Open Directory

Apple's standards-based directory and network authentication services architecture.

Features

Scalable LDAP directory server
- OpenLDAP for providing standards-based access to centralized data
- Berkeley DB for scalable data storage and high-performance indexing
- Replication across multiple servers for maximum scalability and availability
- Tested scalability, supporting up to 200,000 user records

Integrated authentication authority
- MIT's Kerberos Key Distribution Center (KDC) authentication services
- Support for secure single sign-on to all Kerberos-enabled network resources
- SASL for negotiating strongest authentication to non-Kerberized services
- Centralized management and enforcement of password policies

Support for mixed-platform environments
- Login and authentication services for Mac, Windows, and Linux users
- Single directory record and password for each user—regardless of client platform

Easy to deploy and manage
- Server Admin utility for remote setup and administration of services
- Integrated tool for backing up and restoring directory and authentication databases
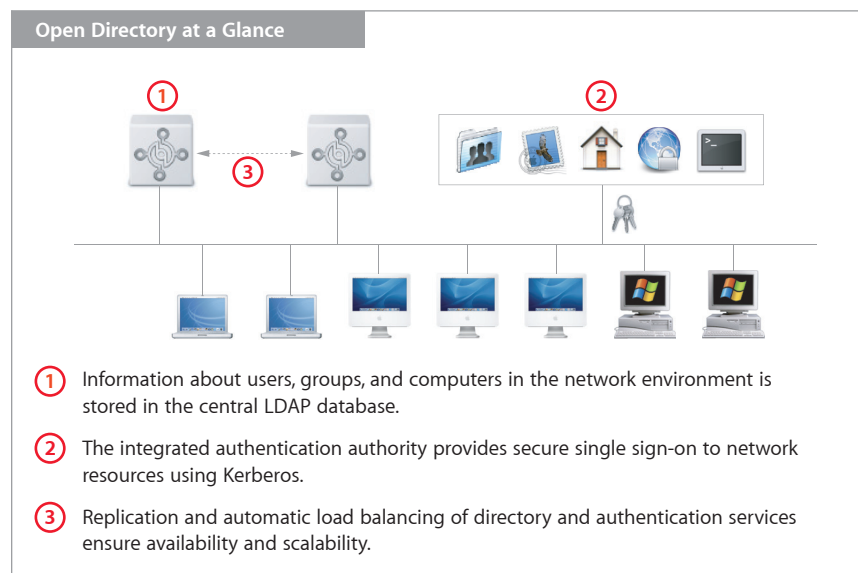- Innovative Workgroup Manager utility for creating and managing directory records

Compatible with existing infrastructure
- Integration with other LDAP servers and Active Directory
- Support for legacy directory services, including BSD configuration files, NIS, and NetInfo

Mac OS X Server includes Open Directory, Apple's standards-based directory and network authentication services architecture. A critical component of any modern network environment, directory services allow you to centralize information about users, groups, and computing resources in your organization. Maintaining this data in a central repository makes it possible for all servers on the network to access the same user accounts, settings, and authentication services. Directory services improve the security and manageability of your network environment, reducing administration costs.

Open Directory makes it easy to integrate Mac OS X client and server systems with your existing network infrastructure. The standards-based architecture provides compatibility with other LDAP servers and even with environments that use proprietary services such as Microsoft's Active Directory or Novell's eDirectory. And for organizations that haven't yet deployed centralized directory services, the Open Directory server in Mac OS X Server offers an easy-to-deploy solution that scales to meet the needs of virtually any network environment.

Combining powerful open source technologies—including OpenLDAP and Kerberos— with Apple's industry-leading administration tools, Open Directory delivers robust directory and authentication services that are extremely easy to set up and manage. And because there are no per-user or per-seat fees, Open Directory can scale with the needs of your organization—without draining your IT budget.

Open Directory at a Glance

① Information about users, groups, and computers in the network environment is stored in the central LDAP database.

② The integrated authentication authority provides secure single sign-on to network resources using Kerberos.

③ Replication and automatic load balancing of directory and authentication services ensure availability and scalability.

Why Deploy Directory Services?

By centralizing information about users and network resources, directory services provide the infrastructure required for managing users, groups, and computers on your network. Directory services can benefit organizations with as few as ten people and are essential for enterprise networks that have thousands of users. Deploying a directory server helps lower administrative costs, improve security, and provide users with a better, more productive computing experience.

Investment protection

The Open Directory architecture allows Mac OS X Server to work seamlessly in virtually any managed network environment, protecting the infrastructure investments you've already made. Using the built-in directory access modules, Mac OS X Server can read and write data stored in any LDAP server—even Microsoft's proprietary Active Directory. The server can also access records in legacy directories such as NIS, NetInfo, and local BSD configuration files (/etc).

Open Directory Server

The Open Directory server built into Mac OS X Server is ideal for organizations that haven't yet deployed a directory server, as well as for businesses and institutions migrating from expensive proprietary solutions. Based entirely on open standards, Open Directory offers robust LDAP services and a built-in authentication authority. And with Apple's innovative management tools and no per-user or per-seat licensing fees, it's also the easiest and most affordable way to deploy centralized directory and authentication services.

Open, standards-based solution

Apple has built the Open Directory server around OpenLDAP, the most widely deployed open source LDAP server, to deliver directory services for Mac and mixed-platform environments. LDAP provides a common language for directory access, enabling you to consolidate information from different platforms and define a single name space for all network resources. Whether you have Mac, Windows, or Linux systems on your network, you can set up and manage a single directory; you don't need to maintain a separate server or separate user records for each platform. This also streamlines the user experience: Users can authenticate to Mac OS X Server and access network resources using a single password, from any platform.

Why LDAP?

First released in 1995 and implemented by key vendors such as IBM and Sun, LDAP enables organizations to consolidate administrative information across platforms using a single name space for all network resources. This is a major improvement over proprietary directory services designed for a specific computing platform (such as NIS and NIS+ for UNIX systems or Active Directory for Windows systems), which define data according to unique, incompatible protocols. The open, extensible nature of LDAP is largely responsible for the widespread adoption of data centralization in heterogeneous network environments.

Strong single sign-on authentication

A robust authentication authority using MIT's Kerberos Key Distribution Center (KDC) is built into the Open Directory server. Kerberos provides strong authentication with the convenience of single sign-on. That means users need authenticate only once, with a single user name and password pair, for access to a broad range of Kerberos-enabled network services. For services that have not been "Kerberized," the integrated SASL service automatically negotiates the strongest-possible authentication protocol.

Reliability and scalability. To store directory information, the Open Directory server uses Berkeley DB, one of the world's most scalable databases, for high-performance indexing of hundreds of thousands of user records. The open standard LDAP and Kerberos technologies make it easy to add clients from any platform and services from many vendors. In addition, a robust replication feature maximizes availability and scalability. By creating replicas of directory and authentication servers, you can easily maintain failover servers for high availability, as well as remote servers for fast client interaction on distributed networks.

Easy setup and management

In addition to simplifying setup of directory and authentication services, Mac OS X Server features powerful administrative tools that make it easy to define and manage directory information. Using the innovative Workgroup Manager application, you can easily set up user accounts, define access privileges, and manage computing resources. Workgroup Manager works with the Open Directory server or any other LDAP solution to access and store user, group, and computer information.

Deploying Open Directory Services

When you install Mac OS X Server, Setup Assistant takes you through the configuration process. With just a few simple steps, you can configure directory and authentication services for your network.

After setup, you can use the Server Admin utility to set up replication services, manage Kerberos authentication and password policies, and monitor Open Directory access and error logs.
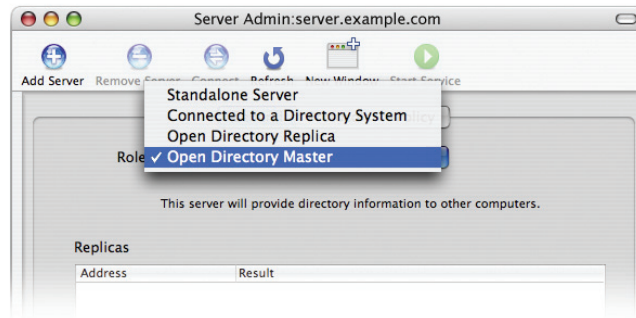
The Directory Access application allows you to further refine the server's directory configuration, if necessary. For example, you can set up connections with multiple directory domains and specify the order in which the server should search through the domains.
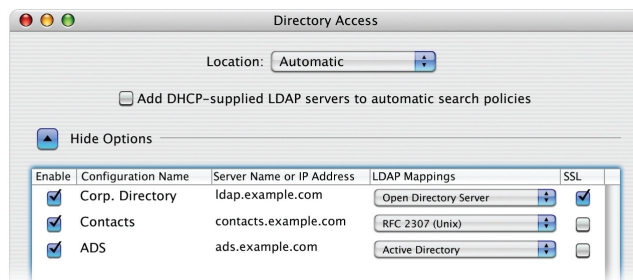
Hosting NT Domain services for Windows clients
Apple has integrated the NT Domain services of the popular open source Samba 3 project with Open Directory, making it possible to host NT Domain services on Mac OS X Server. You can set up Mac OS X Server as a Primary Domain Controller (PDC) or Backup Domain Controller (BDC) for your network, allowing Windows users to authenticate against Mac OS X Server directly from the PC login window. NT Domain services also enable Mac OS X Server to host roaming profiles and network home directories for Windows clients. Now any user in your directory can securely log in and access the same user account, authentication, home directory, and network resources from a Mac or a Windows system. These capabilities make Mac OS X Server ideal for replacing aging Windows NT or Windows 2000 servers, without requiring businesses to transition to an expensive Active Directory infrastructure.

SASL

The Open Directory server uses Simple Authentication and Security Layer (SASL) to support legacy authentication protocols, including NT and LAN Manager, CRAM-MD5, APOP, Diffie-Hellman Exchange, and Two-Way Random. For any service that isn't Kerberos enabled, SASL automatically negotiates the strongest supported authentication method. Using Server Admin, you can enable or disable individual protocols. Since authentication is conducted on the user level, you can mix and match authentication methods for different types of users connecting to your server.

Using single sign-on authentication

Single sign-on requires Kerberos-enabled, or "Kerberized," network services. Most services in Mac OS X Server v10.4 are already Kerberized, including login; mail; FTP, SMB/CIFS, and AFP file services; secure web hosting (over SSL); and SSH. Services that aren't Kerberized can still be authenticated with the Open Directory authentication authority using their native authentication protocols and the same password as Kerberos services. However, these services require users to enter a password every time they access them.

Authentication services and single sign-on

The built-in authentication authority in Open Directory implements MIT's Kerberos technology to provide users with single sign-on access to secure resources throughout your organization. Using strong Kerberos authentication, single sign-on maximizes the security of your network resources while providing easier access to them for authorized users.

Open Directory also supports legacy authentication methods using SASL, so users can have just one password that works everywhere across the network. Even in mixed-platform environments, users can enter the same user name and password to access their home directories, group file servers, or other resources from any system on the network—Mac, Windows, or Linux. In addition to simplifying the user experience, having a single password per user for all network services saves organizations money: It can dramatically reduce the time administrators and help desks spend resetting forgotten passwords, increasing the productivity of network users and support technicians.

Implementing single sign-on

Single sign-on streamlines users' access to secure network resources. Instead of authenticating to each service individually, users type in a password once at login to prove their identity to the Kerberos authentication authority, called a Key Distribution Center (KDC). In response, the KDC issues the user strongly encrypted electronic "tickets," which are used to assure all participating network services that the user has been authenticated securely. The user can then access any authorized network service, without seeing another password dialog.

Kerberos tickets serve as a verification of users' authentication credentials—they don't transmit the user's password to each server the user accesses. This provides stronger security than traditional authentication systems that send passwords over the network for each authentication attempt. Authentication tickets are invalidated when the user logs out or the ticket expires.

Managing authentication policies

Using Server Admin, you can set up and manage password policies for your entire network. For example, you can force users to change passwords at next login, disable user accounts after a certain date, enforce minimum password lengths and other criteria, and disable inactive accounts after a set period of nonuse. User- or group-specific policies (set up in Workgroup Manager) override the general policies set up in Server Admin.
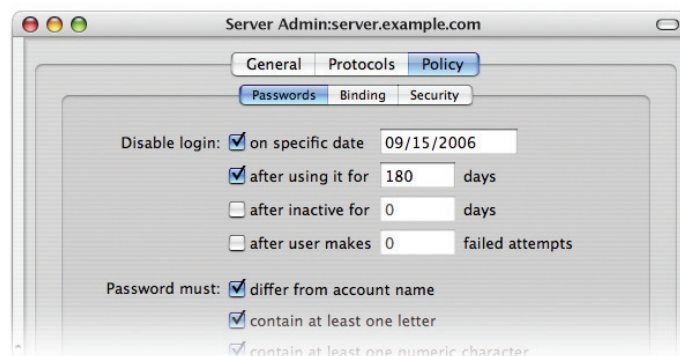
LDAP schema replication
With Mac OS X Server v10.4, the LDAP directory can store its own custom schema and automatically propagate the schema from the Open Directory master to all its replicas.

Open Directory replication
Server Admin makes it easy to set up replication services for Open Directory. Replication allows you to host directory and authentication services on multiple servers for higher availability and greater scalability of the services. Each server gets a copy, or replica, of the Open Directory information and can service client requests. The replica directories automatically synchronize with the master directory, ensuring that user accounts and authentication information remain consistent across distributed network environments.


Replication is essential to delivering high-availability network services. By creating redundant, geographically dispersed directories, you can continue to provide directory and authentication services even in the event of a hardware failure or major power outage. Mac OS X Server provides automatic load balancing between replicated Open Directory servers. This allows you to scale out your directory infrastructure, ensuring responsiveness and maximizing availability of directory services. Open Directory replication can also improve client search and retrieval time on distributed networks by reducing network traffic between remote sites and ensuring rapid access to directory records even if the network connection between two locations is lost.

Managing Directory Data

Automatic discovery of directory services
Mac OS X systems can automatically discover directory services using DHCP Option 95. This feature allows the DHCP server to assign a directory server at the same time that it assigns an IP address to the client. The Automatic Setup feature in Mac OS X Server uses this technology to discover configuration information stored tn the directory, so you can set up an entire rack of servers in minutes.

Apple makes it easy to take full advantage of the powerful capabilities of a managed network environment. The innovative Workgroup Manager application hides the complexities of managing LDAP directory information, providing a simple graphical user interface for setting up user accounts, defining group relationships, and even managing computer settings.* Workgroup Manager allows you to use directory-based management of network resources to simplify administration, provide greater control over organizational resources, and optimize the computing environment for your users.
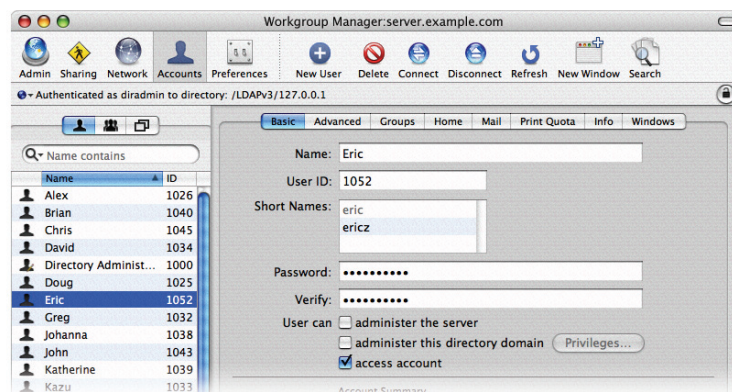
Apple Server Solutions

Open Directory is a robust directory architecture built into Apple's UNIX-based Mac OS X Server operating system. Combining the latest open source technologies with Mac ease of use, Mac OS X Server unleashes the power of Xserve G5, Apple's rack-optimized server hardware. With phenomenal performance, massive storage capacity, high-bandwidth I/O, and integrated remote management tools, Xserve G5 running Mac OS X Server is an unparalleled server solution for businesses, schools, and research centers.

For More Information

For more information about Mac OS X Server, Xserve, and other Apple server solutions, visit www.apple.com/server.

*Requires client systems running Mac OS X v10.2 or later.