



The Directory Services Integration and Administration v10.4 Exam Skills Assessment Guide

To Register

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

To register for an Apple Training course, please visit 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.

The Directory Services Integration and Administration v10.4 Exam (Prometric exam no. 9L0-611) is a computer-based test offered at Authorized Prometric Testing Centers.

The exam is an elective in the Apple Certified System Administrator (ACSA) track. Successful completion of the exam earns Directory Services Integration and Administration 10.4 certification and also contributes 4 credits, valid for 2 years, towards Apple Certified System Administrator (ACSA) certification.

The exam lasts two hours and consists of 65 multiple-choice questions that are based on the knowledge-area objectives listed in this guide.

The score required to pass is 62 percent (40 items correct out of 65). 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 and Mac OS X Server versions 10.4.

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

Understanding Directory Services

This topic has 4 items, drawn randomly from the following objectives:

- Explain the need for directory services to store system data such as user records.
- Identify what system data is appropriate to store using directory services.
- Explain the relationship between a requester, such as an application, and directory services data.
- Explain how directory services enable data to be shared between multiple requesters.
- Describe how directory services allow requesters to retrieve data from multiple sources.
- Explain the purpose of meta directories.
- Define the terms directory service, process, protocol, directory, and directory domain with reference to directory services.
- List the key attributes required by user accounts in Mac OS X

- Compare and contrast storing user record passwords using either shadow hash or crypt.
- List the key attributes required by group accounts in Mac OS X.

Accessing Local Directory Services

This topic has 7 items, drawn randomly from the following objectives:

- Identify the BSD flat files used by Open Directory's BSD flat files plugin.
- Describe the type of data stored in each of the BSD flat files.
- Identify how to use Directory Access to configure Open Directory on a Mac OS X client computer to retrieve user records from BSD flat files.
- Explain what the local NetInfo database is.
- Identify how to use Workgroup Manager to modify data in the local NetInfo database.
- Identify how to use `dscl` to view and modify user local directory service data.
- Describe how the `DirectoryService` process on Mac OS X uses plug-ins to access system information.
- Describe the relationship between the `lookupd` and `DirectoryService` processes in Mac OS X.
- Identify how to use the `lookupd` command-line tool to determine which agents are used and in what order, for a particular category of items.
- Describe the relationship between `lookupd` and the pluggable authentication module (PAM).
- Compare and contrast the services provided by the `lookupd` and `DirectoryService` processes.
- List the local data stores used by Open Directory on Mac OS X.
- Describe how `lookupd` uses agents to search for different types of user information.

Accessing Mac OS X Server Directory Services

This topic has 6 items, drawn randomly from the following objectives:

- Explain what an LDAP database is.
- Describe how data is structured in an LDAP database.
- Explain how a search base, scope, and filter are used when retrieving data from an LDAP database.
- Identify how to use the command-line tool `ldapsearch` to search for a specific entry in a given LDAP database.
- Describe how to use a graphical user interface tool, such as LDAPPER, to search for a specific entry in a given LDAP database.
- Explain how entries are distinguished in an LDAP database.
- Explain how to use Directory Access to configure a Mac OS X client computer to bind to an LDAP server using address and search base values provided by DHCP.

- Identify how to use Directory Access to configure a Mac OS X client computer to bind to a Mac OS X Server computer providing LDAP service, given the server's address and search base.
- Describe how to use Directory Access to configure Mac OS X to use a secure connection to an LDAP server.
- Explain how to use the `dscl` command-line tool to verify that a Mac OS X client computer is bound to a Mac OS X Server computer providing directory services.
- Identify how to use Directory Access to add a Mac OS X Server computer providing directory services to the list of servers used for user authentication, so that a user can log in to the client computer using a user account stored on the server.
- Describe the general sequence for troubleshooting problems with Open Directory records retrieved from an LDAP database.
- Explain the purpose of the Map option in the LDAP plug-in.
- Describe how to use the `ipconfig` command to verify that a client computer is receiving LDAP configuration information from a DHCP server.
- Identify entries in a given LDAP database that map to user, group, and mount Open Directory records.
- Identify which attributes in an entry in an LDAP database map to key attributes in corresponding Open Directory records.
- Describe managed client attributes provided to Mac OS X clients by Mac OS X Server.
- Interpret entries in a network user account to determine why a user is unable to log in using a networked user account.
- Identify the MCX values in a user record that identify the user account as a mobile user account.
- Describe how to use Directory Access to add a Mac OS X LDAP Server to the list of directory servers used for user authentication.
- Identify the key attributes in an Open Directory user record retrieved from an LDAP database on a Mac OS X Server computer.

Integrating Mac OS X With Third-Party Directory Services

This topic has 8 items, drawn randomly from the following objectives:

- List the steps required to integrate a Mac OS X computer into any third-party directory service.
- List directory service plug-ins supported by Mac OS X and identify corresponding directory services with which they could be used.
- Explain how to use an LDAP browsing tool, such as LDAPPER, to verify that a valid connection can be established with an LDAP server.
- Determine which attributes required by Mac OS X are not provided by a specific LDAP server.
- List three ways to supplement attributes required by Mac OS X that are missing from an LDAP server.
- Describe how to use Directory Access to map required Open Directory attributes to unused attributes on an LDAP server.
- Identify how to use Directory Access to configure the LDAP plug-in to use a static value for a required attribute that is missing from an LDAP server.

- Explain how to use variables to supplement required attributes that are missing from an LDAP server.
- Identify when it is appropriate to modify the schema on an LDAP server to provide attributes required by Mac OS X.
- Identify missing attributes when using an eDirectory server to provide user records to a Mac OS X client computer.
- Identify missing attributes when using a Sun LDAP server to provide user records to a Mac OS X client computer.
- List three methods to provide mount records for a client computer retrieving user records from an LDAP server other than Mac OS X Server.
- List three methods to provide managed client data when using user accounts provided by a directory server other than Mac OS X Server.
- List the attributes in a mount record required by Mac OS X to enable a computer to automatically mount a file server volume.
- Tell how to add a mount record in the local NetInfo database to allow a Mac OS X computer to mount a home directory for a user record provided by an LDAP server other than Mac OS X Server.
- List advantages and disadvantages of using NFS to provide home folders for a Mac OS X computer using user records from an LDAP server other than Mac OS X Server.
- Explain why version 3.0 or later should be used when providing networked home folders for Mac OS X computers via Apple Filing Protocol (AFP).
- List the file sharing protocols that can be used to provide networked home folders to Mac OS X computers accessing user accounts through the LDAPv3 plug-in.

Integrating With Kerberos

This topic has 5 items, drawn randomly from the following objectives:

- Define key terms: key distribution center (KDC), Ticket granting ticket, realm, principals, kerberized services, service tickets, service keys, and single sign on.
- Describe what Kerberos is and list advantages and disadvantages of using it with Mac OS X.
- Describe how a client computer interacts with a KDC to gain access to a kerberized service.
- Describe how passwords are verified using Kerberos.
- Summarize how Kerberos is integrated into the startup process of a Mac OS X client computer.
- Describe how to edit the Kerberos configuration files on a Mac OS X client computer to specify the location of the KDC, the type of encryption used, and the name of the Kerberos realm.
- Explain how to use `klist`, `kinit`, and `kdestroy` command-line tools to add, delete, and list Kerberos tickets on a client computer.
- List the search order for Kerberos config files on Mac OS X.
- Describe the contents of the file `edu.mit.Kerberos` on Mac OS X.
- Describe how a user's kerberized authentication method is stored in an LDAP directory when using Mac OS X.

- Describe how the file `edu.mit.Kerberos` is created, configured, and used by Mac OS X.

Accessing Active Directory

This topic has 5 items, drawn randomly from the following objectives:

- Define the basic Active Directory terms: Active Directory domain, Active Directory forest, Computer ID.
- Configure Mac OS X to use the Active Directory Plug-in so that it can authenticate to an Active Directory server.
- Describe the various advanced options available with the Active Directory plug-in in Mac OS X and when they should be used.
- Identify the basic information needed by users authenticating to Active Directory using Mac OS X and the Active Directory plug-in.
- Describe Mac OS X deployment issues with regard to systems configured with the Active Directory plug-in.
- List the steps involved during the login process from Mac OS X when using the Active Directory plug-in and Mac OS X Server to supplement an Active Directory server.
- Use `lookupd` or `dsc1` from the command line to search, browse, and troubleshoot Active Directory lookups on a Windows server.
- Explain benefits of using a Mac OS X Server to supplement directory services provided by an Active Directory server.
- Identify how to use Directory Access to configure a Mac OS X client computer to use an Active Directory server for authentication and a Mac OS X Server computer for managed client information.
- Describe how Mac OS X Server can supplement an Active Directory server for providing MCX information to Mac OS X clients.

OpenLDAP

This topic has 11 items, drawn randomly from the following objectives:

- Compare and contrast the four roles of an Open Directory server.
- Describe the functionality of an Open Directory standalone server.
- Describe the functionality of an Open Directory master server.
- Explain how to use Server Admin to configure a Mac OS X Server computer to act as an Open Directory master.
- List the actions that occur when a Mac OS X Server computer is promoted from being a standalone server to an Open Directory master server.
- Identify the OpenLDAP primary configuration files.
- Describe how to use Server Admin to configure the maximum number of results returned by an Open Directory server.
- Describe how to use Server Admin to configure the amount of time before an Open Directory server times out during a search.
- Identify how to configure DHCP service on a Mac OS X Server computer to provide LDAP configuration information to client computers.

- Describe how to use the `slapd` process tools to manipulate data stored in the LDAP database on a Mac OS X Server computer.
- Determine which tools are appropriate to use to manipulate LDAP data stored on Mac OS X Server.
- Identify the file on a Mac OS X Server computer that contains the LDAP schema used.
- Identify the object classes in the schema used by Mac OS X Server that are specific to Mac OS X Server.
- Explain how to use the Inspector feature of Workgroup Manager to manipulate directory service attributes and values.
- Describe how to use `ldapsearch` to generate an LDIF file based upon data stored in an LDAP database.
- Identify how to use `ldapadd` to add data from an LDIF file to an LDAP database on Mac OS X Server.
- Explain multiple approaches to storing contact information in an LDAP server.
- Describe how to use `ldapadd` to populate a shared LDAP directory on Mac OS X Server with contact information to be used by Address Book.
- Tell how to use the Open Directory Archive and Restore feature on Mac OS X Server to back up and restore an Open Directory server.
- Explain security concerns when using LDAP to provide directory data such as user accounts.
- Describe how to configure the `slapd` process to not allow anonymous binding.
- Describe how to configure Open Directory on Mac OS X Server to use SSL to prevent eavesdropping on LDAP communications with client computers.
- Identify how to tune the performance of the Open Directory server by configuring which attributes in the LDAP database are indexed.
- Explain how to modify the number of LDAP records to cache on Mac OS X Server to tune its performance.

Providing Single Sign-On Authentication

This topic has 7 items, drawn randomly from the following objectives:

- Describe common difficulties in configuring and managing Kerberos that have been addressed by Mac OS X Server.
- Define the terms realm, principal, key distribution center, and ticket with reference to setting up Kerberos service on a Mac OS X Server computer.
- Identify the files used by the Kerberos service running on a Mac OS X Server computer.
- Describe how to use the `kdb5_util` command to export and import data to and from the KDC database on a Mac OS X Server computer.
- Identify the KDC process running on Mac OS X Server.
- Explain the purpose of the `kadmind` process running on Mac OS X Server.
- Identify the configuration files used by the `kadmind` process on Mac OS X Server.
- Explain how to use the `kadmin` and `kadmin.local` command-line utilities to manage Kerberos running on a Mac OS X Server computer.

- Identify KDC entries in the system log.
- Describe how to use a packet sniffer, such as `Ethereal` or `tcpdump`, to identify Kerberos-related network traffic and interpret any error codes they may contain.
- Identify how to use the `klist` utility to determine what encryption method was used to generate keytab files on a Mac OS X Server computer.
- Describe how to use Server Admin to enable Kerberos authentication on a Mac OS X Server computer.
- Explain the role of Password Server on Mac OS X Server.
- Identify the main Password Server process on a Mac OS X Server computer.
- Identify the main files used by the Password Server on a Mac OS X Server computer.
- List which IP ports are used by the Password Server running on Mac OS X Server.
- Identify how to use the `GETIDBYNAME` command to retrieve an administrator's password server ID.
- Tell how to retrieve a user's Password Server ID from the user record.
- Explain the interaction between a client and server during a challenge-response authentication.
- List the authentication plug-ins supported by the Password Server running on a Mac OS X computer.
- Describe how to use Workgroup Manager to configure password policies enforced by Password Server running on Mac OS X Server.
- Explain how to use the `pwpolicy` utility to manipulate password policies on a Mac OS X Server computer.
- Describe how to use Server Admin or NeST to disable authentication methods on a Mac OS X Server computer.
- Explain how passwords are synchronized between Password Server and Kerberos running on a Mac OS X Server computer.
- Explain how Kerberos and Password Server are initially configured.
- Explain how Kerberos and password servers are specified in a user record.

Integrating Kerberos Services

This topic has 5 items, drawn randomly from the following objectives:

- Describe four common ways that Mac OS X Server can participate in a Kerberos realm to authenticate user accounts.
- Describe how a service uses a service ticket to recognize a client authenticated using Kerberos.
- Identify how to use Workgroup Manager to add a Kerberos computer record to the Open Directory master server.
- Explain how to use Server Admin to add a Kerberos record on an Open Directory master server.
- Describe how to use Server Admin to configure a Mac OS X Server computer to join a Kerberos realm already established on an Open Directory master server.
- Explain how to use Server Admin to configure kerberized services running on Mac OS X Server to accept service tickets from a KDC running on a third-party server.

- Describe how to install and enable keytab files from a third-party Kerberos server on a Mac OS X Server computer to allow the Mac OS X Server computer to use the third-party server for Kerberos authentication.
- Identify how to use Server Admin to configure kerberized services running on Mac OS X Server to accept service tickets from a Windows server running Active Directory KDC.
- Explain how to use Server Admin to configure the SMB service running on Mac OS X Server to use authentication provided by an Active Directory KDC.
- Tell how to use the `ktpass` command on a Windows server to generate keytab files to be used on a Mac OS X Server computer.
- Describe how to use `kadmin.local` to configure the KDC in Mac OS X Server to support cross-realm authentication with a KDC running on a third-party server.
- Describe two approaches to address the concern that Kerberos user keys are easily recoverable.
- Describe multiple approaches to counter offline dictionary attacks on Kerberos transactions.
- Explain how to use construct a Kerberos configuration to prevent a man-in-the-middle attack.
- Describe how Kerberos prevents a replay attack.

Replication

This topic has 6 items, drawn randomly from the following objectives:

- Explain the advantages of using Open Directory replicas.
- Describe how to use Server Admin to configure a Mac OS X Server computer to act as an Open Directory replica.
- Explain what happens when a replica is created on a Mac OS X Server computer.
- Identify how to use Server Admin on an Open Directory master computer to specify when data should be replicated out to connected replicas.
- Tell how to configure a Mac OS X client computer to connect to a replication system.
- Describe how to use Server Admin to promote an Open Directory replica to an Open Directory master.
- Describe how redundancy, performance, and network bandwidth needs are met by configuring Mac OS X as an Open Directory replica.
- Identify the most commonly referenced files in a replication architecture and explain their purposes.
- Explain how LDAP data is replicated between Open Directory master and replicas.
- Describe how passwords stored in the Password Server are synchronized between Open Directory master and replicas.
- Explain how KDCs running on an Open Directory master and replicas are synchronized.
- Identify the steps a Mac OS X client computer goes through during startup when it is bound to an Open Directory replica system.
- Explain what happens when a user changes an account password on a Mac OS X client computer that is bound to an Open Directory replica system.

- Identify how to construct a plan for upgrading an existing Open Directory replica system running on Mac OS X Server 10.3 to run on Mac OS X Server v10.4.
- Identify entries in the Password Server and LDAP logs that indicate problems in replicating an Open Directory master server.

Planning and Deploying Directory Services

This topic has 1 item, drawn randomly from the following objectives:

- Evaluate directory service needs and determine how many replica servers, if any, are required.
- Identify how to construct a plan for deploying networked user accounts in a mixed network of Mac OS X and Windows computers.
- Describe how to construct a plan for providing Mac OS X-specific directory service data to Mac OS X computers on a Windows-dominant network.
- Explain the security precautions that should be taken when setting up a directory server.

For More Information

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

© 2005 Apple Computer, Inc. All rights reserved. Apple, the Apple logo, Mac, and Mac OS are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies. Mention of non-Apple products or services is for informational purposes only. Product specifications are subject to change without notice. August 2005