X Server's mail service does not provide the following mail add-ons:

- Virus filtering
- Unsolicited commercial email (*spam*) identification
- Email content filtering

Each one of these add-on services can be configured to work with Mac OS X Server's mail service and can be obtained from various developers.

Using Network Services With Mail Service

Mail service makes use of network services to ensure delivery of email. Before sending an email, your mail service will probably have a Domain Name System (DNS) service determine the Internet Protocol (IP) address of the destination. The DNS service is necessary because people typically address their outgoing mail by using a domain name, such as example.com, rather than an IP address, such as 198.162.12.12. To send an outgoing message, your mail service must know the IP address of the destination. The mail service relies on a DNS service to look up domain names and determine the corresponding IP addresses. The DNS service may be provided by your Internet Service Provider (ISP) or by Mac OS X Server, as explained in the network services administration guide.

Additionally, an *mail exchanger (MX)* record can provide redundancy by listing an alternate mail host for a domain. If the primary mail host is not available, the mail can be sent to the alternate mail host. In fact, an MX record can list several mail hosts, each with a priority number. If the lowest priority host is busy, mail can be sent to the host with the next lowest priority, and so on.

Mail services use DNS like this:

1. The sending server looks at the email recipient's domain name (it's what comes after after the @ in the To address).
2. The sending server looks up the MX record for that domain name to find the receiving server.
3. If found, the message is sent to the receiving server.
4. If the lookup fails to find an MX record for the domain name, the sending server often assumes that the receiving server has the exact same name as the domain name. In this case, the sending server does an Address (A) lookup on that domain name, and attempts to send the file there.

Without a properly configured MX record in the DNS, mail may not reach your intended server.

Configuring DNS for Mail Service

Configuring DNS for mail service is enabling MX records with your own DNS server. If you have an ISP that provides you with DNS service, you will need to contact the ISP so that they can enable your MX records. Only follow these steps if you provide your own DNS Service using Mac OS X Server.

To enable MX records:

1. In Server Admin, select DNS in the Computers & Services pane.
2. Click Settings.
3. Select the Zones tab.
4. Select the Zone you want to use.
5. Click the Add button under the Records pane.
6. Choose MX from the Type pop-up menu.
7. Enter the domain name (like 'example.com') in the From field.
8. Enter the name of the mail server (like 'mail.example.com') in the To field.
9. If you will have more than one mail server, enter a precedence number for that server.

   A lower number indicates that mil server will be chosen first, if available, to receive mail.
10. Click OK.

If you need to set up multiple servers for redundancy, you will need to add additional MX records. See the network services administration guide for more information.

How Mail Service Uses SSL

Secure Sockets Layer (SSL) connections ensure that the data sent between your mail server and your users' mail clients is encrypted. This allows secure and confidential transport of mail messages across a local network. SSL transport does not provide secure authentication, just secure transfer from your mail server to your clients. See the Open Directory administration guide for secure authentication information.

For incoming mail, the mail service supports secure mail connections with mail client software that requests them. If a mail client requests an SSL connection, the mail service can automatically comply, if that option has been enabled. The mail service still provides non-SSL (unencrypted) connections to clients that don't request SSL. The configuration of each mail client determines whether it connects with SSL or not.

For outgoing mail, the mail service supports secure mail connections between SMTP servers. If an SMTP server requests an SSL connection, the mail service can automatically comply, if that option has been enabled. The mail service still can allow non-SSL (unencrypted) connections to mail servers that don't request SSL.

Enabling Secure Mail Transport With SSL

The mail service requires some configuration to provide SSL connections automatically. The basic steps are as follows:

- Generate a Certificate Signing Request (CSR) and create a keychain.
- Use the CSR to obtain an SSL certificate from an issuing authority.

For more information on enabling SSL from the web technologies administration guide and the Open Directory administration guide.

If you already have generated a certificate in a previous version of Mac OS X Server, it won't be compatible with the current mail service.

For detailed instructions for allowing or requiring SSL transport, see the following sections:

- "Configuring SSL Transport for POP Connections" on page 20
- "Configuring SSL Transport for IMAP Connections" on page 21
- "Configuring SSL Transport for SMTP Connections" on page 23

Before You Begin

Before setting up mail service for the first time:

- Decide whether to use POP, IMAP, or both for incoming mail.
- If your server will provide mail service over the Internet, you need a registered domain name. You also need to determine whether your ISP will create your MX records or you will create them in your own DNS service.
- Identify the people who will use your mail service but don't already have user accounts in a directory domain accessible to your mail service. You must create user accounts for these mail users.
- Determine mail storage requirements, and ensure you have enough disk space for your anticipated mail volume.
- Determine your authentication and transport security needs.

How User Account Settings Affect Mail Service

In addition to setting up mail service as described in this chapter, you can also configure some mail settings individually for everyone who has a user account on your server. Each user account has settings that do the following:

- Enable or disable mail service for the user account, or forward incoming mail for the account to another email address.
- Specify the server that provides mail service for the user account.
- Set a quota on the amount of disk space for storing the user account's mail on the server.
- Specify the protocol for the user account's incoming mail: POP, IMAP, or both.

Moving Mail Messages From Apple Mail Server to Mac OS X Server Version 10.3

If you have upgraded your server from a version previous to Mac OS X Server v.10.3, and you have an existing Apple Mail Server database, you must migrate your mail database to Mac OS X Server v.10.3 mail service.

For more detailed instructions and tool descriptions, see "Converting the Mail Store and Database From an Earlier Version" on page 36, and "Using Amsmailtool" on page 36

Overview of Mail Service Tools

The following applications help you set up and manage mail service:

- Server Admin*:* Use to start, stop, configure, and monitor mail service when you install Mac OS X Server.
- *Workgroup Manager:* Use to create user accounts for email users and configure each user's mail options.
- *Terminal:* Use for tasks that involve UNIX command-line tools, such as migrating and restoring the mail database.

Setup Overview

You can have mail service set up and started automatically as part of the Mac OS X Server installation process. An option for setting up mail service appears in the Setup Assistant application, which runs automatically at the conclusion of the installation process. If you select this option, mail service is set up as follows:

- SMTP, POP, and IMAP are all active and using standard ports.
- Standard authentication methods are used (not Kerberos), with POP and IMAP set for clear-text passwords (APOP and CRAM MD-5 turned off) and SMTP authentication turned off.
- Mail is only delivered locally (no mail sent to the Internet).
- Mail relay is restricted.

If you want to change this basic configuration, or if you have not set up your mail service, these are the major tasks you perform to set up mail service:

Step 1: Before you begin, make a plan

See "Before You Begin" on page 15 for a list of items to think about before you start full-scale mail service.

Step 2: Set up MX records

If you want users to be able to send and receive mail over the Internet, you should make sure DNS service is set up with the appropriate MX records for your mail service.

- If you have an ISP that provides DNS service to your network, contact the ISP and have the ISP set up MX records for you. Your ISP will need to know your mail server's DNS name (such as mail.example.com) and your server's IP address.
- If you use Mac OS X Server to provide DNS service, create your own MX records as described in "Configuring DNS for Mail Service" on page 14.
- If you do not set up an MX record for your mail server, your server may still be able to exchange mail with some other mail servers. Some mail servers will find your mail server by looking in DNS for your server's A record. (You probably have an A record if you have a web server set up.)

Note: Your mail users can send mail to each other even if you do not set up MX records. Local mail service doesn't require MX records.

Step 3: Configure incoming mail service

Your mail service has many settings that determine how it handles incoming mail. for instructions, see "Configuring Incoming Mail Service" on page 19.

Step 4: Configure outgoing mail service

Your mail service also has many settings that determine how it handles outgoing mail. For instructions, see "Configuring Outgoing Mail Service" on page 22.

Step 5: Secure your server

If your server exchanges mail with the rest of the Internet, make sure you're not operating an open relay. An open relay is a security risk and enables junk-mail senders (*spammers*) to use your computer resources for sending unsolicited commercial email. For instructions see "Limiting Junk Mail" on page 29, and "Restricting SMTP Relay" on page 30.

Step 6: Configure additional settings for mail service

Additional settings that you can change affect how mail service stores mail, interacts with DNS service, limits junk-mail (*spam*), and handles undeliverable mail. See the following sections for detailed instructions:

- "Working With the Mail Store and Database" on page 35
- "Limiting Junk Mail" on page 29
- "Working With Undeliverable Mail" on page 42

Step 7: Set up accounts for mail users

Each person who wants mail service must have a user account in a directory domain accessible by your mail service. The short name of the user account is the mail account name and is used to form the user's mail address. In addition, each user account has settings that determine how your mail service handles mail for the user account. You can configure a user's mail settings when you create the user's account, and you can change an existing user's mail settings at any time. For instructions, see "Supporting Mail Users" on page 24, and "Configuring Email Client Software" on page 25

Step 8: Create a postmaster account (optional, but advised)

You need to create a user account named "postmaster." The mail service may send reports to the postmaster account. When you create the postmaster account, make sure mail service is enabled for it. For convenience, you can set up forwarding of the postmaster's mail to another mail account that you check regularly. Other common postmaster accounts are named "abuse" (used to report abuses of your mail service) and "spam" (used to report unsolicited commercial email abuses by your users). The user management guide tells you how to create user accounts.

Step 9: Start mail service

Before starting mail service, make sure the server computer shows the correct day, time, time zone, and daylight-saving settings in the Date & Time pane of System Preferences. Mail service uses this information to timestamp each message. An incorrect timestamp may cause other mail servers to handle a message incorrectly.

Also, make sure you've enabled one or more of the mail service protocols (SMTP, POP, or IMAP) in the Settings pane.

Once you've verified this information, you can start mail service. If you selected the Server Assistant option to have mail service started automatically, stop mail service now, and then start it again for your changes to take effect. For detailed instructions, see "Starting and Stopping Mail Service" on page 33.

Step 10: Set up each user's mail client software

After you set up mail service on your server, mail users must configure their mail client software for your mail service. For details about the facts that users need when configuring their mail client software, see "Supporting Mail Users" on page 24.

Configuring Incoming Mail Service

The mail service has settings for requiring various authentication methods for POP and IMAP connections, as well as data transport over SSL.

Enabling Secure POP Authentication

Your POP mail service can protect users' passwords by allowing Authenticated POP (APOP), or Kerberos. When a user connects with APOP or Kerberos, the user's mail client software encrypts the user's password before sending it to your POP service. Before configuring your mail service to require secure authentication, make sure that your users' email applications and user accounts support the method of authentication you choose.

Before enabling Kerberos authentication for incoming mail service, you must integrate Mac OS X with a Kerberos server. If you're using Mac OS X Server for Kerberos authentication, this is already done for you. For instructions, see the Open Directory administration guide.

If you want to *require* either of these authentication methods, then enable only the one.

To set the POP authentication method:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Check APOP, or Kerberos (as desired) in the POP3 list.
5. Click Save.

Enabling Less Secure Authentication for POP

You can choose to allow basic password (clear text) authentication. This is considered to be less secure than APOP or Kerberos because the password itself is transmitted as unencrypted, clear text.

If you want to *require* clear text authentication, then enable Clear as the only authentication method.

To enable clear text POP authentication:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Check Clear
5. Click Save.

The default setting is 32, and the maximum is 300.

Configuring SSL Transport for POP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose to Require, Use, or Don't Use SSL for POP (and IMAP) connections. Before using SSL connections, you must have a security certificate for mail use. See the Open Directory administration guide for more information on enabling SSL.

Setting SSL transport for POP also sets it for IMAP.

To set SSL transport for POP connections:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Select Require, Use, or Don't Use (as desired) in the IMAP and POP SSL section.
5. Click Save.

Enabling Secure IMAP Authentication

Your IMAP mail service can protect users' passwords by requiring that connections use a secure method of authentication. You can choose CRAM MD-5, or Kerberos v5 authentication. When a user connects with secure authentication, the user's mail client software encrypts the user's password before sending it to your IMAP service. Make sure that your users' email applications and user accounts support the method of authentication you choose.

If you configure your mail service to require CRAM MD-5, mail users' accounts must be set to use a Password Server that has CRAM MD-5 enabled. For information, see the Open Directory administration guide.

Before enabling Kerberos authentication for incoming mail service, you must integrate Mac OS X with a Kerberos server. If you are using Mac OS X Server for Kerberos authentication, this is already done for you. For instructions, see the Open Directory administration guide.

To set secure IMAP authentication:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Select CRAM MD-5 or Kerberos (as desired) in the IMAP section.
5. Click Save.

Enabling Less Secure IMAP Authentication

Your IMAP mail service can supply users' passwords by less secure means. These authentication methods are less secure because they don't securely encrypt your users' passwords as they cross the network.

To allow login, plain, or clear IMAP authentication:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Check LOGIN, PLAIN, or Clear in the IMAP list.

Controlling the Number of IMAP Connections

You can adjust the load put on your server by limiting the number of concurrent IMAP connections.

To limit IMAP connections:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the General tab.
4. Click Enable IMAP, if it isn't already checked.
5. Enter the number of concurrent connections you want to allow, then click Save.

   The default setting is 32, and the maximum is 300.

Configuring SSL Transport for IMAP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose to Require, Use, or Don't Use SSL for IMAP connections. Before using SSL connections, you must have a security certificate for mail use. See the Open Directory administration guide for more information on enabling SSL.

Requiring SSL transport for IMAP also requires it for POP.

To configure SSL transport for IMAP connections:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Click Require, Use, or Don't Use (as desired) in the IMAP and POP SSL section.
5. Click Save.

Configuring Outgoing Mail Service

The mail service includes an SMTP service for sending mail. Subject to restrictions that you control, the SMTP service also transfers mail to and from mail service on other servers. If your mail users send messages to another Internet domain, your SMTP service delivers the outgoing messages to the other domain's mail service. Other mail services deliver messages for your mail users to your SMTP service, which then transfers the messages to your POP service and IMAP service.

If you don't choose any method of SMTP authentication, the SMTP server will allow anonymous SMTP mail relay. Requiring SMTP authentication requires authentication for mail relay. Mail addressed to local recipients is still accepted and delivered. Enabling authentication for SMTP *requires* authentication from any of the selected authentication methods prior to relaying mail.

Your mail service also has settings that restrict SMTP mail transfer and thereby limit junk mail. For more information on these settings, see "Limiting Junk Mail" on page 29.

Enabling Secure SMTP Authentication

Your server can guard against being an open relay by allowing SMTP authentication. (An open relay indiscriminately relays mail to other mail servers.) You can configure the mail service to require secure authentication using either the CRAM MD-5 or Kerberos method. You can also allow the less secure plain and login authentication methods, which don't encrypt passwords, if some users have email client software that doesn't support the secure methods.

If you configure your mail service to require CRAM MD-5, mail users' accounts must be set to use a password server that has CRAM MD-5 enabled. For information, see the Open Directory administration guide.

Before enabling Kerberos authentication for incoming mail service, you must integrate Mac OS X with a Kerberos server. If you are using Mac OS X Server for Kerberos authentication, this is already done for you. For instructions, see the Open Directory administration guide.

To allow secure SMTP authentication:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Check CRAM MD-5, or Kerberos (as desired) in the SMTP section.
5. Click Save.

Enabling Less Secure SMTP Authentication

Your server can guard against being an open relay by requiring SMTP authentication. (An open relay indiscriminately relays mail to other mail servers.) Requiring authentication ensures that only known users—people with user accounts on your server—can send mail from your mail service. You can choose to require, allow, or disallow less secure authentication methods (plain text, or login) for SMTP mail service.

Plain authentication sends mail passwords as plain text over the network. Login authentication sends a minimally secure crypt hash of the password over the network.

To allow less secure authentication:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Check either Plain or Login in the SMTP section.
5. Click Save.

Configuring SSL Transport for SMTP Connections

SSL transport enables mail transmitted over the network to be securely encrypted. You can choose to *Require*, *Use*, or *don't Use SSL* for IMAP connections. Before using SSL connections, you must have a security certificate for mail use. See the Open Directory administration guide for more information on enabling SSL.

To configure SSL transport for SMTP connections:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Click Require, Use, or Don't Use (as desired) in the SMTP SSL section.
5. Click Save.

Relaying SMTP Mail Through Another Server

Rather than delivering outgoing mail directly to its various destinations, your SMTP mail service can relay outgoing mail to another server.

Normally, when an SMTP server receives a message addressed to a remote recipient, it will attempt to send that message directly to that server or the server specified in the MX record, if it exists. Depending on your network setup, this method of mail transport may not be desired or even possible. You may then need to relay all outbound messages through a specific server.

- You may need to use this method to deliver outgoing mail through your organization's firewall set up by your organization. In this case, your organization will designate a particular server for relaying mail through the firewall.
- You may find this method useful if your server has slow or intermittent connections to the Internet.

To relay SMTP mail through another server:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Click the General tab.
5. Click "Relay all SMTP mail through this host" and enter the DNS name or IP address of the server that provides SMTP relay.
6. Click Save.

Supporting Mail Users

This section discusses mail settings in your server's user accounts and mail service settings in email client software.

Configuring Mail Settings for User Accounts

To make mail service available to users, you must configure mail settings in your user accounts. For each user, you need to enable mail service, enter the DNS name or IP address of your mail server, and select the protocols for retrieving incoming mail (POP, IMAP, or both). You can also set a quota on disk space available for storing a user's mail.

You configure these settings with the Workgroup Manager application. For instructions, see the user management guide.

Configuring Email Client Software

Users must configure their email client software to connect to your mail service. The following table details the information most email clients need and the source of the information in Mac OS X Server.

Email client software	Mac OS X Server	Example
User name	Full name of the user	Steve Macintosh
Account name Account ID	Short name of user account	steve
Password	Password of user account	
Host name Mail server Mail host	Mail server's full DNS name or IP address, as used when you log in to the server in Server Admin	mail.example.com 192.168.50.1
Email address	User's short name, followed by the @ symbol, followed by one of the following: • Server's Internet domain (if the mail server has an MX record in DNS) • Mail server's full DNS name • Server's IP address	steve@example.com steve@mail.example.com steve@192.168.50.1
SMTP host SMTP server	Same as host name	mail.example.com 192.168.50.1
POP host POP server	Same as host name	mail.example.com 192.168.50.1
IMAP host IMAP server	Same as host name	mail.example.com 192.168.50.1
SMTP user	Short name of user account	steve
SMTP password	Password of user account	

Creating an Administration Account

You may need to create a mail administrator account to maintain and watch mail folders, remove defunct user accounts, and archive mail. This administrator account doesn't need to be a server administrator. Also, this administrator account shouldn't receive mail. It is *not* a normal mail account.

To create a mail administrator account:

1. Create a user to be mail administrator.
2. If you have not created a user record for the mail administrator's account, see the user management guide.
3. Open `/etc/imapd.conf` in a text editor.

   If you are not comfortable using a terminal text editor like emacs or vi, you can use TextEdit.
4. Find the line that reads "admins:"
5. Edit the line to add the account name of the administrator account after the colon.
6. Save your changes.

For more information see the man page for imapd.conf.

Creating Additional Email Addresses for a User

Mail service allows each individual user to have more than one email address. Every user has one email address that is formed from the short name of the user account. In addition, you can define more names for any user account by creating an alias file. Each additional name is an alternate email address for the user at the same domain. These additional email addresses are not additional accounts that require separate quotas or passwords. Most often alias files are used to map "postmaster" users to a real account and give a "firstname.lastname@example.com" email address to a user with a short login account name.

To create an alias:

1. Create a file to be used as an alias list in /etc/aliases, if none exists.
2. For each alias, make a line in the file with the following format:

   alias:localaddress1,localaddress2,...

   For example, for your domain example.com, if you want to give username "bob" an alias of "robert.fakeuser" you should enter:

   ```
   robert.fakeuser: bob
   ```

   This will take mail sent to your mail server for robert.fakeuser@example.com and actually send it to the real mail account bob@example.com.
3. Save your file changes.

4. In Terminal.app, enter the following command:

   ```
   postalias /etc/aliases
   ```

   The text file is processed into a database for faster access.

5. At the prompt, enter the following command:

   ```
   newaliases
   ```

   The alias database will reload.

6. At the prompt, reload the mail server by entering the following command:

   ```
   postfix reload
   ```

   For further information about creating and maintaining email aliases, look at /etc/postfix/alias.

Setting Up Forwarding Email Addresses for a User

You may use this to provide an email redirection service for your users. Any mail sent to the user's email account will be forwarded to the indicated account.

To forward a users mail:

1. In Workgroup Manager, open the user account you want to work with, if it is not already open.

   To open the account, click the Accounts button, then click the globe icon below the toolbar menu and open the directory domain where the account resides. Click the lock to be authenticated. Select the user in the user list.

2. Click the Mail tab.
3. Select Forward.
4. Enter the forwarding email address in the Forward To field.

   Multiple addresses can be entered but must be separated by a comma.

Adding or Removing Virtual Domains

Virtual domains are other domains which can be used in email addresses for your mail users. It is also a list of all the domain names for which it is responsible. You should add any names that are likely to appear after @ in the addresses of mail directed to your server. For example, the list might contain variations of the spelling of your domain name or company name. If you host mail for example.com and example.org, a virtual domain would allow bob@example.com to receive mail addressed to bob@example.com and example.org using the same mailbox.

Your mail settings apply to all domain names in this list.

In order to use a virtual domain, you must have the domain registered and you should have an MX record pointing to your mail server for the domains you wish to enable.

To add or remove virtual domain names for the mail server:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Advanced tab.
4. Click Add and type the domain name of a virtual mail host for which you want your server to be responsible.
5. To remove an item from the list, select it and click Remove.

Note: If you've set up MX records, you don't need to add anything to this list. Your mail service will add names as it discovers them in the course of its daily operation.

If a domain name in this list doesn't have an MX record, only your mail service recognizes it. External mail sent to this domain name will be returned. Place domain names without MX records in this list only as a time saver for local (internal) mail.

Limiting Junk Mail

You can configure your mail service to decrease the volume of unsolicited commercial mail, also known as junk mail and *spam*. You can take steps to block spam that is sent to your mail users.

You can also take steps to prevent senders of junk mail from using your server as a relay point. A *relay point* or *open relay* is a server that unselectively receives and forwards all mail addressed to other servers. An open relay sends mail from any domain to any domain. Junk mail senders exploit open relay servers to avoid having their own SMTP servers blacklisted as sources of spam. You don't want your server blacklisted as an open relay, because other servers may reject mail from your users.

Your mail service can do any of the following to reduce spam:

- Require SMTP authentication
- Restrict SMTP relay, allowing relay only by approved servers
- Reject all SMTP connections from disapproved servers
- Reject mail from blacklisted servers
- Filter SMTP connections

Requiring SMTP Authentication

If your mail service requires SMTP authentication, your server cannot be used as an open relay by anonymous users. Someone who wants to use your server as a relay point must first provide the name and password of a user account on your server.

Your local mail users must also authenticate before sending mail. This means your mail users must have mail client software that supports SMTP authentication or they will be unable to send mail to remote servers. Mail addressed to local recipients will still be accepted and delivered.

To require SMTP authentication, please see "Enabling Secure SMTP Authentication" on page 22, and "Enabling Less Secure SMTP Authentication" on page 23.

Restricting SMTP Relay

Your mail service can restrict SMTP relay by allowing only approved hosts to relay mail. You create the list of approved servers. Approved hosts can relay through your mail service without authenticating. Servers not on the list cannot relay mail through your mail service unless they authenticate first. All hosts, approved or not, can deliver mail to your local mail users without authenticating.

Your mail service can log connection attempts made by hosts not on your approved list.

To restrict SMTP relay:

1 In Server Admin, select Mail in the Computers & Services pane.

2 Click Settings.

3 Select the Filters tab.

4 Check "Accept SMTP relays only from these"

5 Edit the list of hosts.

a Click the Add button to add a host to the list.
b Click the Remove button to delete the currently selected host from the list.
c Click the Edit button to change the currently selected host from the list.
d Enter a single IP address, or the network/netmask pattern such as 192.168.40.0/21

SMTP Authentication and Restricted SMTP Relay Combinations

The following table describes the results of using SMTP authentication and restricted SMTP relay in various combinations.

SMTP requires authentication	Restricted SMTP relay	Result
On	Off	All mail servers must authenticate before your mail service will accept any mail for relay. Your local mail users must also authenticate to send mail.
On	On	Approved mail servers can relay without authentication. Servers that you have not approved can relay after authenticating with your mail service.
Off	On	Your mail service can't be used for open relay. Approved mail servers can relay (without authenticating). Servers that you have not approved can't relay unless they authenticate, but they can deliver to your local mail users. Your local mail users don't have to authenticate to send mail. This is the most common configuration.

Rejecting SMTP Connections From Specific Servers

Your mail service can reject unauthorized SMTP connections from hosts on a disapproved-hosts list that you create. All mail traffic from servers in this list is denied and the SMTP connections are closed after posting a 554 SMTP connection refused error.

To reject unauthorized SMTP connections from specific servers:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Filters tab.
4. Check "Refuse all messages from these."
5. Edit the list of servers.
   - a Click the Add button to add a host to the list.
   - b Click the Remove button to delete the currently selected host from the list.
   - c Click the Edit button to change the currently selected host from the list.
   - d When adding to the list, you can use a variety of notations.
   - e Enter a single IP address.

Rejecting Mail From Blacklisted Senders

Your mail service can reject mail from SMTP servers that are blacklisted as open relays by an ORBS server. Your mail service uses an ORBS server that you specify.

Important: Blocking unsolicited mail from blacklisted senders may not be completely accurate. Sometimes it can prevent valid mail from being received.

To reject mail from blacklisted senders:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the Filters tab.
4. Check "Use these junk mail rejection servers."
5. Edit the list of servers by adding the DNS name of an RBL server.
   - a Click the Add button to add a server to the list.
   - b Click the Remove button to delete the currently selected server from the list.
   - c Click the Edit button to change the currently selected server from the list.
   - d Enter the domain name of the desired RBL server, such as rbl.example.com

Filtering SMTP Connections

You can use the firewall service of Mac OS X Server to allow or deny access to your SMTP mail service from specific IP addresses. Filtering disallows all communication between an originating host and your mail server. Mail service will never receive the incoming connection and no SMTP error will be generated and sent back to the client.

To filter SMTP connections:

1. In Server Admin, select Firewall in the Computers & Services pane.
2. Create a firewall IP filter using the instructions in the network services administration guide using the following settings:
   - Access: Denied
   - Port number: 25 (or your incoming SMTP port, if you use a non-standard port)
   - Protocol: TCP
   - Source: the IP address or address range you want to block
   - Destination: your mail server's IP address
3. If desired, log the packets to monitor the SMTP abuse.
4. Add more new filters for the SMTP port to allow or deny access from other IP addresses or address ranges.

For additional information on the firewall service, see the network services administration guide

Mail Service Maintenance

2

After setting up your mail service, there are some ongoing tasks to keep your mail service running efficiently and smoothly. The Server Admin application has a number of features that help you with these day-to-day tasks.

This chapter describes the maintenance of basic mail service, database, and mail store, including archiving. It also contains information about mail monitoring, logging, and undeliverable mail.

Starting and Stopping Mail Service

Mail service is ordinarily started automatically after you complete the Server Assistant. You can also use the Server Admin application to start and stop mail service at your discretion.

To start or stop mail service:

1 In Server Admin, select Mail in the Computers & Services pane.

2 Click Settings.

3 Select the General tab.

4 Make sure at least one of the mail protocols (SMTP, POP, or IMAP) is enabled.

5 Click Start Service or Stop Service in the menubar.

When the service is turned on, the Stop Service button is available.

If you plan to turn off mail service for an extended period of time, notify users before you stop the mail service.

Reloading Mail Service

Sometimes it is necessary to reload the mail server for mail service setting changes to take effect, for example, after restoring from backup, or altering the alias file. Reloading the mail service can be done without interrupting current mail service.

To reload outgoing mail service:

1. Start Terminal.
2. As root, enter the following command:

```
postfix reload
```

Changing Protocol Settings for Incoming Mail Service

You can change the settings for your incoming mail service. By choosing POP3, IMAP, or both.

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Click the General tab.
4. Enable or disable the IMAP or POP checkbooks as needed.

Improving Performance

Mail service needs to act very fast for a short period of time. It sits idle until a user wants to read or send a message, and then it needs to transfer the message immediately. Therefore, it puts intense but brief demands on the server. As long as other services do not place heavy continuous demands on a server (as a QuickTime streaming server would, for example), the server can typically handle several hundred connected users.

As the number of connected mail users increases, the demand of mail service on the server increases. If your mail service performance needs improvement, try the following actions:

- Adjust the load each mail user can put on your server by limiting the number of mail connections. For instructions, see "Controlling the Number of IMAP Connections" on page 21.
- Move the mail storage location to its own hard disk or hard disk partition. For instructions, see "Specifying the Location for the Mail Database and Mail Store" on page 37.
- Run other services on a different server, especially services that place frequent heavy demands on the server. (Each server requires a separate Mac OS X Server license.)

Working With the Mail Store and Database

The mail database keeps track of messages for all mail service users. Mail service stores messages in separate files. You can do the following with the mail database and files:

- Repair the Mail Store Database.
- Convert the mail database from an earlier version of Mac OS X Server.
- Specify the location where the mail database and files are stored.
- Backup and restore the mail store.

All these tasks are described in this section.

Repairing the Mail Store Database

The mail service updates the database of stored messages each time a message is added, deleted, or moved. Sometimes during these updates, the mailstore's database can become corrupted. When users report that mail messages have "disappeared" or become unreadable, the mail store database may be corrupted and need to be reconstructed.

Reconstructing a database can be done while the mail server is running. Additionally, it can be directed for any user to reconstruct only the affected mailboxes.

To reconstruct a corrupted database:

1. Start Terminal.app.
2. As root user, change to the cyrus user:

   ```
   su cyrus
   ```

3. Enter the following command:

   ```
   /usr/bin/cyrus/bin/reconstruct -r -f /var/spool/imap/[user name]
   ```

For more information about the `reconstruct` command, see their man pages by entering:

```
man reconstruct.
```

Converting the Mail Store and Database From an Earlier Version

If you have used any previous version of Apple Mail Service, you'll need to convert your users' mail messages and mail database to the current format.

To convert an earlier version of the Apple Mail Service mail database run the Terminal tool amsmailtool.

To convert the database:

1. Start Terminal.app.
2. As root user, enter the following command:

```
/usr/bin/cyrus/tools/amsmailtool
```

The conversion tool displays its status in the terminal as each user and mailbox is migrated.

Note: To complete the mail database conversion successfully, the server must have enough available disk space. The amount of available disk space should equal the size of the database file being converted. If there's not enough disk space available, amsmailtool won't convert the mail database and messages.

Using Amsmailtool

The utility amsmailtool, if launched without arguments, runs as follows:

- The tool looks first for the 10.2.x mail database. If it doesn't find one, it looks for the 10.1.x mail database. If both exist, only the first one it finds will be migrated.
- Mail is exported to the default destination directory, creating target mailboxes as needed.
- Each migrated message is marked in the database to prevent duplicate migrations.
- If the migration is canceled, rerunning the tool continues the previous migration by checking if a particular message has already been migrated.

If you want to specify a single type of database, source directory, or target directory to migrate, you may run amsmailtool with certain arguments as options.

To see the complete list arguments and command syntax:

1. Start Terminal.app.
2. As root user, enter the following command:

```
/usr/bin/cyrus/tools/amsmailtool -help
```

Specifying the Location for the Mail Database and Mail Store

If you are starting mail service for the first time and you have no existing mail database, you can specify where the mail database and message files will be stored. By default mail database location is /var/imap/ and the mail store location is /var/spool/imap/.

To specify where mail is stored on the server:

1. If mail service is already running, stop the mail service. See "Starting and Stopping Mail Service" on page 33 for details.
2. In Server Admin, select Mail in the Computers & Services pane.
3. Click Settings.
4. Click the Advanced tab.
5. Enter the path of the location where you want the mail files to be stored in the "Mail store" field.

   You can browse for a location by clicking Browse next to the location field.
6. Restart or reload mail service.

When mail service starts for the first time, it creates an empty mail store at the default location. You can ignore this or delete it after you have specified an alternate mail storage location and restarted mail service.

Note: Changing the mail store location of an existing mail system does *not* move the mail from the old location to the new one.

Backing Up and Restoring Mail Messages

You can back up the mail service data by making a copy of the mail service folder. If you need to restore the mail service data, you can replace the mail service folder with a backup copy. You can back up individual mail storage folders, or the entire mail store, as needed. One command line tool that can be used to back up your mail messages is ditto. See ditto's man page for information.

Important: Stop mail service before backing up or restoring the mail service folder. If you back up the mail service folder while mail service is active, the backup mail database file may go out of sync with the backup folder. If you restore while mail service is active, the active mail database file might go out of sync with the active folder.

An incremental backup of the mail service folder can be fast and efficient. If you back up your mail data incrementally, the only files copied are the small database file and the message files that are new or changed since the last backup.

After restoring the mail service folder, notify users that messages stored on the server have been restored from a backup copy.

If you're using the UNIX Sendmail program or another mail transfer agent instead of Mac OS X Server's SMTP service, you should also back up the contents of the /var/mail folder. This folder is the standard location for UNIX mail delivery.

Monitoring Mail Messages and Folders

This section describes how to perform common administrator tasks for monitoring mail messages. It shows how to:

- Designate an account as a mail administrator account.
- Save mail messages for monitoring and archival purposes.

Allowing Administrator Access to the Mail Folders

You can configure IMAP to allow the server administrator to view the mail service hierarchy. Administrators cannot view mail itself, only users folder locations. Administrators can also create globally shared folders and set user quotas. To take advantage of this administrator access, you must use an email client that allows you to connect via the standard IMAP port (143).

When you connect as the IMAP administrator, you see all the user mail folders stored on the server. Each user's mailbox appears as a separate folder in your mail client. You can remove inactive mailbox folders that belonged to deleted user accounts.

To configure administrator access to the mail folders:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the General tab and select Enable IMAP, if it is not already checked.
4. Select an existing user or create a new user using Workgroup Manger to be an IMAP administrator.
5. If you have not created a user record for the mail administrator's account, see the user management guide.
6. Open /etc/imapd.conf in a text editor.

   If you are not comfortable using a terminal text editor like emacs or vi, you can use TextEdit.
7. Find the line that reads "admins:"
8. Edit the line to add the UID number of the administrator account after the colon.
9. Save your changes.
10. In your email client application, create an account that uses IMAP to connect to your mail service using the mail administrator name.

For more information, see the man page for imapd.conf.

Saving Mail Messages for Monitoring and Archival Purposes

You can configure mail service to send blind carbon copies (Bcc) of each incoming or outgoing message to a user or group that you specify. You might want to do this if you need to monitor or archive messages. Senders and receivers of mail don't know that copies of their mail are being archived.

You can set up the specified user or group to receive the blind carbon copies using POP, then set up a client email application to log in periodically and clean out the account by retrieving all new messages. Otherwise, you may want to periodically copy and archive the messages directly from the destination directory with automated shell commands. You can set up filters in the email client to highlight certain types of messages. Additionally, you can archive all messages for legal reasons.

To save all messages:

1. In Server Admin, select Mail in the Computers & Services pane.
2. Click Settings.
3. Select the General tab.
4. Check "Copy incoming and outgoing messages to" and type a user name or group name.
5. Click Save.

Monitoring Mail Service

This section describes how to use the Server Admin application to monitor the following:

- Overall mail service activity, including the number incoming or outgoing connected mail connections.
- Current connected mail users.
- Mail accounts.
- Mail service logs.

This section also describes how Mac OS X Server reclaims disk space used by logs and how you can reclaim space manually.

Viewing Overall Mail Service Activity

You can use Server Admin to see an overview of mail service activity. The overview reports whether the service is running, when mail service started, and incoming and outgoing connections by protocol.

To see an overview of mail service activity:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click the Overview button.

Viewing the Mail Connections List

The Server Admin application can list the users who are currently connected to the mail service. For each user, you see the user name, IP address of the client computer, type of mail account (IMAP or POP), number of connections, and the connection length.

To view a list of mail users who are currently connected:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click the Connections button.

Viewing Mail Accounts

You can use the Server Admin application to see a list of users who have used their mail accounts at least once. For each account, you see the user name, disk space quota, disk space used, and the percent of space that is available to the user. Mail accounts that have never been used are not listed.

To view a list of mail accounts:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click the Accounts button.

Viewing Mail Service Logs

The mail service maintains four logs, and you can use Server Admin to view them.

- *Server log:* General mail service information goes into the Server log.
- *IMAP log:* IMAP-specific activity goes into this log.
- *POP log:* POP specific activity goes into this log.
- *SMTP log:* SMTP specific activity goes into this log.

To view a mail service log:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click the Logs button.
3. Choose a log type from the Show pop-up menu.

Setting Mail Service Log Detail Level

Mail service logs can show several levels of reported detail. The three levels of detail are:

- Low (errors only)
- Medium (errors and messages)
- High (all events)

To set the mail service log detail:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Logging tab.
4. Choose a detail level from the Log Detail Level pop-up menu.

Archiving Mail Service Logs by Schedule

Mac OS X Server automatically archives mail service logs after a certain amount of time. Each archive log is compressed and uses less disk space than the original log file. You can customize the schedule to archive the logs after a set period of time, measured in days.

To archive logs by schedule:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Logging tab.
4. Enter the desired number of days.

Reclaiming Disk Space Used by Mail Service Log archives

Mac OS X Server automatically reclaims disk space used by mail service logs when they reach a certain size or age. If you are comfortable using the Terminal application and UNIX command-line tools, you can use the command-line tool "diskspacemonitor" to monitor disk space whenever you want, and delete or move the log archives. For additional information, see "diskspacemonitor" in the command-line administration guide.

Dealing With a Full Disk

Mail services become erratic and suffer from data corruption if the disk storing your mail reaches maximum capacity. When your disk reaches full capacity, you'll experience the following behaviors:

- **Postfix behavior**

If the operating system can still spawn the smtpd process, Postfix will try to function and attempt to accept the message. The message will then be rejected with a "disk full" error. Otherwise, its behavior is unpredictable.

- **Cyrus behavior**

If the operating system can still spawn an imapd or pop3d process, the server will attempt to open the user's mail account. Upon success, the user can access mail as normal. Any changes that require database additions and causing the database to grow can cause the process to hang and corrupt the database.

Working With Undeliverable Mail

Mail messages might be undeliverable for several reasons. You can configure your mail service to forward undeliverable incoming mail, limit attempts to deliver problematic outgoing mail, report failed delivery attempts, and change mail service timeouts to increase chances of connection success.

Incoming mail might be undeliverable because it has a misspelled address or is addressed to a deleted user account. Outgoing mail might be undeliverable because it's misaddressed or the destination mail server is not working.

Forwarding Undeliverable Incoming Mail

You can have mail service forward messages that arrive for unknown local users to another person or a group in your organization. Whoever receives forwarded mail that's incorrectly addressed (with a typo in the address, for example) can forward it to the correct recipient. If forwarding of these undeliverable messages is disabled, the messages are returned to sender.

To set up forwarding of undeliverable incoming mail:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the General tab.
4. Check "Forward mail addressed to unknown local users" and type a user name or group name.
5. Click Save.

Where to Find More Information

You can find more information about mail service in books and on the Internet.

Books

For general information about mail protocols and other technologies, see these books:

- A good all-around introduction to mail service can be found in *Internet Messaging,* by David Strom and Marshall T. Rose (Prentice Hall, 1998).
- For more information on MX records, see "DNS and Electronic Mail" in *DNS and BIND,* 3rd edition, by Paul Albitz, Cricket Liu, and Mike Loukides (O'Reilly and Associates, 1998).
- Also of interest may be *Removing the Spam: Email Processing and Filtering,* by Geoff Mulligan (Addison-Wesley Networking Basics Series, 1999).
- To learn about email standards, see *Essential E-Mail Standards: RFCs and Protocols Made Practical,* by Pete Loshin (John Wiley & Sons, 1999).
- To learn more about Postfix, see *Postfix*, by Richard Blum (Sams; 1st edition, 2001)
- To learn more about Cyrus, see *Managing IMAP,* by Dianna Mullet, Kevin Mullet (O'Reilly & Associates, 2000)

Internet

There is an abundance of information about the different mail protocols, DNS, and other related topics on the Internet.

Request for Comments (RFC) documents provide an overview of a protocol or service and details about how the protocol should behave. If you are a novice server administrator, you may find some of the RFC background information helpful. If you are an experienced server administrator, you will find all the technical details about a protocol in its RFC document. You can search for RFC documents by number at this web site:

www.faqs.org/rfcs

For technical details about how mail protocols work, see these RFC documents:

- *POP:* RFC 1725
- *IMAP:* RFC 2060
- *SMTP:* RFC 821 and RFC 822

For more information about Postfix, go to:
www.postfix.org

For more information about Cyrus, go to:
asg.web.cmu.edu/cyrus

For more information about Sendmail, go to:
www.sendmail.org

You can find out more about servers that filter junk mail at this web site:
www.ordb.org

Mailing Lists

3

Mailing lists distribute a single email message to multiple recipients. Mailing lists differ from workgroups in a few fundamental ways. First, mailing lists are not linked to file or directory permissions. Mailing lists can be administered by someone other than the workgroup or server administrator. More importantly, mailing list subscribers do not have to have any kind of account (mail or file access) on the list's server; any email address can be added to the list. Finally, list subscribers can often remove themselves from lists, and add themselves to lists.

Mac OS X Server uses Mailman version 2.1.2 for its mailing list service. You can find more information about Mailman at the website www.list.org.

Setting Up a List

This section describes the process of setting up a mailing list. To do this, you enable the service, define a list name, and add subscribers to the list.

Enabling Mailing Lists

Before you can define mailing lists and subscribers, you need to enable the list service.

To enable the mailing lists:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Click Enable Mailing Lists.
5. Click Save.

Defining a List Name

The list name is the email account name to which mailing list users will send their mail.

To define a list's name:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Click the Add button under the List pane.
5. Enter the list's name.
6. Click Users May Self Subscribe, if necessary.
7. Click Save.

Adding a Subscriber

Server Admin lets you add mailing list subscribers to an existing list. Mailing list subscribers need not have any kind of account (mail or file access) on the list's server; any email address can be added to the list. You must have an existing list to add a subscriber.

If the subscriber is a user on the mail server, you can use the Users and Groups button to add a local subscriber to the list.

To add a single subscriber:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the list to which you want to add a subscriber.
5. Click the Add button under the Users pane.
6. Enter the recipient's email address.

   If you are entering multiple subscribers, enter all the recipients' email addresses or drop a text list onto the User Identifier pane. If the subscribers are users on the mail server, you can use the Users and Groups button to add a local groups to the list.
7. Assign the subscriber privileges.
8. Click OK.

Changing a List

After a list is created, you can add or remove people from an existing list. You may want to give list administration privileges to a user, or change a user's ability to receive or post to the list.

Adding a Subscriber to an Existing List

This is the same procedure as adding a user to a newly created list.

To add a subscriber to an existing list:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the List to which you want to add a subscriber.
5. Click the Add button under the Users pane.
6. Enter the recipient's email address.
7. Assign the subscriber privileges.
8. Click OK.

Removing a List Subscriber

You can remove a subscriber from a mailing list, either forcibly or by request.

To remove a list subscriber

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the list from which you want to remove a subscriber.
5. Select the subscriber from the User pane.

   Hold down the Shift or Command key to select multiple subscribers.
6. Click the Delete button under the Users pane.
7. Confirm the delete.

Changing Subscriber Posting Privileges

Sometimes you may want an "announce only" list, where recipients can't post to the address.

To add or remove a subscriber's posting privileges:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the List from which has the desired subscriber.
5. Select the subscriber from the User pane.
6. Click the Edit button under the Users pane.

   Hold down the Shift or Command key to select multiple subscribers.
7. Uncheck or check "User can post to list" as necessary.
8. Click OK.

Suspending a Subscriber

You can keep a user on a mail list and still allow him or her to post to a list without receiving the list messages. In this case, you can temporarily suspend a user's subscription to a list.

To suspend a user's subscription to a list:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the List from which has the desired subscriber.
5. Select the subscriber from the User pane.
6. Click the Edit button under the Users pane.

   Hold down the Shift or Command key to select multiple subscribers.
7. Uncheck or check "User subscribes to list" as necessary.
8. Click OK.

Administering Lists

Mailing lists can be administered by a designated list member, called "list administrators." List administrators can add or remove subscribers, and can designate other list administrators.

If the designated list administrator is not an administrator of the server, all of his or her tasks are done by sending email to the list address with commands in the subject line or body. To find out more about the commands available to list administrators, please see the website www.list.org.

Designating a List Administrator

When you set up a list, you can designate another user to administer the mailing list.

To designate a list administrator:

1. In Server Admin, select Mail in the Computer & Services list.
2. Click Settings.
3. Select the Mailing Lists tab.
4. Select the list from which has the desired subscriber.
5. Select the subscriber from the User pane.
6. Click the Edit button under the Users pane.
7. Uncheck or check "User can administer the list" as necessary.
8. Click OK.

Where to Find More Information

To find out more about Mailman and its capabilities, see www.list.org.

Glossary

This glossary defines terms and spells out abbreviations you may encounter while working with online help or other Mac OS X Server Documentation. References to terms defined elsewhere in the glossary appear in *italics.*

alias Another name at your domain that is not the user's login name, but will send incoming email to that user.

DNS (Domain Name System) A distributed database that maps IP addresses to domain names. A DNS server, also known as a name server, keeps a list of names and the IP addresses associated with each name.

filter A "screening" method used to control access to your server. A filter is made up of an IP address and a subnet mask, and sometimes a port number and access type. The IP address and the subnet mask together determine the range of IP addresses to which the filter applies.

firewall Software that protects the network applications running on your server. IP Firewall service, which is part of Mac OS X Server software, scans incoming IP packets and rejects or accepts these packets based on a set of filters you create.

IMAP (Internet Message Access Protocol) A client-server mail protocol that allows users to store their mail on the mail server rather than download it to the local machine. Mail remains on the server until the user deletes it.

IP (Internet Protocol) A method used with Transmission Control Protocol (TCP) to send data between computers over a local network or the Internet. IP delivers packets of data, while TCP keeps track of data packets.

ISP (Internet service provider) A business that sells Internet access and often provides web hosting for ecommerce applications as well as mail services.

Kerberos A secure network authentication system. Kerberos uses tickets, which are issued for a specific user, service, and period of time. Once a user is authenticated, it is possible to access additional services without retyping a password (this is called single-sign on) for services that have been configured to take Kerberos tickets. Mac 0S X Server uses Kerberos v5.

LDA (local delivery agent) A mail service agent that transfers mail messages from incoming mail storage to the email recipient's inbox. The LDA is responsible for handling local delivery of messages, and making mail accessible to the user's email application.

list administrator A *mailing list* administrator. List administrators can add or remove subscribers from mailing lists, and designate other list administrators. List administrators are not necessarily local machine or domain administrators.

load balancing The process of distributing the demands by client computers for network services across multiple servers in order to optimize performance by fully utilizing the capacity of all available servers.

MAA (mail access agent) A mail service that communicates with a user's email program to download mail messages or headers to the user's local machine.

mail exchanger The computer that provides your mail service. Synonymous with *mail host*.

mail host The computer that provides your mail service. Synonymous with *mail exchanger*.

mailing list A mail service to distribute a single email message to multiple recipients. Mailing list subscribers do not have to be mail users on your mail server. Mailing lists can be administered by a *list administrator*. Mailing list subscribers can often add or remove themselves from lists.

MTA (mail transfer agent) A mail service that sends outgoing mail, receives incoming mail for local recipients, and forwards incoming mail of nonlocal recipients to other MTAs.

MUA (mail user agent) A mail process on a user's local machine that works with the *MAA* to download mail messages and headers to the user's local machine. This is most commonly referred to as an "email application," or "email program."

MX record (mail exchange record) An entry in a *DNS* table that specifies which computer manages mail for an Internet domain. When a mail server has mail to deliver to an Internet domain, the mail server requests the MX record for the domain. The server sends the mail to the computer specified in the MX record.

name server See *DNS (Domain Name System)*.

open relay A server that receives and automatically forwards mail to another server. Junk mail senders exploit open relay servers to avoid having their own mail servers blacklisted as sources of *spam*.

ORBS (Open Relay Behavior-modification System) An Internet service that blacklists mail servers known to be or suspected of being *open relays* for senders of junk mail. ORBS servers are also known as *RBL (real-time black-hole list)* servers.

percent symbol (%) The command-line prompt in the Terminal application. The prompt indicates that you can enter a command.

POP (Post Office Protocol) A protocol for retrieving incoming mail. After a user retrieves POP mail, it is stored on the user's computer and usually is deleted automatically from the mail server.

privileges Settings that define the kind of access users have to shared items. You can assign four types of privileges to a share point, folder, or file: read and write, read only, write only, and none (no access).

RBL (real-time black-hole list) An Internet service that blacklists mail servers known to be or suspected of being *open relays* for senders of junk mail.

relay point See *open relay.*

short name An abbreviated name for a user. The short name is used by Mac OS X for home directories, authentication, and email addresses.

SMTP (Simple Mail Transfer Protocol) A protocol used to send and transfer mail. Its ability to queue incoming messages is limited, so SMTP usually is used only to send mail, and *POP* or *IMAP* is used to receive mail.

spam Unsolicited email; junk mail.

SSL (Secure Sockets Layer) An Internet protocol that allows you to send encrypted, authenticated information across the Internet.

TCP (Transmission Control Protocol) A method used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. IP takes care of handling the actual delivery of the data, and TCP takes care of keeping track of the individual units of data (called packets) into which a message is divided for efficient routing through the Internet.

UCE (unsolicited commercial email) See *spam*.

UDP (User Datagram Protocol) A communications method that uses the Internet Protocol (IP) to send a data unit (called a datagram) from one computer to another in a network. Network applications that have very small data units to exchange may use UDP rather than TCP.

UID (user ID) A number that uniquely identifies a user. Mac OS X computers use the UID to keep track of a user's directory and file ownership.

user name The long name for a user, sometimes referred to as the user's "real" name. See also *short name*.

virtual domain Another domain which can be used in email addresses for your mail users. A list of all the domain names for which your mail server is responsible.

virtual user An alternate email address (*short name*) for a user. Similar to an *alias*, but it involves another user account.

Index