Mac OS X Server

Advanced Server Administration
Version 10.6 Snow Leopard

Apple
1 Infinite Loop
Cupertino, CA 95014-2084
www.apple.com

019-1410/2009-08-15

Contents

About This Guide

This guide provides a starting point for administering Mac OS X Server v10.6 using its advanced administration tools. It contains information about planning, practices, tools, installation, deployment, and more by using Server Admin.

Advanced Server Administration is not the only guide you need when administering advanced mode server, but it gives you a basic overview of planning, installing, and maintaining Mac OS X Server using Server Admin.

What's in This Guide

This guide includes the following chapters:

- Chapter 1, "System Overview and Supported Standards," provides an overview of Mac OS X Server systems and standards.
- Chapter 2, "Planning Server Usage," gives you advice for planning Mac OS X Server deployment.
- Chapter 3, "Administration Tools," is a reference guide for the tools used to administer servers.
- Chapter 4, "Enhancing Security," is a brief guide to security policies and practices.
- Chapter 5, "Installation and Deployment," is an installation guide for Mac OS X Server.
- Chapter 6, "Initial Server Setup," provides a guide to setting up your server after installation.
- Chapter 7, "Ongoing System Management," explains how to work with Mac OS X Server and services.
- Chapter 8, "Monitoring Your System," shows you how to monitor and log into Mac OS X Server.

Note: Because Apple periodically releases new versions and updates to its software, images shown in this book may be different from what you see on your screen.

Using Onscreen Help

You can get task instructions onscreen in Help Viewer while you're managing Mac OS X Server v10.6. You can view help on a server or an administrator computer. (An administrator computer is a Mac OS X computer with Mac OS X Server v10.6 administration software installed on it.)

To get the most recent onscreen help for Mac OS X Server v10.6:

- Open Server Admin or Workgroup Manager and then:
  - Use the Help menu to search for a task you want to perform.
  - Choose Help > Server Admin Help or Help > Workgroup Manager Help to browse and search the help topics.

  The onscreen help contains instructions taken from *Advanced Server Administration* and other advanced administration guides described later.

To see the most recent server help topics:

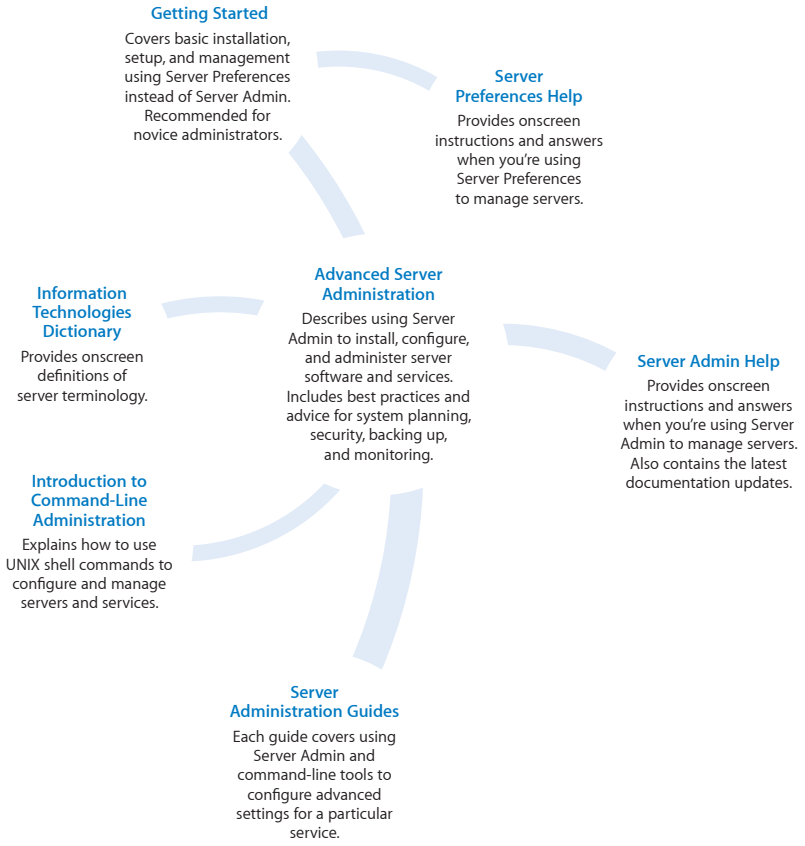
- Make sure the server or administrator computer is connected to the Internet while you're getting help.

  Help Viewer automatically retrieves and caches the most recent server help topics from the Internet. When not connected to the Internet, Help Viewer displays cached help topics.

Document Road Map

Mac OS X v10.6 has a suite of guides which can cover management of individual services. Each service may be dependent on other services for maximum utility. The road map below shows some related documentation that you may need to fully configure your desired service to your specifications. You can get these guides in PDF format from the Mac OS X Server documentation website:

www.apple.com/server/resources/



Viewing PDF Guides Onscreen

While reading the PDF version of a guide onscreen:

- Show bookmarks to see the guide's outline, and click a bookmark to jump to the corresponding section.
- Search for a word or phrase to see a list of places where it appears in the document. Click a listed place to see the page where it occurs.
- Click a cross-reference to jump to the referenced section. Click a web link to visit the website in your browser.

Printing PDF Guides

If you want to print a guide, you can take these steps to save paper and ink:

- Save ink or toner by not printing the cover page.
- Save color ink on a color printer by looking in the panes of the Print dialog for an option to print in grays or black and white.
- Reduce the bulk of the printed document and save paper by printing more than one page per sheet of paper. In the Print dialog, change Scale to 115% (155% for *Getting Started*). Then choose Layout from the untitled pop-up menu. If your printer supports two-sided (duplex) printing, select one of the Two-Sided options. Otherwise, choose 2 from the Pages per Sheet pop-up menu, and optionally choose Single Hairline from the Border menu. (If you're using Mac OS X v10.4 or earlier, the Scale setting is in the Page Setup dialog and the Layout settings are in the Print dialog.)

You may want to enlarge the printed pages even if you don't print double sided, because the PDF page size is smaller than standard printer paper. In the Print dialog or Page Setup dialog, try changing Scale to 115% (155% for *Getting Started,* which has CD-size pages).

Getting Documentation Updates

Periodically, Apple posts revised help pages and new editions of guides. Some revised help pages update the latest editions of the guides.

- To view new onscreen help topics for a server application, make sure your server or administrator computer is connected to the Internet and click "Latest help topics" or "Staying current" in the main help page for the application.
- To download the latest guides in PDF format, go to the Mac OS X Server documentation website:

  www.apple.com/server/resources/
- An RSS feed listing the latest updates to Mac OS X Server documentation and onscreen help is available. To view the feed use an RSS reader application, such as Safari or Mail:

  feed://helposx.apple.com/rss/snowleopard/serverdocupdates.xml

Getting Additional Information

For more information, consult these resources:

- *Read Me documents*—get important updates and special information. Look for them on the server discs.
- *Mac OS X Server website* (www.apple.com/server/macosx/)—enter the gateway to extensive product and technology information.
- *Mac OS X Server Support website* (www.apple.com/support/macosxserver/)—access hundreds of articles from Apple's support organization.
- *Apple Discussions website* (discussions.apple.com/)—share questions, knowledge, and advice with other administrators.
- *Apple Mailing Lists website* (www.lists.apple.com/)—subscribe to mailing lists so you can communicate with other administrators using email.
- *Apple Training and Certification website* (www.apple.com/training/)—hone your server administration skills with instructor-led or self-paced training, and differentiate yourself with certification.

System Overview and Supported Standards

1

Mac OS X Server gives you everything you need to provide standards-based workgroup and Internet services — delivering a world-class UNIX server solution that's easy to deploy and easy to manage.

This chapter contains information to make decisions about where and how you deploy Mac OS X Server. It contains general information about configuration options, standard protocols used, its UNIX roots, and network and firewall configurations necessary for Mac OS X Server administration.

System Requirements for Installing Mac OS X Server v10.6

The Macintosh desktop computer or server onto which you install Mac OS X Server v10.6 must have:

- An Intel processor
- At least 2 gigabytes (GB) of random access memory (RAM)
- At least 10 gigabytes (GB) of available disk space
- A new serial number for Mac OS X Server v10.6

  The serial number used with any previous version of Mac OS X Server will not allow registration for v10.6.

A built-in DVD drive is convenient but not required.

A display and keyboard are optional. You can install server software on a computer that has no display and keyboard by using an administrator computer. For more information, see "Setting Up an Administrator Computer" on page 124.

If you're using an installation disc for Mac OS X Server v10.6, you can control installation from another computer using VNC viewer software. Open-source VNC viewer software is available. Apple Remote Desktop, described on "Apple Remote Desktop" (page 50), includes VNC viewer capability.

What's New in Mac OS X Server v10.6

Mac OS X Server v10.6 offers major enhancements in several key areas:

- Address Book Server

  Mac OS X Server v10.6 introduces the first open standards-based Address Book Server Based on the emerging CardDAV specification, which uses WebDAV to exchange vCards, sharing contacts across multiple computers.

- Remote Access

  Mac OS X Server v10.6 delivers push notifications to users outside your firewall, and a proxy service gives them secure remote access to email, address book contacts, calendars, and specified internal websites.

- Collaboration services improvements

  Mac OS X Server v10.6 augments collaboration features with wiki and blog templates optimized for viewing on iPhone; provides content searching across multiple wikis; and enables attachment viewing in Quick Look. It also introduces My Page, which gives users one convenient place to access web applications, receive notifications, and view activity streams across wikis.

- iCal Server 2

  Mac OS X Server v10.6 has a new iCal Server which includes shared calendars, push notifications, the ability to send email invitations to non-iCal Server users, and a browser-based application for using calendars with many supported browsers.

- Podcast Producer 2

  Mac OS X Server v10.6 has a new Podcast Producer which features an intuitive new workflow editor, support for dual-video source capture, and Podcast Library, which lets you host locally stored podcasts and make them available for subscription by category via Atom web feeds.

- Mail Server improvements

  Mac OS X Server v10.6 mail service increases its performance and scalability using a new engine designed to handle thousands of simultaneous connections. Mail services have been enhanced to include server-side email rules and vacation messages.

- Multicore optimizations

  Mac OS X Server v10.6 supports "Grand Central," a new set of built-in technologies that makes all of Mac OS X Server multicore aware and optimizes it for allocating tasks across multiple cores and processors.

- 64-bit support

  Mac OS X Server v10.6 use 64-bit kernel technology to support up to 16 TB of memory.

- OpenCL support

  Mac OS X Server v10.6 supports OpenCL and makes it possible for developers to use the GPU for general computational tasks.

What's New in Server Admin

Included with Mac OS X Server v10.6 is Server Admin, Apple's powerful, flexible, full-featured server administration tool. Server Admin is reinforced with improvements in standards support and reliability. Server Admin also delivers a number of enhancements:

- Newly refined, streamlined, and integrated Server Assistant
- Smoother interaction with Server Preferences settings
- Improved user interface

Understanding Server Configuration Methods

You can configure and manage Mac OS X Server using two configuration methods: Server Preferences, or the advanced configuration tool suite, which includes Server Admin and its command-line utilities.

Servers administered using the advanced tool suite are the most flexible and require the most skill to administer. Servers administered by Server Preferences have fewer configuration options, but most configuration details are set by Server Preferences, without additional skill or labor. You can customize your server for a variety of purposes using either method.

Using Server Admin and the rest of the advanced configuration tool suite, the experienced system administrator has complete control of each service's configuration to accommodate a wide variety of needs. After performing initial setup with Setup Assistant, you use powerful administration applications such as Server Admin and Workgroup Manager, or command-line tools, to configure advanced settings for services the server must provide.

Using Server Preferences, you can get standard configurations of Mac OS X Server features using automated setup and simplified administration. For more information about using Server Preferences to administer your server, see *Getting Started*.

You can switch between Server Admin and Server Preferences. The setting changes in one application are reflected in the other's settings. However, some advanced or custom configurations can't be inspected or changed in Server Preferences, due to Server Preferences' simplified interface.

The following table highlights the capabilities of each configuration tool.

Service	Set in initial server setup	Server Preferences	Server Admin
Address book	Optional	Yes	Yes
Backup your data (websites, databases, calendar files, etc.)	No	No, use command-line tools and third-party backup solutions	No, use command-line tools and third-party backup solutions
Computer account and computer group management	No	Use Workgroup Manager	Use Workgroup Manager
DHCP, DNS, NAT	Automatic	No	Yes
File sharing (AFP and SMB protocols)	Optional	Yes	Yes
File sharing (FTP and NFS protocols)	No	No	Yes
Firewall (application firewall)	Automatic	Use System Preferences	Use System Preferences
Firewall (IP firewall)	Automatic	Yes	Yes
Gateway (NAT, DNS, DHCP)	Optional	No	Yes
iCal (calendar sharing, event scheduling)	Optional	Yes	Yes
iChat (instant messaging)	Optional	Yes	Yes
Mail with spam and virus filtering	Optional	Yes	Yes
Mobile access	No	No	Yes
MySQL	No	No	Yes
NetBoot and NetInstall (system imaging)	No	No	Yes
Network time	Automatic	No	Yes
Network management (SNMP)	No	No	Yes
NFS	No	No	Yes

Service	Set in initial server setup	Server Preferences	Server Admin
Open Directory master (user accounts and other data)	Optional	Optional	Yes
Podcast Producer	No	No	Yes
Policies and managed preferences	No	Use Workgroup Manager	Use Workgroup Manager
Print	No	No	Yes
Push notification	Automatic	Automatic	Yes
QuickTime Streaming	No	No	Yes
RADIUS	No	No	Yes
Remote login (SSH)	Optional	Use System Preferences	Yes
Software update	No	No	Yes
Time Machine backup of client Macs	Optional	Yes	Yes
Time Machine backup of server	No	Use System Preferences	Use System Preferences
User and Group creation	Optional	Yes	Yes
VPN (secure remote access)	No	Yes	Yes
Web (wikis, blogs, webmail)	Optional	Yes	Yes
Xgrid (computational clustering)	No	No	Yes, and also use Xgrid Admin
Xserve diagnostics	No	Use Server Monitor	Use Server Monitor

Supported Standards

Mac OS X Server provides standards-based workgroup and Internet services. Instead of developing proprietary server technologies, Apple has built on the best open source projects: Samba 3, OpenLDAP, Kerberos, Dovecot, Apache, Jabber, SpamAssassin, and more. Mac OS X Server integrates these robust technologies and enhances them with a unified, consistent management interface.

Because it is built on open standards, Mac OS X Server is compatible with existing network and computing infrastructures. It uses native protocols to deliver directory services, file and printer sharing, and secure network access to Mac, Windows, and Linux clients.

A standards-based directory services architecture offers centralized management of network resources using any LDAP server–even proprietary servers such as Microsoft Active Directory. The open source UNIX foundation makes it easy to port and deploy existing tools to Mac OS X Server.

The following standards-based technologies power Mac OS X Server:

- **Kerberos:** Mac OS X Server integrates an authentication authority based on MIT's Kerberos technology (RFC 1964) to provide users with single sign-on access to secure network resources.

  Using strong Kerberos authentication, single sign-on maximizes the security of network resources while providing users with easier access to a broad range of Kerberos-enabled network services.

  For services that have not yet been *Kerberized,* the integrated SASL service negotiates the strongest possible authentication protocol.

- **OpenLDAP:** Mac OS X Server includes a robust LDAP directory server and a secure Kerberos password server to provide directory and authentication services to Mac, Windows, and Linux clients.

  Apple has built the Open Directory server around OpenLDAP, the most widely deployed open source LDAP server, so it can deliver directory services for both Mac-only and mixed-platform environments.

  LDAP provides a common language for directory access, enabling administrators to consolidate information from different platforms and define one namespace for all network resources. This means there is a single directory for all Mac, Windows, and Linux systems on the network.

- **RADIUS:** Remote Authentication Dial-In User Service (RADIUS) is an authentication, authorization, and accounting protocol used by the 802.1x security standard for controlling network access by clients in mobile or fixed configurations. Mac OS X Server uses RADIUS to integrate with AirPort Base Stations serving as a central MAC address filter database. By configuring RADIUS and Open Directory, you can control who has access to your wireless network.

  Mac OS X Server uses the FreeRADIUS Server Project. FreeRADIUS supports the requirements of a RADIUS server, shipping with support for LDAP, MySQL, PostgreSQL, Oracle databases, EAP, EAP-MD5, EAP-SIM, EAP-TLS, EAP-TTLS, EAP-PEAP, and Cisco LEAP subtypes. Mac OS X Server supports proxying, with failover and load balancing.

- **Mail Service:** Mac OS X Server uses robust technologies from the open source community to deliver comprehensive, easy-to-use mail server solutions. Full support for Internet mail protocols—Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP)—ensures compatibility with standards-based mail clients on Mac, Windows, and Linux systems.

- **Web Technologies:** Mac OS X Server is a complete AMP stack (a bundle of integrated Apache-MySQL-PHP/Perl/Python software). Mac OS X Server web technologies are based on the open source Apache web server, the most widely used HTTP server on the Internet.

  With performance optimized for Mac OS X Server, Apache provides fast, reliable web hosting and an extensible architecture for delivering dynamic content and sophisticated web services. Because web service in Mac OS X Server is based on Apache, you can add advanced features with plug-in modules.

  Mac OS X Server includes everything professional web masters need to deploy sophisticated web services: integrated tools for collaborative publishing, inline scripting, Apache modules, custom CGIs, and JavaServer Pages and Java Servlets. Database-driven sites can be linked to the included MySQL database. ODBC and JDBC connectivity to other database solutions is also supported.

  Web service also includes support for Web-based Distributed Authoring and Versioning, known as WebDAV.

- **File Services:** You can configure Mac OS X Server file services to allow clients to access shared files, applications, and other resources over a network. Mac OS X Server supports most major service protocols for maximum compatibility, including:
  - *Apple Filing Protocol (AFP),* to share resources with clients who use Macintosh computers.
  - *Server Message Block (SMB),* a protocol to share resources with clients who use Windows computers. This protocol is provided by the Samba open source project.
  - *Network File System (NFS),* to share files and folders with UNIX clients.
  - *File Transfer Protocol (FTP),* to share files with anyone using FTP client software.
- **IPv6 (RFC 2460):** IPv6 is the Internet's next-generation protocol designed to replace the current Internet Protocol, IPv4 (or IP).

  IPv6 improves routing and network autoconfiguration. It increases the number of network addresses to over 3×10^{38}, and eliminates the need for NAT-provided addressing. IPv6 is expected to gradually replace IPv4 over a number of years, with the two coexisting during the transition.

  Mac OS X Server's network services are fully IPv6 capable and ready to transition to the next generation addressing as well as being fully able to operate with IPv4.

- **SNMP:** Simple Network Management Protocol (SNMP) is used to monitor network-attached devices' operational status. It is a set of IETF-designed standards for network management, including an Application Layer protocol, a database schema, and a set of data objects.

  Mac OS X Server uses the open source net-snmp suite to provide SNMPv3 (RFCs 3411-3418) service.

- **XMPP:** Extensible Messaging and Presence Protocol (XMPP) is an open XML-based messaging protocol used for messaging and presence information. XMPP serves as the basis for Mac OS X Server's Push Notification service, as well as iChat Server, and all publish and subscribe functions for the server.

Mac OS X Server's UNIX Heritage

Mac OS X Server has a UNIX foundation built around the Mach microkernel and the latest advances from the Berkeley Software Distribution (BSD) open source community. This foundation provides Mac OS X Server with a stable, high-performance, 64-bit computing platform for deploying server-based applications and services.

Mac OS X Server is built on an open source operating system called Darwin, which is part of the BSD family of UNIX-like systems. BSD is a family of UNIX variants descended from Berkeley's version of UNIX. Also, Mac OS X Server incorporates more than 100 open source projects in addition to proprietary enhancements and extended functionality created by Apple.

The BSD portion of the Mac OS X kernel is derived primarily from FreeBSD, a version of 4.4BSD that offers advanced networking, performance, security, and compatibility features.

In general, BSD variants are derived (sometimes indirectly) from 4.4BSD-Lite Release 2 from the Computer Systems Research Group (CSRG) at the University of California at Berkeley.

Although the BSD portion of Mac OS X is primarily derived from FreeBSD, some changes have been made. To find out more about the low-level changes made, see Apple's Developer documentation for Darwin.

Planning Server Usage

2

Before installing and setting up Mac OS X Server do a little planning and become familiar with your options.

The major goals of the planning phase are to make sure that:

- Server user and administrator needs are addressed by the servers you deploy
- Server and service prerequisites that affect installation and initial setup are identified

Installation planning is especially important if you're integrating Mac OS X Server into an existing network, migrating from earlier versions of Mac OS X Server, or preparing to set up multiple servers. But even single-server environments can benefit from a brief assessment of the needs you want a server to address.

Use this chapter to stimulate your thinking. It doesn't present a rigorous planning guide, nor does it provide the details you need to determine whether to implement a particular service and assess its resource requirements. Instead, view this chapter as an opportunity to think about how to maximize the benefits of Mac OS X Server in your environment.

Planning, like design, isn't necessarily a linear process. The sections in this chapter don't require you to follow a mandatory sequence. Different sections in this chapter present suggestions that could be implemented simultaneously or iteratively.

Determining Your Server Needs

During the planning stage, determine how you want to use Mac OS X Server and identify whether there's anything you need to accomplish before setting it up.

For example, you might want to convert an existing server to v10.6 and continue hosting directory, file, and mail services for clients on your network.

Before you install server software, you might need to prepare data to migrate to your new server, and perhaps consider whether it's a good time to implement a different directory services solution.

During the planning stage, you'll also decide which installation and server setup options best suit your needs. For example, *Getting Started* contains an example that illustrates server installation and initial setup in a small business scenario with the server in using Server Preferences.

Determining Whether to Upgrade or Migrate

If you're using a previous version of Mac OS X Server and you want to reuse data and settings, you can upgrade or migrate to v10.6.

You can upgrade to Mac OS X Server v10.6 if you're using the latest update of Mac OS X Server v10.5 Leopard or Mac OS X Server v10.4.11 on Mac OS X servers with Intel processors.

Upgrading is simple because it preserves existing settings and data. You can perform an upgrade using any of the installation methods described in this chapter or the advanced methods described in this guide.

If you can't perform an upgrade, for example when you need to reformat the startup disk or replace your server hardware, you can migrate data and settings to a computer that you've installed Mac OS X Server v10.6 on.

Migration is supported from the latest update of Mac OS X Server v10.5 Leopard or Mac OS X Server v10.4.11 Tiger. For complete information about migrating data and settings to a different Mac or Xserve, see the onscreen help or Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

Setting Up a Planning Team

Involve individuals in the installation planning process who represent various points of view, and who can help answer the following questions:

- What day-to-day user requirements must a server meet? What activities do server users and workgroups depend on the server for?

  If the server is used in a classroom, make sure the instructor who manages its services and administers it daily provides input.

- What user management requirements must be met? Will user computers be diskless and need to be started up using NetBoot? Will Macintosh client management and network home folders be required?

  Individuals with server administration experience should work with server users who might not have a technical background, so they'll understand how specific services might benefit them.

- What existing non-Apple services, such as Active Directory, must the server integrate with?

If you've been planning to replace a Windows NT computer, consider using Mac OS X Server with its extensive built-in support for Windows clients. Make sure that administrators familiar with these other systems are part of the planning process.

- What are the characteristics of the network into which the server will be installed? Do you need to upgrade power supplies, switches, or other network components? Is it time to streamline the layout of facilities that house your servers?

  An individual with systems and networking knowledge can help with these details as well as completing the *Installation & Setup Worksheet* on the *Mac OS X Server Install Disc* or *Administration Tools* CD.

Identifying Servers to Set Up

Conduct a server inventory:

- How many servers do you have?
- How are they used?
- How can you streamline the use of servers you want to keep?
- Do existing servers need to be retired? Which servers can Mac OS X Server replace?
- Which non-Apple servers will Mac OS X Server need to be integrated with? Why?
- Do you have Mac OS X Server computers that need to be upgraded to version 10.6?
- How many new Mac OS X Server computers will you need to set up?

Determining Services to Host on Each Server

Identify which services you want to host on each Mac OS X Server and non-Apple server you decide to use.

Distributing services among servers requires an understanding of users and services. Here are a few examples of how service options and hardware and software requirements can influence what you put on servers:

- Directory services implementations can range from using directories and Kerberos authentication hosted by non-Apple servers to setting up Open Directory directories on servers distributed throughout the world.

  Directory services require thoughtful analysis and planning. The additional information at Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ can help you understand the options and opportunities.

- Home folders for network users can be consolidated onto one server or distributed among various servers. Although you can move home folders, you might need to change a large number of user and share point records, so devise a strategy that will persist for a reasonable amount of time. For information about home folders, see Mac OS X Server help or Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.
- Some services offer ways to control the amount of disk space used by individual users. For example, you can set up home folder and mail quotas for users. Consider whether using quotas will offer a way to maximize the disk usage on a server that stores home folders and mail databases. The additional information at Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ describes home folder and user mail quotas, and service-wide mail quotas.
- Disk space requirements are also affected by the type of files a server hosts. Creative environments need high-capacity storage to accommodate large media files, but elementary school classrooms have more modest file storage needs. The additional information at Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ describe file sharing.
- If you're setting up a streaming media server, allocate enough disk space to accommodate a specific number of hours of streamed video or audio. For hardware and software requirements and for a setup example, see additional information in online help or at Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ .
- The number of NetBoot client computers you can connect to a server depends on the server's Ethernet connections, the number of users, the amount of available RAM and disk space, and other factors. DHCP service needs to be available to the clients and can be provided by a different server than the NetBoot server. For NetBoot capacity planning guidelines, see additional information at Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ .
- Mac OS X Server offers extensive support for Windows users. You can consolidate Windows user support on servers that provide PDC services, or you can distribute services for Windows users among different servers.
- If you want to use software RAID to stripe or mirror disks, you'll need two or more drives (but not FireWire drives) on a server. For more information, see online Disk Utility Help.

Before finalizing decisions about which servers will host specific services, familiarize yourself with information in the administration guides for the services you want to deploy.

Defining a Migration Strategy

If you're using Mac OS X Server v10.4–10.5 or a Windows-based server, examine the opportunities for moving data and settings to Mac OS X Server v10.6.

Upgrading and Migrating from an Earlier Version of Mac OS X Server

If you're using computers with Mac OS X Server v10.4 or v10.5, consider upgrading or migrating them to Mac OS X Server v10.6.

If you're using Mac OS X Server v10.5 or v10.4 and you don't need to move to Intel-processor based hardware, you can perform an upgrade installation. Upgrading is simple because it preserves your existing settings and data.

When you can't use the upgrade approach, you can migrate data and settings. You'll need to migrate, not upgrade, when:

- A version 10.4 or 10.5 server's hard disk needs reformatting or the server doesn't meet the minimum Mac OS X Server v10.6 system requirements. For more information, "System Requirements for Installing Mac OS X Server v10.6" on page 16.
- You want to move data and settings you've been using on a v10.4 or 10.5 server to different server hardware.

Migration is supported from the latest versions of Mac OS X Server v10.5 and v10.4. When you migrate, you install and set up Mac OS X Server v10.6, then restore files onto it from the earlier server, and then make manual adjustments as required.

For complete information, read the additional information at Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ .

Migrating from Windows

Mac OS X Server v10.6 can provide a variety of services to users of Microsoft Windows computers. By providing these services, Mac OS X Server v10.6 can replace Windows servers in small workgroups.

For information about migrating users, groups, files, and more from a Windows-based server to Mac OS X Server, see the additional information at Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ .

Defining an Integration Strategy

Integrating Mac OS X Server into a heterogeneous environment has two aspects:

- Configuring Mac OS X Server to take advantage of existing services
- Configuring non-Apple computers to use Mac OS X Server

The first aspect primarily involves directory services integration. Identify which Mac OS X Server computers will use existing directories (such as Active Directory, LDAPv3, and NIS directories) and existing authentication setups (such as Kerberos).

For options and instructions, see the additional information at Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ . Integration can be as easy as enabling a Directory Utility option, or it might involve adjusting existing services and Mac OS X Server settings.

The second aspect is largely a matter of determining the support you want Mac OS X Server to provide to non-Apple computer users. The additional information at Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ tell you what's available.

Defining Physical Infrastructure Requirements

Determine whether you need to make site or network topology adjustments before installing and setting up servers.

- Who will administer the server, and what kind of server access will administrators need?

  Classroom servers might need to be conveniently accessible for instructors, while servers that host network-wide directory information should be secured with restricted physical access in a district office building or centralized computer facility.

  Because Mac OS X Server administration tools offer complete remote server administration support, there are few times when an administrator should need physical access to a server.
- Are there air conditioning or power requirements that must be met? For this kind of information, see the documentation that comes with server hardware.
- Are you considering upgrading elements such as cables, switches, and power supplies? Now may be a good time to do it.
- Have you configured your TCP/IP network and subnets to support the services and servers you want to deploy?
- Are you considering moving your servers to different IP addresses or hostnames? Now may be a good time to do it.

Defining Server Setup Infrastructure Requirements

The server setup infrastructure consists of the services and servers you set up in advance because other services or servers depend on them.

For example, if you use Mac OS X Server to provide DHCP, network time, or BootP services to other servers, you should set up the servers that provide these services and initiate the services before you set up servers that depend on those services.

The amount of setup infrastructure you require depends on the complexity of your site and what you want to accomplish. In general, DHCP, DNS, and directory services are recommended or required for medium and large server networks:

- The most fundamental infrastructure layer comprises network services like DHCP and DNS.

  All services run better if DNS is on the network, and many services require DNS to work properly. If you're not hosting DNS, work with the administrator responsible for the DNS server you'll use when you set up your servers. DNS requirements for services are published in the service-specific administration guides.

  The DHCP setup reflects your physical network topology.

- Another crucial infrastructure component is directory services, required for sharing data among services, servers, and user computers.

  The most common shared data in a directory is for users and groups, but configuration information such as mount records and other directory data is also shared. A directory services infrastructure is necessary to host cross-platform authentication and when you want services to share the same names and passwords.

Here's an example of the sequence in which you might set up a server infrastructure that includes DNS, DHCP, and directory services. You can set up the services on the same server or on different servers:

Setting up basic server infrastructure:

1. Set up the DNS server, populating the DNS with the host names of the desired servers and services.
2. Set up DHCP, configuring it to specify the DNS server address so it can be served to DHCP clients.

   If desired, set up DHCP-managed static IP address for the servers.
3. Set up a directory server, including Windows PDC service if required, and populate the directory with data, such as users, groups, and home folder data.

   This process can involve importing users and groups, setting up share points, setting up managed preferences, and so forth.
4. Configure DHCP to specify the address of the directory server so it can be served to DHCP clients.

Your specific needs can affect this sequence. For example, to use VPN, NAT, or IP Firewall services, include their setup with the DNS and DHCP setups.

Making Sure Required Server Hardware Is Available

You might want to postpone setting up a server until all its hardware is in place.

For example, you might not want to set up a server whose data you want to mirror until all disk drives you need for mirroring are available. You might also want to wait until a RAID subsystem is set up before setting up a home folder server or other server that will use it.

Minimizing the Need to Relocate Servers After Setup

Before setting up a server, try to place it in its final network location (IP subnet). If you're concerned about preventing unauthorized or premature access during setup, set up a firewall to protect the server while finalizing its configuration.

If you can't avoid moving a server after initial setup, you must change settings that are sensitive to network location before you can use the server. For example, the server's IP address and DNS name, stored in directories and configuration files on the server, must be updated.

When you move a server, follow these guidelines:

- Minimize the time the server is in its temporary location so the amount of information you need to change is limited.
- Postpone configuring services that depend on network settings until the server is in its final location. Such services include Open Directory replication, Apache settings (such as virtual domains), DHCP, and other network infrastructure settings that other computers depend on.
- Wait to import final user accounts. Limit accounts to test accounts so you minimize the user-specific network information (such as home folder location) that you must change after the move.
- After you move the server, you can change its IP address in the Network pane of System Preferences (or use the `networksetup` tool).

  You probably will need to manually adjust service and system settings. For more information on how to do this, see "Understanding Changes to the Server IP Address or Network Identity" on page 132.
- Reconfigure the search policy of computers (such as user computers and DHCP servers) that have been configured to use the server in its original location.

Defining Backup and Restore Policies

All storage systems can fail eventually. Either through equipment wear and tear, accident, or disaster, your data and configuration settings are vulnerable to loss. You should have a plan in place to prevent or minimize your data loss.

Understanding Backup and Restore Policies

There are many reasons to have a backup and restore policy. Your data is subject to failure because of failed components, natural or manmade disasters, or data corruption. Sometimes data loss is beyond your control to prevent, but with a backup and restore plan, you can restore your data.

You need to customize backup and restore policies to take into account your situation, what data needs to be saved, how often, and how much time and effort is used to restore it. Your policy specifies the procedures and practices that fulfill your restoration needs.

Backups are an investment of time, money, and administration effort, and they can affect performance. However, there is a clear return on investment in the form of data integrity. You can avoid substantial financial, legal, and organizational costs with a well-planned, well-executed backup and restore policy.

There are essentially three kinds of restoration needs:

- Restoring a deleted or corrupt file
- Recovering from disk failure (or catastrophic file deletion)
- Archiving data for an organization need (financial, legal, or other need)

Each restoration need determines the type, frequency, and method you use to back up your data.

You might want to keep daily backups of files. This allows for quick restoration of overwritten or deleted files. In such a case you have file-level granularity every day: any single file can be restored the following day.

There are other levels of granularity as well. For example, you might need to restore a full day's data. This is a daily snapshot-level granularity: you can restore your organization's data as it was on a given day.

These daily snapshots might not be practical to maintain every day, so you might choose to keep a set of rolling snapshots that give you daily snapshot-level granularity for only the preceding month.

Other levels of restoration you might want or need could be quarterly or semiannually.

You might also need archival storage, which is data stored only to be accessed in uncommon circumstances. Archival storage can be permanent, meaning the data is kept for the foreseeable future.

Your organization must determine the following:

- What must be backed up?
- What should not be backed up (as per organization policy)?
- How granular are the restoration needs?
- How often is the data backed up?
- How accessible is the data: in other words, how much time will it take to restore it?
- What processes are in place to recover from a disaster during a backup or restore?

The answers to these questions are an integral part of your backup and restore policy.

Understanding Backup Types

There are many types of backup files (explained below), and within each type are many formats and methods. Each backup type serves a unique purpose and has its own considerations.

- **Full Images:** Full images are byte-level copies of data. They capture the state of the hard disk down to the most basic storage unit. These backups also keep copies of the disk filesystem and the unused or erased portion of the disk in question. They can be used for forensic study of the source disk medium. Such detail often makes file restoration unwieldy. Full Image backups are often compressed and are only decompressed to restore the entire file set.
- **Full File-level Copies:** Full file-level copies are backups that are kept as duplicates. They do not capture the finest detail of unused portions of the source disk, but they do provide a full record of the files as they existed at the time of backup. If a file changes, the next full file-level backup copies the entire data set in addition to the file that changed.
- **Incremental Backups:** Incremental backups start with file-level copies, but they only copy files changed since the last backup. This saves storage space and captures changes as they happen.
- **Snapshots:** Snapshots are copies of data as it was in the past. You can make snapshots from collections of files, or more often from links to other files in a backup file set. Snapshots are useful for making backups of volatile data (data that changes quickly), like databases in use or mail servers sending and receiving mail.

These backup types are not mutually exclusive. They exemplify different approaches to copying data for backup purposes. For example, Time Machine uses a full file-level copy as a base backup; then it uses incremental backups to create snapshots of a computer's data on a given day.

Understanding Backup Scheduling

Backing up files requires time and resources. Before deciding on a backup plan, consider the following questions:

- How much data will be backed up?
- How much time will the backup take?
- When does the backup need to happen?
- What else is the computer doing during that time?
- What sort of resource allocation will be necessary?

  For example, how much network bandwidth is necessary to accommodate the load? How much space on backup drives, or how many backup tapes are required? What sort of drain on computing resources will occur during backup? What personnel are necessary for the backup?

You will find that different kinds of backup require different answers to these questions. For example, an incremental file copy might take less time and copy less data than a full file copy (because only a fraction of any given data set will have changed since the last backup).

Therefore an incremental backup might be scheduled during a normal use period because the impact to users and systems may be very low. However, a full image backup might have a very strong impact for users and systems, if done during the normal use period.

Choosing a Backup Rotation Scheme

A backup rotation scheme determines the most efficient way to back up data over a specific period of time. An example of a rotation scheme is the grandfather-father-son rotation scheme. In this scheme, you perform incremental daily backups (son), and full weekly (father) and monthly (grandfather) backups.

In the grandfather-father-son rotation scheme, the number of media sets you use for backup determines how much backup history you have. For example, if you use eight backup sets for daily backups, you have eight days of daily backup history because you'll recycle media sets every eight days.

Understanding Restores

No backup policy or solution is complete without having accompanying plans for data restoration. Depending on what is being restored, you may have different practices and procedures. For example, your organization may have specific tolerances for how long critical systems can be out of use while the data is restored.

Consider the following questions:

- How long will it take to restore data at each level of granularity?

  For example, how long will a deleted file or email take to restore? How long will a full hard disk image take to restore? How long would it take to return the whole network to its state three days ago?

- What process is most effective for each type of restore?

  For example, why would you roll back the entire server for a single lost file?

- How much administrator action is necessary for each type of restore? How much automation must be developed to best use administrators' time?
- Under what circumstances are restores initiated? Who and what can start a restore and for what reasons?

Restore practices and procedures must be tested regularly. A backup data set that does not restore correctly cannot be considered a trustworthy backup. Backup integrity is measured by restore fidelity.

Defining a Backup Verification Mechanism

You should have a strategy for regularly conducting test restorations. Some third-party software providers support this functionality. However, if you're using your own backup solution, you should develop the necessary test procedures.

Other Backup Policy Considerations

Consider the following additional items for your backup policy:

- Should file compression be used? If so, what kind?
- Are there onsite and offsite backups and archives?
- Are there any special considerations for the type of data being stored? For example, for Mac OS X files, can the backup utility preserve file metadata, resource forks, and Access Control List (ACL) privileges?
- Is there sensitive data, such as passwords, social security numbers, phone numbers, medical records, or other legally protected information, that requires special treatment, and that must not be backed up without understanding where the data will flow and be stored?

Choosing Backup Media Type

Several factors help you determine what type of media to choose:

- **Cost.** Use cost per GB to determine what media to choose. For example, if your storage needs are limited, you can justify higher cost per GB, but if you need a large amount of storage, cost becomes a big factor in your decision.

  One of the most cost-effective storage solutions is a hard drive RAID. It provides you with a low cost per GB, and it doesn't require the special handling needed by other cost-effective storage types, such as tape drives.

- **Capacity.** If you back up only a small amount of data, low-capacity storage media can do the job. But if you need to back up large amounts of data, use high-capacity devices, such as a RAID.
- **Speed.** When your goal is to keep your server available most of the time, restoration speed becomes a big factor in deciding which type of media to choose. Tape backup systems can be very cost effective, but they are much slower than a RAID.
- **Reliability.** Successful restoration is the goal of a good backup strategy. If you can't restore lost data, all the effort and cost you spent in backing up data is wasted and the availability of your services is compromised.

  Therefore, it's important that you choose highly reliable media to prevent data loss. For example, tapes are more reliable than hard disks because they don't contain moving parts.
- **Archive life.** You never know when you'll need your backed up data. Therefore, choose media that is designed to last for a long time. Dust, humidity, and other factors can damage storage media and result in data loss.

Command-Line Backup and Restoration Tools

Mac OS X Server provides several command-line tools for data backup and restoration, which include:

- `rsync`. Use to keep a backup copy of your data in sync with the original. The tool `rsync` only copies the files that have changed. By default `rsync` does not preserve extended attributes in files necessary for many Mac OS X Server services.
- `ditto`. Use to perform full backups.
- `tar`. Use to perform full backups.
- `asr`. Use to back up and restore a volume in block copy mode. If the tool is in file copy mode, it does not preserve all necessary extended attributes in files.

For more information about these commands, see their respective man pages.

Note: You can use the `launchctl` command to automate data backup using these commands. For more information about using `launchctl` and `launchd`, see their respective man pages.

Understanding Time Machine as a Server Backup Tool

At its core, Time Machine is a file-level backup solution that runs at regular intervals and archives file changes from the initial file set. Time Machine makes use of UNIX file linking to efficiently store backup intervals as separate browsable file systems, but uses no compression.

Time Machine is a limited tool for data backup and restoration of Mac OS X Server v10.6. It can back up some server configuration settings and the service state. Time Machine does not back up service data.

For example, Time Machine doesn't back up user and group directory records, email, DNS records, Address Book shared groups, iCal Server calendars, and so forth. It only saves the settings made in Server Preferences and Server Admin, and whether a service is on or off. The following service settings and statuses are preserved:

- Address Book Server
- DHCP
- DNS
- File Services (AFP, SMB, NFS, and FTP)
- Firewall
- iCal Server
- iChat Server
- Mail
- Mobile Access
- MySQL
- NAT
- Network Settings
- Podcast Producer
- Print
- Push Notification
- QTSS
- RADIUS
- Remote Access Settings
- Software Update
- VPN
- Web
- Wiki
- Xgrid

For more information about where the necessary data files are stored for backup via other means, see "Critical Configuration and Data Files" on page 155.

Note: You can use the `launchctl` command to automate data backup using the aforementioned commands. For more information about using `launchctl` and `launchd`, see their respective man pages.

Administration Tools

3

Manage Mac OS X Server using graphical applications or command-line tools.

Mac OS X Server v10.6 administration applications must be run from either Mac OS X Server v10.6 or Mac OS X v10.6.

Server Admin

You use Server Admin to administer services on Mac OS X Server computers. Server Admin also lets you specify settings that support multiple services, such as creating and managing SSL certificates, manage file sharing, and specifying which users and groups can access services.

The version of Server Admin included with Mac OS X Server v10.6 can be used to administer the latest version of Mac OS X Server v10.5. However, the current version of Server Admin isn't compatible with administering DNS service or manage certificates in Mac OS X Server v10.5. Use the version of Server Admin that came with Mac OS X Server v10.5 on a computer running Mac OS X Server v10.5 or Mac OS X v10.5.

Information about using Server Admin to manage services appears in the individual administration guides and in onscreen information accessible by using the Help menu in Server Admin.

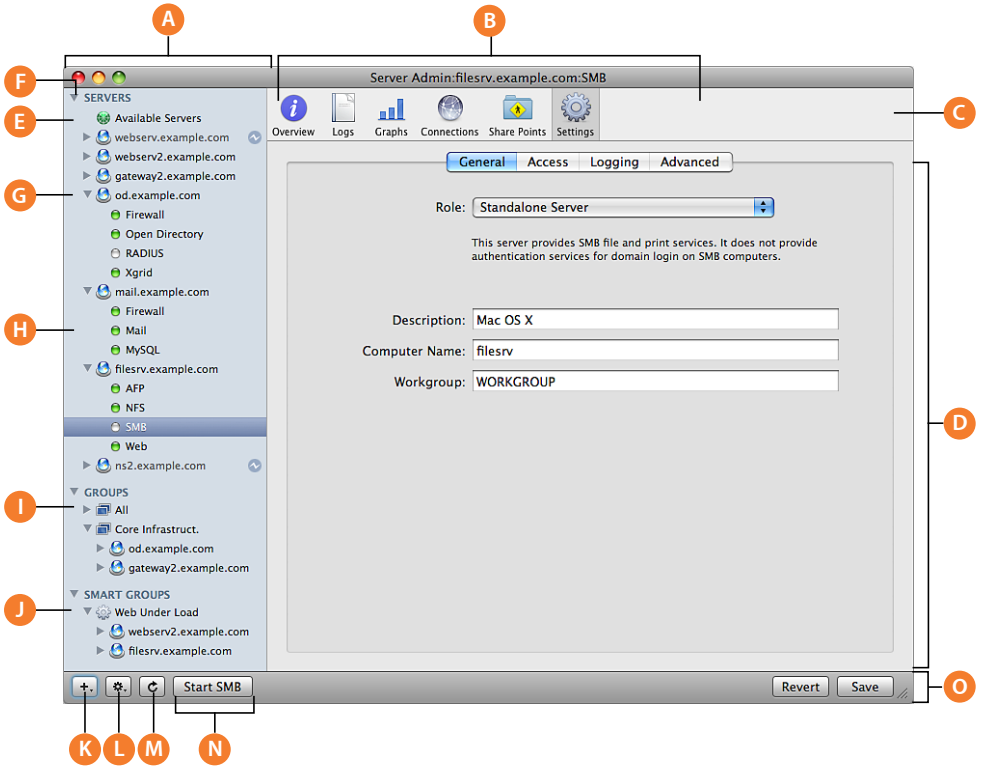
Opening and Authenticating in Server Admin

Server Admin is installed in /Applications/Server/, from which you can open it in the Finder. Or you can open Server Admin by clicking the Server Admin icon in the Dock or clicking the Server Admin button on the Workgroup Manager toolbar.

To select a server to work with, enter its IP address or DNS name in the login dialog box or click Available Servers to choose from a list of servers. Specify the user name and password for a server administrator, then click Connect.

Server Admin Interface

The Server Admin interface is shown here, with each element explained in the following table.



A	**Server List:** Shows servers, groups, smart groups, and if desired, the administered services for each server You select a group to view a status summary for all grouped computers. You select a computer for its overview and server settings. You select a server's service to control and configure the service.
B	**Context Buttons:** Shows available information and configuration panes.
C	**Tool Bar:** Shows available context buttons. If a button is grayed out or can't be clicked, you do not have the administrative permissions to access it.

D	**Main Work Area:** Shows status and configuration options. This looks different for each service and for each context button selected.
E	**Available servers:** Lists the local-network scanner, which you can use to discover servers to add to your server list.
F	**All Servers:** Shows all computers added to Server Admin, regardless of status.
G	**Server:** Shows the hostname of the managed server. Select to show a hardware, operating system, active service, and system status summary.
H	**Service:** Shows an administered service for a server. Select to get service status, logs, and configuration options.
I	**Group:** Shows an administrator created group of servers. Select to view a status summary for all grouped computers For more information, see "Grouping Servers Manually" on page 129.
J	**Smart Group:** Shows an automatic group, populated with servers that meet a predetermined criteria. For more information, see "Grouping Servers Using Smart Groups" on page 129.
K	**Add button:** Shows a pop-up menu of items to add to the Server list: servers, groups, and smart groups.
L	**Action button:** Shows a pop-up menu of actions possible for a selected service, or server, including disconnect server, share the server's screen, and so forth.
M	**Refresh button:** Allows you to send a status request to all computers visible in the Server list.
N	**Service Start/Stop button:** When a service is selected, this button allows you to start or stop the service, as appropriate.
O	**Action bar:** Shows buttons and pop-up menus with commands to act on selected servers or services in the Server list. Click this to save or revert setting changes you've made. This contains the Add button, Action button, service start and stop buttons, and save and revert buttons.

Customizing the Server Admin Environment

To control the Server Admin environment, you have the following options.

- To control the list of services to administer, see "Adding and Removing Servers in Server Admin" on page 128.
- To control the appearance of Server Admin lists, refresh rates, and other behaviors, choose Server Admin > Preferences.
- To group and sort servers available for administration, make groups and smart groups. See "Grouping Servers Manually" on page 129 and "Grouping Servers Using Smart Groups" on page 129.

Server Assistant

Server Assistant is used for:

- Remote server installations
- Initial setup of a local server
- Initial setup of remote servers
- Preparing data for automated setup

The Server Assistant initial page is shown here.

Server Assistant is opened from the Server menu of Server Admin. The following menu items open the assistant:

- Install Remote Server
- Set Up Remote Server
- Create Auto Server Setup Profile

For information about using Server Assistant, use its Help buttons, or see Chapter 6, "Initial Server Setup."

Server Preferences

Server Preferences is the simplified administration application you need for managing Mac OS X Server v10.6. You can use Server Preferences in addition to or instead of Server Admin and Workgroup Manager:

- Manage basic user and group settings.
- Configure essential service settings such as: file sharing service, Address Book service, iCal calendar service, iChat instant messaging service, mail service, network security, web services, VPN remote access service, and Time Machine backup for users' computers.
- Check the status of the server and services.

You can use Server Preferences on any server you want to manage, or you can use it remotely from an administrator computer or another server.

For information about using Server Preferences, see *Getting Started* or Server Preferences Help.

Workgroup Manager

Mac OS X Server includes Workgroup Manager, a user management tool you can use to create and manage user, group, computer, and computer group accounts. You also use it to access the Inspector, an advanced feature that lets you do raw editing of Open Directory entries.

Workgroup Manager is installed in /Applications/Server/, which you can open it in the Finder. Or you can open Workgroup Manager by clicking View > Workgroup Manager in the Server Admin menu bar.

Workgroup Manager works closely with a directory domain. Directory domains are like databases, and are geared towards storing account information and handling authentication.

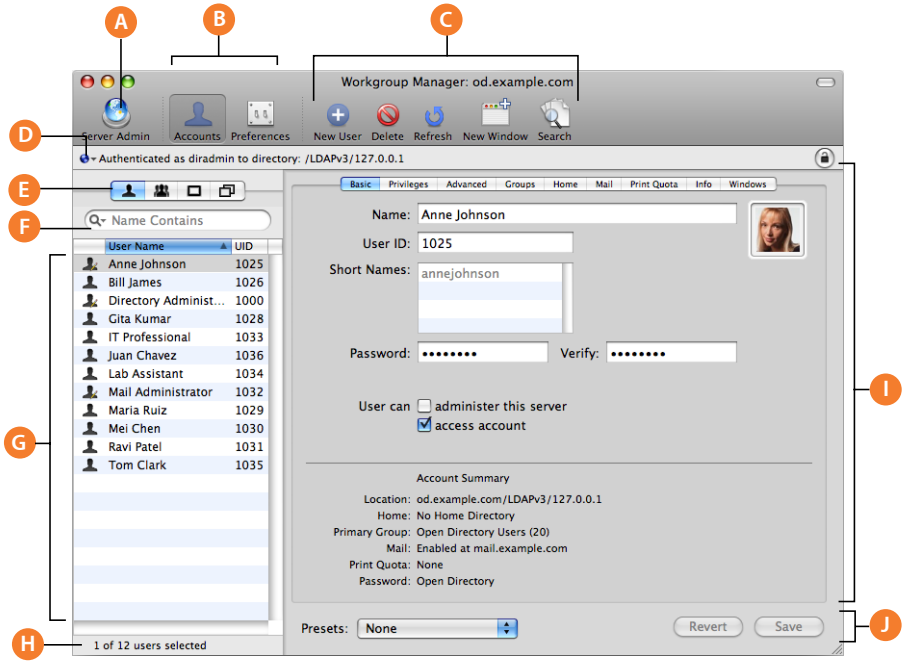
Information about using Workgroup Manager appears in several documents at the Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

After opening Workgroup Manager, you can open a Workgroup Manager window by choosing Server > New Workgroup Manager Window.

Important: When connecting to a server or authenticating in Workgroup Manager, make sure the capitalization of the name you enter matches the name of a server administrator or domain administrator account.

Workgroup Manager Interface

The Workgroup Manager interface is shown here, with each element explained in the following table.



A	**Server Admin:** Click to open the Server Admin application.
B	**Settings Buttons:** Click Accounts to view or edit account settings, or click Preferences to view or edit preference settings.
C	**Tool Bar:** Click the icons to accomplish the various commands. The toolbar is customizable.
D	**Directory path:** Use to view the directory you are editing. Click the globe icon to select a directory domain. Click the lock to authenticate.
E	**Record Type tabs:** Use to view records for users, groups, and computer groups. If the Inspector is enabled, this also contains the Inspector tab.
F	**Text filters:** Use to enter text to filter record names.
G	**Record list display:** Use to view names for a selected record type.
H	**Selection bar:** Use to view the number of records found and selected.
I	**Main Work Area:** Use to work with account, preference, and configuration options. This looks different for each user, group, or preference type.
J	**Action zone:** Use to save and revert changes, and to make and apply preset configurations to selected records.

Customizing the Workgroup Manager Environment

There are several ways to tailor the Workgroup Manager environment:

- To open Workgroup Manager Preferences, choose Workgroup Manager > Preferences.

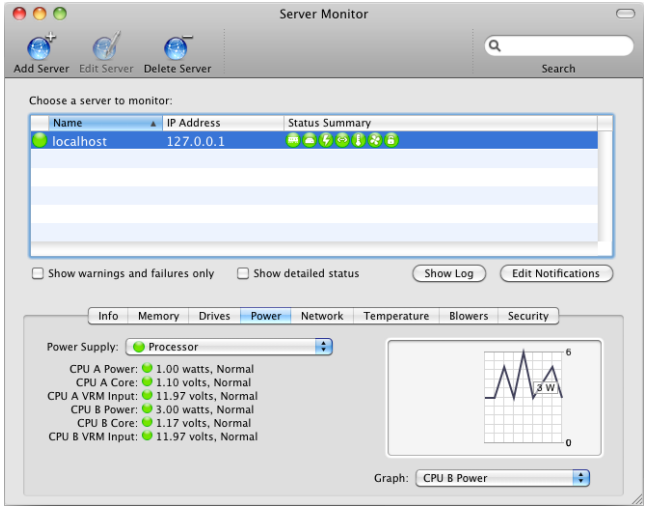
  You can configure options such as if DNS names are resolved, if the Inspector is enabled, if you need to enter a search query to list records, and what the maximum number of displayed records is.

- To customize the toolbar, choose View > Customize Toolbar.
- To include predefined users and groups in the user and group lists, choose View > Show System Users and Groups.
- To open Server Admin, click the Server Admin toolbar button.

Server Monitor

You use Server Monitor to monitor local or remote Xserve hardware and trigger mail notifications when circumstances warrant attention. Server Monitor provides information about the installed operating system, drives, power supply, enclosure and processor temperature, cooling blowers, security, and network.

The Server Monitor interface is shown below.



Server Monitor is installed in /Applications/Server/ when you install your server or set up an administrator computer. To open Server Monitor, click the Server Monitor icon in the Dock or double-click the Server Monitor icon in /Applications/Server/. From within Server Admin, choose View > Server Monitor.

To identify the Xserve computer to monitor, click Add Server, identify the server, and enter user name and password information for an administrator of the server. If adding the local server, use '127.0.0.1' for the IP address. If adding a remote server, enter the server's LOM hostname or IP address.

To specify how often you want to refresh data, use the "Update every" pop-up menu in the Info pane.

To manage different lists of Xserve computers you want to monitor, choose File > Export or File > Import. To consolidate lists into one, choose File > Merge.

The system identifier lights on the front and back of an Xserve computer light when service is required. Use Server Monitor to understand why the lights are on. You can also turn the lights on to identify a specific Xserve computer in a rack of servers by selecting the server and clicking "System identifier light" in the Info pane.

To set up Server Monitor to notify you by mail when an Xserve computer's status changes, click Edit Notifications. For each server, you set up the conditions that you want notification for. The mail message can come from Server Monitor or from the server.

Server Monitor keeps logs of Server Monitor activity for each Xserve computer. To view a log, click Show Log. The log shows, for example, Server Monitor attempts to contact the server and whether a connection was successful. The log also shows server status changes. (The logs don't include system activity on the server.)

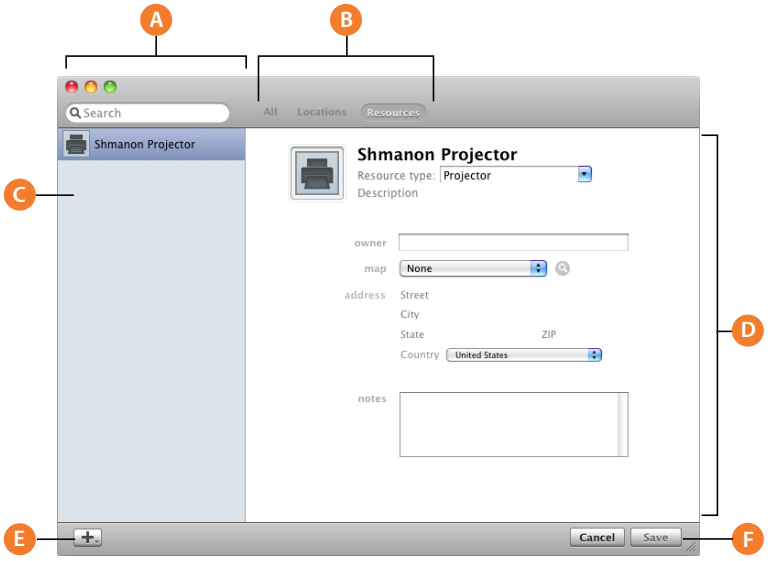
For additional information, see Server Monitor Help.

iCal Service Utility

iCal Service Utility gives users access to shared information about locations and resources. Users can use iCal Service Utility to set up information about shared resources and locations for use with iCal Service.

iCal Service Utility Interface

The iCal Service Utility interface is shown here, with each element explained in the following table.



A	**Search field:** Use to search record types. Numbers appear at the left of the Record Type buttons to indicate the number of matching records.
B	**Record Type buttons:** Click to show the type of directory records desired.
C	**Results list:** Use to view the results of the record search.
D	**Record view:** Use to view the record selected in the Results list.
E	**Add button:** Use to location or resource record.
F	**Save button:** Click to save changes to the selected record.

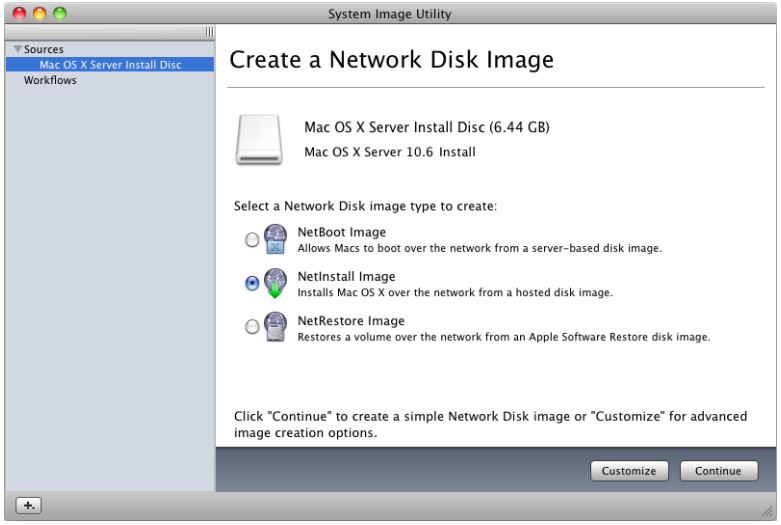
For information about how to use iCal Service Utility, see the onscreen help for iCal Service Utility.

System Image Management

You can use the following Mac OS X Server applications to set up and manage NetBoot and NetInstall images:

- *System Image Utility* creates Mac OS X disk images. It's installed with Mac OS X Server software in the /Applications/Server/ folder.

  The System Image Utility interface is shown below.



- *Server Admin* enables and configures NetBoot service and supporting services. It's installed with Mac OS X Server software in the /Applications/Server/ folder.
- *PackageMaker* creates package files that you use to add software to disk images. Access PackageMaker from Xcode Tools. An installer for Xcode Tools is on the server Install DVD in the Other Installs folder.
- *Property List Editor* edits property lists such as NBImageInfo.plist. Access Property List Editor from Xcode Tools.

The online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ provide instructions for using all these applications.

Media Streaming Management

The online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ provide instructions for administering QuickTime Streaming Server (QTSS) using Server Admin and QuickTime Broadcaster.

Command-Line Tools

If you're an administrator who prefers to work in a command-line environment, you can do so with Mac OS X Server.

From the Terminal application in Mac OS X, you can use the built-in UNIX shells (sh, csh, tsh, zsh, bash) to use tools for installing and setting up server software and for configuring and monitoring services. You can also submit commands from a non-Mac OS X computer.

Mac OS X Server has a command-line version of Server Admin called `serveradmin` that you use to administer the services that Server Admin manages. It is run on the server to be administered over a remote connection.

When managing remote servers, you conduct secure administration by working in a Secure Shell (SSH) session.

Server Status Widget

The Server Status widget lets you monitor Mac OS X Server v10.6 activity from any computer with Mac OS X v10.6 or Mac OS X Server v10.6. Server Status shows you graphs of processor activity, network load, and disk usage.

For information about using the Server Status widget, see *Getting Started* or Server Preferences Help.

RAID Admin

RAID Admin is a tool to administer and monitor Xserve RAID devices. You use RAID Admin to set up Xserve RAID hardware, including:

- Creating, deleting, and expanding RAID arrays
- Monitoring the status of Xserve RAID systems
- Adjusting settings, including system name and password, network address for each RAID controller, fibre channel communication speed, drive cache, and controller cache
- Setting up email notification for system alerts
- Implementing advanced features, such as dividing arrays into slices and updating the firmware of an Xserve RAID system.

Podcast Capture, Composer, and Producer

Podcast Capture takes audio and video from a local or remote camera, captures screen activity, or uploads QuickTime files into Podcast Producer for encoding and distribution. Podcast Composer creates the workflow instructions for Podcast Producer.

Xgrid Admin

You can use Xgrid Admin to monitor local or remote Xgrid controllers, grids, and jobs. You can add controllers and agents to monitor and specify agents that have not yet joined a grid. You also use Xgrid Admin to pause, stop, or restart jobs.

The Xgrid Admin interface is shown here.

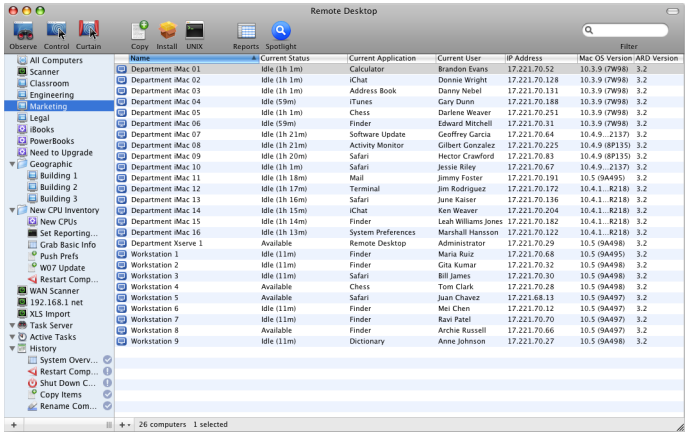
Xgrid Admin is installed in /Applications/Server/ when you install your server or set up an administrator computer. To open Xgrid Admin, double-click the Xgrid Admin icon in /Applications/Server/.

For additional information, see Xgrid Admin help.

Apple Remote Desktop

Apple Remote Desktop (ARD), which you can optionally purchase, is an easy-to-use network-computer management application. It simplifies the setup, monitoring, and maintenance of remote computers and lets you interact with users.

The ARD interface is shown here.



You can use ARD to:

- Control and observe computer screens.
- Configure computers and install software.
- Conduct one-to-one or one-to-many user interactions to provide help or tutoring.
- Perform basic network troubleshooting.
- Generate reports that audit computer hardware characteristics and installed software.

You can also use ARD to control installation on a computer that you start up from an installation disc for Mac OS X Server v10.5 or later, because ARD includes VNC viewer capability.

For more information about Apple Remote Desktop, see www.apple.com/remotedesktop/.

Enhancing Security

4

By vigilantly adhering to security policies and practices, you can minimize the threat to system integrity and data privacy.

Mac OS X Server is built on a robust UNIX foundation that contains many security features in its core architecture. State-of-the-art, standards-based technologies protect your server, network, and data. These technologies include a built-in firewall with stateful packet analysis, strong encryption and authentication services, data security architectures, and support for access control lists (ACLs).

Use this chapter to stimulate your thinking. It doesn't present a rigorous planning outline, nor does it provide the details you need to determine whether to implement a particular security policy and assess its resource requirements. Instead, view this chapter as an opportunity to plan and institute the security policies necessary for your environment.

About Physical Security

The physical security of a server is an often overlooked aspect of computer security. Anyone with physical access to a computer (for example, to open the case, or plug in a keyboard, and so forth) has almost full control over the computer and the data on it. For example, someone with physical access to a computer can:

- Restart the computer from another external disc, bypassing any existing login mechanism.
- Remove hard disks and use forensic data recovery techniques to retrieve data.
- Install hardware-based key-loggers on the local administration keyboard.

In your own organization and environment, you must decide which precautions are necessary, effective, and cost-effective to protect the value of your data and network.

For example, in an organization where floor-to-ceiling barriers might be needed to protect a server room, securing the air ducts leading to the room might also need to be considered. Other organizations might only need a locked server rack or an firmware password.

About Network Security

Network security is as important to data integrity as physical security. Although someone might immediately see the need to lock down an expensive server, he or she might not immediately see the need to restrict access to the data on that same server. The following sections provide considerations, techniques, and technologies to assist you in securing your network.

Firewalls and Packet Filters

Much like a physical firewall that acts as a physical barrier to provide heat and heat damage protection in a building or for a vehicle, a network firewall acts as a barrier for your network assets, preventing data tampering from external sources.

Mac OS X Server's Firewall service is software that protects the network applications running on your Mac OS X Server.

Turning on Firewall service is similar to erecting a wall to limit access. The service scans incoming IP packets and rejects or accepts packets based on the rules you create.

You can restrict access to any IP service running on the server, and you can customize rules for incoming clients or a range of client IP addresses. Services such as Web and FTP services are identified on your server by a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port number.

When a computer tries to connect to a service, Firewall service scans the rule list for a matching rule. When a packet matches a rule, the action specified in the rule (such as allow or deny) is taken. Then, depending on the action, additional rules might be applied.

If the server gets its Internet connection through an AirPort Extreme Base Station (802.11n) or a Time Capsule, you can use it instead of the server's firewall to protect the network. You can automatically manage the base station or Time Capsule in the Security pane of Server Preferences. AirPort automanagement isn't available using Server Admin.

You can also protect a small network with other kinds of Internet sharing routers, but you must manage them manually. For more information, see Mac OS X Server *Getting Started*.

Network DMZ

In computer network security, a demilitarized zone (DMZ) is a network area (a subnetwork) that is between an organization's internal network and an external network like the Internet.

You can make connections from the internal and external network to the DMZ, and you can make connections from the DMZ to the external network, but you cannot make connections from the DMZ to the internal network.

This allows an organization to provide services to the external network while protecting the internal network from being compromised by a host in the DMZ. If someone compromises a DMZ host, he or she cannot connect to the internal network.

The DMZ is often used to connect servers that need to be accessible from the external network or Internet, such as mail, web, and DNS servers.

Connections from the external network to the DMZ are often controlled using firewalls and address translation.

You can create a DMZ by configuring your firewall. Each network is connected to a different port on the firewall, called a three-legged firewall setup. This is simple to implement but creates a single point of failure.

Another approach is to use two firewalls with the DMZ in the middle, connected to both firewalls, and with one firewall connected to the internal network and the other to the external network. This is called a screened-subnet firewall.

This setup provides protection in case of firewall misconfiguration, allowing access from the external network to the internal network.

VLANs

Mac OS X Server provides 802.1q Virtual Local Area Network (VLAN) support on the Ethernet ports and secondary PCI gigabit Ethernet cards available or included with Xserves.

VLAN allows multiple computers on different physical LANs to communicate with each other as if they were on the same LAN. Benefits include more efficient network bandwidth utilization and greater security, because broadcast or multicast traffic is only sent to computers on the common network segment. Xserve VLAN support conforms to the IEEE 802.1q standard.

MAC Filtering

MAC filtering (or layer 2 address filtering) refers to a security access control where a network interface's MAC address, or Ethernet address (the 42-bit address assigned to each network interface), is used to determine access to the network.

MAC addresses are unique to each card, so using MAC filtering on a network permits and denies network access to specific devices, rather than to specific users or network traffic types. Individual users are not identified by a MAC address, only a device, so an authorized person must have an allowed list of devices that he or she would use to access the network.

In theory, MAC filtering allows a network administrator to permit or deny network access to hosts and devices associated with the MAC address, although in practice there are methods to avoid this form of access control through address modification (spoofing) or the physical exchange of network cards between hosts.

Transport Encryption

Transferring data securely across a network involves encrypting the packet contents sent between computers. Mac OS X Server can provide Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL) as the cryptographic protocols that provide secure communications on the Internet for such things as web browsing, mail, and other data transfers.

These encryption protocols allow client and server applications to communicate in a way that helps prevent eavesdropping, tampering, and message forgery.

TLS provides endpoint authentication and communications privacy over the Internet using cryptography. These encrypted connections authenticate the server (so its identity is ensured) but the client remains unauthenticated.

To have mutual authentication (where each side of the connection is assured of the identity of the other), use a public key infrastructure (PKI) for the connecting clients.

Mac OS X Server makes use of OpenSSL and has integrated transport encryption into the following tools and services:

- Server administration using Server Admin and Server Preferences
- User and group management using Workgroup Manager.
- Address Book Server
- iCal Server
- iChat Server
- Mail Service
- Open Directory
- Podcast Producer
- RADIUS
- SSH
- VPN (L2TP)
- Web service

Payload Encryption

Rather than encrypting the transfer of a file across the network, you can encrypt the contents of the file instead. Files with strong encryption might be captured in transit, but would still be unreadable.

Most transport encryption requires the participation of both parties in the transaction. Some services (such as SMTP mail service) can't reliably use such techniques, so encrypting the file itself is the only method of reliably securing the file content.

To learn more about file encryption, see "About File Encryption" on page 55.

About File Security

By default, files and folders are owned by the user who creates them. After they're created, items keep their privileges (a combination of ownership and permissions) even when moved, unless the privileges are explicitly changed by their owners or an administrator. Therefore, files and folders you create are not accessible if they are created in a folder that the users don't have privileges for.

When setting up share points, make sure that items allow appropriate access privileges for the users you want to share them with.

File and Folder Permissions

Mac OS X Server supports the following file and folder permissions:

- Standard Portable Operating System Interface (POSIX) permissions
- Access Control Lists (ACLs)

POSIX permissions let you control access to files and folders based on three categories of users: Owner, Group, and Everyone Else.

Although these permissions control who can access a file or a folder, they lack the flexibility and granularity that many organizations require to deal with elaborate user environments.

ACL permissions provide an extended set of permissions for files or folders and allow you to set multiple users and groups as owners. In addition, ACLs are compatible with Windows Server 2003 and Windows XP, giving you added flexibility in a multiplatform environment.

For more information about file permissions, see the online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/

About File Encryption

Mac OS X has a number of technologies that can perform file encryption, including:

- **FileVault:** FileVault performs on-the-fly encryption on each user's home folder. This encrypts the entire directory in one virtual volume, which is mounted, and the data is unencrypted as needed.

- **Secure VM:** Secure VM encrypts system virtual memory (memory data temporarily written to the hard disk), not user files. It improves system security by keeping virtual memory files from being read and exploited.
- **Disk Utility:** Disk Utility can create disk images whose contents are encrypted and password protected. Disk images act like removable media such as external hard disks or USB memory sticks, but they exist only as files on the computer. After you create an encrypted disk image, double-click it to mount it. Files you drag onto the mounted image are encrypted and stored on the disk image. You can send this disk image to other Mac OS X users. With the unlocking password, they can retrieve the files you locked in the disk image.

Secure Delete

When a file is put in the Trash and the Trash is emptied, or when a file is removed using the `rm` UNIX tool, the files are not removed from disk. Instead, they are removed from the list of files the operating system (OS) tracks and does not write over.

Any space on your hard disk that is free space (places the OS can put a file) most likely contains previously deleted files. Such files can be retrieved using undelete utilities and forensic analysis.

To truly remove the data from disk, you must use a more secure delete method. Security experts advise writing over deleted files and free space multiple times with random data.

Mac OS X Server provides the following tools to allow you to securely delete files:

- Secure Empty Trash (a command in the Finder menu to use instead of "Empty Trash"
- `srm` (a UNIX utility that securely deletes files, used in place of "rm")

About Authentication and Authorization

Authentication is verifying a person's identity, but authorization is verifying that an authenticated person is allowed to perform a certain action. Authentication is necessary for authorization.

In a computing context, when you provide a login name and password, you are authenticated to the computer because it assumes only one person (you) knows the login name and the password. After you are authenticated, the operating system checks lists of people who are permitted to access certain files, and if you are authorized to access them, you are permitted to.

Because authorization can't occur without authentication, authorization is sometimes used to mean the combination of authentication and authorization.

In Mac OS X Server, users trying to access services (like logging in to a directory-aware workstation, or trying to mount a remote volume) must authenticate by providing a login name and password before privileges for the users can be determined.

You have several options for authenticating users:

- **Open Directory authentication.** Based on the standard Simple Authentication and Security Layer (SASL) protocol, Open Directory authentication supports many authentication methods, including CRAM-MD5, APOP, WebDAV, SHA-1, LAN Manager, NTLMv2, and Kerberos.

  Open Directory authentication lets you set up password policies for individual users or for all users whose records are stored in a directory, with exceptions if required. Open Directory authentication also lets you specify password policies for individual directory replicas.

  For example, you can specify a minimum password length or require a user to change the password the next time he or she logs in. You can also disable login for inactive accounts or after a specified number of failed login attempts.

- **Kerberos v5 authentication.** Using Kerberos authentication allows integration into existing Kerberos environments. The Key Distribution Center (KDC) on Mac OS X Server offers full support for password policies you set up on the server. Using Kerberos also provides a feature known as *single sign-on,* described in the next section.

  The following services on Mac OS X Server support Kerberos authentication:

  - Address Book Server
  - Apple Filing Protocol (AFP)
  - File Transfer Protocol (FTP)
  - iCal Server
  - iChat Server
  - Login window
  - Mail Services
  - Network Filing Protocol (NFS)
  - Open Directory (LDAPv3)
  - Printing (IPP)
  - Screen saver
  - Secure Shell (SSH)
  - Server Message Block file service (SMB)
  - Virtual Private Network (VPN)
  - Virtual Network Computing (VNC, known as Screen Sharing in Mac OS X Server)

  - Web Service (Apache via the SPNEGO Simple and Protected GSS-API Negotiation Mechanism protocol)
  - Xgrid
- **Storing passwords in user accounts.** This approach might be useful when migrating user accounts from earlier server versions. However, this approach may not support clients that require network-secure authentication protocols, such as APOP.
- **Non-Apple LDAPv3 authentication.** This approach is available for environments that have LDAPv3 servers set up to authenticate users.
- **RADIUS** (an authentication protocol for controlling network access by clients in mobile or fixed configurations). For more information about RADIUS in Mac OS X Server, see the online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

Single Sign-On

Mac OS X Server uses Kerberos for single sign-on authentication, which relieves users from entering a user name and password separately for every service. With single sign-on, a user always enters a user name and password in the login window. Thereafter, the user does not need to enter a name and password for Apple file service, mail service, or other services that use Kerberos authentication.

To use single sign-on, users and services must be Kerberized—configured for Kerberos authentication—and must use the same Kerberos Key Distribution Center (KDC) server.

User accounts that reside in an LDAP directory of Mac OS X Server and have a password type of Open Directory use the server's built-in KDC. These user accounts are configured for Kerberos and single sign-on.

This server's Kerberized services also use the server's built-in KDC and are configured for single sign-on. This Mac OS X Server KDC can also authenticate users for services provided by other servers. Having additional servers with Mac OS X Server use the Mac OS X Server KDC requires minimal configuration.

Kerberos was developed at MIT to provide secure authentication and communication over open networks like the Internet. Kerberos provides proof of identity for two parties. It enables you to prove who you are to network services you want to use. It also proves to your applications that network services are genuine, not spoofed.

Like other authentication systems, Kerberos does not provide authorization. Each network service determines for itself what it will allow you to do based on your proven identity.

Kerberos allows a client and a server to unambiguously identify each other much more securely than the typical challenge-response password authentication methods traditionally deployed.

Kerberos also provides a single sign-on environment where users must authenticate only once a day, week, or other period of time, easing authentication loads for users. Mac OS X Server and Mac OS X versions 10.3 through 10.6 support Kerberos version 5.

About Certificates, SSL, and Public Key Infrastructure

Mac OS X Server supports services that use Secure Sockets Layer (SSL) to ensure encrypted data transfer. It uses a Public Key Infrastructure (PKI) system to generate and maintain certificates for use with SSL-enabled services.

PKI systems allow the two parties in a data transaction to be authenticated to each other and to use encryption keys and other information in identity certificates to encrypt and decrypt messages traveling between them.

PKI enables multiple communicating parties to establish confidentiality, message integrity, and message source authentication without exchanging secret information in advance.

SSL technology relies on a PKI system for secure data transmission and user authentication. It creates an initial secure communication channel to negotiate a faster, secret key transmission. Mac OS X Server uses SSL to provide encrypted data transmission for mail, web, and directory services.

The following sections contain more background information about key aspects of PKI.

Public and Private Keys

Within a PKI, two digital keys are created: the public key and the private key. The private key isn't distributed to anyone and is often encrypted by a passphrase. The public key is distributed to other communicating parties.

Basic key capabilities can be summed up as follows:

Key type	Capabilities
Public	• Can encrypt messages that can only by decrypted by the holder of the corresponding Private key. • Can verify the signature on a message to ensure that it is coming from a Private key.
Private	• Can digitally sign a message or certificate, claiming authenticity. • Can decrypt messages that were encrypted with the Public key. • Can encrypt messages that can only be decrypted by the private key.

Web, mail, and directory services use the public key with SSL to negotiate a shared key for the duration of the connection.

For example, a mail server will send its public key to a connecting client and initiate negotiation for a secure connection. The connecting client uses the public key to encrypt a response to the negotiation. The mail server, because it has the private key, can decrypt the response. The negotiation continues until the mail server and the client have a shared secret to encrypt traffic between computers.

Certificates

A certificate is an electronic document that contains a public key with identification information (name, organization, email address, and so on). In a public key environment, a certificate is digitally signed by a Certificate Authority, or its own private key (the latter being a self-signed certificate).

A public key certificate is a file in a specified format (Mac OS X Server uses the x.509 format) that contains:

- The public key half of a public-private key pair
- The key user's identity information, such as a person's name and contact information
- A validity period (how long the certificate can be trusted to be accurate)
- The URL of someone with the power to revoke the certificate (its *revocation center*)
- The digital signature of a CA, or the key user

About Certificate Authorities (CAs)

A CA is an entity that signs and issues digital identity certificates claiming that a party is correctly identified. In this sense, a CA is a trusted third party used by other parties when performing transactions.

In x.509 systems such as Mac OS X, CAs are hierarchical, with CAs being certified by higher CAs, until you reach a root authority. A root authority is a CA that's trusted by the parties, so it doesn't need to be authenticated by another CA. The hierarchy of certificates is top-down, with the root authority's certificate at the top.

A CA can be a company that signs and issues a public key certificate. The certificate attests that the public key belongs to the owner recorded in the certificate.

In a sense, a CA is a digital notary public. You request a certificate by providing the CA with your identity information, contact information, and the public key. The CA then verifies your information so users can trust certificates issued for you by the CA.

About Identities

Identities are a certificate and a private key, together. The certificate identifies the user, and the private key corresponds to the certificate. A single user can have several identities; for any given user each certificate could have a different name, email address, or issuer.

These identities are used for different security contexts. For example, one could be used to sign others' certificates, and one could be used to identify the user by email, and these do not need to be the same identity.

In the context of the Mac OS X Server Certificate Manager, identities include a signed certificate and both keys of a PKI key pair. The identities are used by the system keychain and are available for use by various services that support SSL.

About Self-Signed Certificates

Self-signed certificates are digitally signed by the private key corresponding to the public key included in the certificate. This is done in place of a CA signing the certificate. By self-signing a certificate, you're attesting that you are who you say you are. No trusted third party is involved.

About Intermediate Trust

If you are your own CA, and your certificates are not trusted by the default shipping root certificates in Mac OS X, your clients can still be configured to trust your certificates through an intermediate trust.

Trust is the ability of a client to believe the identity of a server when it connects. A trusted server is a known server that the client can transact with securely, without interference from outside and unknown parties.

Mac OS X clients follow x.509 trust validation when accepting certificates, meaning they follow the chain of certificate signers back until they find a trusted root certificate.

Mac OS X lets you specify a trusted anchor (in other words, a certificate that is not a root CA certificate, but that you trust). A client can trust a certificate closer in the chain of trust, or even just the submitted certificate itself. Trusting a certificate that isn't a shipping root anchor is intermediate trust.

To accomplish this, trust needs to be bestowed on certificates instead of to keychains (as was done previously). In v10.4, trust was given to certificates in the keychain called "X509Anchors." The X509Anchors keychain was deprecated starting with Mac OS X v10.5.

Several keychains can hold certificates:

- **SystemRootCertificates:** This keychain holds root certificates that ship with Mac OS X. The certificates already have trust given to them.
- **System:** This keychain holds certificates that the computer administrator can add. All users on a given client can read from this keychain. The trust settings of a certificate in this keychain can override those of a certificate in SystemRootCertificates.
- **Any other keychain:** This holds certificates for a given user and is only accessible to that user. The trust settings of a certificate in this keychain can override those of a certificate in SystemRootCertificates or System.

Trusted certificates can be in any of these locations, but to trust a certificate, trust settings must be given explicitly to a certificate.

To configure clients to trust a certificate:

1. Copy the self-signed CA certificate (the file named ca.crt) onto each client computer.

   This is preferably distributed using nonrewritable media, such as a CD-R. Using nonrewritable media prevents the certificate from being corrupted.
2. Open the Keychain Access tool by double-clicking the ca.crt icon where the certificate was copied onto the client computer.
3. Drag the certificate to the System keychain using Keychain Access.

   Authenticate as an administrator, if requested.
4. Double-click the certificate to get the certificate details.
5. In the details window, click the Trust disclosure triangle.
6. From the pop-up menu next to "When using this certificate," select "Always Trust"

   You have now added trust to this certificate, regardless of who it is signed by.

From the command line

After copying the certificate to the target client computer, perform the following, replacing <certificate> with the file path to the certificate:

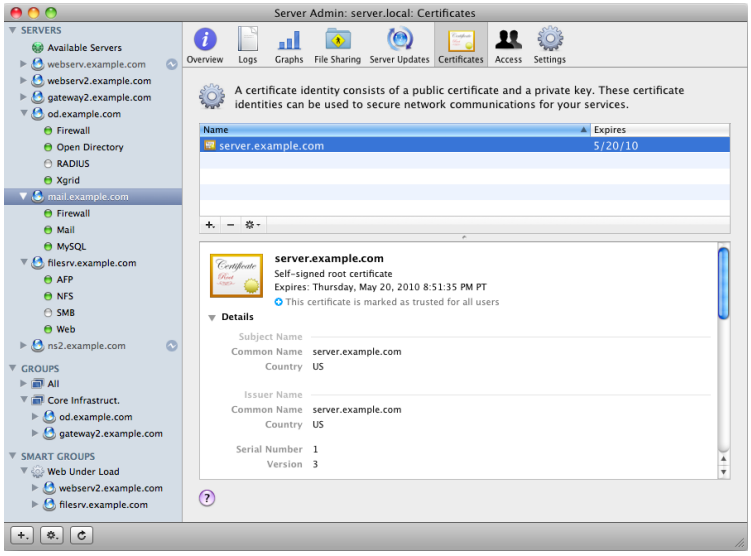
```
sudo /usr/bin/security add-trusted-cert -d -k /Library/Keychains/System.
     keychain <certificate>
```

You can use the security tool to save and restore trust settings as well. For more information on using the `security` command-line tool, see the `security` man page.

Certificate Manager in Server Admin

Mac OS X Server's Certificate Manager is integrated into Server Admin to help you create, use, and maintain identities for SSL-enabled services.

The Server Admin interface is shown below, with Certificates selected.



Certificate Manager provides integrated management of SSL certificates in Mac OS X Server for services that allow the use of SSL certificates. On installation, the server creates a self-signed certificate for immediate use from information you put in during server setup.

Certificate Manager uses Mac OS X's Certificate Assistant to create self-signed certificates and certificate-signing requests (CSRs) to obtain certificates signed by a CA. The certificates, self-signed or signed by a CA, are then accessible by services that support SSL.

Certificate Manager in Server Admin doesn't allow you to sign and issue certificates as a CA, nor does it allow you to sign and issue certificates as a root authority. If you need these functions, you can use Certificate Assistant in Keychain Access (located in /Applications/Utilities/). It provides these capabilities and others for working with x.509 certificates.

Identities that were created and stored in OpenSSL files can also be imported into Certificate Manager. They are accessible to services that support SSL. Self-signed and CA-issued certificates you created in CA Assistant can be used in Certificate Manager by importing the certificate.

Certificate Manager displays the following for each certificate:

- The domain name the certificate was issued for
- The expiration date of the certificate
- When selected, the detailed contents of the certificate

When certificates and keys are imported via Certificate Manager, they are put in the /etc/certificates/ directory. The directory contains four PEM formatted files for every identity:

- The certificate
- The public key
- The trust chain
- The concatenated version of the certificate plus the trust chain (for use with some services)

The certificate and trust chain are owned by the root user and the wheel group, with permissions set to 644. The public key and concatenation file are owned by the root user and the certusers group, with permissions set to 640.

Each file has the following naming convention:

<common name>.<SHA1 hash of the certificate>.<cert | chain | concat | key>.pem

For example, the certificate for a web server at example.com might look like this:

www.example.com.C42504D03B3D70F551A3C982CFA315595831A2E3.cert.pem

Readying Certificates

Before you can use SSL in Mac OS X Server's services, you must create or import certificates. You can create self-signed certificates, create certificates and then generate a Certificate Signing Request (CSR) to send to a CA, or import certificates previously created with OpenSSL.

If you have previously generated certificates for SSL, you can import them for use by Mac OS X Server services. The OpenSSL keys and certificates must be in PEM format.

Select a CA to sign your certificate request. If you don't have a CA to sign your request, consider becoming your own CA and then import your CA certificates into the root trust database of your managed machines.

When you set up Mac OS X Server, the Server Assistant creates a self-signed certificate based on information you provided when it's first installed. It can be used for any service that supports SSL. When your clients choose to trust the certificate, SSL connections can be used without user interaction from that point on.

This initial self-signed certificate is used by Server Admin and Server Preferences to encrypt administrative functions.

Creating a Self-Signed Certificate

A self-signed certificate is generated at server setup. Although it is available for use, you may want to customize the information in the certificate, so you would create a new self-signed certificate. This is especially important if you plan on having a CA sign your certificate.

When you create a self-signed certificate, Certificate Manager creates a private–public key pair in the System keychain with the key size specified (512 - 2048 bits). It then creates the corresponding self-signed certificate.

If you're using a self-signed certificate, consider using an intermediate trust for it and import the certificate into the System keychain on all client computers (if you have control of the computers). For more information about using intermediate trust, see "About Intermediate Trust" on page 61.

To create a self-signed certificate:

1. In Server Admin, select the server that has services that support SSL.
2. Click Certificates.
3. Click the Add (+) button and choose Create a Certificate Identity.

   Certificate Assistant launches, populated with information needed to generate the certificate.
4. If you override the defaults, choose "Let me override defaults" and follow the onscreen instructions.
5. When finished, click Continue.
6. Confirm the certificate creation by clicking Continue.

   The Certificate Assistant generates a key pair and certificate. Certificate Manager encrypts the files with a random passphrase, puts the passphrase in the System keychain, and puts the resulting PEM files in /etc/certificates/.

Requesting a Certificate from a Certificate Authority

Certificate Manager helps you create a CSR to send to your designated CA.

You need a certificate for the CA to sign. You can use the one that was generated at server setup, but more likely you will want to generate one that has all the details the CA requires before signing. If you need to generate a certificate before getting it signed, see "Creating a Self-Signed Certificate" on page 65.

To request a signed certificate:

1. In Server Admin, select the server that has services that support SSL.
2. Click Certificates.
3. Select the certificate you want signed.

4 Click the Action button below the certificates list and choose "Generate Certificate Signing Request (CSR)."

Certificate manager creates the signing request and shows the ASCII text version in the sheet.

5 Click Save to save the CSR to the disk.

Your CA will have instructions on how to transfer the CSR to the signer. Some CAs require you to use a web interface; others require sending the CSR in the body of a mail message. Follow the instructions given by the CA.

The CA will return a newly signed certificate, which replaces the one you generated. For instructions on what to do now with your newly signed certificate, see "Replacing an Existing Certificate" on page 71.

Creating a Certificate Authority

To sign another user's certificate, you must create a CA. Sometimes a CA certificate is referred to as a root or anchor certificate. By signing a certificate with the root certificate, you become the trusted third party in that certificate's transactions, vouching for the identity of the certificate holder.

If you are a large organization, you might decide to issue or sign certificates for people in your organization to use the security benefits of certificates. However, external organizations might not trust or recognize your signing authority.

To create a CA:

1 Start Keychain Access.

Keychain Access is found in the /Applications/Utilities/ directory.

2 In the Keychain Access menu, select Certificate Assistant > Create a Certificate Authority.

The Certificate Assistant starts. It will guide you through the process of making the CA.

3 Choose to create a Self Signed Root CA.

4 Provide the Certificate Assistant with the requested information and click Continue.

You need the following information to create a CA:

- An email address
- The name of the issuing authority (you or your organization)

You also decide if you want to override the defaults and whether to make this CA the organization's default CA. If you do not have a default CA for the organization, allow the Certificate Assistant to make this CA the default.

In most circumstances, do not override the defaults. If you do not override the defaults, skip to step 16.

5. If you override the defaults, provide the following information in the next few screens:
   - A unique serial number for the root certificate
   - The number of days the CA functions before expiring
   - The type of user certificate this CA is signing
   - Whether to create a CA website for users to access for CA certificate distribution
6. Click Continue.
7. Provide the Certificate Assistant with the requested information and click Continue.

   You need the following information to create a CA:
   - An email address of the responsible party for certificates
   - The name of the issuing authority (you or your organization)
   - The organization name
   - The organization unit name
   - The location of the issuing authority
8. Select a key size and an encryption algorithm for the CA certificate and then click Continue.

   A larger key size is more computationally intensive to use, but much more secure. The algorithm you choose depends more on your organizational needs than a technical consideration.

   DSA and RSA are strong encryption algorithms. DSA is a United States Federal Government standard for digital signatures.
9. Select a key size and an encryption algorithm for the certificates to be signed, and then click Continue.
10. Select the Key Usage Extensions you need for the CA certificate and then click Continue.

    At a minimum, you must select Signature and Certificate Signing.
11. Select the Key Usage Extensions you need for the certificates to be signed and then click Continue.

    Default key use selections are based on the type of key selected earlier in the Assistant.
12. Specify other extensions to add the CA certificate and click Continue.
13. Select the keychain "System" to store the CA certificate.
14. Choose to trust certificates on this computer signed by the created CA.
15. Click Continue and authenticate as an administrator to create the certificate and key pair.
16. Read and follow the instructions on the last page of the Certificate Assistant.

    You can now issue certificates to trusted parties.

Using a CA to Create a Certificate for Someone Else

You can use your CA certificate to issue a certificate to someone else. By doing so you are stating you want to be a trusted party that can certify the identity of the certificate holder.

Before you can create a certificate for someone, that person must generate a CSR. The user can use the Certificate Assistant to generate the CSR and mail the request to you. You then use the CSR's text to make the certificate.

To create a certificate for someone else:

1. Start Keychain Access.

   Keychain Access is found in the /Applications/Utilities/ directory.

2. In the Keychain Access menu, select Certificate Assistant > Create a Certificate for Someone Else as a Certificate Signing Authority.

   The Certificate Assistant starts, and guides you through the process of making the certificate.

3. Drag the CSR and drop it on the target area.

4. Choose the CA that is the issuer and sign the request.

   You can choose to override the request defaults.

5. Click Continue.

   If you override the request defaults, provide the Certificate Assistant with the requested information and click Continue.

   The Certificate is now signed. The default mail application launches with the signed certificate as an attachment.

Importing a Certificate Identity

You can import a previously generated OpenSSL certificate and private key into Certificate Manager. The items are listed as available in the list of identities and are available to SSL-enabled services.

The OpenSSL keys and certificates must be in PEM format.

To import an existing OpenSSL style certificate:

1. In Server Admin, select the server that has services that support SSL.
2. Click Certificates.
3. Click the Add (+) button and choose Import a Certificate Identity.
4. Drag the PEM file containing the private key to the sheet.
5. Drag the PEM file containing the public certificate to the sheet.
6. If needed, drag associated nonidentity certificates to the sheet as well.

7 Click the Import button.

If prompted, enter the private key passphrase.

Managing Certificates

After you create and sign a certificate, you won't do much more with it. Since certificates cannot be edited, you can either delete, replace, or revoke certificates after they are created. You cannot change certificates after a CA signs them.

If the information a certificate possesses (such as contact information) is no longer accurate, or if you believe the private key is compromised, delete the certificate.

If you have previously generated certificates for SSL, you can import them for use by services. The OpenSSL keys and certificates must be in PEM format.

If you chose custom locations for your SSL certificates with Leopard Server, you must import them into Certificate Manager if you want them to be available for services.

Custom filesystem locations for certificates cannot be managed for services using Server Admin for Mac OS X Server v10.6. To use custom file locations, you must edit the configuration files directly.

When certificates and keys are imported via Certificate Manager, they are put in the /etc/certificates/ directory. The directory contains four PEM formatted files for every identity:

- The certificate
- The public key
- The trust chain
- The concatenated version of the certificate plus the trust chain (for use with some services)

Each file has the following naming convention:

<common name>.<SHA1 hash of the certificate>.<cert | chain | concat | key>.pem

For example, the certificate for a web server at example.com might look like this:

www.example.com.C42504D03B3D70F551A3C982CFA315595831A2E3.cert.pem

After they are imported, Certificate Manager encrypts the files with a random passphrase. It puts the passphrase in the System keychain, and puts the resulting PEM files in /etc/certificates/.

Editing a Certificate

After you add a certificate signature, you can't edit the certificate. You must replace it with one generated from the same private key.

For instructions on how to do this, see "Replacing an Existing Certificate" on page 71.

Distributing a CA Public Certificate to Clients

If you're using self-signed certificates, a warning appears in most user applications saying that the CA is not recognized. Other software, such as the LDAP client, refuses to use SSL if the server's CA is unknown.

Mac OS X Server ships only with certificates from well-known commercial CAs. To prevent this warning, your CA certificate must be distributed to every client computer that connects to the secure server.

To distribute your certificate to your clients:

1. Copy the self-signed CA certificate (the file named ca.crt) onto each client computer.

   This is preferably distributed using nonrewritable media, such as a CD-R. Using nonrewritable media prevents the certificate from being corrupted.
2. Open the Keychain Access tool by double-clicking the ca.crt icon where the certificate was copied onto the client computer.
3. Drag the certificate to the System keychain using Keychain Access.

   Authenticate as an administrator, if requested.
4. Double-click the certificate to get the certificate details.
5. In the details window, click the Trust disclosure triangle.
6. From the pop-up menu next to "When using this certificate," select "Always Trust."

   You have now added trust to this certificate, regardless of who it is signed by.

From the command line

After copying the certificate to the target client computer, perform the following where <certificate> is the file path to the certificate:

```
sudo /usr/bin/security add-trusted-cert -d -k /Library/Keychains/System.
     keychain <certificate>
```

You can use the security tool to save and restore trust settings as well. For more information on using the `security` tool, see the `security` man page.

Deleting a Certificate

When a certificate has expired or been compromised, you must delete it.

To delete a certificate:

1. In Server Admin, select the server that has services that support SSL.
2. Click Certificates.
3. Select the Certificate Identity to delete.
4. Click the Remove (-) button and select Delete.

5 Click Save.

Renewing an Expiring Certificate

Certificates have an expiration date and must be renewed periodically. Renewing a certificate is the same as replacing a certificate with a newly generated one with an updated expiration date.

To renew an expiring certificate:

1 Request a new certificate from the CA.

If you are your own CA, create one using your own root certificate.

2 In Server Admin in the Server list, select the server that has the expiring certificate.

3 Click Certificates.

4 Select the Certificate Identity to renew.

5 Click the Action button and select "Replace Certificate with Signed or Renewed Certificate."

6 Drag the renewed certificate to the sheet.

7 Click Replace Certificate.

Replacing an Existing Certificate

If you change the DNS name of the server or any virtual hosts on the server, you must replace an existing certificate with an updated one.

To replace an expiring certificate:

1 Request a certificate from the CA.

If you are your own CA, create one using your own root certificate.

2 In Server Admin in the Server list, select the server that has the expiring certificate.

3 Click Certificates.

4 Select the Certificate Identity to replace.

5 Click the Action button and select "Replace Certificate with Signed or Renewed Certificate."

6 Drag the replacement certificate to the sheet.

7 Click Replace Certificate.

Using Certificates

In Server Admin, services like Web, Mail, VPN, and so on display a pop-up list of certificates that the administrator can choose from. The services vary in appearance and therefore the pop-up list location varies. Consult the administration guide for the service you're trying to use with a certificate.

SSH and SSH Keys

SSH is a network protocol that establishes a secure channel between your computer and a remote computer. It uses public-key cryptography to authenticate the remote computer. It also provides traffic encryption and data integrity exchanged between computers.

SSH is frequently used to log in to a remote machine to execute commands, but you can also use it to create a secure data tunnel, forwarding through an arbitrary TCP port. You can also use SSH to transfer files using SFTP and SCP. By default, an SSH server uses the standard TCP port 22.

Mac OS X Server uses OpenSSH as the basis for its SSH tools. Notably, portable home directory synchronization is provided via SSH.

Key-Based SSH Login

Key-based authentication is helpful for such tasks as automating file transfers and backups and for creating failover scripts because it allows computers to communicate without a user needing to enter a password.

Important: Key-based authentication has risks. If the private key you generate becomes compromised, unauthorized users can access your computers. You must determine whether the advantages of key-based authentication are worth the risks.

Generating a Key Pair for SSH

The following outlines the process of setting up key-based SSH login on Mac OS X and Mac OS X Server. To set up key-based SSH, you must generate the keys the two computers will use to establish and validate the identity of each other.

This doesn't authorize all users of the computer to have SSH access. Keys must be generated for each user account.

To do this, run the following commands in Terminal:

1. Verify that an .ssh folder exists in your home folder by entering the command:

   ```
   ls -ld ~/.ssh.
   ```

   If `.ssh` is listed in the output, move to step 2. If `.ssh` is not listed in the output, run `mkdir ~/.ssh` and continue to step 2.

2. Change directories in the shell to the hidden `.ssh` directory by entering the following command:

   ```
   cd ~/.ssh
   ```

3. Generate the public and private keys by entering the following command:

   ```
   ssh-keygen -b 1024 -t rsa -f id_rsa -P ''
   ```

The -b flag sets the length of the keys to 1,024-bits, -t indicates to use the RSA hashing algorithm, -f sets the file name as id_rsa, and -P followed by two single-quote marks sets the private key password to be null. The null private key password allows for automated SSH connections.

Keys are equivilant to passwords so you should keep them private and protected.

4 Copy the public key into the authorized key file by entering the following command:

```
cat id_rsa.pub >> authorized_keys2
```

5 Change the permissions of the private key by entering the following command:

```
chmod go-rwx ~/.ssh/.id_rsa
```

Set the permissions on the private key so the file can only be changed by the owner.

6 Copy the public key and the authorized key lists to the specified user's home folder on the remote computer by entering the following command:

```
scp authorized_keys2 username@remotemachine:~/.ssh/
```

To establish two-way communication between servers, repeat this process on the second computer.

The process must be repeated for each user that needs to open key-based SSH sessions. The root user is not excluded from this requirement. The home folder for the root user on Mac OS X Server is located at /var/root/.

Key-Based SSH with Scripting Sample

A cluster of servers is an ideal environment for using key-based SSH.

The following Perl script is a trivial scripting example that should not be implemented, but it demonstrates connecting over an SSH tunnel to all servers defined in the variable serverList, running softwareupdate, installing available updates, and restarting the computer if necessary.

The script assumes that key-based SSH was set up for the root user on all servers to be updated.

```
#!/usr/bin/perl
# \@ is the escape sequence for the "@" symbol.
my @serverList = ('root\@exampleserver1.example.com',
'root\@exampleserver2.example.com');
foreach $server (@serverList) {
open SBUFF, "ssh $server -x -o batchmode=yes 'softwareupdate -i -a' |";
while(<SBUFF>) {
my $flag = 0;
chop($_);
#check for restart text in $_
my $match = "Please restart immediately";
```

```
$count = @{[$_ =~ /$match/g]};
if($count > 0) {
$flag = 1;
}
}
close SBUFF;
if($flag == 1) {
"ssh $server -x -o batchmode=yes shutdown -r now"
}
}
```

Administration Level Security

Mac OS X Server can use another level of access control for added security. Administrators can be assigned to services they can configure. These limitations are enacted on a server-by-server basis. This method can be used by an administrator with no restrictions to assign administrative duties to other admin group users.

This results in a tiered administration model, where some administrators have more privileges than others for assigned services. This results in a method of access control for individual server features and services.

For example, Alice (the lead administrator) has control over all services on a given server and can limit the ability of other admin group users (like Bob and Cathy) to change settings on the server. She can assign DNS and Firewall service administration to Bob, while leaving Mail service administration to Cathy.

In this scenario, Cathy can't change the firewall or any service other than mail. Likewise, Bob can't change any services outside of his assigned services.

Tiered administration controls are effective in Server Admin and the serveradmin command-line tool. They are not effective against modifying UNIX configuration files throughout the system. Protect UNIX configuration files with POSIX-type permissions or ACLs.

Setting Administration Level Privileges

Mac OS X Server can use another level of access control for added security. Administrators can be limited to specific services they can configure. These limitations are enacted on a server-by-server basis. This method can be used by an administrator with no restrictions to assign administrative duties to other admin group users.

This results in a tiered administration model, where some administrators have more privileges than others for their assigned services. This results in a kind of access control for individual server features and services.

You can determine which services other admin group users can modify. To do this, the administrator making the determination must have full, unmodified access.

The process for setting administration level privileges is found in "Tiered Administration Permissions" on page 149.

Service Level Security

You use a Service Access Control List (SACL) to enforce who can use a service. It is not a means of authentication. It is a list of those who have access rights to use a service.

SACLs allow you to add a layer of access control on top of standard and ACL permissions.

Only users and groups in an SACL can access its corresponding service. For example, to prevent users from accessing AFP share points on a server, including home folders, remove the users from the AFP service's SACL.

Server Admin in Mac OS X Server allows you to configure SACLs. Open Directory authenticates user accounts and SACLs authorize use of services. If Open Directory authenticates you, the SACL for login window determines whether you can log in, the SACL for AFP service determines whether you can connect for Apple file service, and so on.

Setting SACL Permissions

SACLs allow you to specify which users and groups have access to Mac OS X Server services, including AFP, FTP, and Windows file services.

To set SACL permissions for a service:

1. Open Server Admin.
2. Select the server from the Servers list.
3. Click Settings.
4. Click Access.
5. To restrict access to all services or deselect this option to set access permissions per service, select "For all services."
6. If you deselected "For all services," select a service from the Service list.
7. To provide unrestricted access to services, click "Allow all users and groups."

   If you want to restrict access to certain users and groups:

   - Select "Allow only users and groups below."
   - Click the Add (+) button to open the Users & Groups window.
   - Drag users and groups from the Users & Groups window to the list.
8. Click Save.

Security Best Practices

Server administrators must make sure that adequate security measures are implemented to protect a server from attacks. A compromised server risks the resources and data on the server and risks the resources and data on other connected systems. The compromised system can then be used as a base to launch attacks on other systems within or outside your network.

Securing servers requires an assessment of the cost of implementing security with the likelihood of a successful attack and the impact of that attack. It is not possible to eliminate all security risks but it is possible to minimize risks to efficiently deal with them.

Best practices for server system administration include the following:

- Update your systems with critical security patches and updates.
- Check for updates regularly.
- Install antivirus tools, use them regularly, and update virus definition files and software regularly.

  Although viruses are less prevalent on the Mac platform than on Windows, viruses still pose a risk.
- Restrict physical access to the server.

  Because local access generally allows an intruder to bypass most system security, secure the server room, server racks, and network junctures. Use security locks. Locking your systems is a prudent thing to do.
- Make sure there is adequate protection against physical damage to servers and ensure that the climate control functions in the server room.
- Take additional precautions to secure servers.

  For example, enable firmware passwords, encrypt passwords where possible, and secure backup media.
- Secure logical access to the server.

  For example, remove or disable unnecessary accounts. Accounts for outside parties should be disabled when not in use.
- Configure SACLs as needed.

  Use SACLs to specify who can access services.
- Configure ACLs as needed.

  Use ACLs to control who can access share points and their contents.
- Protect any account with root or system administrator privileges by following recommended password practices using strong passwords.

  For more information about passwords, see "Password Guidelines" on page 77 .

- Do not use administrator (UNIX "admin" group) accounts for daily use.

  Restrict the use of administration privileges by keeping the admin login and password separate from daily use.

- Back up critical data on the system regularly, with a copy stored at a secure off-site location.

  Backup media is of little use in recovery if it is destroyed with the computer during a fire. Test your backup and recovery contingency plans to ensure that recovery actually works.

- Review system audit logs regularly and investigate unusual traffic.
- Disable services that are not required on your system.

  A vulnerability that occurs in any service on your system can compromise the entire system. In some cases, the default configuration (out of the box) of a system leads to exploitable vulnerabilities in services that were enabled implicitly.

  Turning on a service opens up a port that users can access your system from. Although enabling Firewall service helps avoid unauthorized access, an inactive service port remains a vulnerability that an attacker might exploit.

- Enable Firewall service on servers, especially at the network frontier and DMZ.

  Your server's firewall is the first line of defense against unauthorized access. For more information, see the onscreen help or Mac OS X Server Resources website at www.apple.com/server/macosx/resources/. Consider also a third-party hardware firewall as an additional line of defense if your server is highly prone to attack.

- If needed, install a local firewall on critical or sensitive servers.

  Implementing a local firewall protects the system from an attack that might originate within the organization's network or from the Internet.

- For additional protection, implement a local Virtual Private Network (VPN) that provides a secure encrypted tunnel for communication between a client computer and your server application. Some network devices provide a combination of functions: firewall, intrusion detection, and VPN.
- Administer servers remotely.

  Manage your servers remotely using applications like Server Admin, Server Monitor, RAID Admin, and Apple Remote Desktop. Minimizing physical access to the systems reduces the possibility of mischief.

Password Guidelines

Many applications and services require that you create passwords to authenticate. Mac OS X includes applications that help create complex passwords (using Password Assistant), and securely store your passwords (using Keychain Access).

Creating Complex Passwords

Use the following tips to create complex passwords:

- Use a mix of alphabetic (upper and lower case), numeric, and special characters (such as ! and @).
- Don't use words or combinations of words found in a dictionary of any language.
- Don't append a number to an alphabetic word (for example, "wacky2") to fulfill the constraint of having a number.
- Don't substitute "look alike" numbers or symbols for letters (for example, "GR33N" instead of "GREEN").
- Don't use proper names.
- Don't use dates.
- Create a password of at least 12 characters. Longer passwords are generally more secure than shorter passwords.
- Use passwords that can't be guessed even by someone who knows you and your interests well.
- Create as random a password as possible.

You can use Password Assistant (located in /System/Library/CoreServices) to verify the complexity of your password.

Installation and Deployment

5

Whether you install Mac OS X Server on a single server or a cluster of servers, there are tools and processes to help the installation and deployment succeed.

Some computers come with Mac OS X Server software already installed. Other computers need the server software installed. For example, installing Mac OS X Server v10.6 on a computer with Mac OS X makes the computer a server with Mac OS X Server.

Installing Mac OS X Server v10.6 on Mac OS X Server v10.2–v10.5 upgrades the server software to v10.6.

This chapter includes instructions for a fresh installation of Mac OS X Server v10.6 using a variety of methods.

Installation Overview

You've already planned and decided how many and what kind of servers you are going to install.

Step 1: Confirm you meet the requirements

Make sure your target server meets the minimum system requirements. For more information see:

- "System Requirements for Installing Mac OS X Server" on page 81
- "Hardware-Specific Instructions for Installing Mac OS X Server" on page 81

Step 2: Gather your information

Gather all the information you need before you begin. This helps to make sure the installation goes smoothly, and helps you make planning decisions.

For planning your installation, see:

- Chapter 2, "Planning Server Usage," on page 24

Step 3: Set up the environment
If you are not in complete control of the network environment (DNS servers, DHCP server, firewall, and so forth) coordinate with your network administrator before installing. A functioning DNS system with full reverse lookups and a firewall to allow configuration constitute a minimum for the setup environment.

If you plan on connecting the server to an existing directory system, you must also coordinate efforts with the directory administrator. See the following:

- "Setting Up Network Services" on page 82
- "Connecting to the Directory During Installation" on page 82
- "SSH During Installation" on page 82
- "Preparing an Administrator Computer" on page 83

If you are administering the server from another computer, you must create an administration computer.

Step 4: Start up the computer from an installation disk
You can't install onto the disk the computer is started from, but you can upgrade. For clean installations and upgrades, you must start up the server from an installation disk, not from the target disk. See the following:

- "About Starting Up for Installation" on page 84
- "Remotely Accessing the Install DVD" on page 88
- "Starting Up from the Install DVD" on page 85
- "Starting Up from an Alternate Partition" on page 85
- "Starting Up from a NetBoot Environment" on page 91

Step 5: Prepare the target disk
If you are doing a clean installation, you must prepare the target disk by making sure it has the right format and partition scheme. See the following:

- "Preparing Disks for Installing Mac OS X Server" on page 92
- "Choosing a File System" on page 93
- "About Hard Disk Partitioning" on page 94
- "About Creating a RAID Set" on page 96
- "Erasing a Disk or Partition" on page 99

Step 6: Start the installer
The installer application takes software from the startup disk and server software packages and installs them on the target disk. See the following:

- "Identifying Remote Servers When Installing Mac OS X Server" on page 90
- "Installing Server Software Interactively" on page 99
- "Installing Locally from the Installation Disc" on page 100

- "Installing Remotely with Server Assistant" on page 101
- "Installing Remotely with Screen Sharing and VNC" on page 102
- "Using the installer Command-Line Tool to Install Server Software" on page 104

Step 7: Set Up Services
Restart from the target disk to proceed to setup. For more information about server setup, see Chapter 6, "Initial Server Setup."

System Requirements for Installing Mac OS X Server

The Mac desktop computer or server where you install Mac OS X Server v10.6 must have the following:

- An Intel processor
- At least 2 gigabytes (GB) of random access memory (RAM)
- At least 10 gigabytes (GB) of available disk space
- A new serial number for Mac OS X Server 10.6

  The serial number used with any previous version of Mac OS X Server will not allow registration in v10.6.

A built-in DVD drive is convenient but not required.

A display and keyboard are optional. You can install server software on a computer that has no display and keyboard by using an administrator computer. For more information, see "Setting Up an Administrator Computer" on page 124.

If you're using an installation disc for Mac OS X Server v10.6, you can control installation from another computer using VNC viewer software. Open-source VNC viewer software is available. Apple Remote Desktop, described on "Apple Remote Desktop" (page 50), includes VNC viewer capability.

Hardware-Specific Instructions for Installing Mac OS X Server

When you install server software on Xserve systems, the procedure you use when starting the computer for installation is specific to the kind of Xserve hardware you have. You may need to refer to the documents that came with your Xserve, where these procedures are documented.

Gathering the Information You Need

Use the *Installation & Setup Worksheet* to record information for each server you want to install. The information below provides supplemental explanations for items on the worksheet.

Setting Up Network Services

Before you can install, you must set up the following for your network service:

- **DNS:** You must have a fully qualified domain name for each server's IP addess in the DNS system. The DNS zone must have the reverse-lookup record for the name and address pair. Not having a stable, functioning DNS system with reverse lookup leads to service failures and unexpected behaviors.
- **Static IP Address:** Make sure you have a static IP address already planned and assigned to the server.
- **DHCP:** Do not assign dynamic IP addresses to servers. If your server gets its IP address through DHCP, set up a static mapping in the DHCP server, so your server gets (via its Ethernet address) the same IP address every time.
- **Firewall or routing:** In addition to any firewall running on your server, the subnet router might have specific network traffic restrictions in place. Make sure the server's IP address is available for the traffic it will handle and the services you will run.

Connecting to the Directory During Installation

To use a server as an Open Directory master, make sure it has an active Ethernet connection to a secure network before installation and initial setup. If the server doesn't have an active directory connection during setup, you can create an Open Directory master later using Server Admin or Server Preferences.

To use a server bound to another directory server (Open Directory, Active Directory, or other OpenLDAP), make sure you have the DNS name and IP address of the master directory server before installation.

SSH During Installation

When you start up a computer from a server installation disc, SSH starts so that remote installations can be performed.

Important: Before you install or reinstall Mac OS X Server, make sure the network is secure because SSH gives others access to the computer over the network. For example, design the network topology so you can make the server computer's subnet accessible only to trusted users.

About the Server Install Disc

You can install server software using the *Mac OS X Server Install Disc*. This installation disc contains everything to install Mac OS X Server.

Mac OS X Server Install Disc

The Install Disc has a Documentation folder with *Getting Started*, *Installation & Setup Worksheet*, and a Read Me file. It also contains an Other Installs folder, which has the following installer packages:

- ServerAdministrationSoftware.mpkg

  Use this package to install the administration tools on a computer running Mac OS X v10.6 to make it an administrator computer.

- iPhoneConfigurationUtility.pkg

  Use this package to install software that makes and distributes iPhone configuration files.

- X11User.pkg

  Use this package to install software to allow the server to function as an X Windowing System display server.

- Xcode.mpkg

  Use this package to install the free development tools for Mac OS X. This includes system administration utilities like PackageMaker and Property List Editor.

Administration Tools CD

In addition to the installation disc, Mac OS X Server includes the *Administration Tools* CD. You use this disc to set up an administrator computer. This disc has a Documentation folder with *Getting Started*, *Installation & Setup Worksheet*, and an acknowledgments page. It also contains:

- ServerAdministrationSoftware.mpkg

  Use this package to install the administration tools on a computer running Mac OS X Snow Leopard to make it an administrator computer.

- iPhoneConfigurationUtility.pkg

  Use this package to install software that makes and distributes iPhone configuration files.

- Two developer tools: PackageMaker and Property List Editor

Preparing an Administrator Computer

You can use an administrator computer to install, set up, and administer Mac OS X Server on another computer. An administrator computer is a computer with Mac OS X Server v10.6 or Mac OS X v10.6 that you use to manage remote servers. You cannot run the server administration tools from a Leopard or Leopard Server computer.

When you install and set up Mac OS X Server on a computer that has a display and keyboard, it's already an administrator computer. To make a computer with Mac OS X into an administrator computer, you must install additional software.

Important: If you have administrative applications and tools from Mac OS X Server v10.4 or earlier, do not use them on a computer with Mac OS X v10.6 or Mac OS X Server v10.6.

To install Mac OS X Server v10.6 administration tools:

1. Make sure the Mac OS X computer has Mac OS X Server v10.6 installed.
2. Insert the Administration Tools CD.
3. Open the Installers folder.
4. Open ServerAdministrationSoftware.mpkg to start the Installer, and then follow the onscreen instructions.

About Starting Up for Installation

The computer can't install to its own startup volume, so you must start up in some other way, such as:

- DVDs
- Alternate volumes (second partitions on the hard disk, or external FireWire disks)
- NetBoot

The computer must install from the same disk or image that started up the computer. Mounting another share point with an installer won't work. The installer uses some of the files currently active in the booted system partition for the new installation.

Before Starting Up

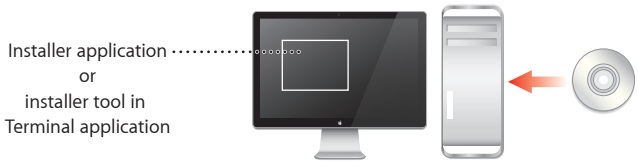
If you're performing a clean installation rather than upgrading an existing server, back up any user data that's on the disk or partition where you'll install the server software.

If you're upgrading an existing server, make sure that saved setup data won't be detected and used to set up the server. Server Assistant looks for saved setup data on all mounted disks and in all directories the server is configured to access. The saved setup data will overwrite the server's existing settings.

For more information about automatic server setup, see "Using Automatic Server Setup" on page 115.

Starting Up from the Install DVD

This is the simplest method of starting the computer, if you have physical access the server and it has DVD drive.



If the target server is an Xserve with a built-in DVD drive, start the server using the Install DVD by following the instructions in *Xserve User's Guide* for starting from a system disc.

If the target server has no built-in DVD drive, you can use an external FireWire DVD drive. You can also install server software on an Xserve system that lacks a DVD drive by moving its drive module to another Xserve system that has a DVD drive.

To start up the computer with the installation disc.

1. Turn on the computer and insert the *Mac OS X Server Install Disc* into the DVD drive.

   If you're using a built-in DVD drive, you can restart the computer directly to the DVD by holding down the C key. You can release the C key when you see the Apple logo.

   Alternatively, you can restart the computer by holding down the Option key, selecting the icon representing the installation disc, and then clicking the right arrow. You must use this method if you are starting up from an external DVD drive.

   If you're installing on an Xserve, the procedure for starting up from a DVD may be different.

   For more information, see *Xserve User's Guide* or the *Quick Start* guide that came with your Xserve.

2. Open the Install Mac OS X Server application and click the Restart button.

   The application is in the *Mac OS X Server Install Disc* window.

3. If you see an Install button instead of a Restart button in the lower-right corner of the application window, click Install and proceed through the Installer panes by following the onscreen instructions.

Starting Up from an Alternate Partition

For a single server installation, preparing to start up from an alternate partition can be more time-consuming than using the Install DVD. The time required to image, scan, and restore the image to a startup partition might exceed the time taken to install once from the DVD.

However, if you are reinstalling regularly, or if you are creating an external Firewire drive-based installation to take to various computers, or if you need some other kind mass distribution (such as clustered Xserves without DVD drives installed), this method can be very efficient.

This method is suited to installing on computers that you do not have easy physical access to. With sufficient preparation, this method can be modified for easy mass deployment of licensed copies of Mac OS X Server.

To use this method, you must have an existing installation of some kind on the computer. It is intended for environments where a level of existing infrastructure of Mac OS X Server is present, and might be unsuitable for a first server installation.

To start from an alternate partition, there are four basic steps.

Step 1: Prepare the disks and partitions on the target computer.
Before you proceed, you must have at least two partitions on the target computer. The first is the initial and final startup partition; the second is the temporary installer partition. You can use a single disk with multiple partitions or you can use multiple disks. You use Disk Utility to prepare the disks.

For more information about preparing and partitioning a hard disk, see the Disk Utility help.

Step 2: Create a restorable image of the Install DVD.
This step doesn't need to be done on the target computer. It can be done on an administrator computer, but there must be enough free space to image the entire Install DVD. See "To create an image of the Install DVD" on page 86.

Step 3: Restore the image to the alternate partition.
You can restore the disk image to a partition within the computer or to an external hard disk. When complete, the restored partition functions like the Install DVD. Make sure the alternate partition is at least the size of the disk image. See "To restore the image to a free volume" on page 87.

Step 4: Select the alternate partition as the startup disk.
After the partition is restored, it's a startup and installer disk for your server. Now start up the computer from that partition. After the computer is running, it is a Mac OS X Server installer, exactly as if you had started the computer from the DVD.

To create an image of the Install DVD

1. Insert the Install DVD.
2. Launch Disk Utility.
3. Select the first session icon under the optical drive icon.

   This is in the list of devices on the left side of the window.

4 Select File > New > Disk Image from <device>.

5 Give the image a name; select Read-only, Read/Write, or Compressed as the image type; and then click Save.

6 After the image is complete, select the image from list on the left.

7 In the menu, select Images > Scan Images for Restore.

8 Provide an administrator login and password as needed.

The installer disk image can now be restored to your extra partition.

From the command line

If you prefer to use the command line, you can use `hdiutil` to create the disk image, and `asr` to scan the image for restore. All commands must be done with superuser or root privileges.

For example, the first command creates the disk image Installer.dmg from the device at disk1s1. The second command scans the image Installer.dmg and readies it for restore.

```
hdiutil create -srcdevice disk1s1 Installer.dmg
asr imagescan --source Installer.dmg
```

To restore the image to a free volume

1 Start up the target computer.

2 Make sure the image does not reside on the partition that is to be erased.

3 Launch Disk Utility.

4 In the list of devices on the left side of the window, select the installer DVD image.

5 Click the Restore tab.

6 Drag the installer image from the left side of the window to the Source field.

7 Drag the alternate partition from the list of devices on the left side of the window to the Destination field.

8 Select Erase Destination.

9 Click Restore.

From the command line

To use the command line, use the `asr` tool to restore the image to the partition. Restoring the disk image to the partition will erase all existing data on the partition. The basic syntax is: `sudo asr restore -s <compressedimage> -t <targetvol> --erase`

The `asr` tool can also fetch the target image from an HTTP server using http or https URLs as its source, so the image doesn't need to reside on the target computer. For more information about `asr` and its capabilities, see the `asr` man page.

Tip: You can use `asr` to restore a disk over a network, multicasting the blocks to client computers. Using the multicast server feature of `asr`, you could put a copy of the installer image on a partition of all computers that can receive the multicast packets.

For example, restoring an image called Installer.dmg to the partition ExtraHD would be:

```
sudo asr restore -s Installer.dmg -t ExtraHD --erase
```

Remotely Accessing the Install DVD

When used as the startup disc, the Install DVD provides some services for remote access. After you start up from DVD, access using Server Assistant, SSH, and VNC are available.

Server Assistant allows you to view and configure the server installation with the same user interface you would see if you were installing locally. Server Assistant runs on Mac OS X v10.6 and Mac OS X Server v10.6.

VNC enables you to use a VNC viewer (like Screen Sharing or Apple Remote Desktop) to view the user interface as if you were using the remote computer's keyboard, mouse, and monitor. All the things you could do at the computer using the keyboard and mouse are available remotely, as well as locally. This excludes hardware restarts (using the power button to shut down and restart the computer), other hardware manipulation, or holding down keys during startup. VNC viewers are available for all popular computing platforms.

SSH enables you to have command-line access to the computer with administrator privileges.

To access the computer with Server Assistant

1. Start the target computer from the Install DVD for Mac OS X Server v10.6 or later.

   The procedure you use depends on the target server hardware.

   To learn more about startup disk options, see "About Starting Up for Installation" on page 84.
2. On an administrator computer, open Server Admin.
3. In the Server menu, select "Install Remote Server."

   The Server Assistant launches.
4. Enter the IP address or DNS name of the target server.

   If you do not know the IP address or DNS name of the target server, you must identify it first. For more information about this process, see "Identifying Remote Servers When Installing Mac OS X Server" on page 90.
5. For the password, enter the default password for installation.

This is usually the first eight characters of the server's built-in hardware serial number.

For more information about this password, see "About Server Serial Numbers for Default Installation Passwords" on page 90.

To access the computer with VNC:

1. Start the target computer from the Install DVD for Mac OS X Server v10.6 or later.

   The procedure you use depends on the target server hardware.

   To learn more about startup disk options, see "About Starting Up for Installation" on page 84.

2. Use your VNC viewer software to open a connection to the target server.

   If you do not know the IP address or DNS name of the target server, you must identify it first. For more information about this process, see "Identifying Remote Servers When Installing Mac OS X Server" on page 90.

3. For the password, enter the default password for installation.

   This is usually the first eight characters of the server's built-in hardware serial number.

   For more information about this password, see "About Server Serial Numbers for Default Installation Passwords" on page 90.

   If you're using Apple Remote Desktop as a VNC viewer, enter the password but don't specify a user name.

To access the computer using Screen Sharing:

1. Locate and select the server in the Shared section of a Finder window sidebar.

   If the remote server isn't listed in the Shared section of a Finder window sidebar, you can connect by choosing Go > Connect to Server and then entering vnc://*serveraddress*, where *serveraddress* is the DNS name or IP address of the server whose screen you want to share.

2. Select the remote server and click Share Screen in the Finder window.

3. For the password, enter the default password for installation.

   This is usually the first eight characters of the server's built-in hardware serial number.

   For more information about this password, see "About Server Serial Numbers for Default Installation Passwords" on page 90.

   Don't specify a user name.

To access the computer with SSH:

1. Start the target computer from the Install DVD for Mac OS X Server v10.6 or later.

   The procedure you use depends on the target server hardware.

   To learn more about startup disk options, see "About Starting Up for Installation" on page 84.

2 Identify the target server.

If you don't know the IP address and the remote server is on the local subnet, you can find servers using the comannd line. For more information about this process, see "Identifying Remote Servers When Installing Mac OS X Server" on page 90.

3 Use the Terminal to open a secure shell connection to the target server.

The user name is root.

4 For the password, enter the default password for installation.

This is usually the first eight characters of the server's built-in hardware serial number.

For more information about this password, see "About Server Serial Numbers for Default Installation Passwords" on page 90.

About Server Serial Numbers for Default Installation Passwords

Server serial numbers are used for more than inventory tracking. The server's built-in hardware serial number is used as the default password for remote installation. The password is case-sensitive.

To find a server's serial number, look for a label on the server. If you're installing on an older computer that has no built-in hardware serial number, use 12345678 for the password.

If you replace a main logic board on an Intel Xserve, the built-in hardware password is "System S" (no quotes).

Identifying Remote Servers When Installing Mac OS X Server

When using Server Assistant, you must be able to recognize the target server in a list of servers on your local subnet or you must enter the IP address of the server (in IPv4 format: 000.000.000.000) if it resides on a different subnet. Information provided for servers in the list includes IP address, DNS name, and Media Access Control (MAC) address (also called hardware or Ethernet address).

If you use VNC viewer software to remotely control installation of Mac OS X Server v10.6 or later, it might let you select the target server from a list of available VNC servers. If not, you must enter the IP address of the server (in IPv4 format: 000.000.000.000).

The target server's IP address is assigned by a DHCP server on the network. If no DHCP server exists, the target server uses a 169.xxx.xxx.xxx address unique among servers on the local subnet. Later, when you set up the server, you can change the IP address.

If you don't know the IP address and the remote server is on the local subnet, you can find servers that are awaiting install finding the the Bonjour service name "_sa-rspndr._tcp."

You can use the `dns-sd` tool to identify computers on the local subnetwhere you can install server software. Enter the following from a computer on the same local network as the server:

```
dns-sd -B _sa-rspndr._tcp.
```

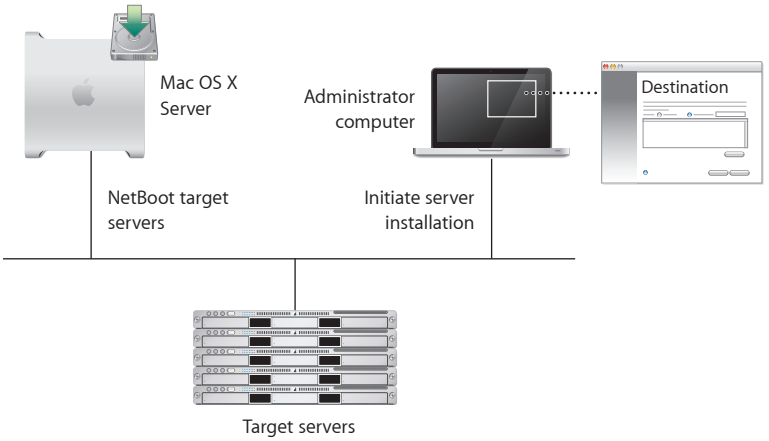
This command returns the IP address and the EthernetID (in addition to other information) of servers on the local subnet that have started up from the installation disk.

Similarly, servers awaiting setup use the service name "_svr-unconfig._tcp." and can be found by entering:

```
dns-sd -B _svr-unconfig._tcp.
```

Starting Up from a NetBoot Environment

If you have an existing NetBoot infrastructure, this is the easiest way to perform mass installation and deployment. You can use this method for clusters that have no optical drive or existing system software.



This method can also be used in environments where large numbers of servers must be installed in an efficient manner.

This section won't tell you how to create the necessary NetBoot infrastructure. If you want to set up NetBoot and NetInstall options for your network, servers, and client computers, see the manuals at www.apple.com/server/resources/.

This section has instructions to create a NetInstall image from the Mac OS X Server Install Disk and start a server from it. There is no need to make preparations to the hard disk.

Step 1: Create a NetInstall image from the Install DVD
This step doesn't need to be done on the target computer. It can be done on an administrator computer that has enough free space to image the entire Install DVD.

Step 2: Start up the computer from the NetBoot server
There are four ways of doing this, depending on your environment.

To create a NetInstall image from the Install DVD:

1. Launch System Image Utility from /Applications/Server/.
2. Select the Install DVD on the left, and choose NetInstall image on the right.
3. Click Continue.
4. Enter a name for the image and a description.

   This information is seen by clients selecting it a startup disk.
5. Click Create and then choose a save location for the disk image.

Upon completion, you can use this image with an existing NetBoot server to start up a server for installation.

For more information about NetInstall images and System Image Utility, including customization options, see the documentation at www.apple.com/server/resources/.

To start up the computer from the NetBoot server:

- In the target computer GUI, select the NetInstall disk from the Startup Disk pane of the System Preferences.
- Restart the computer, holding down the "n" key.

  The first NetBoot server to respond to the computer will start up the computer with its default image.
- Restart the computer, holding down the Option key.

  The computer will show you the available startup disks, locally on the computer and remotely from NetBoot and NetInstall servers. Select a disk and continue the startup.
- Use the command-line locally or remotely to specify the NetBoot server that the computer will start up from:

```
sudo bless --netboot --server bsdp://<netbook server host name, server.
     example.com>
```

Preparing Disks for Installing Mac OS X Server

Before performing a clean installation of Mac OS X Server, you can partition the server computer's hard disk into multiple volumes, create a RAID set, or erase the target disk or partition.

If you're using an installation disc for Mac OS X Server v10.6, you can perform these tasks from another networked computer using VNC viewer software, such as Apple Remote Desktop, before beginning a clean installation.

WARNING: Before partitioning a disk, creating a RAID set, or erasing a disk or partition on a server, preserve user data you want to save by copying it to another disk or partition.

Choosing a File System

A file system is a method for storing and organizing computer files and the data they contain on a storage device such as a hard disk. Mac OS X Server supports several types of file systems. Each file system has its own strengths. You must decide which system fits your organization's needs.

For more information, see developer.apple.com/technotes/tn/tn1150.html.

The following systems are available for use:

- Mac OS Extended (Journaled) aka HFS+J
- Mac OS Extended (Journaled, Case-Sensitive) aka HFSX

About Mac OS Extended (Journaled) aka HFS+J

An HFS+J volume is the default file system for Mac OS X Server.

An HFS+J volume has an optional journal to speed recovery when mounting a volume that was not unmounted safely (for example, as the result of a power outage or crash). The journal makes it easy to restore the volume structures to a consistent state, without scanning all structures.

The journal is used only for volume structures and metadata. It does not protect the contents of a fork. In other words, this journal protects the integrity of the underlying disk structures, but not data that is corrupted due to a write failure or catastrophic power loss.

More information about HFS+J can be found in Apple's Developer Documentation at:

developer.apple.com/documentation/MacOSX/Conceptual/BPFileSystem/Articles/Comparisons.html

About Mac OS Extended (Journaled, Case-Sensitive) aka HFSX

HFSX is an extension to HFS Plus and allows volumes to have case-sensitive file and directory names. Case-sensitive names means that you can have two objects whose names differ only by the case of the letters in the same directory at the same time. For example, you could have Bob, BOB, and bob in the same directory as uniquely named files.

A case-sensitive volume is supported as a start volume format. An HFSX file system for Mac OS X Server must be specifically selected when erasing a volume and preparing a disk before initial installation.

If you are planning to use NFS, you should use case-sensitive HFSX.

An HFSX volume can be case sensitive or case insensitive. Case sensitivity (or lack thereof) is global to the volume. The setting applies to all file and directory names on the volume. To determine whether an HFSX volume is case-sensitive, use Disk Utility to examine the format of the disk.

Note: Do not assume that an HFSX volume is case sensitive. Always use Disk Utility to determine case sensitivity or case insensitivity. Additionally, don't assume your third-party software solutions work correctly with case sensitivity.

Important: Case-sensitive names do not ignore Unicode ignorable characters. This means that a single directory can have several names that are considered equivalent using Unicode comparison rules, but they are considered distinct on a case-sensitive HFSX volume.

About Hard Disk Partitioning

The minimum recommended size for an installation partition is 10 GB. A much larger volume is recommended for a configuration that keeps shared folders and group websites on the startup volume together with the server software.

Partitioning the hard disk creates a volume for server system software and additional volumes for data and other software. Partitioning erases previous contents of the disk.

Erasing a disk is another way of saying that you have given a disk a single volume partition and erased that volume.

Consider dedicating a hard disk or a volume of a partitioned hard disk to server software. Put additional software, share points, websites, and so forth on other disks or volumes. With this approach, you can upgrade or reinstall the server software without affecting your other software or user data. If you must store additional software or data on the system volume, consider mirroring it to another drive.

Tip: Having an extra, empty partition or two on the target installation disk can give you additional flexibility in installation and deployment. For example, additional space can give you a place to temporarily mirror your current installation before performing an in-place update, or it can give you a fast installer disk.

Partitioning a Disk

You can use the Installer to open Disk Utility and then use Disk Utility to partition the installation target disk into desired volumes. You can erase the target volume using the Mac OS Extended format, Mac OS Extended (Journaled) format, Mac OS Extended format (Case-Sensitive) format, and Mac OS Extended (Journaled, Case-Sensitive) format. You cannot partition the active startup disk or erase the active startup volume.

You can select an existing partition and choose resize, Add (+), or Delete (–). However, you can't delete or resize the startup partition. You also can't select the startup volume and then choose an entirely new partition scheme from the pop-up menu.

To partition a disk using Disk Utility

1. Launch Disk Utility.

   If you are in the Installer, Disk Utility is available from the Utilities menu.

   Otherwise, launch the application from /Applications/Utilities/Disk Utility.

2. Select the disk to be partitioned.

   Selecting a volume on the disk allows you to erase the volume but does not create a different partition scheme.

3. Click Partition.

4. Choose your partition scheme and follow the instructions in the window to set all necessary parameters.

5. Click Apply.

   You can find instructions for partitioning the hard disk into multiple volumes, creating a RAID set, and erasing the target disk or partition by viewing Disk Utility Help. To view Disk Utility Help, open Disk Utility on another Mac computer with Mac OS X v10.6 and choose Help > Disk Utility Help.

From the command line

You can use the diskutil command-line tool to partition and erase a hard disk. Normally, you would use a remote shell (SSH) to log in to the newly started computer to use this method. The tool to partition disks is diskutil.

Just like using Disk Utility, you can erase the target volume using the Mac OS Extended format, Mac OS Extended (Journaled) format, Mac OS Extended format (Case-Sensitive) format, and Mac OS Extended (Journaled, Case-Sensitive) format.

You cannot delete or resize the active startup disk or erase the active startup volume.

All potentially destructive diskutil operations must be performed with superuser or root privileges.

Additional information about diskutil and other uses can be found in *Introduction to Command-Line Administration*. For complete command syntax for `diskutil`, consult the tool's man page.

The specific command issued depends on your disk format needs and the hardware in use. Take care to use command-line arguments that apply to your specific needs.

The following command is a sample, which partitions a computer's only 120 GB hard disk into two equal 60 GB journaled HFS+ volumes ("BootDisk" and "DataStore"), which can start up an Intel-based Mac computer.

The basic syntax is:

```
diskutil partitionDisk device numberOfPartitions GPTFormat <part1Format
     part1Name part1Size> <part2Format part2Name part2Size>
```

So the command is:

```
diskutil partitionDisk disk0 2 GPTFormat JournaledHFS+ BootDisk 50%
     JournaledHFS+ DataStore 50%
```

About Creating a RAID Set

If you're installing Mac OS X Server on a computer with multiple internal hard disks, you can create a RAID set to optimize storage capacity, improve performance, and increase reliability in case of a disk failure.

For example, a mirrored RAID set increases reliability by writing your data to two or more disks at once. If one disk fails, your server uses another disk in the RAID set.

You can use Disk Utility to set up a RAID set. There are two types of RAID sets and one additional disk option available in Disk Utility:

- **A striped RAID set (RAID 0)** splits files across the disks in the set. A striped RAID set improves the performance of your software because it can read and write on all disks in the set at the same time. You might use a striped RAID set if you are working with large files, such as digital video.
- **A mirrored RAID set (RAID 1)** duplicates files across the disks in the set. Because this scheme maintains copies of the files, it provides a continuous backup of them. In addition, it can help keep data available if a disk in the set fails. Mirroring is recommended if shared files or applications must be accessed frequently.

  You can set up RAID mirroring after installing Mac OS X Server if you install on a disk that isn't partitioned. To prevent data loss, set up RAID mirroring as soon as possible.
- **A concatenated disk set** lets you use several disks as a single volume. This is not a true RAID set and offers no redundancy or performance increase.

You can combine RAID sets to combine their benefits. For example, you can create a RAID set that combines the fast disk access of a striped RAID set and the data protection of a mirrored RAID set. To do this, create two RAID sets of one type and then create a RAID set of another type, using the first two RAID sets as the disks.

The RAID sets you combine must be created with Disk Utility or `diskutil` in Mac OS X v10.4 or later.

You cannot mix the method of partitioning used on the disks in a RAID set. (The PPC platform is APMFormat and the Intel platform is GPTFormat.)

Mac Pro desktop computers and Intel-based Xserves can start from a software RAID volume. Some Intel-based Macs do not support starting up from software RAID volumes. If you start Intel-based Macs from a software RAID volume, the computer might start up with a flashing question mark.

The following computers do not support starting up from software RAID volumes:

- iMac (Early 2006)
- Mac mini (Early 2006)

If you need more sophisticated RAID support, consider a hardware RAID.

Creating a RAID Set Using Disk Utility

You can use the Installer to open Disk Utility and then use Disk Utility to create the RAID set from available disks. Creating a RAID set erases the contents of the disks involved, so it isn't necessary to erase the disks before creating the RAID set.

RAID set volumes can be Mac OS Extended format, Mac OS Extended (Journaled) format, Mac OS Extended format (Case-Sensitive) format, Mac OS Extended (Journaled, Case-Sensitive) format, and MS-DOS FAT format. For more information about volume formats, see "Preparing Disks for Installing Mac OS X Server" on page 92.

You cannot create a RAID set from the startup disk.

To create a RAID set using Disk Utility:

1. Launch Disk Utility.

   If you are in the Installer, Disk Utility is available from the Utilities menu; otherwise, launch the application from /Applications/Utilities/Disk Utility.

2. Select the disk to be part of the RAID set.

   You can't select your startup disk.

   When creating RAID sets or adding disks, specify the disk instead of a partition.

3. Click RAID.

4. Choose your RAID set type.

5 Drag the disks to the window.

6 Follow the instructions in the window to set parameters.

7 Click Create.

You can find instructions for partitioning the hard disk into multiple volumes, creating a RAID set, and erasing the target disk or partition by viewing Disk Utility Help. To view Disk Utility Help, open Disk Utility on another Mac computer with Mac OS X v10.6 and choose Help > Disk Utility Help.

From the command line

You can use the diskutil command-line tool to create a RAID set. Normally, you would use a remote shell (SSH) to log in to the newly started computer to use this method.

You can use `diskutil` to can create a RAID volume that is Mac OS Extended format, Mac OS Extended (Journaled) format, Mac OS Extended format (Case-Sensitive) format, Mac OS Extended (Journaled, Case-Sensitive) format, or MS-DOS FAT format. However keep in mind the following:

- You cannot create a RAID from the startup disk.
- When creating RAID sets or adding disks, specify the entire disk instead of a partition on that disk.
- All potentially destructive diskutil operations must be done with superuser or root privileges.

For complete command syntax for diskutil, consult the tool's man page.

Use command-line arguments that apply to your specific needs. The following command is a sample, which creates a single mirrored RAID set (RAID 1) from the first two disks installed in the computer (disk0 and disk1), with the resulting RAID volume called MirrorData.

The basic syntax is:

```
diskutil createRAID mirror setName format device device ...
```

So the command is:

```
diskutil createRAID mirror MirrorData JournaledHFS+ disk0 disk1
```

Erasing a Disk or Partition

You have several options for erasing a disk, depending on your preferred tools and your computing environment:

- **Erasing a disk using Disk Utility:** You can use the Installer to open Disk Utility and then use it to erase the target volume or another volume. You can erase the target and all other volumes using the Mac OS Extended format or Mac OS Extended (Journaled) format. You can erase other volumes using those formats, as well as Mac OS Extended format (Case-Sensitive) format, or Mac OS Extended (Journaled, Case-Sensitive) format.

  You can find instructions for partitioning the hard disk into multiple volumes, creating a RAID set, and erasing the target disk or partition by viewing Disk Utility Help. To view Disk Utility Help, open Disk Utility on another Mac computer with Mac OS X v10.6 and choose Help > Disk Utility Help.

- **Erasing a disk using the command line:** You can use the command line to erase disks using the tool diskutil. Erasing a disk using diskutil deletes all volume partitions. The command to erase a complete disk is:

  ```
  diskutil eraseDisk format name [OS9Drivers | APMFormat | MBRFormat |
     GPTFormat] device
  ```

  For example:

  ```
  diskutil eraseDisk JournaledHFS+ MacProHD GPTFormat disk0
  ```

  There is also an option to securely delete data by overwriting the disk with random data multiple times. For more details, see diskutil's man page.

  To erase a single volume on a disk, a slightly different command is used:

  ```
  diskutil eraseVolume format name device
  ```

  For example:

  ```
  diskutil eraseVolume JournaledHFS+ UntitledPartition /Volumes/
     OriginalPartition
  ```

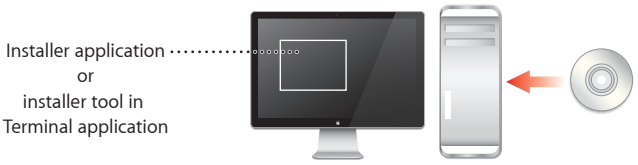
  For complete command syntax for `diskutil`, consult the tool's man page.

Installing Server Software Interactively

You can use the installation disc to install server software interactively on a local server, on a remote server, or on a computer with Mac OS X installed.

Installing Locally from the Installation Disc

You can install Mac OS X Server directly onto a computer with a display, a keyboard, and a DVD drive attached, as shown in the following illustration:



If you have an Install DVD, the optical drive must be able to read DVD discs.

You can also install directly onto a computer that lacks a display, keyboard, and optical drive capable of reading your installation disc. In this case, you start the target computer in target disk mode and connect it to an Intel-based administrator computer using a FireWire cable.

You use the administrator computer to install the server software on the target computer's disk or partition, which appears as a disk icon on the administrator computer.

To install server software locally:

1. Start up the target computer using the Install DVD, installer partition, or NetInstall disk.

   For startup options, see "About Starting Up for Installation" on page 84.

2. When the Installer opens, if you want to perform a clean installation, use the Utilities menu to open Disk Utility to prepare the target disk or partition before proceeding.

   If you have not prepared your disk for installation, do so now with Disk Utility. For more instructions on preparing your disk for installation, see "Preparing Disks for Installing Mac OS X Server" on page 92.

3. Proceed through the Installer panes by following the onscreen instructions.

4. When the Install Mac OS X Server pane appears, select a target disk or volume (partition) and make sure it's in the expected state.

   If you want to customize what software is included in the installation, click Options in the Select a Destination pane.

5. Proceed through the Installer panes by following the onscreen instructions.

   If you're using an administrator computer to install onto a server in target disk mode and connected using a FireWire cable, complete the following:

   a. Quit Server Assistant when it starts on the administrator computer.

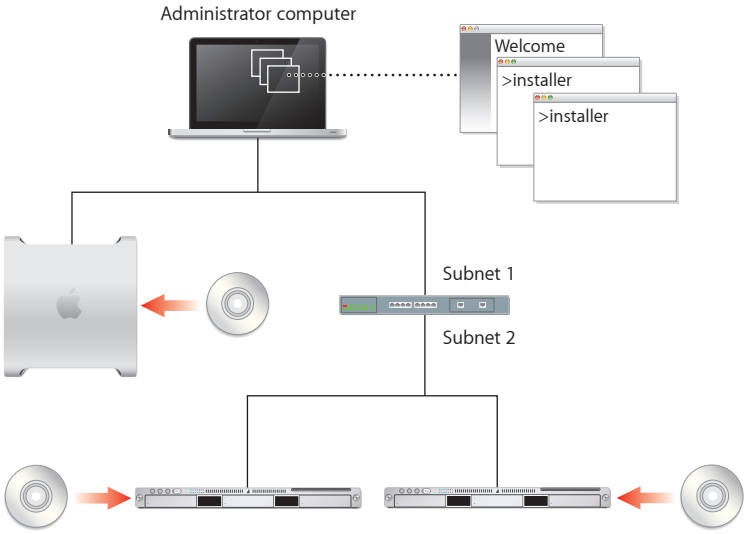
   b. Shut down the administrator computer and the server.

   c. Start up the administrator computer and the server normally (not in target disk mode).

After installation is complete, the target server restarts and you can perform initial server setup. Chapter 6, "Initial Server Setup," on page 108 describes how.

Installing Remotely with Server Assistant

To install Mac OS X Server on a remote server from the server Install DVD, installation partition, or NetInstall disk, you need an administrator computer from which to use Server Assistant to manage the installation:



After the computer starts up from the Install Disk, you can control and manage the server from an administration computer.

Important: If you have administrative applications and tools from Mac OS X Server v10.5 or earlier, do not use them with Mac OS X Server v10.6.

To use the Installer user interface, use VNC to view and interact with the remote installer. For more information, see "Installing Remotely with Screen Sharing and VNC" on page 102.

You don't need to be an administrator on the local computer to use Server Assistant.

To install on a remote server by using Server Assistant:

1. Start up the target computer using the Install DVD, installer partition, or NetInstall disk.

   If you need more information on your startup options, see "About Starting Up for Installation" on page 84.

2. After the target computer starts, launch Server Admin in the /Applications/Server/ folder on the administrator computer.

3 Select the target server from the list of servers waiting for installation.

If neither the target server nor the list appear, make sure the target server is on the same local subnet as the administrator computer.

4 If the target computer is not on the same local subnet as the administrator computer, add the server manually.

a Choose Install Remote Server from the Server menu of Server Admin.

b Enter the IP address or DNS name of the target server.

If you do not know the IP address or DNS name of the target server, you must identify it first. For more information about this process, see "Identifying Remote Servers When Installing Mac OS X Server" on page 90.

5 For the password, enter the default password for installation.

This is usually the first eight characters of the server's built-in hardware serial number.

For more information about this password, see "About Server Serial Numbers for Default Installation Passwords" on page 90.

6 Proceed by following the onscreen instructions.

7 When the Volumes pane appears, select a target disk or volume (partition), make sure it's in the expected state and click Continue.

8 Proceed by following the onscreen instructions.

While installation proceeds, you can open another Server Assistant window to install server software on other computers. Choose Server > Install Remote Server to do so.

After installation is complete, the target server restarts and you can perform initial server setup. Chapter 6, "Initial Server Setup" describes how.

Installing Remotely with Screen Sharing and VNC

If you're using an installation disc for Mac OS X Server v10.6 or later, you can control installation from another computer using a VNC viewer, like Mac OS X's built-in Screen Sharing, open source VNC viewer software, or Apple Remote Desktop. This allows you to remotely control preparation of the target disk or partition before beginning installation.

You can partition the hard disk into multiple volumes, create a RAID set, or erase the target disk or partition.

The process for remotely installing with VNC is the same as installing locally at the keyboard and monitor, except that you must first connect to the VNC server on the target computer with a VNC client, like Apple Remote Desktop.

For detailed instructions for connecting to a computer running from an Install DVD, see "Remotely Accessing the Install DVD" on page 88.

Important: If you perform an upgrade, make sure that saved setup data won't be detected and used by the server. If saved setup data is used, the server settings are not compatible with the saved settings and can cause unintended consequences. For more information, see "How a Server Searches for Saved Setup Data Files" on page 118.

To install on a remote server by using Screen Sharing and VNC:

1. After the target computer has started from the server Install DVD, installation partition, or NetInstall disk, access the server using Screen Sharing or VNC client software on the administrator computer.
2. After the connection begins, proceed as though you were using a keyboard and mouse at the server.
3. Choose the language you want the server to use and click Continue.
4. When the Installer opens, if you want to perform a clean installation, use the Utilities menu to open Disk Utility to prepare the target disk or partition before proceeding.

   If you have not prepared your disk for installation, do so now with Disk Utility. For more instructions on preparing your disk for installation, see "Preparing Disks for Installing Mac OS X Server" on page 92.
5. Proceed through the Installer panes by following the onscreen instructions.
6. When the Install Mac OS X Server pane appears, select a target disk or volume (partition) and make sure it's in the expected state.

   To customize what software is included in the installation, click Options in the Select a Destination pane.
7. Proceed through the Installer panes by following the onscreen instructions.

After installation is complete, the target server restarts and you can perform initial server setup. Chapter 6, "Initial Server Setup," on page 108 describes how.

Changing a Remote Computer's Startup Disk

Sometimes you may need to explicitly set a remote computer's startup disk. You can do this via the command line using the `bless` command.

The tool Apple Remote Desktop can change a computer's startup disk. Apple Remote Desktop is not included with Mac OS X Server, and is available separately for purchase.

To change a remote computer's startup disk

```
# Method 1
sudo bless --folder "/Volumes/<disk>/System/Library/CoreServices"
     --setBoot
```

```
sudo shutdown -r now
# Method 2
sudo systemsetup -liststartupdisks
sudo systemsetup -setstartupdisk <path to disk root>
```

Using the installer Command-Line Tool to Install Server Software

You use the `installer` tool to install server software on a local or remote computer from the command line. For information about `installer`, see the `installer` man page.

These instructions assume you started up the computer using the Install DVD, installer partition, or NetInstall disk. If not, see "About Starting Up for Installation" on page 84.

To use installer to install server software:

1. Start a command-line session with the target server by choosing from the following:
   - **Installing a local server:** When the Installer opens, choose Utilities > Open Terminal to open the Terminal application. Use `su root`.
   - **Installing a remote server:** Follow the instructions on "Remotely Accessing the Install DVD" on page 88 for SSH connections. Use `ssh root@<ip address>`.

     If you don't know the IP address or DNS name of the server, see "Identifying Remote Servers When Installing Mac OS X Server" on page 90.
2. For the password, enter the default password for installation.

   This is usually the first eight characters of the server's built-in hardware serial number.

   For more information about this password, see "About Server Serial Numbers for Default Installation Passwords" on page 90.
3. Identify the target server volume where you want to install the server software.

   To list the volumes available for server software installation from the installation disc, type:

   ```
   /usr/sbin/installer -volinfo -pkg /System/Installation/Packages/
        OSInstall.mpkg
   ```

   You can also identify a NetInstall image you've created and mounted:

   ```
   /usr/sbin/installer -volinfo -pkg /Volumes/<name_of_install_image>/
        System/Installation/Packages/OSInstall.mpkg
   ```

   The list displayed reflects your particular environment, but here's an example showing three available volumes:

   ```
   /Volumes/Mount 01
   /Volumes/Mount1
   /Volumes/Mount02
   ```

4 If you haven't already done so, prepare the disks for installation.

For more information about preparing the disks for installation, see "Preparing Disks for Installing Mac OS X Server" on page 92.

If the target volume has the latest Mac OS X Server v10.5 or 10.4.11 installed, when you run `installer` it upgrades the server to v10.6 and preserves user files.

If you're not upgrading but performing a clean installation, back up the user and settings files you want to preserve, then use `diskutil` to erase the volume and format it to enable journaling:

```
/usr/sbin/diskutil eraseVolume HFS+ "Mount 01" "/Volumes/Mount 01"
/usr/sbin/diskutil enableJournal "/Volumes/Mount 01"
```

You can also use `diskutil` to partition the volume and to set up mirroring. For more information about the command, see the `diskutil` man page.

Important: Don't store data on the hard disk or hard disk partition where the operating system is installed. With this approach, you won't risk losing data if you need to reinstall or upgrade system software. If you must store additional software or data on the system partition, consider mirroring the drive.

5 Install the operating system on the target volume.

For example, to use Mount 01 in the example in step 4 to install from a server installation disc, enter:

```
/usr/sbin/installer -verboseR -lang en -pkg /System/Installation/
     Packages/OSInstall.mpkg -target "/Volumes/Mount 01"
```

If you're using a NetInstall image, the command identifies them as step 3 shows.

When you enter the -lang parameter, use one of the following values: en (for English), de (for German), fr (for French), or ja (for Japanese).

During installation, progress information appears. While installation proceeds, you can open another Terminal window to install server software on another computer.

6 When installation from the disc is complete, restart the server by entering:

```
/sbin/reboot
```

or

```
/sbin/shutdown -r
```

Server Assistant opens on the target computer when installation is complete. You can now set up the server. For more information, see Chapter 6, "Initial Server Setup."

Installing Multiple Servers

Most Efficient Methods of Installation

The most efficient method of installation would be completely automated. Opening the Terminal application and using the `installer` tool to initiate each server software installation doesn't accomplish this efficiently.

However, scripting the command-line tool (using known values for server IP addresses, for example) to automate multiple simultaneous installations can be very efficient.

To completely automate server installation, you must script the `installer` tool and have a high measure of control over the network infrastructure.

For example, to have known IP addresses and the appropriate hardware serial numbers included in your script, you cannot rely on the randomly assigned IP addresses. You can use DHCP assigned static addresses to remove that uncertainty and ease your scripting considerations.

Additionally, you can create a NetInstall server on the target servers' local network that can install an operating system. If you combine this with saved auto setup files, you can easily automate installation of multiple computers without much human interaction.

The methods, scripting languages, and possibilities are too many to list in this guide.

More Interactive Methods of Installation

When running Server Assistant from an administration computer to install on multiple machines, you still have to open a connection to each server one at a time.

You can use VNC viewer software or the `installer` tool to initiate multiple server software installations.

After using a VNC viewer to control installation of Mac OS X Server v10.6 on one remote computer, you can use the VNC viewer to open a connection to another remote computer and control installation on it. Because this involves interacting with each server individually, it is a less efficient method of installing on multiple servers.

Upgrading a Computer from Mac OS X to Mac OS X Server

This is not supported in Mac OS X Server v10.6. Perform a clean installation instead.

How to Keep Current

After you've set up your server, you'll want to update it when Apple releases server software updates.

There are several ways to access update releases of Mac OS X Server:

- In Server Admin, select a server in the Servers list, then click the Server Updates button.

  Note: The Server Updates button refers only to updates for the server's operating system software from Apple. Third-party software is not updated when used. Additionally, it does not control software updates hosted in the Software Update service.

- Use the Software Update pane of System Preferences, if you are logged locally into the server.
- Use the `softwareupdate` command-line tool.
- Download a disk image of the software update from:

  www.apple.com/support/downloads

Initial Server Setup

6

Basic characteristics of your Mac OS X Server are established during server setup. The server can operate in three different configurations: advanced, standard, and workgroup.

After installing server software, the next task is to set up the server. There are several ways to set up a server:

- Set up servers interactively.
- Automate the setup by using setup data you've saved in a file or on a server available to the newly installed server.

Information You Need

To understand and record information for each server you want to set up, see the *Installation & Setup Worksheet* on the Install DVD or the *Administration Tools* CD. The following chapter provides supplemental explanations for some items on the worksheet.

When you upgrade from the latest Mac OS X Server v10.5 or v10.4.11, Server Assistant displays existing server settings, but you can change them. Use the *Installation & Setup Worksheet* to record settings you want the v10.6 server to use.

Postponing Server Setup Following Installation

Server Assistant opens on a server that hasn't been set up and waits for you to begin the setup process. To set up the server later, you can postpone the setup process by using the server's keyboard, mouse, and display.

To postpone setting up Mac OS X Server:

- In Server Assistant, press Command-Q on the server's keyboard and then click Shut Down.

When you restart the server, Server Assistant opens again.

If you're setting up a server without a keyboard or display, you can enter the following in the Terminal application to shut down the server remotely:

```
sudo shutdown now
```

Connecting to the Network During Initial Server Setup

Before setting it up for the first time, try to place a server in its final network location (subnet). If you're concerned about preventing unauthorized or premature access during setup, you can set up a firewall to protect the server while you're finalizing its configuration.

If you can't avoid moving a server after initial setup, you must change settings that are sensitive to network location before it can be used. For example, the server's IP address and DNS name, stored in directories and configuration files on the server, must be updated. For more information, see "Changing the Server's DNS Name After Setup" on page 144.

Configuring Servers with Multiple Ethernet Ports

Your server has a built-in Ethernet port and might have additional Ethernet ports built in or added on.

When you're using Server Assistant to interactively set up servers, all of a server's available Ethernet ports are listed and you select them to activate and configure. When you work in Server Assistant's offline mode, you click an Add button to create a list of ports to configure.

If you enable more than one port, you specify the order for the ports to be used by the server when routing traffic to the network. Although the server receives network traffic on any active port, network traffic initiated by the server is routed through the first active port.

For a description of port configuration attributes, see the *Installation & Setup Worksheet* from the Install DVD or the *Administration Tools* CD.

About Settings Established During Initial Server Setup

During server setup, the following basic server settings are established:

- The language to use for server administration and the computer keyboard layout is defined.
- The server software serial number is set.
- A time zone is specified, and network time service is set up.
- A server administrator user is defined and the administrator's home folder is created.

- Default SSH and Apple Remote Desktop state is enabled.
- Network interfaces (ports) are configured.

  TCP/IP and Ethernet settings are defined for each port you want to activate.
- Network names are defined.

  The primary DNS name, computer name are defined by the administrator, and local hostname is derived from the computer name.

  For more information about names of Mac OS X Server, see "Understanding Mac OS X Server Names."
- Basic Directory information is set up. (Optional)

  The server is set up as an Open Directory Master, or it is set to obtain directory information from another a directory service, or the directory setup can be deferred until first login.

  For more information, see "Specifying Initial Open Directory Usage."
- Some services are chosen and configured.

  For a list of which services are enabled at startup, see "Understanding Server Configuration Methods."

If you're upgrading, the current settings are maintained through the setup process. Other settings, such as share points you've defined and services you've configured, are also preserved. For a complete description of what's upgraded and actions, see the online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

You can perform initial server setup only once without reinstalling a server. To change settings established during setup, you use Server Admin, Workgroup Manager, or Directory Utility (in /System/Library/CoreServices/) to manage directory settings.

Specifying Initial Open Directory Usage

During setup of Mac OS X Server v10.6, you specify how the server stores and accesses user accounts and other directory information. You choose whether the server connects to a directory system or works as a standalone server.

If you're setting up multiple servers and one or more will host a shared directory, set up those servers before setting up servers that will use those shared directories.

When you set up a server initially, you specify its directory services configuration. Choices are:

- **Create Users and Groups**

  This setting makes the server an Open Directory Master or uses the server's local users and groups for authentication.

- **Import Users and Groups**

  This setting connects the server to an existing Open Directory or Active Directory system, importing the users and groups from an existing directory system.

  You can import Open Directory users or Active Directory users. You must provide a directory administrator name and password.

- **Configure Manually**

  This setting used to set up the server to obtain directory information from a shared directory domain that's been set up on another server. You can connect to Open Directory servers or Active Directory servers.

  You can also defer directory configuration during setup by declining to specify a connection in the assistant.

After setup, use Server Admin or the Login Options section of Account preferences of System Preferences to refine the server's directory configuration, if necessary. You can create or change a connection to a directory system by using Login Options. You can use Accounts preferences to set up connections to multiple directory servers, including Open Directory and Active Directory. You can make the server an Open Directory master or replica by using Server Admin to change the server's Open Directory service settings.

From Accounts preferences, you can open Directory Utility if you need to set up connections to other kinds of directory servers or specify the search policy. Directory Utility lets you set up connections to other non-Apple directory systems and specify a search policy (the order in which the server should search through the domains).

For information about changing directory services, see the online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

Note: If you connect Mac OS X Server v10.6 to a directory domain of Mac OS X Server v10.2 or earlier, users defined in the older directory domain cannot be authenticated with the MS-CHAPv2 method. This method may be required to securely authenticate users for the VPN service of Mac OS X Server v10.6. Open Directory in Mac OS X Server v10.6 supports MSCHAPv2 authentication, but Password Server in Mac OS X Server v10.2 doesn't support MS-CHAPv2.

Not Changing Directory Usage When Upgrading

When you are setting up a server that you're upgrading to v10.6 from the latest v10.5 or 10.4.11 and you want the server to use the same directory setup it's been using, choose "Configure Manually" (but decline to provide directory service settings) in Server Assistant.

Even if you want to change the server's directory setup, selecting "Configure Manually" is the safest option, especially if you're considering changing a server's shared directory configuration.

Changing from hosting a directory to using another server's shared directory or vice versa, or migrating a shared NetInfo domain to LDAP are examples of directory usage changes you should make *after* server setup to preserve access to directory information about your network.

For information about directory usage options available to you and how to use Directory Utility (in /System/Library/CoreServices/) and Server Admin to make directory changes, see the online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

Setting Up a Server as a Standalone Server

A standalone server stores and accesses account information in its local directory domain. The standalone server uses its local users and groups to authenticate clients for its file, mail, and other services. Other servers and client computers can't access the standalone server's local directory domain or authenticate their own users with it.

Users and groups are managed in the Accounts pane of System Preferences.

When a user attempts to log in to the server or use a service that requires authentication, the server authenticates the user by consulting the local database. If the user has an account on the system and supplies the relevant password, authentication succeeds.

To get this configuration, you choose Create Users and Groups from the assistant, but decline to create an Open Directory Master.

Binding a Server to Multiple Directory Servers

Automatic server setup allows you to bind to multiple servers. You need to save setup data, then you have to modify the plist file by hand. In the saved setup data, you will find the "directoryServers" key in the plist file, and it's an array. You add items (or in this case directory servers) to the array. The server binds to all of the servers listed in the array.

For more information on making saved server setup data, see "Using Automatic Server Setup" on page 115 and "Creating and Saving Setup Data" on page 116.

You can also bind to multiple directories interactively after initial server setup by using the Login Options section of Accounts Preferences.

For instructions, see p. 72 of *Getting Started*; repeat steps 3 and 4 to connect to additional directory servers. To set up advanced directory server connections, you would click Open Directory Utility in step 2.

To interactively connect to an additional directory server:

1. Open the Accounts pane of System Preferences on your server.
2. Click Login Options and then click Open Directory Utility.
3. Click the Add (+) button, and then choose the directory server from the pop-up menu or enter the directory server's DNS name or IP address.
4. If the dialog expands to show Client Computer ID, User Name, and Password fields, enter the name and password of a user account on the directory server.

   For an Open Directory server, you can enter the name and password of a standard user account; you don't need to use a directory administrator account. If the dialog says you can leave the name and password fields blank, you can connect without authentication, although this is less secure.

   For an Active Directory server, you can enter the name and password of an Active Directory administrator account or a standard user account that has the "Add workstations to domain" privilege.

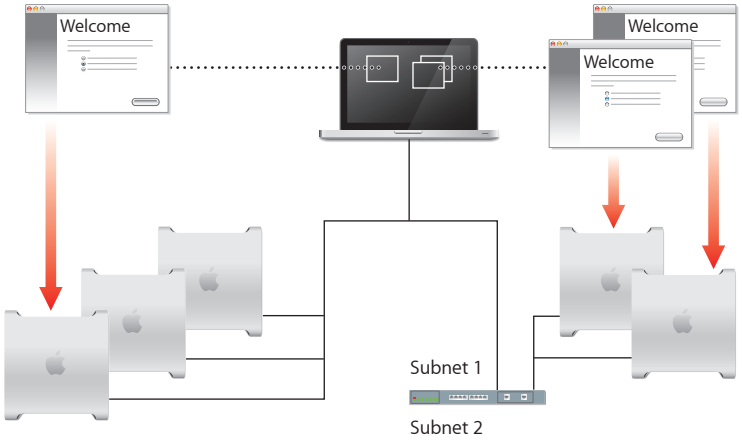
Setting up Servers Interactively

The simplest way to set up a few servers is to use Server Admin's guided interview process after establishing a connection with each server in turn. If you have only a few servers to set up, the interactive approach is useful. You can use the interactive approach to set up a local server, a remote server, or several remote servers.

Server Assistant will display the Network pane separately for each server you're setting up remotely, even if you're setting up a list of servers. You then enter all network settings manually, if necessary. You provide server setup data interactively, then initiate setup immediately.

Set up DNS and DHCP (if used for static IP address allocation) for your servers before setup. While not strictly mandatory, doing so will simplify the setup and post-setup processes. For example, if the server's DNS name is already associated to an IP address (with reverse lookup), and the IP address will be allocated to the server's MAC address by a DHCP server on the network, you will already have needed information for setup without doing the additional manual configuration work during and after setup.

The following illustration shows target servers on the same subnet as the administrator computer in one scenario and target servers on a different subnet in the other scenario. Both setup scenarios can be used to set up servers on the same and different subnets.



If a target server is on a different subnet, you must supply its IP address or DNS name. Servers on the same subnet are listed by Server Assistant, so you select servers from the list.

After server software is installed on a server, you can use the interactive approach to set it up remotely from an administrator computer that can connect to the target server.

To set up servers interactively:

1. Make sure the DHCP or DNS servers you specify for the server you're setting up to use are running.
2. Make sure the target servers have been newly installed and are waiting for setup.
3. Fill out the *Installation & Setup Worksheet* from the Install DVD or *Administration Tools* CD.

   After installation, Server Assistant opens.
4. If you are installing on a remote server, open Server Admin, select "Ready for Setup" in the list on the left, and then select the servers you want to set up.

   After you click Set Up, Server Assistant opens and lists all the servers you selected in Server Admin.

   If instead you choose Server > Set Up Remote Server, Server Assistant doesn't list any servers in the Server pane, and you have to add them one by one by clicking Add.
5. Select the target servers from the configuration list.

If the computer you want to configure doesn't appear in the list, you can add it manually by clicking the Add button and supplying the requested information.

6 Remove computers from the configuration list that you don't want to set up by selecting them and clicking the Remove button.

7 Authenticate to the target server.

You need authenticate for each listed server by selecting it, clicking Authenticate, and entering the server's password. The password is usually the first eight characters of the hardware serial number. For an upgraded server, it's the password of the root user. To figure out what password to use, see "About Server Serial Numbers for Default Installation Passwords" on page 90.

8 Click Continue, and continue to follow the onscreen instructions.

9 Enter the setup data you've recorded on the worksheet as you move through the Assistant's panes, following the onscreen instructions.

If you're setting up multiple servers, you don't need to manage each setup in a separate Server Assistant window. Server Assistant steps you through the necessary panes for each server on the list.

After you enter setup data, Server Assistant displays a summary of the data.

10 Review the setup data you entered and, if necessary, click Go Back to change it.

11 To save the setup data as a text file or in a form you can use for automatic server setup (a saved setup file), click Details; then click Save Setup Profile.

To encrypt a configuration file, select Passphrase Encryption from the Encryption pop-up menu, and finally enter the encryption passphrase. You must supply the passphrase before a target server can use an encrypted setup file.

To see how this information can be used, see "Using Automatic Server Setup" on page 115.

12 To initiate setup, click Set Up.

When server setup is complete, you can log in as the server administrator user created during setup to configure services as needed.

13 See the Mac OS X Server Next Steps document that's placed on the server desktop during setup.

For more information about the Next Steps document, see "After Setting Up a Server" on p. 69 of *Getting Started*.

Using Automatic Server Setup

When you have more than a few servers to set up, consider using automatic server setup. This approach also provides a way to preserve setup data so it can be reused if you need to reinstall server software.

The automatic approach is useful when you:

- Have more than a few servers to set up
- Want to prepare for setting up servers that aren't yet available
- Want to save setup data for backup purposes
- Need to reinstall servers frequently

You can keep backup copies of setup data files on a network file server. Alternatively, you can store setup data files in a local partition that won't be erased when you reinstall server software.

To use automatic server setup, you use Server Assistant to specify setup data for each computer or batch of computers.

Finally, you provide that setup data to the target servers. You can provide the data using a variety of methods, like storing files on the hard disk or removable storage. By default, saved setup data is encrypted for extra security.

When a server starts up for the first time, it searches for automatic setup data to configure itself before it starts the interactive Setup Assistant.

Automatic server setup requires two main steps:

Step 1: Create the setup data files. The following sections can help you create setup data files.

- "Creating and Saving Setup Data" on page 116
- "Using Encryption with Setup Data Files" on page 118

Step 2: Make the setup data files available to a freshly installed server. The following sections can help you make the data available to the servers:

- "How a Server Searches for Saved Setup Data Files" on page 118
- "Setting Up Servers Automatically Using Data Saved in a File" on page 119

Creating and Saving Setup Data

When you want to work with saved setup data, determine a strategy for naming, encrypting, storing, and serving the data.

The best way to create setup data is to use Server Admin to launch Server Assistant, which lets you work with setup data without connecting to specific servers. You specify setup data and then save it in a file. Target servers where Mac OS X Server v10.6 software has been installed detect the presence of the saved setup information and use it to set themselves up.

You can define generic setup data that can be used to set up *any* server. For example, you can define generic setup data for a server that's on order, or to configure 50 Xserve computers you want to be identically configured. You can also save setup data that's tailored for a server.

Important: When you perform an upgrade, make sure that saved setup data won't be detected and used by the server. If saved setup data is used, existing server settings are overwritten by the saved settings.

If you intend to create a generic setup file because you want to use the file to set up more than one server, don't specify network names (computer name and local hostname) and make sure that each network interface (port) is set to be configured using DHCP or BootP.

To create a setup data file:

1. Fill out the *Installation & Setup Worksheet* from the Install DVD or *Administration Tools* CD.
2. On an administrator computer, open Server Admin.
3. In the Server menu, select "Create Auto Server Setup File."

   The Server Assistant launches.
4. Enter the setup data as you move through the Assistant panes, following the onscreen instructions.
5. After entering setup information, choose to save the file as encrypted or unencrypted.

   If you encrypt the file, provide a passphrase. You must supply the passphrase before a target server can use an encrypted setup file. For more information, see "Using Encryption with Setup Data Files" on page 118.

   To use an encrypted setup file in an automated setup, see "Setting Up Servers Automatically Using Data Saved in a File" on page 119.
6. To restrict the setup file to certain computers, select "Restrict for use with certain computers" in the Save Configuration pane.

   You can restrict the setup files by:
   - Serial number
   - MAC address
   - IP address
   - DNS name
7. Click Save.

   When you click Save, you can give the profile any filename you like as long as it ends with *.plist*.

Using Encryption with Setup Data Files

Saved setup data can be encrypted for extra security. Before a server sets itself up using encrypted setup data, it must have access to the passphrase used when the data was encrypted.

For interactive setup, the passphrase is entered using Server Assistant during setup.

If you want to store the password for non-interactive setup, the file containing the passphrase file should be named the same as the saved setup data. Put the text file containing the passphrase in the same folder as the corresponding auto setup profile but with a ".pass" extension.

How a Server Searches for Saved Setup Data Files

A new server sets itself up using saved setup data it finds while using the following search sequence. When the server finds saved setup data that matches the criteria described, it stops searching and uses the data to set itself up.

- It looks on all volumes for a folder at the root named "Auto Server Setup," starting at the start volume and then searching the rest alphabetically.

  Mounted share points are also searched, so any automounted or manually mounted share point can contain the auto setup files. For example, you can use `automount` or `mount_afp` via the command-line to mount a share point while the server is waiting for setup.

- It searches through "Auto Server Setup" folders, looking for a file with the extension ".plist". There is no naming convention for the plist.

  The plist file must contain the key "VersionNumber" with value "4" or it will be ignored.

- It evaluates all profile plists found to evaluate the most specific match.

  Most-specific to least-specific criteria are:

  - Hardware serial number
  - MAC address
  - IP address
  - DNS name (fully qualified)
  - Computer name
  - None of the above

If a saved setup data profile contains multiple network connection services, Server Assistant tries to match hardware (MAC) addresses. Failing that, it tries to match interface (BSD port) names. If a profile has multiple conditions, it applies to a computer that satisfies any of them.

If setup data is encrypted, the server needs the correct passphrase before setting itself up. You can use Server Assistant to supply the passphrase interactively, or you can supply the passphrase in a file containing the passphrase in the same folder as the corresponding auto setup profile but with a ."pass" extension.

Important: When you perform an upgrade, make sure that saved setup data won't be detected and used by the server you're upgrading. If saved setup data is used, existing server settings are overwritten by the saved settings.

Setting Up Servers Automatically Using Data Saved in a File

After you install server software, you can set up the server automatically using data saved in a file.

To have the server configure itself without further input, place the previously generated auto setup data file in a location where target servers can detect it.

To reuse saved setup data after reinstalling a server, store the server's setup files on a different local partition that isn't erased when you reinstall the server. The setup files are detected and reused after each reinstallation.

Important: Saved setup files cannot be applied *after* a server has restarted after installation and is awaiting setup. Automatic setup data needs to be in place before a server begins setup.

If you do not have an existing local partition where the saved setup file can be stored during installation, you need to copy the setup file to the target server after installation and then restart the target server. This allows the server to search for the setup data when it starts up.

For more information on where the server looks for setup data, see "How a Server Searches for Saved Setup Data Files" on page 118.

If you have not previously created saved setup data, see "Creating and Saving Setup Data" on page 116.

If the setup data is encrypted, make the passphrase available to target servers. For more information, see "Using Encryption with Setup Data Files" on page 118.

To use setup data from a file remotely:

1 Create the folder for the setup file on the remote server.

   a Connect to the remote server.

   ```
   ssh root@<server address>
   ```

   b Create the saved setup folder on the remote server.

   ```
   mkdir /Auto\ Server\ Setup
   ```

2 Copy the saved setup file from the administrator computer to the remote target computer.

   The password is the same for ssh connections during installation. For more information abotu passwords, see "About Server Serial Numbers for Default Installation Passwords" on page 90.

   ```
   scp <local setup file> root@<server address>:"/Auto\ Server\ Setup"
   ```

3 Restart the server using the command-line tool `shutdown`.

   a Connect to the remote server.

   ```
   ssh root@<server address>
   ```

   b Restart the remote server.

   ```
   shutdown -r now
   ```

Setting a Mac OS X Server Serial Number from the Command Line

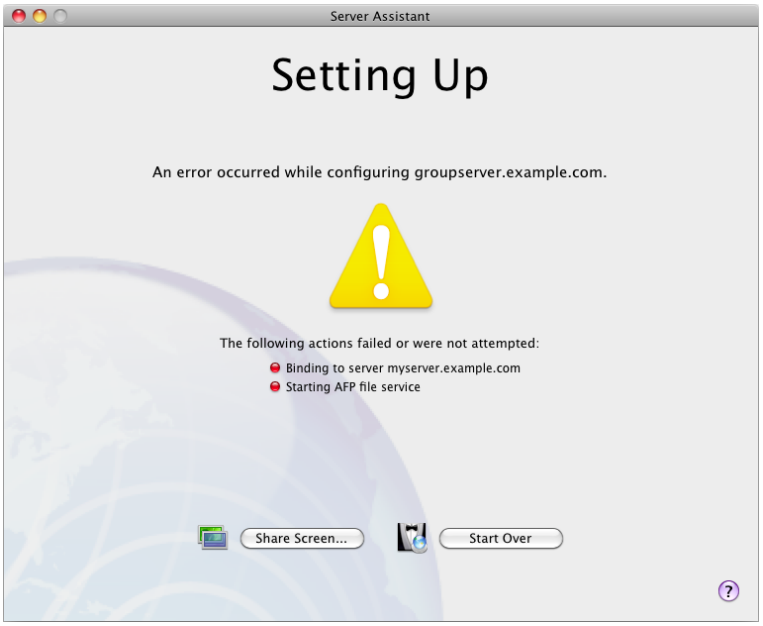
After an automatic setup, you might need to set a specific Mac OS X serial number for your server. For example, you might have completed an automatic setup with a generic setup data profile and now you need to put individual serial numbers to their respective servers.

To set the server serial number

```
sudo serversetup -setServerSerialNumber <serialnumber-dash-separated>
     [<name> <organization>]
```

Handling Setup Errors

When a server encounters a setup problem, Server Assistant shows a description of the setup error, and gives some opportunity to either fix it or try again.



If you are setting up the target server remotely, you are given the option to share its screen and interact via the Server Assistant.

If setup fails because a passphrase file can't be found when using setup data saved in a file, you can:

- Use Server Assistant (if installing locally) or Screen Sharing (if installing remotely) to supply a passphrase interactively.
- Supply the passphrase in a text file and restart setup.

  For information on how to supply the passphrase, see "Using Encryption with Setup Data Files" on page 118

If a remote server setup fails for any other reason, repeat initial setup before trying to reinstall the server software.

If a local server setup fails, restart the computer, rerun Server Assistant, and reinitiate setup, or reinstall the server software.

Setting Up Services

After installation and initial startup, the first time you open Server Admin, you see any services that were configured during server setup listed underneath the server's name in the server list. If no services were configured during server setup, Server Admin prompts you to select the services you want to configure on the server.

You add services for administration and configure services using Server Admin and add users and groups using Workgroup Manager.

Before you can enable or configure and service in Server Admin, it must be added to the administered service list.

The following sections survey initial setup of individual services and tell you where to find instructions for tailoring services to support your needs.

Adding Services to the Server View

Before you can set up services, you must add the service to the server view in Server Admin. For example, by default, no services can be seen for your server. As you select services to administer, configuration panes become accessible in a list underneath your computer name.

The first time you launch Server Admin and connect to a new server, you are prompted to select the services you want to set up and configure on that server. When you select services from the list, those services appear underneath the server hostname in the server list.

To change services to administer:

1. Open Server Admin.
2. Select a server, click the Settings button in the toolbar, and then click the Services tab.
3. Select the checkbox for each service you want to turn on.

From the command-line:

```
sudo serveradmin settings info:serviceConfig:services:com.apple.
     ServerAdmin.<service name>:configured = yes
```

Setting Up Open Directory

Unless your server must be integrated with another vendor's directory system or the directory architecture of a server you're upgrading needs changing immediately, you can begin using the directories you configured during server setup.

The online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ provide instructions for all aspects of Open Directory domain and authentication setup, including:

- Setting up client computer access to shared directory data
- Replicating LDAP directories and authentication information of Open Directory masters
- Integrating with Active Directory and other non-Apple directories
- Configuring single sign-on
- Using Kerberos and other authentication techniques

Setting Up User Management

Unless you're using a server exclusively to host Internet content (such as web pages) or perform computational clustering, you probably want to set up user accounts in addition to the administrator accounts created during server setup.

The online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/ tell you how to use Workgroup Manager to connect to the directory, define user settings, set up group accounts and computer groups, define managed preferences, and import accounts.

To set up a user account:

1. Open Workgroup Manager.
2. Authenticate to the directory as the directory administrator.
3. At the top of the application window, click the Accounts button to select the directory you want to add users to.
4. Click the New User button.
5. Specify user settings in the panes that appear.

You can set up user accounts by using Workgroup Manager to import settings from a file.

Setting Up All Other Services

All services of Mac OS X Server require specialized setup instructions to tailor the service to your specific needs.

For step-by-step instructions for setting up and managing the services, see the online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

Ongoing System Management 7

This chapter shows you how to complete ongoing management for your systems, including setting up administrator computers, designating administrators, and maintaining service uptime.

Read the following sections as a basic introduction to Mac OS X Server management:

Computers You Can Use to Administer a Server

To administer a server locally using the graphical administration applications (in /Applications/Server/) log in to the server as a server administrator and open them.

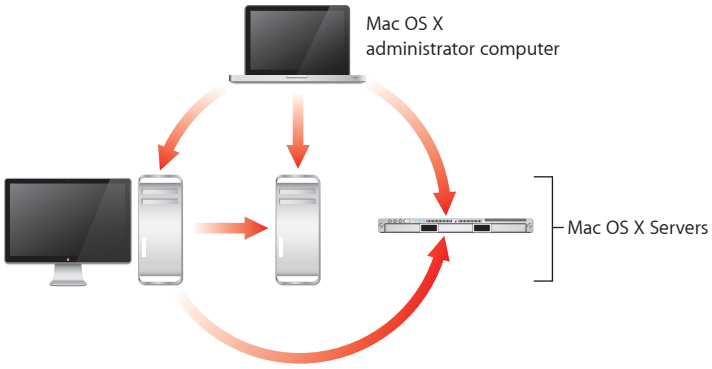
To administer a remote server, open the applications on an administrator computer. An administrator computer is any Mac OS X Server v10.6 or Mac OS X v10.6 or later computer where the administration tools have been installed from the *Mac OS X Server Admin Tools* CD. See "Setting Up an Administrator Computer" on page 124.

You can run command-line tools from the Terminal Application (in /Applications/Utilities/) on any Mac OS X Server or Mac OS X computer. You can also run command-line tools from a UNIX workstation.

Setting Up an Administrator Computer

An administrator computer is a computer with Mac OS X v10.6 or Mac OS X Server v10.6 or later that you use to manage remote servers.

In the following illustration, the arrows originate from administrator computers and point to servers the administrator computers might be used to manage.



When you've installed and set up a Mac OS X Server that has a display, keyboard, and optical drive, it's already an administrator computer. To make a computer with Mac OS X into an administrator computer, you must install additional software.

Mac OS X Server v10.6 administration tools require:

- Mac OS X v10.6
- 1 GB of RAM
- 1 GB of unused disk space

To enable remote administration of Mac OS X Server from a Mac OS X computer:

1. Insert the *Mac OS X Server Admin Tools* CD.
2. Open the Installer folder.
3. Start the installer (ServerAdministrationSoftware.mpkg) and follow the onscreen instructions.

Using a Non-Mac OS X Computer for Administration

You can use a non-Mac OS X computer that offers SSH support, such as a UNIX workstation, to administer Mac OS X Server using command-line tools. For more information, see the online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

You can also use any computer that can run a VNC viewer to administer Mac OS X Server. Administering the server via VNC is the same as using the server's keyboard, mouse, and monitor locally.

You enable a VNC server on Mac OS X Server by enabling Screen Sharing in the Sharing pane of System Preferences.

Using the Administration Tools

Information about administration tools can be found on the pages indicated in the following table.

Use this application or tool	To	See
Command-line tools	Administer a server using a UNIX command shell.	"Command-Line Tools" (page 48)
iCal Service Utility	Add locations and resources to your iCal server.	"iCal Service Utility" (page 46)
Installer	Install server software or upgrade it from v10.4 or 10.5.	"Using the installer Command-Line Tool to Install Server Software" (page 104)
QTSS Web Admin, QuickTime Broadcaster, and QuickTime Player	Manage media playlists and prepare it for streaming or progressive download.	"Media Streaming Management" (page 47)
Server Admin	Configure and monitor services and administrator access, and configure share points. Set up and manage QuickTime media streaming.	"Working with Settings for a Specific Server" (page 130) "Server Admin" (page 38)
Server Assistant	Set up a v10.6 server.	"Setting up Servers Interactively" (page 113)
Server Monitor	Monitor Xserve hardware.	"Using Server Monitor" (page 172)
System Image Utility	Manage NetBoot and NetInstall disk images.	"System Image Management" (page 47)
Workgroup Manager	Administer accounts and their managed preferences.	"Workgroup Manager Basics" (page 150)
Xgrid Admin	Monitor local or remote Xgrid controllers, grids, and jobs.	"Xgrid Admin" (page 49)
Apple Remote Desktop (optional)	Monitor and control other Macintosh computers.	"Apple Remote Desktop" (page 50)

Working with Pre-v10.6 Computers from v10.6 Servers

You can use the version of Server Admin included with Mac OS X Server v10.6 to administer the latest Mac OS X Server v10.5.

Using Mac OS X Server v10.6 will not administer DNS hosted on a server version earlier than v10.6.

You can use Workgroup Manager on a v10.6 server to manage Mac OS X clients running the latest Mac OS X v10.5. However, after you edit a user record using Workgroup Manager on v10.6, you can only access it using Workgroup Manager on v10.6.

Ports Used for Administration

For Apple's administration applications to function, the following ports must be enabled.

Port number and type	Tool used
22 TCP	SSH command-line shell
311 TCP	Server Admin (with SSL)
625 TCP	Workgroup Manager
389, 686 TCP	Directory
80 TCP	QuickTime Streaming Management
4111 TCP	Xgrid Admin

In addition, other ports must be enabled for each service you want to run on your server. For a port reference guide, see the online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

Ports Open By Default

After setup, the firewall is off by default in Advanced Server mode, and therefore all ports are open. When the firewall is on, all ports are blocked except the following for all originating IP addresses:

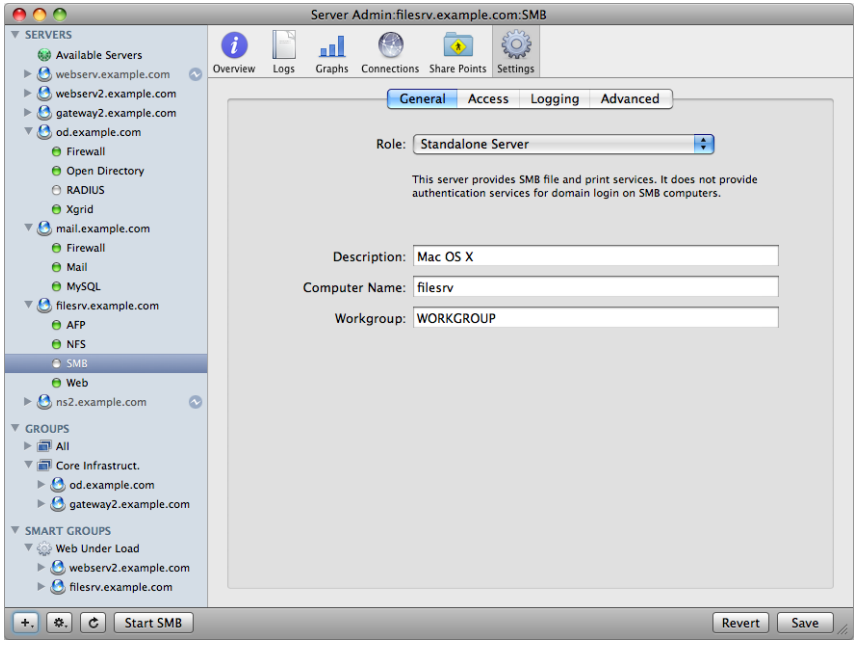
Port number and type	Service
22 TCP	SSH command-line shell
311 TCP	Server Admin (with SSL)
626 UDP	Serial number support
625 TCP	Remote Directory Access
ICMP incoming and outgoing	standard ping
53 UDP	DNS name resolution

Server Admin Basics

You use Server Admin to administer services on Mac OS X Server computers. Server Admin also lets you specify settings that support multiple services, such as creating and managing SSL certificates and specifying which users and groups can access services.

Adding and Removing Servers in Server Admin

The servers you can administer using Server Admin appear in the Servers list on the left side of the application window.



You can add a server to the Servers list and log in to it in two ways:

- Click the Add (+) button in the bottom action bar and choose Add Server.
- Choose Server > Add Server from the menu bar.

The next time you open Server Admin, any server you've added is displayed in the list. To change the order of servers in the list, drag a server to the new location in the list.

You can remove a server from the Servers list in a similar fashion. First you select the server to remove, then do one of the following:

- Click the Perform Action button in the bottom action bar and choose Disconnect then Remove Server.
- Choose Server > Disconnect, and then choose Server > Remove Server from the menu bar.

If a server in the Servers list appears gray, double-click the server or click the Connect button in the toolbar to log in again. To enable auto-reconnect the next time you open Server Admin, select the "Remember this password in my keychain" while you log in.

Grouping Servers Manually

Server Admin displays computers in groups in the Server List section of the application's window. The default server list is called the All Servers list. This is a list of administered computers that you have added and authenticated to. You can create other groups to organize the computers on your network.

Server groups have the following capabilities:

- You can create as many lists as you want.
- Servers can appear in more than one list.
- Groups can be made in any organization scheme you can imagine: geographic, functional, hardware configuration, even color.
- You can click a group name to see a status overview of all servers in the group.

You can make more specific, targeted groups of servers from your All Servers list. First, create blank lists and then add servers to them from the All Servers list.

To create a server group:

1. Under the Server list at the bottom of the Server Admin window, click the Add (+) button.
2. Select Add Group, and name the group.

   To rename groups, click the group and let the mouse hover over the name for a few seconds. When the name becomes editable, rename the group.
3. Drag the servers from the All Servers group to the newly created group.

Grouping Servers Using Smart Groups

Server Admin displays computers in groups in the Server List section of the application's window. The default server list is called the All Servers list. This is a list of administered computers that you have added and authenticated to.You can create a server list that populates based on custom criteria. This is referred to as a Smart Group.

After you create a smart group, any server added to the All Server list (or other specified list) that matches the criteria is added to the smart group.

You can match the following criteria:

- Visible services
- Running services
- Network throughput
- CPU utilization

- IP address
- OS version

To create a server smart group:

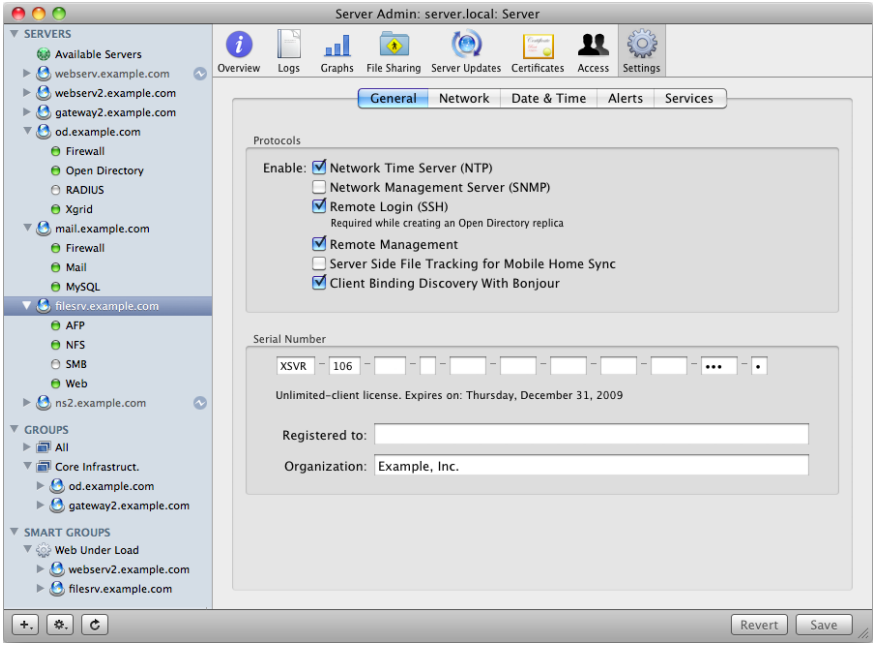
1. Under the Server list at the bottom of the Server Admin window, click the Add (+) button.
2. Select Add Smart Group.
3. Name the smart group.
4. Define the criteria that servers will appear in the list and click OK.

   The group appears in the Server list.

Working with Settings for a Specific Server

To work with general server settings, select a server in the Servers list. You then select from a number of buttons in the toolbar that show configuration options or tabs of configuration options.

The following shows the Settings pane for a server:



The following table contains a summary of what you find for each button:

Toolbar button	Shows
Overview	Information about the server's hardware, software, services, and status.
Logs	The system log and security systems log.
Graphs	A pictorial history of server activity.
Sharing	Configuration options for defining file sharing folders, share points, and automounts.
Server Updates	Software updates available from Apple to update the server's software. This only controls updates to the server's own software.
Certificates	The server's security certificates.
Settings	The server's network settings, server software serial number, service access controls, and other information.

When you click Settings, you have access to the following panes:

- **General pane:** Click General to work with the server serial number or to enable Simple Network Management Protocol (SNMP), Network Time Protocol (NTP), Secure Shell (SSH), Remote Management, and server-side mobile home-sync feature support.

  SNMP is a standard that facilitates computer monitoring and management. The server uses the open source net-snmp project for its SNMP implementation. Although no server administration tools use or require SNMP, it enables the server to be monitored and managed from third-party SNMP software such as HP OpenView.

  Use the NTP checkbox to enable NTP service. For information about NTP, see the online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

  SSH is a shell you can use to access command-line tools to remotely administer the server with. Mac OS X Server uses the open source OpenSSH project for its SSH implementation. SSH is also used for other remote server administration tasks, such as initial server setup, Sharing management, and displaying file system paths and the contents of folders in the server administration tools. SSH must be enabled while creating an Open Directory replica, but it can be disabled afterwards.

  Remote Management allows the server to be administered by Apple Remote Desktop (ARD). You enable and disable ARD administration in this pane in addition to the Sharing pane of System Preferences.

  Client Binding Discovery with Bonjour offers directory services to client computers on the local subnet, allowing the users to choose whether to bind to the server.

Server-side file tracking for mobile home-sync is a feature of mobile home folders. For information about when to enable this feature, see the online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

- **Network pane:** Click Network to view or change the server's computer name or local hostname, or to see a list of network interfaces and addressing information for this server.

  The computer name is what a user sees when browsing the network (/Network). The local hostname is usually derived from the computer name, but it can be changed.

  The network interfaces table shows the name of the interface, the type of addressing (IPv4, or IPv6), the IP address, and the DNS name found by reverse lookup for the address.

- **Date & Time pane:** Click Date & Time to set the server's date and time, NTP source preference, and time zone. For more information about NTP, see the online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

- **Notifications pane:** Click Notifications to configure Mac OS X Server's automatic event notifications.

  You set the mail address and notification trigger in this pane. For more information about notifications, see "Using Server Status Notification in Server Admin" on page 175.

- **Access pane:** Click Access to control user access to some services and to designate administration privileges for users.

  When you select the Services tab, you set up access to services to users and groups (referred to as service access control lists, or service ACLs). You can set up the same access to all services, or you can select a service and customize its access settings. Access controls are simple. Choose between enabling all users and groups to use services or enabling only specific users and groups to use services.

  When you select the Administrators tab, you designate users to have administration or monitoring privileges for the services on the server. For detailed information about these settings, see "Defining Administrative Permissions" on page 150.

- **Services pane:** Click Services to show or hide services in Server Admin for this server.

Understanding Changes to the Server IP Address or Network Identity

When you change a server's IP address, DNS name, local hostname, or computer name, there might be additional configuration steps needed for each service provided. Each service relies on IP addresses or names differently; therefore, the exact combination of steps relies on your individual setup.

The following sections give guidance regarding the types of changes will be necessary for a name or IP address change.

Understanding Mac OS X Server Names

Three names are used by Mac OS X Server: computer name, local hostname, and DNS name. They are used by different parts of the system for different reasons, and are not linked. Changing the computer name and the local hostname is not the same thing as changing the DNS name.

- The computer name is a user-friendly name for the system and is shown in the Finder and tools like Apple Remote Desktop.
- The local hostname is a domain name, usable only on the local network, and is published to other services which are Bonjour-aware.
- The DNS name is the Internet host name, which is a fully qualified domain name. Only the DNS name is the Internet-routable name that services use for network identity.

Understanding IP Address or Network Identity Changes on Infrastructure Services

Some services are infrastructure services. This means they provide the basic addressing, name resolution, and routing necessary for other services to function. Infrastructure services include:

- DNS
- DHCP
- Directory Service
- Firewall
- Mobile Access
- NAT
- NetBoot
- RADIUS
- VPN

Generally, changing the IP address or name of an infrastructure server requires an intimate knowledge of the new network configuration and topology as well as manual setting changes. Changes to these infrastructure services can cause widespread disruption of other services until the correct setting modifications are made.

DNS

For a server not hosting DNS, changing a server's IP address requires changes to the data in the DNS server. Minimally, the server's NS, A, and PTR records must be changed. Because the DNS information for the server is hosted elsewhere, those records must be updated manually on the DNS server.

Your network configuration might have other domains, computers, and record types that are impacted by a server's IP address change (SRV records, for instance). These other records should be examined thoroughly after any change to a server's IP address.

If the server is a DNS server, use the tool `changeip` to change the NS, A, and PTR records. Changing a DNS server's IP address directly impacts any client computer that uses the DNS server. For example, the DNS server's IP address could be provided to DHCP clients automatically, so all DHCP clients rely on the DNS server's correct IP address. All DNS names for all domains hosted by the DNS server must be examined.

Because of DNS caching, many clients might not respond to changes in the DNS system as quickly as needed. To expedite DNS server setting propagation, update all wireless access points, DHCP servers, manually configured IP address clients, and DHCP address clients by restarting them or renewing their DHCP leases.

In summary, clients that refer to the DNS server's IP address for name resolution need to be updated to use the new IP address.

Changing a server's DNS name or domain impacts all other services that rely on the server's domain name resolving correctly in DNS. The affected services include:

- Directory service
- Kerberos service and Kerberos Realm names
- WINS server names
- DHCP supplied search domains

DHCP

Changing the IP address of a DHCP server might invalidate all subnets and static IP addresses handled by the server. Additionally, the change in IP address might result in unreachable search domain names, WINS server names, or LDAP URLs. Examine these settings, if needed.

Many clients might not respond to the changes in the DHCP system immediately. After a DHCP server change, update all wireless access points, manually configured IP address clients, and DHCP address clients by restarting them or renewing their DHCP leases.

Changing the domain name of a DHCP server could also make obsolete the search domain names, WINS server names, or LDAP URLs. Changing the only hostname segment to a fully qualified domain name might not have the same effect.

Directory Service and Kerberos

Changing the IP address of an Open Directory Server might invalidate the data records themselves (computer records, or user home directories). None of the contents of the records are altered when you change the IP address, only the configuration.

Changing the DNS name of the directory server requires that all bound machines be rebound to the new directory name and address.

If you have set up a Kerberos environment, the Kerberos realm does not change when the hostname is changed.

Firewall
Changing the IP address of the Firewall can significantly alter the effectiveness of the service. In Mac OS X Server v10.6, IP firewall rules are stored and referenced as address groups. A change to the IP address of the firewall server might prevent traffic to the address groups from being routed, and therefore none of the specific firewall rules would be applied.

Check all firewall rules when changing the IP address of the firewall server.

Mobile Access (Proxy Services)
Most proxy services should remain relatively unaffected by a change to IP address or domain name. If you have edited the com.apple.securityproxy_mail.plist manually to have the proxy server connect to *itself* for some service by some other address than the link-local address (127.0.0.1 or localhost), you must change it manually again.

However, proxy services are affected if the IP address or DNS name of the destination servers changes. If you change a *proxied* services' name or address, you must reconfigure Proxy Service.

If you configured an HTTP Secure Proxy virtual host, you must delete and re-create the proxy mappings of any proxied servers.

NAT
NAT should not be affected by a change to the server's IP address or DNS name.
All clients behind the NAT server still have contact with the NAT router by the internal IP address. If you made manual modifications to the NAT service configuration files, make sure those changes are compatible with the new IP address or DNS name.

NetBoot
NetBoot does not require reconfiguration after changing the IP address or DNS name. However, all clients that use it must reselect the server after the changes.

RADIUS
If you change the RADIUS server IP address, you might need to check or reconfigure the IP addresses of the associated base stations. Additionally, if you're using SSL certificates, you must regenerate or repurchase the certificates. You must use Server Admin to import the new certificates, and then configure the service's new certificate.

VPN

VPN servers allocate IP address ranges to VPN clients and mediate DNS queries of VPN clients. Any of these can be affected by a change to the VPN server's IP address or domain name. Additionally, the VPN server contains routing definitions based on IP addresses. A change to the IP address can make those routing addresses unreachable.

Check all the VPN settings when changing the IP address of the VPN server.

Understanding IP Address or Network Identity Changes on Web and Wiki Services

Some services are classified as web services. This means they provide the interaction, back-end database storage, and media streaming of websites hosted on the server. Web services include:

- Web
- MySQL
- QTSS
- Wiki
- Certificates for web and wiki service

Generally, these services in the initial default configuration are resilient and adjust to changes made to the IP address or the server name. However, if your web services are customized, they might need manual configuration changes to maintain service integrity.

Web

If you change the web server's DNS name or IP address, you must modify the domain name and web server aliases. You should also check the site load balancer members.

If you change the web server's DNS name, you must modify virtual hosts that use SSL. Virtual hosts that use SSL need new certificates. You might need to regenerate or repurchase the certificates. Use Server Admin to import the new certificates, then configure each virtual host's new name and certificate.

If you change the web server's IP addresses, use Server Admin to change any virtual hosts that use a specific IP address. The default wild-card virtual host doesn't need to be modified.

For either change, if you configured Mobile Access for web (or possibly other proxy settings), delete and recreate the proxy settings for all affected hosts.

MySQL

In general, MySQL is not affected by changing an IP address or DNS name. However, none of the data in the databases is altered when the DNS name or IP address are changed. You are responsible for replacing references to the DNS name and address (if used) in your databases.

If you set a database root password, there might be entries in the database GRANT table (database=mysql, table=user) that refer to the previous server DNS name. In this case, use Server Admin to reset the root password, which will then reflect the current server identity.

Server administrators should make sure that MySQL clients that have saved references to the DNS name of the MySQL Service are updated to reflect any change in the server identity.

QTSS

The typical default configuration will not need further configuration after changing the DNS name or IP address of QTSS. If you configured specific IP bindings, change those to the new address and restart the service. Relays you defined might have invalid IP addresses after an IP address change.

Wiki

Wiki service remains unaffected by a change in the IP address, assuming Apache is still functioning and DNS names change.

However, wikis can be configured to specific DNS names. If you manually edited configuration files to restrict wiki access to DNS names, make the relevant changes in those files.

Certificates for Web and Wiki Services

Web and wiki servers that use SSL will need new certificates. You might need to regenerate or repurchase the certificates. You must use Server Admin to import the new certificates, then configure each service's, or site's, new certificate.

Understanding IP Address or Network Identity Changes on File Services

File services provide file storage and retrieval for network clients. File services include:

- AFP
- SMB
- NFS
- FTP

For the most part, changing the network address or DNS name of a file server has no internal affect on file services. The file service processes monitor network interfaces for changes and adapt as necessary without administrator intervention. No further configuration is required.

A few places might need configuration settings changed:

- **SMB:** The computer name defaults to the unqualified primary DNS name. Changing the DNS name of the server causes a mismatch between the DNS name and the defined computer name.
- **FTP:** The service can use SSL certificates, and will need new certificates. You might need to regenerate or repurchase the certificates. Use Server Admin to import the new certificates, then configure each service's new certificate.

Additionally, clients might have URLs, bookmarks, favorites or documentation that refers to previous DNS names or IP addresses. Ensure that client information is updated to reflect the new name or address.

Finally, you might have other software that interfaces with file servers (for example, automated scripts) and refers to old DNS names and IP addresses. Update those applications or scripts as well.

Understanding IP Address or Network Identity Changes on Mail Services

Mail services are the suite of services that provide mail delivery, retrieval, and processing. Mail services include:

- IMAP and POP
- SMTP
- Mailing List
- Anti-virus and anti-spam
- Certificates for mail services

Most mail services require a restart after changing a DNS name or IP address of the mail server. If you manually changed configuration files, you might need to edit them manually again. Additionally, some mail services require a full shutdown and startup (rather than a simple service reload) to get the address and identity changes.

There are many places in the mail services configuration panes where you enter domain names, mail host names, relay host names, and mail addresses. Any change you make to the DNS name could potentially have an affect on the service. Double-check name and IP address settings carefully.

IMAP and POP

Dovecot, the IMAP and POP service, loads the fully-qualified domain name at startup and configuration reload. After a change, Dovecot must be restarted or given a SIGHUP command, at a minimum).

You must also restart if you manually edited the listen or ssl_listen parameters.

SMTP

Postfix, the SMTP service, is very sensitive to network address and identity changes. The information it stores about the DNS name, the IP address, and network interfaces is only loaded once at service startup. To resume service after a change to the DNS name or the IP address, you must fully stop the service, and restart it.

You must also restart it if you manually edited the inet_interfaces, inet_protocols, smtp_bind_address, myhostname, or mydomain configuration parameters.

Mailing List

Mailman, the mailing list service, tracks the incoming and outgoing mail hosts by reading them on startup. If you change the hostname or IP address, restart Mailman for it to honor the configuration changes.

Antivirus and Antispam

ClamAV, the antivirus service, gets its listening address at startup as well. After making any changes to the DNS name or IP address, you must stop and restart to resume service.

SpamAssassin, the anti-spam service, gets its configuration information at startup and can reload configuration data while running. To load new configuration data, restart SpamAssassin or give it a SIGHUP command, at a minimum.

Certificates for Mail Services

Mail servers that use SSL need new certificates. You might need to regenerate or repurchase the certificates. Use Server Admin to import the certificates, then configure each service's new certificate.

Understanding IP Address or Network Identity Changes on Collaboration Services

Collaboration services provide tools to coordinate people and time. Collaboration services include:

- Calendar service
- Address Book service
- iChat service
- Certificates for collaboration services

Address Book Service

Changing the IP address of an Address Book server does not affect new connections to the server; however, it can disconnect existing client connections. If you manually edited the BindHTTPPorts or BindSSLPorts options in the carddavd.plist file, edit them again and restart the service.

Changing the DNS name of an Address Book server necessitates restarting the service. If you manually edited the ServerHostName setting in the carddavd.plist file, you might need to do so again before restarting the service.

iCal Service

The iCal Server is based on the same underlying technology as the Address Book Server, so the needs are the same.

Changing the IP address of an iCal server does not affect new connections to the server; however, it can disconnect existing client connections. If you manually edited the BindHTTPPorts or BindSSLPorts options in the caldav.plist file, you must edit them again and restart the service.

Changing the DNS name of an iCal server necessitates restarting the service. If you manually edited the ServerHostName setting in the caldavd.plist file, you might need do so again before restarting the service.

iChat Service

The iChat service is highly resilient to network and identity changes on the primary Ethernet port. No additional configuration is necessary if you've changed the DNS name or IP address of the iChat server.

However, the jabber IDs associated with the server do not update to the new iChat server DNS name. For example, changing the server from example.com to example.net, Joe's jabber ID (joe@example.com) doesn't migrate to joe@example.net.

The jabber IDs for service users can be changed using the `jabber_autobuddy` tool. The tools modifies the database by changing the @host.com part of user names associated with the old domain to reflect the new domain, as well as secondary references (individual- and group-based buddies) that reference the old domain.

To migrate the jabber IDs, run the following commands:

```
sudo serveradmin stop jabber
sudo jabber_autobuddy --move-domain <old_domain> <new_domain>
sudo serveradmin start jabber
```

Additionally, the tool makes an automatic backup of the previous database (/var/jabberd/sqlite/jabberd2_bak.db), which can be stored or restored as needed.

Certificates for Collaboration Services

AddressBook, iCal, and iChat servers that use SSL will need new certificates. You might need regenerate or repurchase the certificates. Use Server Admin to import the new certificates, then configure each service's new certificate.

Understanding IP Address or Network Identity Changes on Podcast Producer

Podcast Producer is a complex service. It uses a number of other services and computers to perform its work. Because several Xgrid Agent computers and camera capture computers depend on contact with the Podcast Producer server, changes to the IP address or DNS name must be coordinated for affected computers, not just the main Podcast Capture server.

If Podcast Producer server is run on a computer providing DNS to a network or is run on a computer providing directory services to a network as an Open Directory Master, resolve the conflicts and network conditions for those services before attempting to account for changes done to Podcast Producer

For more information on how address and identity changes affect DNS and directory services, see "Understanding IP Address or Network Identity Changes on Infrastructure Services" on page 133.

Changing the IP address or DNS name might necessitate changing settings for the following services and software:

- DNS server
- Open Directory server
- Xgrid Controller
- NFS file service
- Xsan and its MDC configuration (if used for file storage)
- Mail Services (if used by a workflow)
- Wiki Server (if used by a workflow)
- iChat Server (if used by a workflow)
- QMaster (if used by a workflow)
- Final Cut Server (if used by a workflow)

You can reduce the number of services to reconfigure by initially defining an alias record in DNS (a CNAME record) and using the DNS name alias as the DNS name for configuration purposes.

If any listed servers use SSL, they will need new certificates. You might need to regenerate or repurchase the certificates. Use Server Admin to import the certificates, then configure each service's new certificate.

To change the IP address of the Podcast Producer computer:

1. Stop the Xgrid job queue when empty (or stop and empty it).
2. Reconfigure DNS, Open Directory, DHCP, and other infrastructure services.

   For example, in DNS, change the A record IP address of the Podcast Producer server.
3. Use `changeip` to change the IP address of the Podcast Producer server.
4. Restart (or renew the DHCP leases of) all Podcast Camera Agents.
5. Restart (or renew the DHCP leases of) all Xgrid Agents used for the Podcast Producer workflow grid.

   Alternatively, instead of restarting the computers, you flush the Directory services cache (using `dscacheutil` and sending a HUP to the mDNSResponder daemon).

To change the DNS name of the Podcast Producer computer:

1. Stop the Xgrid job queue when empty (or stop and empty it).
2. Reconfigure DNS, Open Directory, DHCP, and other infrastructure services.

   For example, in DNS, change the A record host name of the Podcast Producer server.
3. Use `changeip` to change the DNS name of the Podcast Producer server.
4. Restart (or renew the DHCP leases of) all Podcast Camera Agents.
5. Restart (or renew the DHCP leases of) all Xgrid Agents used for the Podcast Producer workflow grid.

   Alternatively, instead of restarting the computers, flush the Directory services cache (using `dscacheutil` and sending a HUP to the mDNSResponder daemon).
6. Unbind the Podcast Camera Agents from the previous DNS name and rebind them to the new name.
7. Reconfigure Xgrid Agents to use the new DNS name.
8. Reconfigure services used in the workflow to reference the new DNS name, if needed.
9. Update and reissue an SSL certificates that contain the server's DNS name.
10. Reconfigure Kerberos service on the server (using Directory Binding or `ssoutil`).
11. Update any scripted or automated software that submits data to or polls data from Podcast Producer.

Understanding IP Address or Network Identity Changes on Other Services

The remaining services affected by changes to the IP address or network identity include:

- Print
- Push Notification

- Software Update Service
- Xgrid

After Software Update changes the DNS name or IP address, a number of changes must be made by the clients. However, the following guidelines for the server should be followed.

Print
Print service needs no changes if the IP address changes. If the DNS name changes, the administrator must restart print service to re-register the service with Bonjour to publish the name change.

If you made custom configurations of the cupsd.conf file, or configured /Config/Printers entries in the directory service, review those custom configurations and update them if needed.

If you assigned per-queue printing quotas to user accounts, update the account quotas to reflect the new server DNS name if needed.

Also, make sure that printing clients that have saved references to the DNS name of print queues are updated to use the new DNS name.

Push Notification
Push notification servers should be cleared or removed from the service before changing the server's IP address or DNS name.

Re-enable push notification after the network identity has changed.

Software Update Server
Software Update must be restarted after changes are made to the DNS name or IP address of the service. Afterward, update the list of available software updates.

Also, make sure clients that saved references to the DNS name of the Software Update server are updated to use the new DNS name.

Xgrid
Xgrid service must be restarted after changes are made to the DNS name or the IP address of the service. Changes to the DNS name or IP address should be made when the Xgrid job queue is empty and stopped.

If you use Kerberos for client authentication to the controller, resolve Kerberos configuration issues before attempting to reconfigure for Xgrid service.

If you change the DNS name of the controller, reconfigure all Xgrid Agents to use the new controller's new DNS name.

Changing the IP Address of a Server

You can change the IP address of a server using the Network pane of System Preferences or the `networksetup` tool.

Do not turn off the primary network interface and then turn it back on with a different address. Several services will not get the needed notification to update their configuration.

Changing your IP address can have significant unintended consequences, depending on the services your server provides. For information on the effects of changing the IP addresses, see "Understanding Changes to the Server IP Address or Network Identity" on page 132.

The `changeip` command-line tool can accomplish manually what is done automatically, and it is still available.

Changing the Server's DNS Name After Setup

If you change a server's DNS name after setup, the name must be changed with your DNS service provider.

Until the server's DNS name matches the name with the DNS service provider, several services will not function. Changing your DNS name can have significant unintended consequences, depending on the services your server provides.

For information on the effects of changing the DNS name, see "Understanding Changes to the Server IP Address or Network Identity" on page 132.

The DNS name is the Internet host name, which is a fully qualified domain name. Only the DNS name is the Internet-routable name that services use for network identity.

To change the DNS name

```
sudo scutil --set OldName <NewName.domain.tld>
```

You can use the `scutil` command-line tool to set the computer name and local hostname. For more information, see the `scutil` man page.

Do not use the `changeip` command-line tool to change DNS names, even though the tool is still available.

Changing the Server's Computer Name and the Local Hostname

The computer name is a user-friendly name for the system and is shown in the Finder and tools like Apple Remote Desktop.

The local hostname is a domain name, usable only on the local network, and is published to other services which are Bonjour-aware.

You can use the `scutil` command-line tool to set the local hostname and local hostname. For more information, see the `scutil` man page.

Do not use the `changeip` command-line tool to change computer names, even though the tool is still available.

To change computer name and local hostname:

- Change the names in the Network pane of the Settings section for the server in Server Admin.

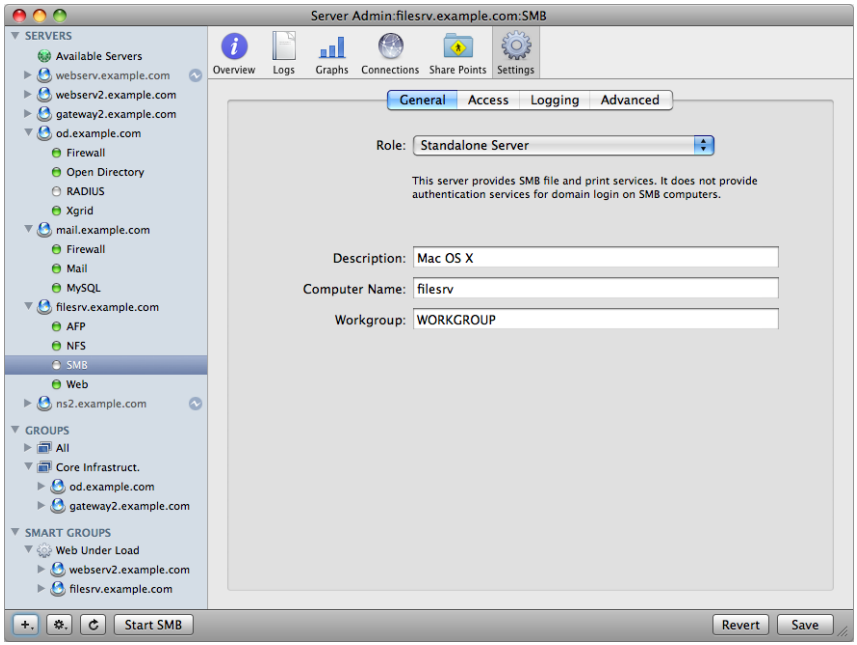
From the command line:

```
sudo scutil --set ComputerName <newComputerName>
sudo scutil --set LocalHostName <newLocalHostName>
```

Administering Services

To work with a service on a server selected in the Servers list of Server Admin, click the service in the list under the server. You can view information about a service (logs, graphs, and so forth) and manage its settings.

The following is a sample service configuration pane in Server Admin.



To start or stop a service, select it and then click Start <service name> or Stop <service name> in the bottom action bar.

Adding and Removing Services in Server Admin

Server Admin can only show you the services you are administering, hiding all other service configuration panes until needed. Before you can administer a service, it must be enabled for the specific server; then that service appears under the server name in the main Server list.

To add or remove a service in Server Admin:

1. Select the server that will host the service.
2. Click the Settings button in the toolbar.
3. Click Services.
4. Select the service and click Save.

   The service now appears in the list, ready for configuration.

Importing and Exporting Service Settings

To copy service settings from one server to another or to save service settings in a plist file for reuse later, use the Export Service Settings command in Server Admin.

To export service settings:

1. Select the server.
2. From the menu bar, choose Server > Export > Service Settings.
3. Select the services whose settings you want to copy.
4. Click Save.

   The file that is created contains all service configuration information as a plist XML document.

To import service settings:

1. Select the target server to receive the settings.
2. Choose Server > Import > Service Settings from the menu bar.
3. Find and select the saved service file.

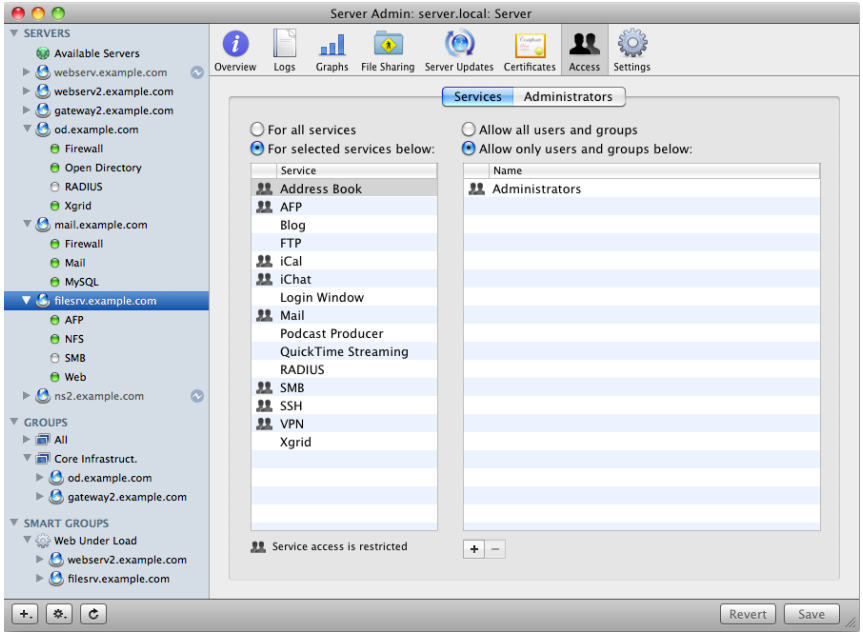
   The only file you can use with this function is a properly formatted XML-based plist file, generated from the settings export.
4. Click Open.

Controlling Access to Services

You can use Server Admin to configure which users and groups can use services hosted by a server. You set up access to services to users and groups using SACLs. You can set up the same access to all services, or you can select a service and customize its access settings.

Access controls are simple. Choose between allowing all users and groups to use services or allowing selected users and groups to use services. You can separately specify access controls for individual services, or you can define one set of controls that applies for all services that the server hosts.

The following shows the Service Access Control List pane in Server Admin:



To configure service access SACLs

1. Select a server in the Servers list.
2. Click Settings, then click Access.
3. Click Services.
4. Choose a service, and choose whether to allow everyone access to it or whether to allow specified users access to the service.
5. If you have chosen to specify users, add the users and groups as desired.

Using SSL for Remote Server Administration

You can control the level of security of communications between Server Admin and remote servers by choosing Server Admin > Preferences.

By default, Server Admin treats communications with remote servers as encrypted using SSL. This uses a self-signed 128-bit certificate installed in /etc/servermgrd/ssl.crt when you install the server. Communications use HTTPS (port 311). If this option isn't possible, HTTP (port 687) is used and clear text is sent between Server Admin and the remote server.

If you want a greater level of security, also select "Require valid digital signature (SSL)." By default, "Require valid digital signature (SSL)" is disabled. This option uses an SSL certificate installed on a remote server to ensure that the remote server is a valid server.

Before enabling this option, use the instructions in "Requesting a Certificate from a Certificate Authority" on page 65 for generating a CSR, obtaining an SSL certificate from an issuing authority, and installing the certificate on each remote server.

Instead of placing files in /etc/httpd/, place them in /etc/servermgrd/. You can also generate a self-signed certificate and install it on the remote server.

You can use Server Admin to set up and manage self-signed or -issued SSL certificates used by mail, web, Open Directory, and other services that support them.

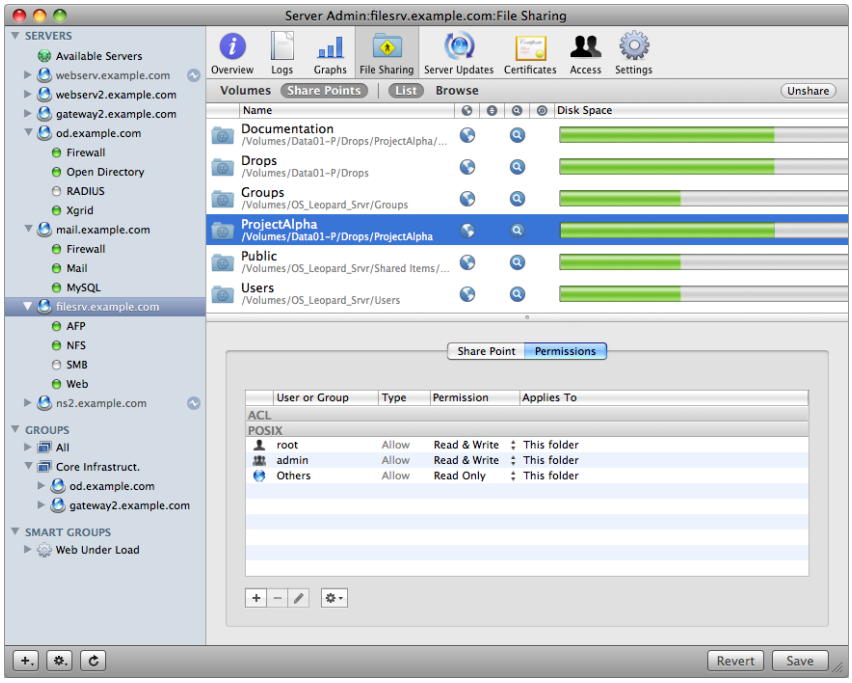
"Certificate Manager in Server Admin" on page 62 provides instructions for using Server Admin to create, organize, and use security certificates for SSL-enabled services. Individual service administration guides describe how to configure specific services to use SSL.

If you're interested in higher levels of SSL authentication, see the information at www.modssl.org.

Managing Sharing

To work with share points and access control lists, click the File Sharing icon in the Server Admin toolbar. Learn more in the online help and Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

The following is the File Sharing configuration pane in Server Admin.



Tiered Administration Permissions

In previous releases of Mac OS X Server, there were two classes of users: admin and everyone else. Admin users could make any change to the settings of any service or change any directory data including passwords and password policies.

In Mac OS X Server v10.6, you can now grant individuals and groups specific administrative permissions without adding them to the UNIX "admin" group. In other words, you can make them administrator users.

There are two levels of permissions:

- **Administer:** This level of permission is analogous to being in the UNIX admin group. You can change any setting on the server for the designated server and service only.
- **Monitor:** This level of permission allows you to view Overview panes, Log panes, and other information panes in Server Admin, as well as general server status data in server status lists. You do not have access to any saved service settings.

Any user or group can be given these permissions for all services or for selected services. The permissions are stored on a per-server basis.

The only users that can change the tiered administration access list are users that are in the UNIX admin group.

Server Admin updates to reflect what operations are possible for a user's permissions. For example, some services are hidden or the Settings pane is dimmed when you can only monitor that service.

Because the feature is enforced on the server side, the permissions also impact the usage of serveradmin, dscl, dsimport, and pwpolicy command-line tools because these tools are limited to the permissions configured for the administrator in use.

Defining Administrative Permissions

You can decide if a user or group can monitor or administer a server or service without giving them the full power of a UNIX administrative user. Assigning effective permissions to users creates a tiered administration, where some but not all administrative duties can be carried out by designated individuals.

To assign permissions:

1. Open Server Admin.
2. Select a server, click the Settings button in the toolbar, and then click the Access tab.
3. Click the Administrators tab.
4. Select whether to define administrative permissions for all services on the server or for select services.
5. If you define permissions by service, select the related checkbox for each service you want to turn on.

   If you define permissions by service, be sure to assign administrators to all the active services on the server.
6. Click the Add (+) button to add a user or group from the users and group window.

   To remove administrative permissions, select a user or group and click the Remove (-) button.
7. For each user or group, select the permissions level next to the user or group name.

   You can choose Monitor or Administer.

   The capabilities of Server Admin to administer the server are limited by this setting when the server is added to the Server list.

Workgroup Manager Basics

You use Workgroup Manager to administer the following accounts: user accounts, group accounts, and computer lists. You also use it to set preferences for Mac OS X user accounts, group accounts, computers, and to access the Inspector, an advanced feature that lets you do raw editing of Open Directory entries.

The following topics describe general Workgroup Manager usage. Instructions for conducting specific administration tasks are available in Workgroup Manager help and the Mac OS X Server Resources website at www.apple.com/server/macosx/resources/.

Opening and Authenticating in Workgroup Manager

Workgroup Manager is installed in /Applications/Server/. You can open it in the Finder, the Dock, or by selecting View > Workgroup Manager in the menu bar of Server Admin.

When you open Workgroup Manager on the server you're using without authenticating, you have read-only access to information displayed in the local domain. To make changes, click the lock icon to authenticate as a server administrator.

This approach is most useful when you're administering various servers and working with several directory domains.

To authenticate as an administrator for a server, local or remote, enter the server's IP address or DNS name in the login dialog box or click the directory path area of the Workgroup Manager window to choose another directory server. Specify the user name and password for an administrator of the server, then click Connect.

Use this approach when you work most of the time with a specific server.

After opening Workgroup Manager, you can open a Workgroup Manager window for a different computer by clicking New Window in the toolbar or choosing Server > Connect.

Important: When you connect to a server in Workgroup Manager, make sure the long or short user name you specify matches the capitalization in the user account. It is case sensitive.

Administering Accounts

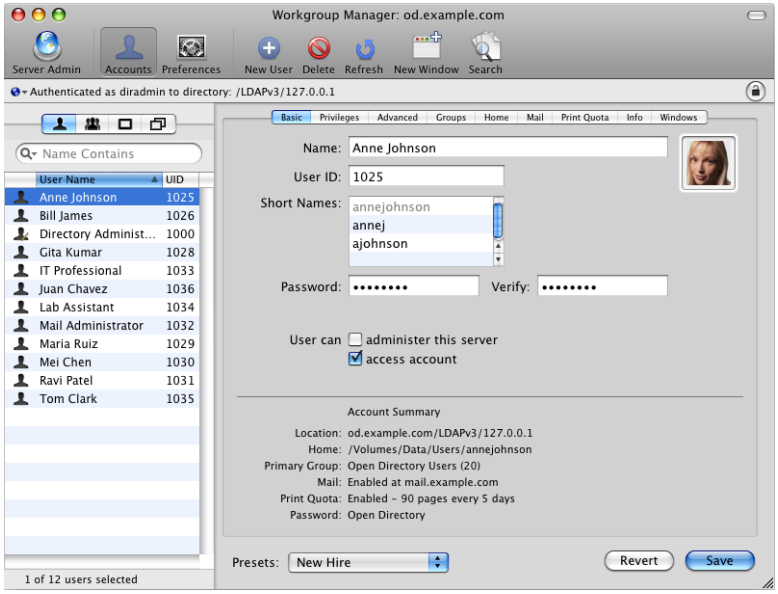
User accounts and group memberships are not administered in Server Admin. You use Workgroup Manager to add and remove users and groups.

What follows is a brief synopsis of account administration using Workgroup Manager. Do not use this section as your only source of information about accounts.

Working with Users and Groups

After you log in to Workgroup Manager, the account window appears, showing a list of user accounts.

The following is a sample user record configuration pane in Workgroup Manager:



Initially, accounts listed are those stored in the last directory node of the server's search path. When you use other Workgroup Manager windows, such as Preferences, click Accounts in the toolbar to return to the account window.

To specify the directories that store accounts you want to work with, click the small globe icon. To work with different accounts in different Workgroup Manager windows, click New Window in the toolbar.

To administer the accounts listed, click the Users, Groups, Computers, or Computer Groups button on the left side of the window. You can filter the accounts listed by using the pop-up search list above the accounts list.

To simplify defining an account's initial attributes when you create the account, use presets. A preset is an account template.

To create a preset, select an account, set up all the values the way you want them, then choose Save Preset from the Presets pop-up menu at the bottom of the window.

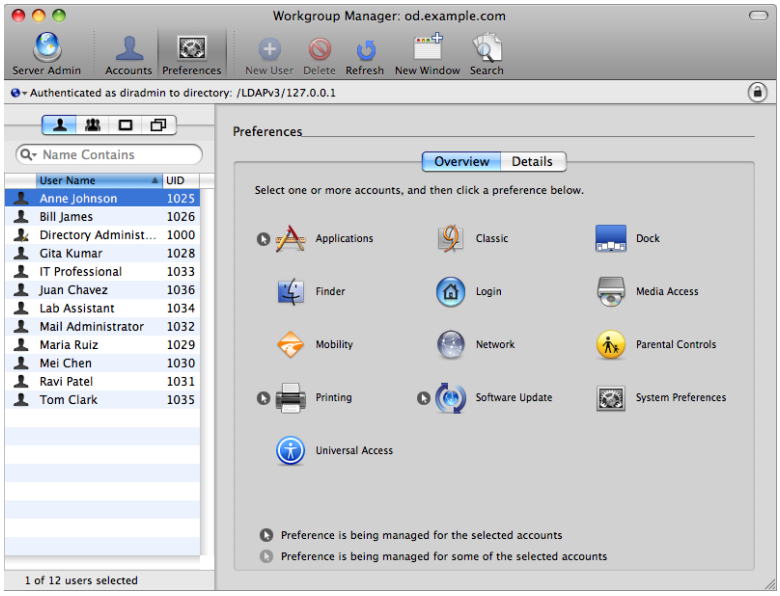
To work with only accounts that meet specific criteria, click Search in the toolbar. The Search features include the option for batch editing selected accounts.

To import or export accounts, select the accounts, then choose Server > Import or Server > Export, respectively.

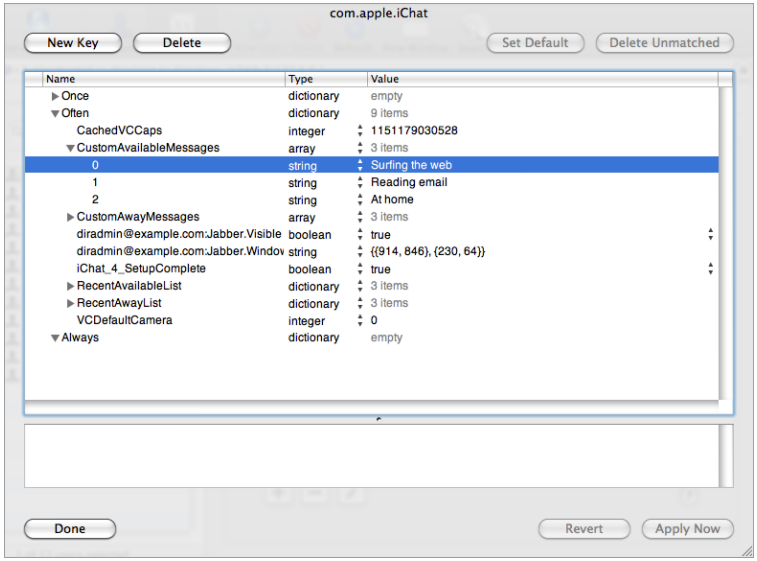
Defining Managed Preferences

To work with managed preferences for user accounts, group accounts, or computer lists, click the Preferences icon in the Workgroup Manager toolbar.

The following is the User Preference Management Overview pane in Workgroup Manager:



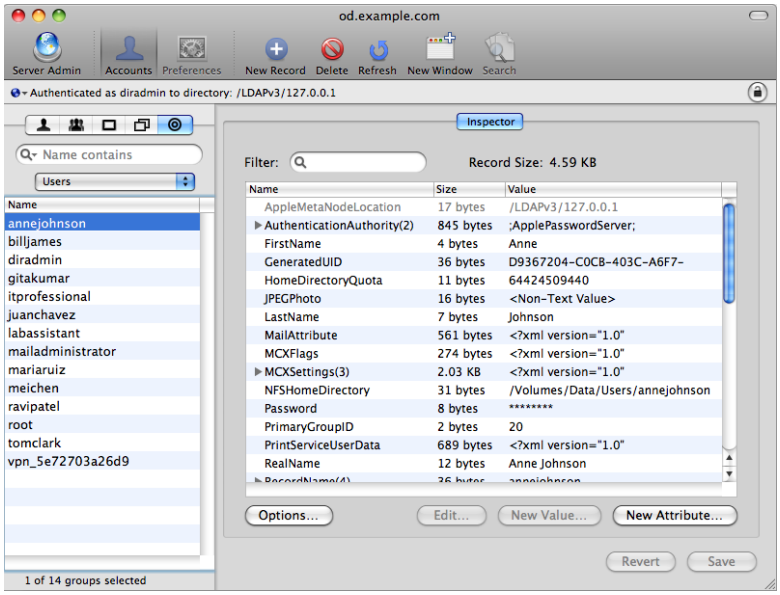
Click Details to use the preference editor to work with preference manifests. The following is a sample of the preference editor sheet in Workgroup Manager:



Working with Directory Data

To work with raw directory data, use Workgroup Manager's Inspector.

The following is the record Inspector pane in Workgroup Manager:



To display the inspector:

1. Choose Workgroup Manager > Preferences.
2. Enable "Show 'All Records' tab and inspector" and click OK.
3. Select the "All records" button (which looks like a bull's-eye) to access the Inspector.
4. Use the pop-up menu above the Name list to select the records of interest.

For example, you can work with users, groups, computers, share points, and many other directory objects.

Customizing the Workgroup Manager Environment

There are several ways to tailor the Workgroup Manager environment:

- You can control the way Workgroup Manager lists accounts and other behaviors by choosing Workgroup Manager > Preferences.
- To customize the toolbar, choose View > Customize Toolbar.
- To include predefined users and groups in the user and group lists, choose View > Show System Users and Groups.
- To open Server Admin so you can monitor and work with services on specific servers, click the Server Admin icon in the toolbar.

Service Configuration Assistants

Server Admin has configuration assistants to guide you through setting up services that require more setup than a single configuration pane. The assistants present you with all configuration panes necessary to fully enable a service.

Assistants are available for the following services:

- **Server Assistant:** This assistant helps you configure remote servers, install Mac OS X Server remotely, and make automatic server setup data files.
- **Gateway Setup:** This assistant helps you set up your server as a network gateway. Launch the assistant using a button in the lower right side of NAT service's Overview page.
- **Mail:** This assistant helps you set up incoming and outgoing mail service. Launch the assistant using a button in the lower right side of Mail service's Overview page.
- **RADIUS:** This assistant helps you set up RADIUS authentication for Apple Airport wireless access points. Launch the assistant using a button in the lower right side of RADIUS service's Overview page.
- **Xgrid:** This assistant helps you set up Xgrid controllers. Launch the assistant using a button in the lower right side of Xgrid service's Overview page.

Critical Configuration and Data Files

When backing up system settings and data, take special care to make sure all your critical configuration files are backed up. The nature and frequency of your backups depend on your organization's backup, archive and restore policies.

For more information about creating a backup and restore policy, see "Defining Backup and Restore Policies" on page 31.

The following is a list of configuration and data files for services available on Mac OS X Server.

Time Machine backs up service states and configuration files, but not files with your created data. To see which services Time Machine backs up, see "Understanding Time Machine as a Server Backup Tool" on page 36.

General

File type	Location
Service states	/System/Library/LaunchDaemons/*
SSH configuration files and host's public / private keys	/etc/ssh/*
System keychain	/Library/Keychains/System.keychain

Address Book Service

File type	Location
Configuration files	/etc/cardavd/cardavd.plist
Data	/Library/AddressBookServer/Documents/

iCal Service

File type	Location
Configuration files	/etc/caldavd/caldavd.plist
Data	/Library/CalendarServer/Documents/

iChat Server

File type	Location
Configuration files	/etc/jabberd/*
Data	mysqldump jabberd2 > jabberd2.backup.sql

Firewall Service

File type	Location
Configuration files	/etc/ipfilter/*

Mail Service

The following are configuration files and data stores for Mail services.

Mail—SMTP Server Postfix

File type	Location
Configuration files	/etc/postfix/
Data: (default locations)	/var/spool/postfix/

Mail—POP/IMAP Server Dovecot

File type	Location
Configuration files	/etc/dovecot/dovecot.conf
	/etc/dovecot/partition_map.conf
Data: (default locations)	/var/mail/
	/var/spool/imap

Mail—Amavisd

File type	Location
Configuration files	/etc/amavisd.conf
Data: (default locations)	/var/amavis/

Mail—Clam AV

File type	Location
Configuration files	/etc/clamav.conf
	/etc/freshclam.conf
Data: (default locations)	/var/clamav/
	/var/virusmails/

Mail—Mailman

File type	Location
Configuration files	/var/mailman/
Data: (default locations)	/var/mailman/

Mail—SpamAssassin

File type	Location
Configuration files	/etc/mail/spamassassin/local.cf
Data: (default locations)	/etc/mail/spamassassin/

MySQL Service

File type	Location
Configuration files	There is no config file for MySQL, but the administrator can create one, which should be backed up if present. /etc/my.cnf
Data: (default locations)	/var/mysql/
	mysqldump --all-databases > all.sql

NAT Service

File type	Location
Configuration files	/etc/nat/*

Notifications

File type	Location
Configuration files	/etc/emond.d/
	/etc/emond.d/rules/
	/Library/Keychains/System.keychain

OpenDirectory Service

The entire Open Directory configuration can be saved with the archive feature.

Filetype	Location
Configuration files	/etc/openldap/slapd.conf
Data: (default locations)	/etc/openldap/ (stop `slapd`, and then backup with `slapcat`)

PHP

File type	Location
Configuration files	There is no config file for PHP, but the administrator can create one (copying /etc/php.ini.default to /etc/php.ini and modifying it), which should be backed up if present. /etc/php.ini
Data: (default locations)	Designated by administrator

QuickTime Streaming Server

File type	Location
Configuration files	/Library/QuickTimeStreamingServer/Config/*
	/Library/QuickTimeStreamingServer/Playlists/*
	/Library/Application Support/Apple/QTSS Publisher/*
Data: (default locations)	/Library/QuickTimeStreamingServer/Movies/*
	~user/Sites/Streaming/*

Tomcat App Server

Filetype	Location
Configuration files	/Library/Tomcat/conf/
Data: (default locations)	/Library/Tomcat/webapps/

Web Service

File type	Location
Configuration files	/etc/apache2/* (for Apache 2.2)
	/etc/httpd/* (for Apache 1.3)
	/etc/webperfcache/*
	/Library/Keychains/System.keychain
Data: (default locations)	/Library/WebServer/Documents/
	/Library/Logs/WebServer/*
	/Library/Logs/Migration/webconfigmigrator.log (Apache config migration log)

The default location for web content is configurable and is most likely modified and extended to include multiple virtual host content and WebDAV directories.

Note: Log files for web service are a critical source of revenue for some sites and should be considered for backup. The location is configurable and can be determined using Server Admin.

Wiki and Blog Server

File type	Location
Configuration files	/etc/wikid/*
	/Library/Application Support/Apple/WikiServer(wiki themes and template files)
Data: (default locations)	/Library/Collaboration/
Log files: (default location)	/Library/Logs/wikid/*

Improving Service Availability

Eliminating single points of failure and using Xserve and hardware RAID can boost your server availability.

Other things you can do range from simple solutions like using power backup, automatic restart, and ensuring proper operational conditions (for example, adequate temperature and humidity levels) to more advanced solutions involving link aggregation, load balancing, Open Directory replication, and data backup.

Eliminating Single Points of Failure

To improve the availability of your server, reduce or eliminate single points of failure. A single point of failure is any component in your server environment that, if it fails, causes your server to fail.

Some single points of failure include:

- Computer system
- Hard disk
- Power supply

Although it is almost impossible to eliminate all single points of failure, you should minimize them as much as possible. For example, using a backup computer and a file storage pool for Mac OS X Server eliminates the computer as a single point of failure.

Although master and backup computers can fail at once or one after the other, the possibility of such an event happening is negligible.

Another way to prevent a computer from failing is to use a backup power source and take advantage of hardware RAID to mirror the hard disk. With hardware RAID, if the main disk fails, the system can still access the same data on the mirror drive, as is the case with Xserve.

Using Xserve for High Availability

Xserve is designed for extra reliability and hence, high availability.

Although you can use desktop systems like the Mac Pro to provide Mac OS X Server services very reliably, Xserve has the following additional features that make it ideal for high availability situations.

- Xserve has eight fans. In the case of a single fan failure, the other fans speed up to compensate, allowing your server to keep running.
- An independent drive architecture isolates the drives electrically, preventing a single drive failure from causing unavailability or performance degradation of the surviving drives—a common problem with multidrive SCSI implementations.
- Xserve uses Error Correction Code (ECC) logic to protect the system from corrupt data and transmission errors.

  Each DIMM has an extra memory module that stores checksum data for every transaction. The system controller uses this ECC data to identify single-bit errors and corrects them on the fly, preventing unplanned system shutdowns.

  In the rare event of multiple-bit errors, the system controller detects the error and triggers a system notification to prevent bad data from corrupting further operations.

  You can set the Server Monitor software to alert you if error rates exceed the defined threshold.
- Xserve has built-in hardware RAID mirroring, which protects your server from failing if the main drive fails.

For more information about Xserve, visit www.apple.com/xserve/.

Using Backup Power

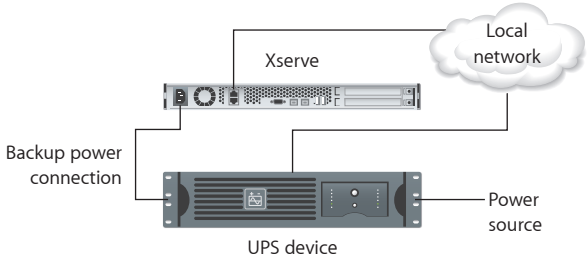
In the architecture of a server solution, power is a single point of failure. If power goes out, your servers go down without warning. To prevent a sudden disruption in services, consider adding a backup source of power.

Depending on your application, you might choose to use a standby electrical generator or Uninterruptible Power Supply (UPS) devices to gain enough time to notify users of an impending shutdown of services.

Using UPS with Xserve

Xserve does not provide serial port connectivity to UPS, but it can monitor UPS power through the network if the UPS unit has a management network card. For more information, check with UPS vendors.

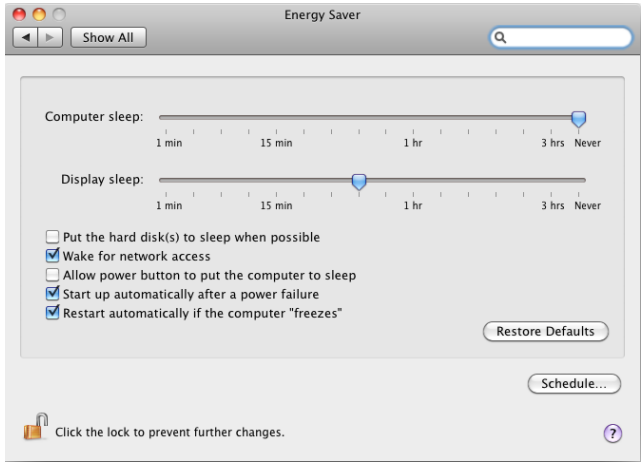
The following illustration is an example of an Xserve connected to a UPS via a network:



Setting Up Your Server for Automatic Restart

You can set up Energy Saver options on your Mac OS X Server computer to automatically restart if it goes down due to a power failure or system freeze.

The following is the Energy Saver panel of System Preferences:



The automatic restart options are:

- **Restart automatically after a power failure.** The power management unit automatically starts up the server after a power failure.
- **Restart automatically if the computer freezes.** The power management unit automatically starts up the server after the server stops responding, has a kernel panic, or freezes.

When you select the option to restart after a freeze, Mac OS X Server spawns the `watchdogtimerd` daemon, which every 30 seconds commands your computer to restart after 5 minutes.

Each time the command is sent, the restart timer is reset. Thus, the timer won't reach 5 minutes as long as the server is running. If the computer freezes, the power management unit restarts it after 5 minutes.

To enable automatic restart:

1. Log in to the server as an administrator.
2. Open System Preferences and click Energy Saver.
3. Select restart options.
4. Close System Preferences.

Ensuring Proper Operational Conditions

One factor that can cause your servers to malfunction is overheating. This is especially a problem when you cluster computers in a small space. Other factors such as humidity and power surges can also adversely impact your server.

To protect your servers, make sure you house them in a place where you can control these factors and provide ideal operating conditions. Check the electrical and environmental requirements for your systems to find what these conditions are.

In addition, make sure the facility you deploy your server has a fire alarm, and prepare a contingency plan to deal with this risk.

Providing Open Directory Replication

If you plan to provide Open Directory services, consider creating replicas of your Open Directory master. If the master server fails, client computers can access the replica.

Link Aggregation

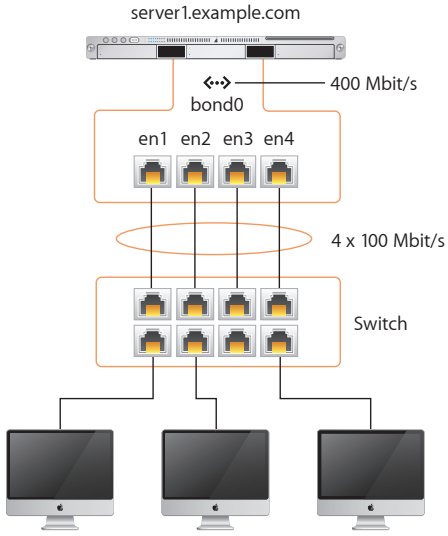
Although not common, the failure of a switch, cable, or network interface card can cause your server to become unavailable. To eliminate these single points of failure, you can use link aggregation or trunking. This technology, also known as IEEE 802.3ad, is built into Mac OS X and Mac OS X Server.

Link aggregation allows you to aggregate or combine multiple physical links connecting your Mac to a link aggregation device (a switch or another Mac) into a single logical link. The result is a fault-tolerant link with a bandwidth equal to the sum of the bandwidths of the physical links.

For example, you can set up an Xserve with four 1-Gbit/s ports (en1, en2, en3, and en4) and use the Network pane of System Preferences to create a link aggregate port configuration (bond0) that combines en1, en2, en3, and en4 into one logical link.

The resulting logical link will have a bandwidth of 4 Gbit/s. This link also provides fault tolerance. If a physical link fails, your Xserve's bandwidth will shrink, but the Xserve can still service requests as long as not all physical links fail at once.

The following illustration shows four Ethernet ports aggregated as a single interface:



Link aggregation also allows you to take advantage of existing or inexpensive hardware to increase the bandwidth of your server. For example, you can form a link aggregate from a combination of multiple 100-Mbit/s links or 1-Gbit/s links.

About the Link Aggregation Control Protocol (LACP)

IEEE 802.3ad Link Aggregation defines a protocol called Link Aggregation Control Protocol (LACP) that is used by Mac OS X Server to aggregate (combine) multiple ports into a link aggregate (a virtual port) that can be used for TCP and UDP connections.

When your define a link aggregate, the nodes on each side of the aggregate (for example, a computer and a switch) use LACP over each physical link to:

- Determine whether the link can be aggregated
- Maintain and monitor the aggregation

If a node doesn't receive LACP packets from its peer (the other node in the aggregate) regularly, it assumes that the peer is no longer active and removes the port from the aggregate.

In addition to LACP, Mac OS X Server uses a frame distribution algorithm to map a conversation to a specific port. This algorithm sends packets to the system on the other end of the aggregate only if packet reception is enabled. In other words, the algorithm won't send packets if the other system isn't listening.

Mapping a conversation to a specific port guarantees that packet reordering does not occur.

Link Aggregation Scenarios

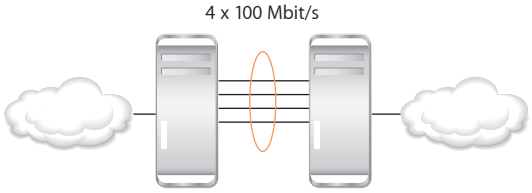
Following are three common aggregation scenarios that you can set up:

- Computer to computer
- Computer to switch
- Computer to switch-pair

These scenarios are described in the following sections.

Computer to Computer

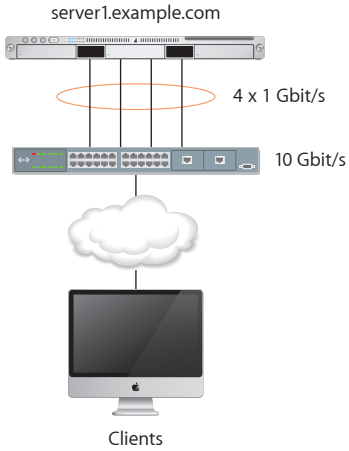
In this scenario, you connect the servers directly (as shown in the following illustration) using the physical links of the link aggregate.



This allows the two servers to communicate at a higher speed without the need for a switch. This configuration is ideal for ensuring back-end redundancy.

Computer to Switch

In this scenario shown in the following illustration, you connect your server to a switch configured for 802.3ad link aggregation.



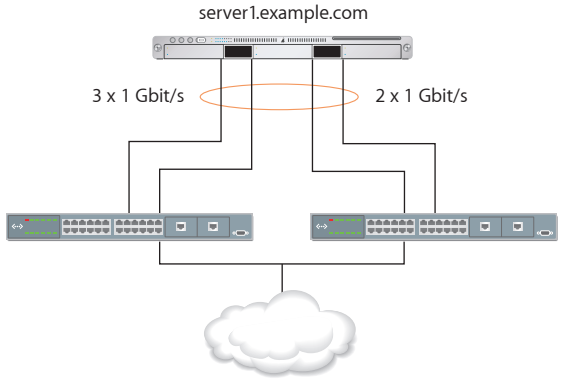
The switch should have bandwidth for handling incoming traffic equal to or greater than that of the link aggregate (logical link) you define on your server.

For example, if you create an aggregate of four 1-Gbit/s links, you should use a switch that can handle incoming traffic (from clients) at 4 Gbit/s or more. Otherwise, the increased bandwidth advantage in the link aggregate won't be fully realized.

Note: For information about how to configure your switch for 802.3ad link aggregation, see the documentation provided by the switch manufacturer.

Computer to Switch-Pair

In this scenario shown in the following illustration, you improve on the computer-to-switch scenario by using two switches to eliminate the switch as a single point of failure:



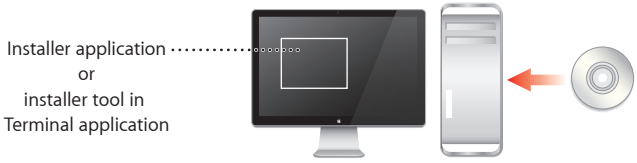
For example, you can connect two links to the master switch and the remaining links to the backup switch. As long as the master switch is active, the backup switch remains inactive. If the master switch fails, the backup switch takes over transparently.

Although this scenario adds redundancy that protects the server from becoming unavailable if the switch fails, it results in decreased bandwidth.

Setting Up Link Aggregation in Mac OS X Server

To set up your Mac OS X Server for link aggregation, you need a Mac with two or more IEEE 802.3ad-compliant Ethernet ports. In addition, you need at least one IEEE 802.3ad-compliant switch or another Mac OS X Server computer with the same number of ports.

You create a link aggregate on your computer in the Network pane of System Preferences.



To create a link aggregate:

1. Log in to the server as an administrative user.
2. Open System Preferences.
3. Click Network.
4. Click the Gear button and choose Manage Virtual Interfaces in the pop-up menu.
5. Click the Add (+) button, and select New Link Aggregate in the pop-up menu.

   Note: You only see this option if you have two or more Ethernet interfaces on your system.
6. In the Name field, enter the name of the link aggregate.
7. Select the ports to aggregate from the list.
8. Click Create.
9. Click Done.

By default the system gives the link aggregate the interface name bond<*num*>, where <*num*> is a number indicating precedence. For example, the first link aggregate is named bond0, the second is bond1, and the third is bond2.

The interface name bond<*num*> assigned by the system is different from the name you give to the link aggregate port configuration. The interface name is for use at the command line, but the port configuration name is for use in the Network pane of System Preferences.

For example, if you enter the command `ifconfig -a`, the output refers to the link aggregate using the interface name and *not* the port configuration name:

```
bond0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
inet6 fe80::2e0:edff:fe08:3ea6 prefixlen 64 scopeid 0xc
inet 10.0.0.12 netmask 0xffffff00 broadcast 10.0.0.255
ether 00:e0:ed:08:3e:a6
media: autoselect (100baseTX <full-duplex>) status: active
supported media: autoselect
bond interfaces: en1 en2 en3 en4
```

You do not delete or remove a link bond from the Network Pane of System Preferences. You remove the bond through the Manage Virtual Interfaces sheet used to create the bond.

Monitoring Link Aggregation Status

You can monitor the status of a link aggregate in Mac OS X and Mac OS X Server using the Status pane of the Network pane of System Preferences.

To monitor the status of a link aggregate:

1. Open System Preferences.
2. Click Network.
3. From the list of network interfaces on the left, choose the link aggregate port virtual interface.
4. Click Advanced in the lower right side of the window.
5. Select the Bond Status tab.

   The Status pane displays a list containing a row for each physical link in the link aggregate. For each link, you can view the name of the network interface, its speed, its duplex setting, the status indicators for incoming and outgoing traffic, and an overall assessment of the status.

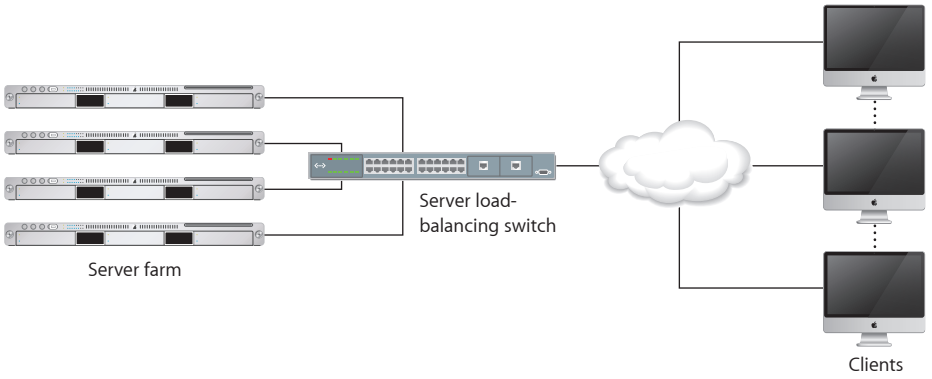
   Note: The Sending and Receiving status indicators are color-coded. Green means the link is active (turned on) and connected. Yellow means the link is active but not connected. Red means the link can't send or receive traffic.
6. To view more information about a link, click the corresponding entry in the list.

Load Balancing

One factor that can cause services to become unavailable is server overload. A server has limited resources and can service a limited number of requests simultaneously. If the server gets overloaded, it slows down and can eventually crash.

One way to overcome this problem is to distribute the load among a group of servers (a server farm) using a third-party load-balancing device. Clients send requests to the device, which then forwards the request to the first available server based on a predefined algorithm. The clients see only a single virtual address, that of the load-balancing device.

Many load-balancing devices also function as switches (as shown in the following illustration), providing two functions in one, which reduces the amount of hardware you need to use.



Note: A load-balancing device must be able to handle the aggregate (combined) traffic of the servers connected to it. Otherwise, the device becomes a bottleneck, which reduces the availability of your servers.

Load balancing provides several advantages:

- **High availability.** Distributing the load among multiple servers helps you reduce the chances that a server will fail due to server overload.
- **Fault tolerance.** If a server fails, traffic is transparently redirected to other servers. There might be a brief disruption of service if, for example, a server fails while a user is downloading a file from shared storage, but the user can reconnect and restart the file download process.
- **Scalability.** If demand for your services increases, you can transparently add more servers to your farm to keep up with demand.
- **Better performance.** By sending requests to the least-busy servers, you can respond faster to user requests.

Daemon Overview

By the time a user logs in to a Mac OS X system, a number of processes are running. Many of these processes are known as daemons. A daemon is a background process that provides a service to users. For example, the cupsd daemon coordinates printing requests, and the httpd daemon responds to requests for web pages.

Viewing Running Daemons

To see the daemons running on your system, use the Activity Monitor application (in /Applications/Utilities/). This application lets you view information about all processes, including their resource usage.

You will see the following daemons, regardless of what services are enabled:

- launchd (timed job and watchdog process)
- servermgrd (administration tool interface process)
- serialnumberd (license compliance process)
- mDNSresponder (local network service discovery process)

Using launchd for Daemon Control

Although some UNIX-like systems use other tools, Mac OS X Server uses a daemon called launchd to control process initialization and timed jobs.

The launchd daemon is the preferred alternative to the following common UNIX tools: init, rc, the init.d and rc.d scripts, SystemStarter, inetd and xinetd, atd, crond and watchdogd. All of these services should be considered deprecated and administrators are strongly encouraged to move process management duties to launchd.

There are two utilities in the launchd system: launchd daemon and launchctl utility.

The launchd daemon has also replaced init as the first process spawned in Mac OS X and is therefore responsible for starting the system at startup. The launchd daemon manages the daemons at both a system and user level. It can:

- Start daemons on demand
- Monitor daemons to make sure they keep running

Configuration files are used by launchd to define the parameters of services and daemons run. The configuration files are plist files stored in the LaunchAgents and LaunchDaemons subdirectories of the Library folders.

For more information about creating the launchd configuration files, see the following Developer Documentation page:

developer.apple.com/documentation/MacOSX/Conceptual/BPSystemStartup/Articles/LaunchOnDemandDaemons.html

The launchctl utility is the command-line tool used to control launchd. It can:

- Load and unload daemons
- Start and stop launchd controlled jobs
- Get system utilization statistics for launchd and its child processes
- Set environment settings

Monitoring Your System

8

Effective monitoring allows you to detect potential problems before they occur and gives you early warning when they occur.

Detecting potential problems allows you to take steps to resolve them before they impact server availability of your servers. In addition, getting an early warning when a problem occurs allows you to take corrective action quickly and minimize disruption to your services.

Planning a Monitoring Policy

Gathering data about your systems is a basic function of good administration. Different types of data gathering are used for different purposes:

- **Historical data collection:** Historical data is gathered for analysis. This could be used for IT planning, budgeting, and getting a baseline for normal server conditions and operations. What kinds of data do you need for these purposes? How long does it need to be kept? How often does it need to be updated? How far in the past does it need to be collected?
- **Real-time monitoring:** Real-time monitoring is for alerts and detecting problems as they happen. What are you monitoring? How often? Does that data tell you what you need to know? Are some of these real-time collections for historical purposes?
- **Debugging:** Recurring problems can be analyzed and fixed if properly tracked. Even if you don't control source code, good debugging logs and data can increase the ability of the developer to address your issues. How can you capture what is going wrong? How often? Does that data tell you what you need to know? Are they problems you can fix on your end, or do you need vendor support?

Planning Monitoring Response

The response to your monitoring is as important as the data collection. In the same way a backup policy is pointless without a restore strategy, a monitoring policy makes little sense without a response policy.

Several factors can be considered for a monitoring response:

- What are relevant response methods? In other words, how will the response take place?
- What is the time to response? What is an acceptable interval between failure and response?
- What are the scaling considerations? Can the response plan work with all expected (and even unexpected) frequencies of failure?
- Are there testing monitoring systems in place? How do you know the monitoring policy is catching the data you need, and how do you know the responses are timely and appropriate? Have you tested the monitoring system recently?

Using with Server Status Widget

The Server Status Dashboard widget is provided for quick access and information about a single system. The Server Status widget lets you monitor Mac OS X Server v10.6 activity from any computer with Mac OS X v10.6. Server Status shows you graphs of processor activity, network load, disk usage, and whether the service is polled hourly, daily, or weekly.

You can also see up to six running services and their status reports. By clicking on the service, you can open Server Admin to the related service overview panel.

To configure the Server Status widget:

1. Add the widget to the Dashboard like any other widget.
2. Enter the server IP address or domain name.
3. Supply an administrative or monitoring login name and password.
4. Click Done.

To change the server address, login name, or password, click the information button (i) at the top of the widget and change the settings.

Using Server Monitor

The Server Monitor application can issue alerts via mail, cell phone, or pager notification as soon as it detects critical problems. Built-in sensors detect and report essential operating factors like power, temperature, and the condition of several key components.

The Server Monitor interface allows you to quickly detect problems. In the main window, Server Monitor lists each server on a separate line, with temperature information and the status of each of its components, including fans, disk drives, memory modules, power supplies, and Ethernet connections.

A green status indicator shows the component is OK, a yellow status indicator notes a warning, and a red status indicator notes an error.

Server Monitor works for Xserves only. For more information about Server Monitor, choose Server Monitor Help from Server Monitor's Help menu.

Using RAID Admin for Server Monitoring

Like Server Monitor, you can configure RAID Admin to send a mail or a page when a component is in trouble. For every unit, RAID Admin displays the status of the unit and each of its components, including disk drives, fibre channel, and network connections.

RAID Admin uses green, yellow, or red status indicators. You can also configure it to send you a mail or a page when a component is in trouble.

In addition, RAID Admin provides you with an overview of the status of the Xserve RAID units that appear in the main window.

For more information about RAID Admin, choose RAID Admin Help from RAID Admin's Help menu.

Using Console for Server Monitoring

Use Console to monitor relevant log files for potential problems that might cause your server to fail.

For example, you can monitor your web server's /var/log/httpd/access_log file for signs of denial of service (DoS) attacks. If you detect these signs, you can immediately implement a planned response to prevent your web server from becoming unavailable.

To improve your log monitoring efficiency, consider automating the monitoring process using AppleScript or Terminal commands like `grep` and `launchd`.

Using Disk Monitoring Tools

Running out of disk space can cause your server to become unreliable and probably fail. To prevent this from happening, you must constantly monitor disk space usage on your servers and delete or back up files to clear disk space.

Mac OS X Server ships with a number of command-line tools to monitor disk space on your computer:

- `df`. This command tells you how much space is used and how much is available on every mounted volume.

  For example, the following command lists local volumes and displays disk usage:

```
df -Hl
Filesystem Size Used Avail Capacity Mounted on
/dev/disk0s9 40G 38G 2.1G 95% /
```

In this example, the hard disk is almost full with only 2.1 GB left. This tells you that you should act immediately to free space on your hard disk before it fills up and causes problems for your users.

- `du`. This command tells you how much space is used by specific folders or files.

  For example, the following command tells you how much space is used by each user's home folder:

  ```
  sudo du -sh /Users/*
  3.2M /Users/Shared
  9.3M /Users/omar
  8.8M /Users/jay
  1.6M /Users/lili
  ```

  Knowing who's using most of the space on the hard disk lets you contact users and have them delete unused files.

  Note: With Workgroup Manager, you can set disk quotas for users and generate disk usage reports.

- `diskspacemonitor`. This command lets you automate the process of monitoring disk space usage. When the amount of free disk space drops below the level you specify, `diskspacemonitor` executes shell scripts that send you a notification. This command defines two action levels:
  - Alert—Sends you a warning message when disk space usage reaches 75%.
  - Recover—Archives rarely used files and deletes unneeded files when disk space usage reaches 85%.

For more information about these commands, see the corresponding man page.

Using Network Monitoring Tools

Degradation in network performance or other network problems can adversely affect the availability of your services. The following network monitoring tools can alert you to problems early, so you can take corrective action to avoid or minimize down time.

- To monitor network activity, use the `tcpdump` utility in Mac OS X Server. This utility prints the headers of incoming and outgoing packets on a network interface that match specified parameters.

  Using `tcpdump` to monitor network traffic is especially useful when trying to detect denial of service (DoS) attacks. For example, the following command monitors incoming traffic on port 80 on your computer:

  ```
  sudo tcpdump -i en0 dst port 80
  ```

If you detect an unusual number of requests coming from the same source, use Firewall service to block traffic from that source.

For more information about `tcpdump`, see the corresponding man page.

- Consider using Ruby, Perl, shell scripts, or AppleScript to automate the monitoring process. For example, using `tcpdump` to monitor traffic can be time consuming, so automation is necessary.
- Consider using Ethereal, an X11 open source packet sniffing tool that you can run in the X11 environment on Mac OS X Server. Unlike `tcpdump`, this tool has a graphical user interface and a set of powerful network analysis tools.

  For more information about Ethereal, see www.ethereal.com/.
- You can use other third-party tools that automatically analyze network traffic and alert you to problems.

Using Server Status Notification in Server Admin

Server Admin has an easy to use notification system that can keep you informed of your server's hard disk status, software status, and certificate status. Server Admin will send a mail to any address (local or not) when:

- There is less than a specified percentage of free space left on any system hard disk.
- Software Update packages are available from Apple for the server.
- A certificate has expired or will soon expire.

To use the email functionality, the server starts SMTP. Make sure the firewall allows SMTP traffic from the server.

To set a notification:

1. Open Server Admin.
2. Select a server, click the Settings button in the toolbar, and then click the Notifications tab.
3. Below the "Addresses to notify" field, click the Add (+) button and add an address.
4. Repeat as needed, then click Save.

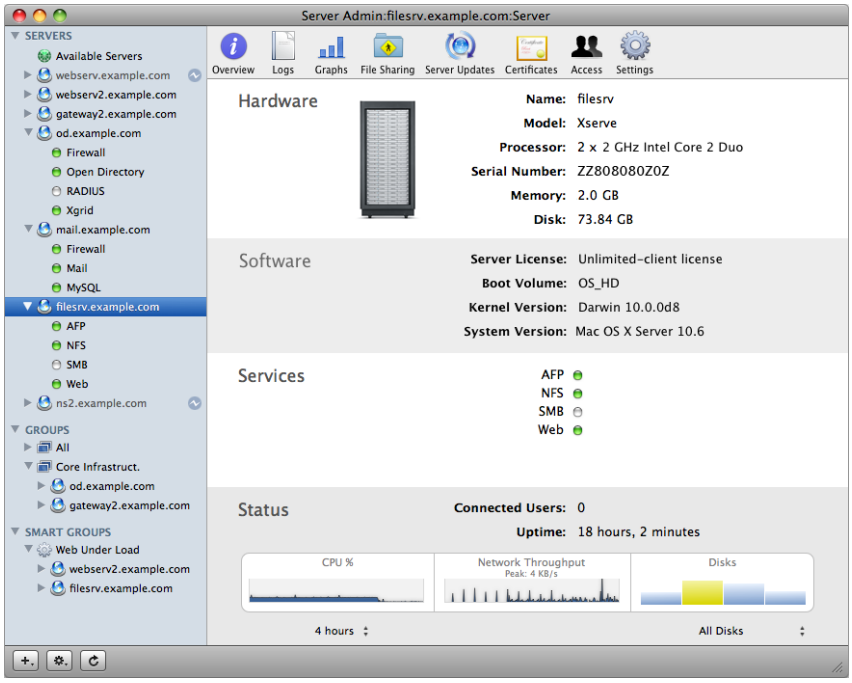
Monitoring Server Status Overviews Using Server Admin

Server Admin has several ways to see a status overview, from detailed information for a single server to a simplified overview for many servers.

To see a status overview for one server:

- Select a server in the Server list.

The following shows a sample Overview pane for a single server.



This overview shows basic hardware, operating system versions, active services, and graphs of CPU history, network throughput history, and disk space.

- Use the `serveradmin` XML web interface.

  a Open Safari to the following URL:

  https://<server address>:311/servermgr_info.html

  b Select getState from the pop-up menu.

  c Click Send Command.

  The web page returns an XML text version of the server overview.

Using Remote Kernel Core Dumps

A kernel panic is a type of error that occurs when the core (kernel) of an operating system receives an instruction in an unexpected format or when it fails to handle properly. A kernel panic can also follow when the operating system can't recover from a different type of error. A kernel panic can be caused by damaged or incompatible software or, more rarely, damaged or incompatible hardware.

When a server kernel panics it abruptly halts all normal system operations. Usually, a kernel process named `panic()` outputs an error message to the console and stores debugging information in nonvolitile memory to be written to a crash log file upon restarting the computer. Saving the memory contents of the core and associated debugging information is called a "core dump."

This debugging information is highly technical, but system administrators can use this information to:

- Record details about machines that are panicking and why.

  For example, if you manage a large number of Mac OS X Servers, you might want to monitor which servers are panicking and why. You can use this information to determine how frequently kernel panics occur, whether there are common symptoms, and, most importantly, whether third-party kernel extensions are involved.

- Perform offline debugging on high-availability systems.

  If you manage a high-availability server and you have problems with server panicking, you can capture a kernel core dump, immediately restart the server, and then debug the problem without interrupting service.

  For more information on debugging core dumps see Developer Technical Note #2118 at developer.apple.com/technotes/tn2004/tn2118.html#SECDEBUG.

You can configure a Mac OS X Server computer so that, when the machine panics, it transmits a core dump of the kernel to a remote core dump server via TCP/IP. The core dump server uses a daemon to collect the kernel core dump from the client and writes it to a file on the hard disk. You can then analyze the core dump using a variety of tools, most notably GDB.

CAUTION: The core dump of kernel memory is sent to the server in the clear. It's possible that this data might include sensitive information. Therefore, configure your network so this data can't be seen by unauthorized persons. For example, use switched hubs, a firewall, or a VPN.

To use a FireWire connection to transmit a core dump (a useful alternative when the kernel panic on the client involves the built-in Ethernet driver or some other network code), see the Read Me file in the FireWire SDK for Mac OS X that describes the setup process for using FireWire to transmit a core dump.

The following sections contain information to set up a remote listening server, which receives core dump information from panicked computers, and to set up a server to send its core dump information to the remote listening server via TCP/IP over Ethernet.

Setting Up a Core Dump Server

You can use any Mac OS X v10.5 or later computer to be a core dump server that fits the following criteria. The core dump server must:

- Have a static IP address.
- Be IPv4 network-accessible to all clients using UDP port 1069.

  You cannot put the core dump server behind a firewall or NAT unless all clients using it are also behind it. You cannot use IPv6-only addresses for the server.
- Have enough disk storage space for multiple dumps.

  In general, core dumps are large. Core dumps can be as small as 200 MB to 500 MB but they can be much larger, depending on the kernel map size, physical memory size, memory usage during the panic, and other factors. Make sure you have enough free disk space.

To set up a core dump server on a computer running a system earlier than Mac OS X v10.5, more extensive configuration is needed. See Developer Technical Note #2118at developer.apple.com/technotes/tn2004/tn2118.html.

Setting up a core dump server:

1. Create a core dump directory named "PanicDumps," owned by user "root," and group "wheel," which is writable by everyone.

   Using the command line, type:

   ```
   sudo mkdir /PanicDumps
   sudo chown root:wheel /PanicDumps
   sudo chmod 1777 /PanicDumps
   ```
2. Activate the core dump server process (kdumpd).

   Using the command line, type:

   ```
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.kdumpd.
        plist
   ```

   After this command is executed, the core dump server process starts. This step does not need to be repeated when the server restarts.
3. Verify that the core dump server process is running.

   Using the command line, type:

   ```
   sudo launchctl list | grep kdump
   ```

   The result should list com.apple.kdumpd.
4. Make sure UDP port 1069 is open for core dump connections.

   When the core dump server is active, configure Mac OS X computers as clients to send their kernel panic information to this server. See "Setting Up a Core Dump Client" on page 179.

Setting Up a Core Dump Client

A core dump client sends its kernel panic debug information to the core dump server address specified in its NVRAM settings.

The information is transmitted at the time of the panic, so before restarting the computer, allow some time for the data to be sent to the server. The time necessary depends on the file size of the core dump and the speed of the network connection between the client and server.

For clients using v10.5 or earlier, see developer.apple.com/technotes/tn2004/tn2118.html.

Setting up a core dump client:

1. Modify the "boot-args" NVRAM variable to include the "debug" flag 0x0400, and the "_panicd_ip" flag with the IP address of the core dump server.

   The following example uses the core dump server IP address 192.168.1.250. Substitute the IP address of your own core dump server.

   ```
   sudo nvram boot-args="debug=0x0400 _panicd_ip=192.168.1.250"
   ```

   Important: You can reset the boot-args NVRAM variable whenever you install new system software, including software updates, and when you change the startup disk using System Preferences.

2. If the core dump client is running Mac OS X Server, modify the watchdogtimerd behavior to either keep it from restarting the server before the core dump is complete, or modify the amount of time it waits before restarting the server.

   To disable automatic restarting, turn off the "Restart automatically after a power failure" option in the Options tab of the Energy Saver System Preferences pane.

   To increase the amount of time before automatic restarting, add a "count" program argument larger than 6 (but smaller than 480) to the `watchdogtimerd` configuration file at /System/Library/LaunchDaemons/com.apple.watchdogtimerd.plist.

   For more information about the arguments and options, see the `watchdogtimerd(8)` man page.

3. Restart the computer for the settings to take effect.

   For additional NVRAM debug flags that are useful in core dump debugging, see Developer Technical Note #2118, subsection "Debug Flags in Depth,"at developer.apple.com/technotes/tn2004/tn2118.html

Configuring Common Core Dump Options

By default, core dumps happen using UDP port 1069 over the built-in Ethernet (en0) interface, and the resulting files are stored in /PanicDumps on the core dump server. However, you can configure the core dump to use:

- An alternate UDP port
- An alternate network interface
- An alternate file destination
- A specific network router

Changing any of these options requires that you restart the computers to reload the new settings. All settings assume the core dump client and the core dump server are using Mac OS X v10.5 or later.

Option	Action
To set an alternate UDP port...	On the core dump server, change the SockServiceName string property from 1069 to the desired port in /System/Library/LaunchDaemon/com.apple.kdump.plist. On the core dump client, add the `_panicd_port` flag to the NVRAM `boot-args`. For example, to change it to UDP port 12345, add "_panicd_port=12345" to the list of `boot-args` flags.
To set an alternate network interface...	On the core dump client, add the `kdp_match_name` flag to the NVRAM `boot-args`. For example, to change it to always use en1, add "kdp_match_name=en1" to the list of `boot-args` flags after the `_panicd_ip` flag. AirPort interfaces cannot be used to transmit core dumps.
To set an alternate file destination...	On the core dump server, change the expected directory location in the /System/Library/LaunchDaemons/com.apple.kdumpd.plist file, ProgramArguments string, then reload the kdumpd process.
To specify a network router...	On the core dump client, add the `_router_ip` flag to the NVRAM `boot-args`. For example, to change it to use the router 10.0.0.1, add "_router_ip=10.0.0.1" to the list of `boot-args` flags after the `_panicd_ip` flag.

To change the location of the core dump directory, change the expected directory location in the com.apple.kdumpd.plist file, then reload the process.

About Simple Network Management Protocol (SNMP)

SNMP is a common protocol for monitoring the status of network equipment (for example, routers and smart switches), computers, and other networkable devices like Uninterruptable Power Supplies. Mac OS X Server uses Net-SNMP to implement SNMP v1, SNMP v2c, and SNMP v3 using IPv4 and IPv6.

SNMPv2 is the default access protocol and the default read-only community string is "public."

Enabling SNMP reporting

SNMP access isn't enabled by default on Mac OS X Server. To use SNMP tools to poll your Mac OS X Server for data, you must configure and then enable the service.

To enable SNMP

1. Open Server Admin.
2. Select a server, click the Settings button in the toolbar, and then click the General tab.
3. Select Network Management Server (SNMP).
4. Click Save.

   When SNMP is active, anyone with a route to the SNMP host can collect SNMP data from it.
5. Configure the basic SNMP parameters from the command line.

   The SNMP process will not start until /etc/snmpd.conf is configured for the current site. To configure, see "Configuring snmpd" on page 181.

   Note: The default configuration of snmpd uses privileged port 161. For this reason and others, it must be executed by root or using setuid. Only use setuid as root if you understand the ramifications. If you do not, seek assistance or additional information. Flags available for snmpd will change the uid and gid of the process after it starts. For more information, see the snmpd man page.

Configuring snmpd

The configuration (.conf) file for snmpd is typically at /etc/snmpd.conf. If you have an environment variable SNMPCONF, snmpd will read any files named snmpd.conf and snmpd.local.conf in these directories. The snmpd process can be started with a -c flag to indicate other conf files. For more information about which conf files can be used, see the snmpd man page.

Configuration files can be created and installed more elegantly using the included script /usr/bin/snmpconf. As root, use this script with the -i flag to install the file at /usr/share/snmp/. Otherwise, the default location for the file to be written is the user's home folder (~/). Only root has write permission for /usr/share/snmp/.

Because snmpd reads its configuration files at startup, changes to configuration files require that the process be stopped and restarted. You can stop snmpd with ProcessViewer or at the command line (`kill -HUP <pid>`).

To enable and configure SNMP:

- Use the /usr/bin/snmpconf command, which takes you through a basic text-based setup assistant for configuring the community name and saves the info in the configuration file.

  The snmp config file is located in /usr/share/snmp/snmpd.conf.

SNMP Configuration Example

Step 1: Customize data

1. To customize the data provided by snmpd, add an snmpd.conf file using /usr/bin/snmpconf as root or using sudo, by executing this command:

   ```
   /usr/bin/snmpconf -i
   ```

   If there are existing configuration files, you can read them into the assistant and incorporate their contents with the output of the assistant.

2. Choose to read-n the file by indicating the file at /etc/snmp/snmpd.conf.

   You then see a series of text menus.

3. Make these choices in this order:

   a. Select file: 1 (snmpd.conf).

   b. Select section: 5 (System Information Setup).

   c. Select section: 1 (The [typically physical] location of the system.).

   d. The location of the system: type text string here — such as "server_room."

   e. Select section: f (finish).

   f. Select section: f (finish).

   g. Select File: q (quit).

   You have created an snmpd.conf file with a creation date of today.

   To verify its creation enter `ls -l /usr/share/snmpd.conf`.

Step 2: Restart snmpd to take changes

1. Open Server Admin.
2. Select a server, click the Settings button in the toolbar, and then click the General tab.
3. Deselect Network Management Server (SNMP).
4. Click Save.

   You can also do this via the command line by killing and restarting the smnpd process as root:

   ```
   /usr/sbin/snmpd
   ```

Step 3: Collect SNMP information from the host

- To get the SNMP-available information you added, execute this command from a host that has SNMP tools installed:

```
/usr/bin/snmpget -c public <hostname> system.sysLocation.0
```

Replace <hostname> with the name of the target host.

You should see location you provided. In this example, you would see:

```
SNMPv2_MIB::system.sysLocation.0 = STRING:\"server_room\"
```

The other options in the menu you were working in are:

```
/usr/bin/snmpget -c public <hostname> system.sysContact.0
/usr/bin/snmpget -c public <hostname> system.sysServices.0
```

The final .0 indicates you are looking for the index object. The word public is the name of the SNMP community that you did not alter.

If you need information about either of these or if you need explanations of SNMP syntax, tutorials are available at net-snmp.sourceforge.net.

Additional Information about SNMP

Additional information about SNMP can be found here.

Man pages

Entering `man -k snmp` in the Terminal will provide a list of the known man pages.

Web sites

The Net SNMP-Project:

- www.net-snmp.org
- net-snmp.sourceforge.net

Books

Essential SNMP by Douglas Mauro, Kevin Schmidt

Publisher: O'Reilly (Second Edition Sept 2005)

ISBN: 0-596-00840-6, 460 pages

Tools to Use with SNMP

In addition to snmpget, other SNMP tools are installed, and third-party suites (free and commercial) are available with varying complexity and reporting.

About Notification and Event Monitoring Daemons

To monitor and log system events, the operating system runs several daemons that intercept application messages and log them or act on them.

There are two main notification daemons: syslogd and emond.

- **syslogd:** The syslogd daemon is a standard UNIX method of monitoring systems. It logs messages in accordance with the settings found in /etc/syslog.conf. You can examine the output files specified in that configuration by using a file printing or editing utility because they are plain text files. Administrators can edit these settings to fine-tune what is being monitored.

  Many administrators will tail or scrape the log file, meaning they will have scripts parse the log files and perform some action if a designated bit of information is present in the log. These home-grown notifications vary in quality and usefulness and are tailored to the script-writer's specific needs.

  You can configure the syslogd daemon to send and receive log file information to or from a remote server (by editing /System/Library/LaunchDaemons/com.apple.syslogd.plist). This is not recommended because syslogd does not use secure means to send log messages across the net.

- **emond:** The emond daemon is the event monitoring system for Mac OS X Server v10.6. It is a unified process that handles events passed from other processes, acts on the events as designated in a defined rule set, and then notifies the administrator.

  Currently, emond is the engine used for Server Admin's mail notification system. It is not used for Server Monitor's notifications.

  The high-level service receives events from the registered client, analyzes whether the event requires handing based on rules provided by the service at the time it was registered and, if handling is required, the action related to that event is performed. To accomplish this the emond daemon has three main parts: the rules engine, the events it can respond to, and the actions it can take.

  The emond rules engine works in the following manner. It:

  - Reads the config info from /etc/emond.d/emond.conf.
  - Reads in the rules from plist files in the /etc/emond.d/rules/ directory.
  - Processes the startup event.
  - Accepts events until terminated.
  - Processes the rules associated with the event, triggering as needed.
  - Performs actions specified by the rules that were triggered.
  - Runs as the least privileged possible (nobody).

WARNING: The file formats and settings in emond.conf and rules plists are not documented for customer use. Tampering could result in an unusable notification system and is unsupported.

Logging

Mac OS X Server maintains standard UNIX log files and Apple-specific process logs. Logs for the OS can be found in:

- /var/log
- /Library/Logs
- ~/Library/Logs

Each process is responsible for its own logs, the log level, and verbosity. Each process or application can write its own log file or use a system standard log, like syslog. You can use the Console application (in /Applications/Utilities) to read these and other plain-text log files regardless of location.

The logs are set to roll (compress and rename the log file) every 5 MB.

Most services in Mac OS X Server have a logging pane in Server Admin. You can use these panes to set logging levels and view the logs for any particular service.

Syslog

The system log, syslog, is a consolidated catch-all location for process log messages. syslog has several levels of available log detail. If you select low detail logging, detailed messages are not saved, but high detail logging results in large and possibly unhelpfully large log files.

The level of logging you use for syslog can be tuned by process and should be relevant to the level necessary for successful notification and debugging.

Syslog log levels (in ascending order from least to most detail)

Level name	Level indicator in syslog.conf	Amount of detail
None	.none	None
Emergency	.emerg	Least
Alert	.alert	
Error	.err	
Warning	.warn	
Notice	.notice	
Info	.info	
Debug	.debug	Most

Syslog Configuration File

The Syslog configuration file can be found at /etc/syslog.conf. Each line has the following format:

<facility>.<loglevel> <path to logfile>

Replace <facility> with the process name writing to the log. The path is the standard POSIX path to the log file. You can use asterisks (*) as wildcards. For example, the setting for the kernel is:

```
kern.* /var/log/system.log
```

This shows that all messages to the log of all levels from the kernel are to be written in the file /var/log/system.log.

Likewise, the following setting is an example of all emergency messages from all processes being sent to a custom emergencies log file:

```
*.emerg /var/log/emergencies.log
```

Directory Service Debug Logging

If you are using Open Directory and you want debugging information from directory services processes, you must use a different logging method than systemlog. You must enable debug logging for the process manually. When enabled, this debug logging writes messages to the log file at:

/Library/Logs/DirectoryService/DirectoryService.debug.log

You must perform the following commands with superuser permissions (sudo or root):

To manually turn on/off debug logging for directory services:

```
killall -USR1 DirectoryService
```

To start debugging at startup:

```
touch /Library/Preferences/DirectoryService/.DSLogAPIAtStart
```

Note: The debug log is not self-documented and is not intended for normal logging. It is very verbose and very opaque. It shows API calls, plugin queries, and responses.

Open Directory Logging

The configuration file can be found at /etc/openldap and the logs are found in/var/log/slapd.log. Each directory transaction generates a separate transaction log in the OpenLDAP databse. The database and transaction logs can be found at/var/db/openldap/openldap-data.

The slapd process, which governs Open Directory usage, has an additional parameter for extra logging. The following command enables the additional logging:

```
slapconfig -enableslapdlog
```

To run slapd in debugging mode:

1. Stop and remove slapd from launchd's watch list:

```
launchctl unload /System/Library/LaunchDaemons/org.openldap.plist
```

2. Restart slapd in debug mode:

```
sudo /usr/libexec/slapd -d 99
```

AFP Logging

The server side of Apple File Service Protocol (AFP) keeps track of access and errors, but it does not have much debugging information. However, you can add client-side logging to AFP clients to help monitor and troubleshoot AFP connections.

To enable client-side logging:
Perform all these actions on the AFP client computer.

1. Set the client debug level (levels 0-8):

```
defaults write com.apple.AppleShareClientCore -dict-add afp_debug_level 4
```

2. Set the client log message recipient (in this case, syslog):

```
defaults write com.apple.AppleShareClientCore -dict-add afp_debug_syslog
     1
```

3. Enable syslog to catch the debugging messages from the client.

   You do this by adding *.debug /var/log/debug.log to the syslogd.conf file.

4. Restart the syslog process.

Additional Monitoring Aids

You can use additional aids for monitoring Mac OS X Server. There are a number of third-party server monitoring packages, as well as an additional Apple monitoring tool.

The inclusion of third-party tools in the following list does not constitute an endorsement of or support for these products. They are listed for informational purposes only.

- **Apple Remote Desktop (ARD):** This software package contains many features that allow you to interact with, get reports on, and track computers running Mac OS X and Mac OS X Server. It has several powerful administration features and excellent reporting capabilities.
- **Nagios (third-party):** This tool is an open source computer system and network monitoring application.
- **Growl (third-party):** This tool is a centralized, extensible notification service that supports local and remote notification.

Push Notification Server

9

Provide increased server responsiveness to clients and reduce server load with Push Notification Server.

Mac OS X Server v10.6 uses an XMPP Pubsub architecture for the Push Notification Server. XMPP Pubsub is an open standard extention to XMPP (XEP-060) that allows servers and clients to communicate as needed, rather than clients continually asking the server for updates.

A service (like iCal or mail) maintains a simple connection with the client and the service informs the client that there is new data. This differs from previous methods, where calendar or mail clients contacted the server at regular intervals, requesting data, if present.

With the previous method of notification, the server must attend to each client, regardless of whether the client has data waiting for it. By using the new push method of client updating, only clients with new data are contacted, and only as needed.

About Push Notification Server

Mac OS X Server v10.6 push notification uses the same underlying technology as iChat server, but you don't need to run iChat on a computer that is running push notification.

Push notification is available for the following services:

- iCal Server
- Mail Server

Clients of these services must support push notification to make use of it. Apple's client applications on Mac OS X v10.6, and iPhone 3.0 client applications support push notification service. Third-party client applications may support it.

Mac OS X Server v10.6 push notification is not the same system as push notification for iPhone application development. You cannot use Mac OS X Server v10.6 to host iPhone application push notification.

Starting and Stopping Push Notification

When you start push notification on a server, the service broadcasts its availability on the local network to other services that support it. This means that when a different server turns on a service that supports push notification, the push notification server address populates the settings of the pushing service.

You must still enable Push Notification support for the pushing service before it works.

Additionally, you can choose to encrypt the data passed between the client and the push server by choosing an SSL certificate. This does not encrypt the data between the client and the pushing service. To encrypt transport between the pushing service and the client, enable SSL with the pushing service.

To enable Push Notification:

1. Use Server Admin to connect to the server.
2. Enable administration of Push Notification.

   This only needs to be done the first time you use Server Admin to administer the server.

   For more information about adding a service to the administered services list, see "Adding and Removing Services in Server Admin" on page 146.
3. From the list of administered services for the desired server, select Push Notification.
4. Click the "Start Push Notification" or "Stop Push Notification" as needed.

From the command line:

```
# setting Server Admin administration of push notification
sudo serveradmin settings info:serviceConfig:services:com.apple.
     ServerAdmin.Notification:configured = yes
# on the notification server
sudo serveradmin start notification
```

Changing a Service's Push Notification Server

If push notification is configured on the server, it is listed in the location on the service's settings pane. If another computer on the subnet is configured as a push notification server, it appears in the service's setting pane. You can use these instructions to specify a different server.

Each service that can use push notification must have push notification enabled, and can use a unique push notification server.

Important: Push notification servers should be cleared or removed from the service before changing the server's IP address or DNS name. You then re-enable push notification after the network identity has changed.

Be sure to make the relevant changes to your firewall to allow network access to the push notification server.

For more specific instructions, see each service's help.

To change the existing push notification server:

1. In Server Admin, select a server and choose the service.
2. Click the Settings button in the toolbar

   You might need to navigate to additional tabs, depending on the chosen service.
3. Select Remove near the push notification area.
4. In the new sheet, enter the host name of the push notification server, enter an administrator's name and password for the push notification server, and click Ok.
5. Click Save, then restart the service.

Index

D

P

Q

R

S

T