Apple Technical White Paper

Best Practices for Integrating OS X with Active Directory

OS X Yosemite v10.10

December 2014

Contents

Introduction to directory services support in OS X

Large organizations need to manage user identities and access across a variety of services in their environment. A directory service is a central location to securely store information about users, groups, and computer objects within an organization. Services and resources that are joined to the directory service can use it to verify user access to secured resources. With a directory service, an administrator can manage user authentication and authorization in a centralized location that will propagate across the entire organization. Directory services can also be used to advertise resources, such as printers, or to look up public information about users or groups.

Some of the benefits of integrating computer systems with directory services include enforcing strong authentication policies, managing access to resources, and providing a seamless authentication experience.

OS X supports the management of user login identities with the conventional approach of networked directory services, as well as modern Mobile Device Management (MDM) technologies. Managing OS X with MDM offers the flexibility of managing and updating configurations and policies with devices over the air.

Out of the box, OS X seamlessly integrates with a variety of directory service technologies, including Active Directory, Microsoft's implementation of directory services. When integrated into Active Directory, OS X supports password policy, user and group account lookups, single sign-on using Kerberos, and more. Built-in tools make it easy to deploy a single Mac or a fleet of thousands.

OS X and Active Directory

Apple's support for Active Directory within OS X enables Mac clients and servers to integrate smoothly into existing Active Directory environments, and provides the option of deploying a single directory services infrastructure that can support both Mac and Windows clients.

OS X offers native Active Directory integration. Users can use the same credentials to log in to their Mac as they use with other computers and services.

When fully integrated with Active Directory, OS X offers an environment in which users:

- Can use the same credentials to authenticate and gain authorization to secured resources
- Are subject to the organization's domain password policies
- Benefit from single sign-on access to Active Directory resources through Kerberos
- Can request and be issued user and computer certificate identities from an Active Directory Certificate Services server
- Can automatically traverse a Distributed File System (DFS) namespace and mount the appropriate underlying Server Message Block (SMB) server

Domain password policy

At bind time (and at periodic intervals thereafter), OS X queries the Active Directory domain for the password policies. These policies are enforced for all network or mobile accounts on the Mac. During a login attempt while the network accounts are available, OS X queries Active Directory to determine the length of time before a password change is required. By default, if a password change is required within 14 days, the login window prompts the user to change it. If the user accepts the prompt and changes the password, the change occurs in Active Directory as well as in the mobile account (if one is configured), and the login keychain password is updated. If the user dismisses the prompt, the login window will prompt the user until the day before expiration. A password change will be required within 24 hours for login to proceed.

Login Window Password Expiration Interval
An administrator can change the default expiration notification for the Login Window from the command line:

```
defaults write /
Library/Preferences/
com.apple.loginwindow
PasswordExpirationDays
-int <number of days>
```

Single sign-on

Single sign-on is a process in which a user can provide authentication information once, receive a token, and use it to access resources for as long as the token is valid. This strategy makes it possible to maintain secure access to resources without the system prompting the user for credentials every time access is requested.

OS X supports single sign-on with Active Directory through Kerberos. When integrated into an Active Directory environment, OS X prioritizes

Kerberos for all authentication activities. The use of other authentication protocols such as Microsoft's NT LAN Manager (NTLM) Digest and Basic can be prohibited on the network, without affecting Mac computers or services provided by OS X Server within the Active Directory environment. When a user logs in to a Mac using an Active Directory account, the Active Directory domain controller automatically issues a Kerberos Ticket Granting Ticket (TGT). When the user attempts to use any service on the domain that supports Kerberos authentication, the TGT is used to generate a ticket for that service without requiring the user to authenticate again. If a policy is set to require a password to dismiss the screensaver, OS X will attempt to renew the TGT upon successful authentication.

To properly support Kerberos, both forward and reverse Domain Name System (DNS) records should be accurate for Kerberized servers. System clock time is also important. Clock skew must be less than five minutes for servers and clients. Best practice is to use Network Time Protocol (NTP) on OS X using a reliable source such as time.apple.com.

Several command-line Kerberos administration tools are available on OS X, including:

```
kinit - acquire initial Kerberos credentials

klist - list Kerberos credentials

kdestroy - remove Kerberos credentials
```

See the man pages in Terminal.app for more information on how to use these tools.

The graphical application, Ticket Viewer, can also be used to manage Kerberos tickets. It can be launched from Keychain Access and is located at /System/Library/CoreServices/Ticket Viewer.app.

Deploying certificate identities

OS X includes native support for acquiring certificate identities from an Active Directory Certificate Services server. Both user and computer identities can be deployed for use with services such as EAP-TLS, S/MIME, or VPN.

By using a configuration profile and the AD Certificate payload, identities can be transparently deployed from the issuing certificate authority (CA). These identities can be associated with specific services by configuring those services in the same configuration profile. The configuration profile can be deployed manually, via a script, as part of a Mobile Device Management (MDM) enrollment, or via a client-management solution.

Issuing user identities requires user account credentials upon installation, and computer identities use the computer object and password. Local administrator privilege is required to install computer identities.

It's important to establish any necessary trust with your enterprise CA as part of deploying the certificate identity. Best practice is to supply the certificates for the root and any intermediates in the certificate chain. This can be done using the Certificates payload in a configuration profile. The same profile can contain the AD Certificate request and the configured service (network or VPN, for example). You may find it more convenient to deploy certificate trust with a separate profile, so that trust can be updated independent of the identity deployment and service configuration.

By default, when a certificate identity that has been deployed with a configuration profile is within 14 days of expiration, the logged-in user will receive a Notification Center message. The user should click the notification to be redirected to the Profiles pane in System Preferences and an Update button will appear for the profile with the expiring certificate identity. When the user clicks Update, the profile will be reinstalled, creating another certificate request to the issuing CA and associating it with any configured services in the profile.

See Knowledge Base article HT5357 for more information on acquiring a certificate identity using a configuration profile:

http://support.apple.com/kb/HT5357

DFS namespace support

OS X supports traversing DFS namespaces. A Mac bound to Active Directory can query Windows Internet Naming Service (WINS) servers and domain controllers in the Active Directory Site to resolve the appropriate SMB server for a particular namespace automatically.

The "Connect to Server" feature in Finder is used to specify the fully qualified domain name of the DFS namespace and include the DFS root to mount the network file system. For example, in "Connect to Server," enter:

```
smb://resources.company.com/DFSroot
```

OS X will use any available Kerberos tickets and mount the underlying SMB server and path. In some Active Directory configurations, it may be necessary to populate the Search Domains field in the DNS configuration for the network interface with the fully qualified Active Directory domain name.

See Knowledge Base article HT4794 for more information on DFS namespace resolution:

http://support.apple.com/kb/ht4794

Certificate Identity Expiration Interval

An administrator can change the default expiration notification for certificate identities. You can use Profile Manager in OS X Server to configure the number of days in advance of a certificate expiring before users will be notified.

Administrators can also configure the notification system wide by specifying the following keys:

```
sudo defaults write /
Library/Preferences/
com.apple.mdmclient
CertificateRenewalTimeP
ercent -int 50
```

where 50 is the desired percentage of time left on the validity of the certificate identity. Valid values are integers from 1 to 50. Values set in the configuration profile payload take precedence over the system setting.

Impact of mobility

Directory services can hold vast amounts of sensitive data, and should be kept secure. Almost always, querying the service is restricted to trusted devices on trusted networks. This means that remote computers such as laptops require an active VPN connection to access the directory service. For mobile users who may not often have a need for VPN, the device could be off network for extended periods of time. Even when VPN is used regularly, it is a user space process. Logging in at the login window authenticates against the locally cached credential store, not the live data in the directory service. Password changes made in the directory service may not yet be reflected on mobile devices.

Best practice for changing a mobile user account password on a Mac that is bound to the directory service is to use the Users & Groups preference pane in System Preferences while the computer can contact the directory service. The login window will notify the user if network accounts are unavailable. To verify connectivity to the directory service when logged in, select Login Options in the sidebar of the Users & Groups preference pane and check the Network Account Server field. A green indicator means the directory service is available. Select the mobile user account in the sidebar and select the Change Password button.

This process ensures that the user account password is changed in the remote directory service, in the locally cached credential store (dslocal), and that the login keychain password is updated. The login keychain is an encrypted store in the user's home folder that contains sensitive information such as application and Internet passwords, as well as user certificate identities. By default, the password to decrypt this container is the same as the user account password and is automatically unlocked at login.

If the network account password is changed while a Mac is offline, and the user attempts to log in when returning to the network, the Mac will be unable to unlock the login keychain. OS X will prompt the user to update the keychain password. If the user cannot provide the previous password, there's an option to create a new keychain.

With local-only accounts, a password policy can be applied with a configuration profile, achieving organizational policy compliance while simplifying login keychain and user account password synchronization.

Mac as a mobile device

MacBook Pro and MacBook Air are inherently mobile devices. Directory services were initially conceived to support multiple users logging in to a single computer connected to the directory service via a persistent trusted network connection. Deploying a portable computer to a single user who frequently transitions between a variety of networks requires a different strategy.

Mobile devices often may not have access to an organization's directory service. Therefore, any updates made in the directory services may not be reflected on the mobile devices right away. Administrators may need to update client computer policies and configurations remotely, at scale, regardless of the device's network posture. To achieve this, administrators can use Mobile Device Management (MDM).

The same process and philosophy for deploying configurations and policy to iOS can be applied to OS X. By using Apple Push Notification service, MDM can notify Mac computers that a configuration or policy update is available. When a Mac receives the push notification, it will silently and securely check in with the MDM server using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol to retrieve the updated policy or configuration data, as long as the client has an Internet connection. In this scenario, there is no prerequisite for the device to be on VPN or an explicitly trusted network.

Many of the original benefits of joining a directory service and using network accounts are provided by using MDM or a client management solution. Password and client policies, including certificate identities, can be deployed and updated over the air. Devices can still be joined to the directory service at the system level to provide user and group resolution for authorization to services such as network file servers. By doing so, the complexity of maintaining network accounts on the local Mac is eliminated.

Single sign-on can still be achieved by leveraging the command line `kinit`, which can be implemented in AppleScript to create a simple graphical application to acquire the initial Kerberos ticket. More sophisticated solutions are available from Apple Professional Services. Contact your Apple representative for more information.

Joining a Mac to Active Directory

OS X uses DNS to query the topology of the Active Directory domain. It uses Kerberos for authentication and Lightweight Directory Access Protocol (LDAP) for user and group resolution. Options for joining a Mac to Active Directory include using the Directory Utility application, a configuration profile, or the command line.

System Preferences

1. On the Mac client, open the Users & Groups pane in System Preferences, available from the Apple menu.
2. Click Login Options. Then click Join (or Edit if the Mac is already bound to another directory service) to the right of Network Account Server.
3. Click Open Directory Utility.
4. After Directory Utility opens, click Services and then double-click Active Directory.
5. Enter the DNS host name of the Active Directory domain you want to bind to the computer you're configuring.
6. The Client Computer ID is the name of the computer object in Active Directory, which is populated with the LocalHostName of the Mac by default. You can change this according to your organization's needs.
7. (Optional) Set advanced options.
8. If the advanced options are hidden, click Show Advanced Options. Then set options in the User Experience, Mappings, and Administrative panes.

   User Experience options:

   - Create mobile account at login
     This creates a local account to be accessed off network. A confirmation dialog can be required when an account is used to log in to the Mac for the first time.

   - Force local home directory on startup disk
     Disable this option when using pure network home directories. This option is required for mobile accounts.

   - Use UNC path from Active Directory to derive network home location
     When this option is enabled, if the Active Directory user account record has a home folder specified, the Mac mounts the location and creates a link in the Dock. The default protocol is SMB, but it can be set to AFP.

   - Default user shell
     UNIX systems require a command-line shell, and `/bin/bash` is the OS X default.

Mappings options:

- By default, OS X dynamically generates unique UIDs and GIDs for Active Directory accounts on a system. Ordinarily this is sufficient. However, if managing UIDs and GIDs is required, map to the appropriate attributes in the user record in Active Directory here.

Administrative options:

- Prefer this domain server
  By default, OS X uses site information and domain controller responsiveness to determine the appropriate domain controller to use. If a domain controller in the same site is specified here, it will be consulted first. If the domain controller is unavailable, OS X will revert to default behavior.
- Allow administration by
  When enabled, members of the listed Active Directory groups are granted administrative privileges over the local Mac. By default, domain admins and enterprise admins are listed. Specify desired security groups here.
- Allow authentication from any domain in the forest
  By default, OS X automatically searches all domains for authentication. To restrict authentication to only the domain the Mac is bound to, disable this checkbox.

9. Click Bind.
10. Enter the user name and password of a user who has permission to join computers to Active Directory.

    This doesn’t need to be an administrator user. Domain-joining privilege can be assigned to any user. If the Mac is creating the object in Active Directory, the user needs to have “Read” and “Create All Child Objects” permissions on the container specified. By default, OS X is set to create the object in the Computers container, but any container or organizational unit can be used. If the object already exists, the user must be a member of the group with the ability to join the account as specified in Active Directory Users and Computers.

Configuration profiles

The Directory payload in a configuration profile has the ability to configure the Mac to join Active Directory. This can be another option to automate joining Active Directory across a fleet of Mac computers. As with other configuration profile payloads, the Directory payload can be deployed manually, via a script, as part of an MDM enrollment, or via a client-management solution. For more information, see Knowledge Base article HT5981:

http://support.apple.com/kb/HT5981

The Profile Manager service In OS X Server includes a graphical interface for creating advanced Active Directory configuration options in the Directory payload.

Command line

The functionality of Directory Utility and the Directory payload is also accessible from the command-line interface with the `dsconfigad` command. For example, the following command can be used to join a system to Active Directory:

```
dsconfigad -preferred ads01.example.com -a COMPUTERNAME
  –domain example.com -u administrator -p "password"
```

After you've bound a system to the domain, you can use `dsconfigad` to set the administrative options in Directory Utility:

```
dsconfigad -alldomains enable -groups domain
  admins@example.com, enterprise admins@example.com
```

When using `dsconfigad` in a script, you must include the clear-text password used to join to the domain. Typically, an Active Directory user with no other administrator privileges is delegated the responsibility of joining clients to the domain. This user name and password pair is stored in the script. It's common practice for the script to securely delete itself after binding so this information no longer resides on the disk.

There is little advantage to using command line scripts to join Active Directory instead of configuration profiles.

Advanced Active Directory configuration options

The native support for Active Directory includes options that aren't exposed in the Directory Utility application. To access these advanced options, use either the Directory payload in a configuration profile, or the `dsconfigad` command-line binary. See `man dsconfigad` for complete usage.

Computer object password interval

When a Mac system is bound to Active Directory, it sets a computer account password that's then stored in the System keychain. This computer account password is automatically changed by the client. The default password interval is every 14 days, but you can use the Directory payload or `dsconfigad` command-line tool to set any interval that your policy requires. Setting the value to 0 disables automatic changing of the account password:

```
dsconfigad -passinterval 0
```

Note: The computer object password is stored as a password value in the System keychain. To retrieve the password, open Keychain Access, select the System keychain and select the Passwords category. Find the entry that looks like "/Active Directory/DOMAIN" where DOMAIN is the NetBIOS name of the Active Directory domain. Double-click this item and select the "Show password" check box. Authenticate as a local administrator as needed.

Namespace support

OS X supports authenticating multiple users with the same short names (or login names) that exist in different domains within the Active Directory forest. By enabling namespace support with the Directory payload or the `dsconfigad` command-line tool, a user in one domain can have the same short name as a user in a secondary domain. Both users have to log in using the name of their domain followed by their short names (DOMAIN \short name), similar to logging in to a Windows PC. To enable this support, use the following command:

```
dsconfigad -namespace forest
```

OS X Server enabling single sign-on

For OS X Server, supported services can use Kerberos, enabling single sign-on for Active Directory clients by enabling the following:

```
dsconfigad -enablesso
```

Packet signing and encryption

The Open Directory client is able to both sign and encrypt the LDAP connections used to communicate with Active Directory. Along with the signed SMB support that's present in OS X, it shouldn't be necessary to downgrade the site's security policy to accommodate Mac clients. The signed and encrypted LDAP connections also eliminate any need to use LDAP over SSL. If SSL connections are required, use the following command to configure Open Directory to use SSL:

```
dsconfigad -packetencrypt ssl
```

Note that the certificates used on the domain controllers must be trusted for SSL encryption to be successful. If the domain controller certificates aren't issued from the OS X native trusted system roots, install and trust the certificate chain in the System keychain. Certificate authorities trusted by default in OS X are in the System Roots keychain. To install certificates and establish trust, import the root and any necessary intermediates using the Certificates payload in a configuration profile, use the Keychain Access located in /Applications/Utilities, or use the `security` command as follows:

```
/usr/bin/security add-trusted-cert -d -p basic -k
  /Library/Keychains/System.keychain <path to
  certificate file>
```

Restrict Dynamic DNS

OS X attempts to update its Address (A) record in DNS for all interfaces by default. If multiple interfaces are configured, this may result in multiple records in DNS. To manage this behavior, specify which interface to use when updating the Dynamic Domain Name System (DDNS) by using Directory payload or the `dsconfigad` command-line tool. Specify the BSD name of the interface in which to associate the DDNS updates. The BSD name is the same as the Device field, returned by running this command:

```
networksetup -listallhardwareports
```

To restrict DDNS updates to the built-in Ethernet port, for example, use this command:

```
dsconfigad -restrictDDNS en0
```

OS X Exchange support

OS X includes native support for connecting to Microsoft Exchange. The Mail, Calendar, Contacts, Notes, and Reminders applications all include support for Exchange accounts. Configuring access to Exchange accounts can be done manually using the Internet Accounts pane in System Preferences or automatically by deploying an Exchange payload in a configuration profile. The Profile Manager service in OS X Server includes graphical support for configuring an Exchange payload for use with OS X.

OS X uses the Exchange Web Services protocol and supports Kerberos for single sign-on. Many powerful features are supported without the need for installing additional software, including calendar delegation, Global Address List (GAL) and LDAP queries, and free/busy lookup.

Binding a Mac to Active Directory isn’t a prerequisite for configuring the Mac to use Exchange.

Troubleshooting

The native support for Active Directory in OS X easily integrates into the majority of Active Directory implementations. Several tools are available to help debug specific issues.

opendirectoryd debug logging

To enable `opendirectoryd` debug logging, see Knowledge Base article HT4696:

http://support.apple.com/kb/HT4696

Packet trace

A packet trace can be helpful, particularly to debug login or binding issues. For more information, see this Technical Q&A:

https://developer.apple.com/library/ios/qa/qa1176/_index.html

One way to capture a packet trace at the login window is to enable Remote Login on the client and use Secure Shell (SSH) to remotely connect and start the trace.

By default, packets between Active Directory clients and servers are encrypted. Use this command to disable encryption:

```
dsconfigad -packetencrypt disable
```

Use this command to reenable encryption:

```
dsconfigad -packetencrypt allow
```

When capturing traffic for the following ports:

UDP 53	- DNS
TCP 88	- Kerberos
TCP 389	- LDAP
TCP/UDP 464	- Kerberos Password Changes (KPasswd)
TCP 3268	- Global Catalog (LDAP)

For example, to capture traffic over the built-in Ethernet connection to a file called "capture.pcap," use the following syntax for `tcpdump`:

```
tcpdump -K -i en0 -s 0 -w capture.pcap port 88 or port
  464 or port 53 or port 389 or port 3268
```

Wireshark is a popular graphical network protocol analyzer that has a version for OS X.

DNS

OS X relies on accurate DNS records for discovering the Active Directory domain topology, and is a common source of issues. Use the `dig` command to test that the Mac can read the proper DNS records. In the following example, replace `example.com` with the DNS of the Active Directory domain:

```
dig -t SRV _ldap._tcp.example.com
```

This should return the IP address of the domain controllers for `example.com`. If it doesn't, the Mac systems aren't using the same server for DNS as the Active Directory clients, or the DNS server is misconfigured.

Domain controller reachability

At bind time, the native Active Directory support in OS X builds a list of domain controllers to contact based on Active Directory site and response time. This list is also updated on network transitions. To check the last used domain controller on OS X:

```
/usr/libexec/PlistBuddy -c "print 'last used servers':'/
  Active Directory/EXAMPLE':host" /Library/Preferences/
  OpenDirectory/DynamicData/Active\ Directory/
  EXAMPLE.plist
```

where EXAMPLE is the NetBIOS name of the Active Directory domain. This command requires `sudo` privileges.

To confirm network reachability to service ports on a domain controller, use `/usr/bin/telnet`. For example, to check connectivity to a domain controller's Kerberos services:

```
telnet dc01.example.com 88
```

If successful, the reply should look like:

```
Trying 192.168.1.110...
Connected to dc01.example.com.
Escape character is ‘^]'.
```

Type Control-C to cancel. Repeat for other required service ports.

TCP 88	- Kerberos
TCP 389	- LDAP
TCP/UDP 464	- Kerberos Password Changes (KPasswd)
TCP 3268	- Global Catalog (LDAP)

Query Active Directory

Use the command line utility `/usr/bin/id` to query Active Directory to evaluate an Active Directory user account. This can be done while you're logged in to the Mac as a local account. Enter:

```
id sydney.bailey

uid=1943048728(sydney.bailey) gid=832964810(CORP\Domain
Users) groups=832964810(CORP\Domain Users),12(everyone),
62(netaccounts),701(com.apple.sharepoint.group.1)
```

where `sydney.bailey` is the username of the record to query. The output indicates the group membership of the user record returned by Active Directory.

Authenticate to Active Directory

Use the command line utility `/usr/bin/su` to authenticate to Active Directory as a particular user. This can be done while you're logged in to the Mac as a local account.

```
su sydney.bailey

Password:

bash-3.2$
```

Notice the change in shell prompt. Use `/usr/bin/whoami` to verify your current session.

```
bash-3.2$ whoami

sydney.bailey

bash-3.2$
```

If successful, this verifies connection and authentication to Active Directory.

Conclusion

With mobile devices and laptop computers growing in popularity, and one-user-to-one-computer-system deployments becoming more common, multiuser logins managed by a network directory service are becoming less of a requirement. OS X embraces the future of client policy with Mobile Device Management while supporting conventional directory services. OS X natively integrates into the majority of Active Directory implementations with ease while taking advantage of the advances in MDM client management capabilities.

Resources

See the following Apple Support Knowledge Base articles for more information:

- **OS X: Active Directory naming considerations when binding**
  http://support.apple.com/kb/TS1532
- **OS X Server: Packet encryption via SSL for Active Directory clients**
  http://support.apple.com/kb/HT4730
- **How to request a certificate from a Microsoft Certificate Authority using DCE/RPC and the Active Directory Certificate profile payload**
  http://support.apple.com/kb/HT5357
- **How to request a certificate from a Microsoft Certificate Authority using the ADCertificatePayloadPlugin**
  http://support.apple.com/kb/HT4784
- **OS X Server: Changing opendirectoryd logging levels**
  http://support.apple.com/kb/ht4696
- **OS X Mavericks: Using advanced Active Directory options in a configuration profile**
  http://support.apple.com/kb/HT5981
- **OS X Yosemite: List of available trusted root certificates**
  http://support.apple.com/kb/HT6005

Apple Inc.

Other company and product names mentioned herein are trademarks of their respective companies. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Apple assumes no responsibility with regard to the performance or use of these products. All understandings, agreements, or warranties, if any, take place directly between the vendors and the prospective users. Every effort has been made to ensure that the information in this document is accurate. Apple is not responsible for printing or clerical errors.

12/2/14