Apple Technical White Paper

Best Practices for Integrating OS X with Active Directory

OS X Mountain Lion v10.8

Contents

Introduction

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.

Apple's Built-in Solution

Large organizations have a need to manage user identities and access across a variety of services in their environment. It's common practice to consolidate users, groups, and computing resources into a centralized, directory services infrastructure. Out of the box, OS X seamlessly integrates with a variety of directory-service technologies, including Active Directory.

Apple's implementation of a centralized directory service is called Open Directory. Integrated into the foundation of OS X, Open Directory is responsible for providing directory and network authentication services for both OS X clients and OS X Server. Open Directory uses open-standard protocols such as LDAP, Kerberos, and SASL.

Although Apple provides its own native, directory services platform through Open Directory, OS X supports access to a variety of other platforms, including Active Directory. While every Active Directory installation is different, OS X integrates well with the vast majority of platforms with minimal effort.

OS X offers Active Directory integration through a directory service. With this support, the user doesn't need to maintain a separate directory or separate user records to support OS X systems. Users can move between different computers, while still adhering to enterprise policies for strong authentication and password-protected access to network resources.

When fully integrated with Active Directory, OS X offers a complete managed environment where users can:

- Access any Mac in the integrated environment using the same credentials they would use to access Windows PCs.
- Require adherence to the Active Directory password policies.
- Benefit from single sign-on access to Active Directory resources through Kerberos.

Users can have local home directories while maintaining access to the network-based home folder specified in their Active Directory record.

Apple support for Active Directory extends to OS X Server as well. Integrating OS X Server is just as easy as integrating a client system—in fact, the process is essentially the same. This allows Windows-based departments to take advantage of file sharing, web services such as wikis and blogs, Profile Manager, and other services in OS X Server while using their existing Active Directory infrastructure for identification and authentication. Secure network services hosted on OS X Server also support single sign-on for both OS X and Windows clients.

Address Book and Mail

The Address Book application in OS X provides a flexible and convenient way to store contact information. Address Book can use common network technologies, such as LDAP, to query servers for contact information. This allows a Mac to look up contact information stored within Active Directory. Users can configure the use of an LDAP server, such as an Active Directory domain controller, even if their Mac hasn't been integrated into the Active Directory domain.

Users can select the Directory Services group in Address Book and search for a user by name or email address. Once the appropriate contacts are found, users can drag them to their local Address Book. This can be helpful to users who want to add or modify contact information, but don't have permission to change Active Directory records.

Address Book is integrated with Mail, iChat, and other applications in OS X. This allows these other applications to access the same set of contact information available to Address Book. Mail, for example, searches Active Directory for contact information as users type a contact's name and offers matching contacts for autocompletion of the email address (provided email addresses are included in Active Directory for user accounts).

Additional information can be added to user accounts within Active Directory, such as an instant-messaging user name or blog address, using Microsoft's management tools. This information appears in Address Book along with other contact information.

How to Integrate OS X with Active Directory

Getting Started

Using these simple steps, you can configure a Mac client to use DNS and Active Directory to determine the geometry of your Active Directory domain, find the nearest domain controller, and create a new computer account in the domain—if there isn't an existing one with the computer ID you've chosen.

On the Mac client, open the Users & Groups pane in System Preferences, available from the Apple menu. Select Login Options, then click Join (or Edit if the Mac is already bound to another directory service) next to Network Account Server. Click Open Directory Utility on the sheet that expands. The Directory Utility application launches. Ensure Services is selected and double-click Active Directory. Enter the name of your Active Directory domain. 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. This can be changed according to your organization's needs.

If desired, click the Show Advanced Options disclosure triangle.

Computer accounts
Each Mac system has a unique computer account in Active Directory. If you clone a system or integrate NetBoot with Active Directory, all the cloned systems are assigned the same computer account. This means that it's important to be careful when changing a computer account, as any change breaks authentication from all systems using that account. Best practice is to join the Mac system to Active Directory as a post-imaging procedure.

- **User experience**
    - Create mobile account at login
      This creates a local account to be accessed off network. You can require a confirmation dialog when an account logs 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 enabled, if the 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, and can be set to afp if desired.
    - Default user shell
      UNIX system requires a command-line shell, and /usr/bin/bash is the OS X default.
- **Mappings**
  By default, OS X dynamically generates unique UIDs and GIDs for Active Directory accounts on a system. Ordinarily this is sufficient. However, if there's a need to manage the UIDs and GIDs, you can map to the appropriate fields in the user record in Active Directory that contain the values.
- **Administrative**
    - Prefer this domain server
      By default, OS X uses Site Information and Domain Controller responsiveness to determine the appropriate Domain Controller to use. Override this behavior here.
    - 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. This can be modified as necessary.
    - Allow authentication from any domain in the forest
      By default, OS X automatically searches all domains for authentication. Disable the behavior here to select specific domains to authenticate to.

Click Bind and enter the user name and password of a user who has permission to join clients. This doesn't need to be an administrator user—you may assign the privilege 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. If the object is being precreated, the user must be a member of the group with the ability to join the account as specified in Active Directory Users and Computers.

Command-Line Configuration

Windows Server Versions

Joining a Mac system to Active Directory has been successfully tested with Windows Server 2000, 2003, 2003 R2, 2008, and 2008 R2. The domain can be in either native or mixed mode without any change in the functionality of the OS X clients.

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

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

Once you've bound a system to the domain, you can use `dsconfigad` to set the administrative options that are available in Directory Access:

```
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 is no longer resident on the disk.

Configuration Profile Binding

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.

In-Depth Directory Service Information

Start by enabling directory services debug logging:

```
odutil set log debug
```

Now when you attempt to join Active Directory, you can look at the log at /var/log/opendirectoryd.log to see what's occurring.

When you've accomplished a successful join, use the same command to disable the debug logging:

```
odutil set log default
```

It may also be helpful to examine a packet trace of the client attempting to join to the domain. By default, the traffic is encrypted. To disable encryption:

```
/usr/sbin/dsconfigad -packetencrypt disable
```

To reenable encryption:

```
/usr/sbin/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.out," you could use the following syntax for `tcpdump`:

```
tcpdump –K -i en0 -s 0 -w capture.out 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.

Enterprise Integration Challenges

DNS Service

Since Active Directory relies on DNS service (SRV) records, the Mac client must be using the same DNS servers as all the Windows clients on the network. 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 your Active Directory domain:

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

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

OS X client attempts to dynamically update DNS records hosted by Active Directory, both the forward (A) and reverse (PTR) records.

Site awareness
Open Directory is able to use DNS service records and site information stored within Active Directory to find and communicate with the most appropriate domain controllers (typically ones in close proximity in multisite networks). By querying Active Directory for site information and polling the site's domain controllers, a Mac integrated in Active Directory can find not only the closest domain controllers, but also the ones that respond the quickest. Using this information, Open Directory chooses domain controllers and Global Catalogs, and communicates with them until a network change occurs or a domain controller stops responding.

Passwords

Because OS X uses Kerberos, it inherently supports Active Directory password policies and enforces restrictions on the length and complexity of passwords on client systems. Mac users can also change their passwords using the User & Groups preference pane in OS X.

In the days leading up to password expiration, users are notified that their password is about to expire. This gives them the opportunity to change their password in Active Directory, which resets the expiration timer, using the Users & Groups preference pane on the Mac client. When the password is within 24 hours of expiration, users can't complete login until they've changed their password.

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 is every 14 days, but you can use the `dsconfigad` command-line tool to set any interval that your policy requires.

Single Sign-on

Apple and Microsoft both support Kerberos to provide a secure single sign-on environment. When integrated into an Active Directory environment, OS X uses Kerberos exclusively for all authentication activities. The use of Microsoft's NT LAN Manager (NTLM) suite of protocols, including both NTLMv1 and NTLMv2, can be prohibited on the network as needed, without effecting 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 generates a ticket for that service without requiring the user to authenticate again.

You can use the Kerberos administration tools on a Mac to view currently issued tickets both from the command line, where klist displays the current tickets, or by using the graphical Ticket Viewer utility located at /System/Library/CoreServices/Ticket Viewer.app.

Namespace Support

With OS X, you have the option of supporting multiple users with the same short names (or login names) that exist in different domains within the Active Directory forest. By enabling namespace support, using 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.

Signed Connections

Open Directory is able to both sign and encrypt the LDAP connections used to communicate with Active Directory. Along with the signed Server Message Block (SMB) support that's present in OS X, you shouldn't need to downgrade your site's security policy to accommodate Mac clients. The signed and encrypted LDAP connections also eliminate any need to use LDAP over Secure Sockets Layer (SSL). If your site requires SSL connections, you can configure Open Directory to use SSL using the following command:

```
/usr/sbin/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 well-known certificates whose roots are installed by default, you must install and trust the root certificate in the System keychain. To manually install the root certificate, import it using the Certificates payload in a configuration profile, use 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>
```

Certificate Deployment

Client-side certificates for use with secure technologies such as 802.1X, VPN, and S/MIME are becoming more widely deployed. OS X has the ability to acquire a client certificate from a Microsoft Certification Authority. OS X 10.8 Mountain Lion uses the DCE/RPC protocol, bypassing the need for a web enrollment. The web UI of Profile Manager offers full support for defining the certificate request payload in a configuration profile. This can be combined with other payloads in the same configuration profile to simplify deployment of certificate-based technologies.

For example, a single configuration profile can include the Directory payload to bind to Active Directory, the Certificate payload that includes the root certificate of the Microsoft Certification Authority (to establish the necessary trust), the AD Certificate payload for the client certificate request, and the Network payload to configure the network interface for an 802.1X-authenticated network (for example EAP-TLS). This configuration profile can be deployed manually, via a script, as part of a mobile device management enrollment, or via a client-management solution. Additional payloads can be configured as needed.

Deployment Strategies

Policy Management

OS X offers a complete managed-client environment where every aspect of the Mac user experience can be restricted or controlled. Although technically different from the way Windows group policies are implemented in Active Directory, the effect is very similar. When fully integrated, a user's access to any OS X components can be restricted, and the user environment—including OS X features and third-party applications—can be preset or completely controlled.

Depending on the level of management your organization requires and the level of integration you want to use, there are several options for implementing client management for Mac computers:

Configuration Profiles

Because Windows and OS X handle preferences differently, the Mac is unable to use Group Policy Objects (GPOs) in Active Directory. Instead, policy data can be delivered to Apple devices through the use of configuration profiles.

Client and account configuration as well as policy data and certificate deployment can all be accomplished with configuration profiles. These profiles can be deployed manually as part of the deployment image, or managed by enrolling the device in a mobile device management solution.

Clients still use Active Directory for user authentication, while Open Directory supplies Managed Preferences only.

Do nothing

Open Directory automatically enables authentication to Active Directory, including full support of password policies. With Open Directory, you can also set up network home directories for Mac users contained in Active Directory. Although this doesn't allow for client management, it does offer a fully functional environment in which standard users can be configured as nonadministrator users on Mac clients. This allows you to ensure that they won't be able to change any system settings.

Use Profile Manager

Profile Manager allows an administrator to configure policies outside of a directory service. In this scenario, a user would either opt in to service configuration and policy settings or join the client to a Profile Manager server via a web interface. The user would then authenticate against Active

Directory, and the policies and settings would already exist locally on the Mac client. If the Mac is bound to a profile server, any changes to policies trigger a push notification, after which the Mac contacts the Profile Manager service to update policies and settings.

Use a third-party management solution

Mobile device management and client management vendors such as Absolute, AirWatch, JAMF Software, MobileIron, and others can manage OS X policy data with configuration profiles in a manner similar to Profile Manager. These solutions allow for updates to client policy without the need for the client to have access to the directory service.

Use a third-party Active Directory solution

Products from Beyond Trust, Centrify, Thursby, and Quest allow policy data to be stored in the Active Directory domain without requiring IT teams to extend the schema. In general, these solutions allow policies to be set as Group Policy Objects in Active Directory, as is done for Windows clients. Each solution replaces OS X native Active Directory capabilities with each third-party's client-side directory services plug-in.

Home Directories

Regardless of your strategy for policy management, you can set up users with local homes, in addition to accessing the network home directory specified in the user record in Active Directory. OS X can be set to automatically mount that share at login.

Local

With the default configuration of the Apple Active Directory in Directory Services, the user's home stays on the local system without any change to the user record in Active Directory. If a network home is defined in the user record, that share mounts on the desktop when the user logs in.

Distributed File System (DFS)
OS X also supports home directories and mounting of file shares via DFS. The Universal Naming Convention (UNC) path is the same as the SMB path, but if the name is hosted in a DFS namespace, the share is mounted correctly.

Network

To define a network home in the Mac user's Active Directory record, use a URL in the form of \\server\share\user—just as you would for a Windows user. When interpreted by the Active Directory configuration on the Mac, the server name is added to the Active Directory domain, forming a URL: smb://server.ad.domain/share/user.

Note: If the user's domain is different from the domain of the user's home folder, it may be necessary to put the fully qualified name of the server in the URL. So instead of //server/share/user, you'd use //server.userad.domain/share/home. Using a Mac-friendly naming convention doesn't effect the Windows systems on the network.

The Mac user's network home can be hosted on either OS X Server or a Windows server with either AFP or SMB. You can even host home

AFP network homes
It's also possible to use an afp:// URL for your home directories. In Active Directory, the URL remains in the standard UNC. On the Mac, however, you can allow the client to translate the SMB path into an AFP path.

directories for both OS X and Windows clients on OS X Server, providing Mac services over AFP and Windows services over SMB.

Conclusion

Apple 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 and Windows handle preferences differently. OS X uses xml data delivered via configuration profiles to update configurations, policies, and certificates and have similar capabilities as Group Policy Objects do in Active Directory.

For information on the best practices discussed in this paper, or any other aspect of integrating OS X systems with Active Directory, please contact your Apple representative or Apple Authorized Reseller for assistance.

Appendix A: More Information

Please see the following Apple Support Knowledge Base articles for more information:

- **Mac 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

Appendix B: Third-Party Add-on Solutions

If your deployment requires Distributed File System (DFS) shares or Group Policy Objects (GPOs), you can choose a third-party product to extend the capabilities of the Apple solution.

- **GroupLogic ExtremeZ-IP** www.grouplogic.com
  With this Apple Filing Protocol (AFP) server for Windows servers, Mac clients can access files on a Windows server using the native file-sharing protocol, AFP.
- **Centrify DirectControl** www.centrify.com
  This Active Directory plug-in enables OS X to use Active Directory GPOs without requiring any schema modification.
- **PowerBroker Identity Services Enterprise Edition**
  www.beyondtrust.com
  This Active Directory plug-in enables OS X to use Active Directory GPOs without requiring any schema modification.
- **Thursby ADmitMac** www.thursby.com
  This directory services Active Directory plug-in and SMB client supports DFS shares.
- **Objective Development Sharity** www.obdev.at/products/sharity
  This SMB client supports DFS shares.
- **Quest Authentication Services** www.quest.com
  This Active Directory plug-in enables OS X to use Active Directory GPOs without requiring any schema modification.

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 manual is accurate. Apple is not responsible for printing or clerical errors.

1/2/13