



# System Administration Using Mac OS X Server v10.3 Exam Skills Assessment Guide

The System Administration Using Mac OS X Server v10.3 Exam (Prometric exam no. 9L0-607) is a computer-based test offered at Authorized Prometric Testing Centers. The exam is one of two required exams in the Apple Certified System Administrator (ACSA) 10.3 track. You must pass this exam and the System Administration of Mac OS X Clients v10.3 Exam (Prometric exam no. 9L0-606) to become an ACSA 10.3.

The exam lasts two hours and consists of 86 multiple-choice questions that are based on the knowledge-area objectives listed in this guide.

The score required to pass is 60 percent (52 items out of 86). Eight demographic questions are presented but are not scored.

To prepare for the exam, read through the objectives in this guide to determine which areas you need to review. You will not have access to any resources or references during the exam. Please note that the exam is based on Mac OS X Server version 10.3.

The number of test questions drawn from each knowledge area is indicated for each topic below. Please note that although this guide divides the objectives into 13 knowledge areas, questions are presented randomly during the exam. Also note that UNIX commands and processes are shown in a monospaced font in the exam.

## Server Installation and Setup

This topic has eight items, drawn randomly from the following objectives:

- Describe how to:
  - Partition a server's drive remotely with command-line tools such as `ssh`, `disktool`, and `pdisk`.
  - Identify computers that are booted from the Mac OS X Server Install Disk 1 and ready for installation using `sa_srchr`.
  - Install Mac OS X Server remotely using `ssh` and the Mac OS X Server Installer.
  - Install Mac OS X Server on multiple computers using Apple Software Restore, NetBoot, and Network Install.
  - Configure Mac OS X Server locally and on a remote computer, using Server Assistant and command-line tools such as `systemsetup` and `serversetup`.
  - Configure multiple Mac OS X Server computers using a server setup text file, configuration file, or directory record created in Server Assistant.
  - Update a Mac OS X Server computer to Mac OS X version 10.3 with Apple Remote Desktop and with the `softwareupdate` command-line tool.
  - Clone the startup volume of a Mac OS X Server computer with Apple Software Restore.

- Save a service config.plist file in Server Admin to be used to configure a service on another Mac OS X Server computer.
- Monitor and manage disk functions using command-line tools such as `df`, `pdisk`, `newfs`, `newfs_hfs`, and `disktool`.

## Setting Up the Network

This topic has six items, drawn randomly from the following objectives:

- Identify how to:
  - Secure a private network segment by using Server Admin to configure and provide Network Address Translation (NAT) service.
  - Configure a secure local Domain Name Service (DNS) server with Server Admin.
  - Configure a forwarding DNS server.
  - Enable IP forwarding using `sysctl`.
  - View routing tables using `netstat`.
  - Create static routes for a server.
  - Enable the firewall service and create firewall rules using Server Admin and `ipfw`.
  - Route traffic between private and public networks by configuring a server's network interfaces in System Preferences.
  - Redirect incoming requests to the NAT service.
- Differentiate between:
  - A router and a gateway.
  - The default, host, and network entries in a routing table.
  - Advantages and disadvantages of implementing NAT services.

## Network and Service Security

This topic has six items, drawn randomly from the following objectives:

- Identify how to:
  - Configure Secure Shell (SSH) to access a service on Mac OS X Server.
  - Create an encrypted tunnel between Mac OS X Server 10.3 and another computer using OpenSSH.
  - Generate a private/public key pair with OpenSSH for use in Digital Signal Algorithm (DSA) and Rivest, Shamir, and Adleman (RSA) certificate authentication to a service.
  - Generate a private key with OpenSSL.
  - Create an OpenSSL Certificate Signing Request (CSR) and request a certificate from a certificate authority.
  - Create a self-signed Certificate Authority (CA) certificate with OpenSSL.
  - Use OpenSSL to open a communication tunnel through HTTPS.
  - Use `certtool` to import a Secure Socket Layer (SSL) certificate into Keychain and to display its contents.
  - Use `security` to display and modify keys and certificates.
  - Configure Mac OS X Server to provide access to an internal NAT network over Virtual Private network (VPN).
  - Alter the authentication method for VPN connections.

- Configure network routing definitions in the VPN service so that clients use the local router for all non-VPN traffic.
- Using `netstat`, verify that VPN clients are using only VPN for traffic on a private network.
- Differentiate between:
  - SSH and SSL.
  - Symmetric and asymmetric encryption.
  - Point to Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol (L2TP/IPSec) transport protocols for VPN service.
  - Certificates and shared secrets in L2TP transport protocols for VPN services.

## OpenLDAP

This topic has eight items, drawn randomly from the following objectives:

- Describe how to:
  - Configure Open Directory with Server Assistant.
  - Configure Lightweight Directory Access Protocol (LDAP) settings for directory services with Server Admin.
  - Configure an LDAP directory that is accessible from any host on the network that provides secure connections and that can manage a high volume of connections from client computers.
  - Configure an OpenLDAP server to use SSL authentication.
  - Enable LDAP bind authentication so that users are authenticated using LDAP.
  - Populate directory data so that Mac OS X clients can browse for services.
  - Populate Directory Services and OpenLDAP to provide contact information to standard LDAP clients such as Address Book.
  - Populate LDAP domains with mounting information so that, upon login, users automatically mount to their home directories.
  - Promote a Mac OS X LDAP server to an Open Directory Master with Server Admin.
  - Enable Dynamic Host Control Protocol (DHCP) with LDAPv3 servers, so that access to an LDAP server is automatic via DHCP.
  - Manage the information in a shared LDAP directory, manipulating attributes and values with Workgroup Manager.
  - Enable directory services logging with `slapconfig`.
  - Troubleshoot and resolve directory services issues using logs.
- Identify:
  - Configuration files used by OpenLDAP.
  - The Open Directory roles that Mac OS X Server 10.3 fulfills.
  - Object classes that are unique to Mac OS X Server 10.3 OpenLDAP schema.

## Single Sign-on

This topic has five items, drawn randomly from the following objectives:

- Identify:
  - The various Mac OS X technologies that underlie the Single Sign-on architecture.

- The processes, tools, and files associated with Password Server and those associated with Kerberos on Mac OS X Server.
- The records and attributes in a shared directory that define the authentication method as either Password Server or as Kerberos.
- The Simple Authentication and Security Layer (SASL) plug-ins included with Password Server.
- Describe how to:
  - Configure Mac OS X Server as a Key Distribution Center (KDC).
  - Use Server Admin to promote a Mac OS X Server to a KDC.
  - Use `kadmin` to remotely administer a KDC on Mac OS X Server.
  - Configure data mappings to allow Kerberos authentication.
  - Configure network user accounts so that users are authenticated using Kerberos or using Password Server.
  - Use SASL to store user passwords.
  - Use Password Server to manage user passwords.
  - Back up and restore the KDC database with `kdb5_util`.
  - Locally administer a KDC with `kadmin_local`.
  - Monitor Password Server and KDC traffic to and from the server using `tcpdump`.
  - Troubleshoot and resolve issues with the KDC and Password Server using `system.log`.
  - Define and set password policies for user accounts in a shared directory using Workgroup Manager and `pwdpolicy`.
  - Create and manage Password Server replication intervals with `mkpassdb`.
  - Disable Password Server plug-ins with `NeST`.
  - Add user accounts to Password Server with `NeST`.
- Describe:
  - The Kerberos authentication process.
  - The challenge-response authentication mechanism used by Password Server.
  - The automatic configuration process for Password Server and KDC to keep them synchronized.

## Integrating Kerberos Services

This topic has eight items, drawn randomly from the following objectives:

- Identify how to configure:
  - Mac OS X Server to provide authentication services as a KDC.
  - Mac OS X Server to use authentication services from a third-party KDC.
  - Multiple Mac OS X Server computers to work together in one Single Sign-on system.
  - Open Directory on Mac OS X Server to search multiple directory domains, including Windows Active Directory.
  - A secure Kerberos realm using caching, timestamps, and embedding IP addresses in tickets.
  - The Server Message Block (SMB) service running on Mac OS X Server to use authentication provided by an Active Directory KDC.
- Describe:

- Four common ways Mac OS X Server can participate in a Kerberos realm to authenticate user accounts.
- How to deploy Mac OS X Server as a supplementary directory to an Active Directory KDC.

## Replication

This topic has five items, drawn randomly from the following objectives:

- Identify the benefits and requirements of load balancing and redundancy in an Open Directory environment.
- Describe how to:
  - Plan and deploy a replication system.
  - Set up an Open Directory replica.
  - Set up multiple Mac OS X computers for load balancing and redundancy.
  - Promote an Open Directory replica to an Open Directory master.
  - Migrate an Open Directory server to an Open Directory master.
  - Back up the local directory service databases using `nidump` and other command-line tools.
  - Troubleshoot issues with replication.

## Disk Quotas

This topic has four items, drawn randomly from the following objectives:

- Identify how to:
  - Implement user disk quotas using Workgroup Manager or command-line tools such as `edquota`, `quotacheck`, `quotaon`, and `quotaoff`.
  - Monitor disk usage by users and groups using command-line tools such as `quota`, `repquota`, and `du`.
  - Automate disk quota administration with scripts.
- Identify quota files created when quotas are implemented.

## File Sharing

This topic has eight items, drawn randomly from the following objectives:

- Identify how to:
  - Assess network file service needs and choose appropriate technologies.
  - Provide Apple File Services to multiple versions of Apple Filing Protocol (AFP) client.
  - Select the appropriate permissions model for AFP share points.
  - Using Workgroup Manager, configure AFP and Network File System (NFS) share points to be mounted on client computers automatically.
  - Use Workgroup Manager to share a locally mounted NFS volume on Mac OS X Server with other computers over AFP.
  - Create scripts to monitor a file server's storage capacity.

## Dynamic Web Services

This topic has seven items, drawn randomly from the following objectives:

- Describe how to:
  - Configure and monitor the Apache web server with Server Admin and command-line tools.
  - Configure the Apache web server by manually editing configuration files.
  - Identify which directives Server Admin modifies in the configuration files.
  - Use Server Admin to enable Secure Socket Layer (SSL) for websites.
  - Initialize and start MySQL on Mac OS X Server.
  - Configure a MySQL database in Mac OS X Server for use with dynamic web applications.
  - Configure a website in Mac OS X Server to use JBoss, Tomcat, Common Gateway Interface (CGI), PHP: Hypertext Preprocessor (PHP), Server-Side Includes (SSI), Java 2 Platform, Enterprise Edition (J2EE), and WebObjects for dynamic content.
  - Configure a website in Mac OS X Server to use JSP and servlets with Tomcat.
  - Use content management tools to manage content authoring permissions.
  - Use monitoring tools to analyze web server traffic and performance.
  - Analyze Apache log files.
  - Rotate log files.

## Mail Services

This topic has seven items, drawn randomly from the following objectives:

- Identify how to:
  - Define a mail security plan for a given network.
  - Restrict the maximum amount of data that a mail client can store on the server.
  - Configure Apple Mail Server so that it only relays mail from specified hosts.
  - Use `telnet` to test and verify that Apple Mail Server is not acting as an open relay.
  - Isolate and solve mail problems caused by incorrect DNS configuration.
  - Locate and back up the Apple Mail database, and restore it when it becomes corrupted.
- Describe:
  - Postfix architecture.
  - Factors that affect performance of the Apple Mail Server.
  - Apple Mail Server log files and the types of entries each contains.

## Backup

This topic has six items, drawn randomly from the following objectives:

- Describe how to:
  - Create a system to back up and archive server configuration files.
  - Choose a backup medium appropriate to the situation.
  - Use `rsync_hfs` to synchronize user data for backup.
  - Use `md5` to validate the integrity of backup data.
  - Use scripts to combine `hdiutil`, `rsync_hfs`, and `md5` into a single backup solution.
  - Back up and restore live databases such as LDAP and Cyrus mail databases.

- Describe common policies for archiving data.

## High Availability

This topic has eight items, drawn randomly from the following objectives:

- Describe how to:
  - Configure a server to restart automatically after a power failure or if it stops responding.
  - Enable, configure, and trigger IP failover, then restore the initial state.
  - Configure `watchdog` to start, monitor, and restart key processes.
  - Use Mac OS X Server utilities and command-line tools to monitor a Mac OS X Server computer.
  - Use Server Monitor to monitor Xserve hardware status such as the performance of the power supply and UPS, the state of the cooling fans, and the temperature of the enclosure and CPUs.
  - Use command-line tools to monitor and troubleshoot file system issues.
  - Use tools to monitor the state of an Xserve system's security.
- Describe:
  - What happens on IP failover and failback.
  - The function of the `watchdog` process.
  - Which Mac OS X Server high availability features are important for different types of service.

## To Register

To register for an Apple Training course, please visit [www.apple.com/training](http://www.apple.com/training) or call 800-848-6398. To schedule an onsite course at your organization's location, please call 800-848-6398 or email [abouttraining@apple.com](mailto:abouttraining@apple.com).

You are required to have an Apple Tech ID number before registering for an exam. You can apply for a Tech ID by following the instructions at [certifications.apple.com](http://certifications.apple.com).

Then, to register for an exam, call Prometric toll-free at 888-APL-EXAM (888-275-3926) or register online at [2test.com](http://2test.com).

## For More Information

Please visit [www.apple.com/training](http://www.apple.com/training) or call 800-848-6398 for more information about all Apple Training courses and certification programs.