Integrating Mac OS X 10.6 with Active Directory

1 April 2010

Introduction

Apple Macintosh Computers running Mac OS X 10.6 can be integrated with the Boston University Active Directory to allow use of Active Directory (AD) credentials for authentication. Mac OS X Server can be added into the equation to enable more complex, full-featured management for multiple Mac OS X workstations. **This document was written for a pre-release version of Mac OS X 10.6, and may not be completely accurate.**

About this document

This document is intended for system administrators. It is not intended for individual users, and it assumes some familiarity with both Active Directory and with Mac OS X and Mac OS X Server. This document covers only the initial integration of the discussed technologies; implementing specific services and accomplishing specific management tasks is left to the administrator.

Prerequisites

This document covers integration of Max OS X 10.6 or later with Active Directory as it has been deployed at Boston University. It is possible to use older versions of Mac OS X with AD as well, but it is a slightly different procedure and is not covered here. Use of the latest available version of the operating system is strongly recommended - the Directory Services components in Mac OS X get updated with every patch, and by applying all available patches you ensure that your systems have all of the latest security fixes and bug fixes.

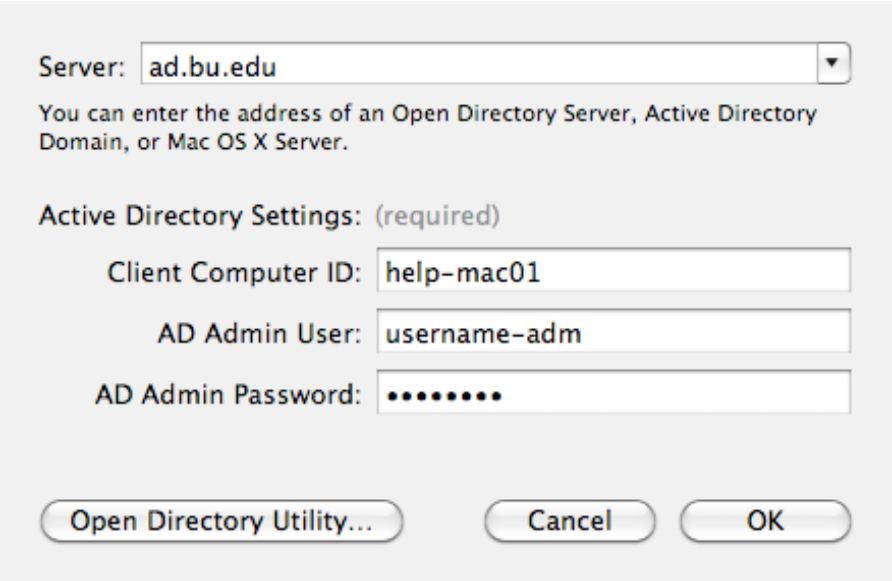
In addition to having one or more Macintosh computers with 10.6, you need either to be an OU administrator for your department, or be able to enlist your departmental OU administrator's assistance to complete the procedures outlined herein. If you plan to use Mac OS X Server, it needs to be version 10.5.3 or higher. This document discusses Mac OS X Server version 10.6, but a 10.6 client should be useable with a 10.5.x server - see the older version of this document for configuring such a server. You must have a static IP address and a hostname for the server. It is recommended that you try this process on one or more test systems before using it in a production environment, as the Office of Information Technology can provide only limited support for this process at this time.

Getting started

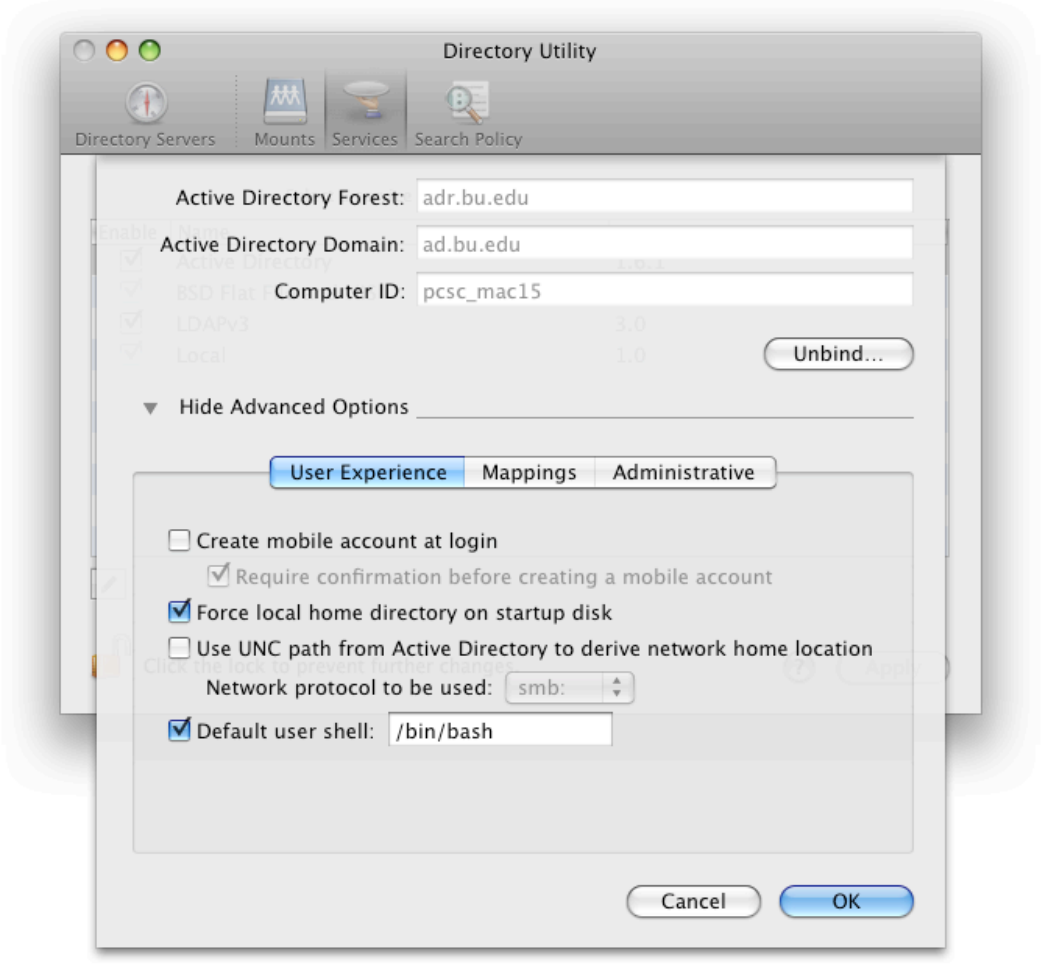
As mentioned above, there are two modes in which Macs may be integrated with AD. The simplest method is to integrate the Mac client systems directly. This will enable authentication against Active Directory, which has the benefit of simplifying user account administration for such systems. To integrate a client, first install the operating system and

all available patches. **You must be running at least 10.5.3 *before* continuing**. Once the client is fully patched, you should configure it as desired, with application software and system-wide settings as you desire them. Any local accounts should be named in such a way as to avoid overlap with account names in the Active Directory, as a local account will override any Active Directory account with the same username. Once you've reached this point, it may be useful to create an image of the system, especially if you desire to integrate multiple, hardware-identical systems with Active Directory. Next, you should configure network settings on the client system(s). If you are using static IP addresses, it is recommended that the computer name in the Sharing section of the System Preferences be set to match the hostname associated with the machine's IP address. This is not strictly necessary, but it can simplify management moving forward. Additionally, it is a good practice for the machine's name to take the form of *department-description*, e.g., for the Office of Information Technology, a computer's name might be oit-testmac04. Consistent, meaningful naming is useful when managing a computer that is a member of one or more directory systems.

Once the machine is fully configured, the next step is to bind it to the Active Directory. To do this, log into the Macintosh with local administrator rights and open /Applications/System Preferences. In System Preferences, click on the Accounts preference pane. Click on the area in the left-hand column titled "Login Options", then click on Join... to join a new network account server. Now, enter the appropriate information into the dialog Snow Leopard will automatically determine the type of server from the address entered. The Computer ID will be based on the name in the Mac's Sharing settings; ideally, the name entered here should be identical to the DNS hostname associated with the machine's IP address. Using a single, consistent name for DNS, the Sharing settings, and the AD machine account eliminates much potential confusion for your end users. The Active Directory Domain field should be set to ad.bu.edu, and the credentials should simply be those of your department's OU administrator. *(See the image below for reference.)*



When you click OK, the machine will display a progress indicator as the bind is effected. Once the bind has taken place, click the Edit... button in the Accounts window, then click the Open Directory Utility... icon at the bottom of the window. One major change from previous versions of Mac OS X to 10.6 is the exclusion of the Directory Utility application from the Utilities folder. Directory Utility can either be opened in the way just described or by going to /System/Library/CoreServices. Authenticate to make changes, then double-click Active Directory, then click the disclosure triangle next to Show Advanced Options to expand the window. Under User Experience, uncheck “Use UNC path from Active Directory” and make sure that “Force local home” is checked. Configure the default user shell appropriately, either with the default of bash or with /usr/bin/false if you wish to disable shell access for AD users. Check “Create mobile account” for systems that will not have an always-on network connection: it will enable cached credentials. This is most appropriate for laptops.



On the Mappings tab, set “Map UID to attribute” to bu-ph-index-id-numeric. This will ensure that AD accounts use the actual Global UID for any given user, which is a necessity if your Macs will interact with any other UNIX-based services, such as AFS or NFS, and has the further benefit of ensuring consistency between workstations if you are deploying more than one. On the Administrative tab, add any additional groups that you wish to allow administrative access for into the “Allow administration by” box.

At this point, authentication with AD credentials should be working. Restart the the computer and try logging in with an Active Directory account. You **do not** need to prepend AD\ or anything similar–simply use the login name on its own. If it does not work, see the troubleshooting section at the end of this document.

Using Open Directory in conjunction with Active Directory

By deploying a Mac OS X Server which is bound to Active Directory, and by binding client workstations to both the Mac OS X Server and to AD, it is possible to use many of Mac OS X’s workstation management features in conjunction with AD accounts. To begin this process, first configure one or more workstations and ensure that they have been successfully bound to AD, as per the first section of this document.

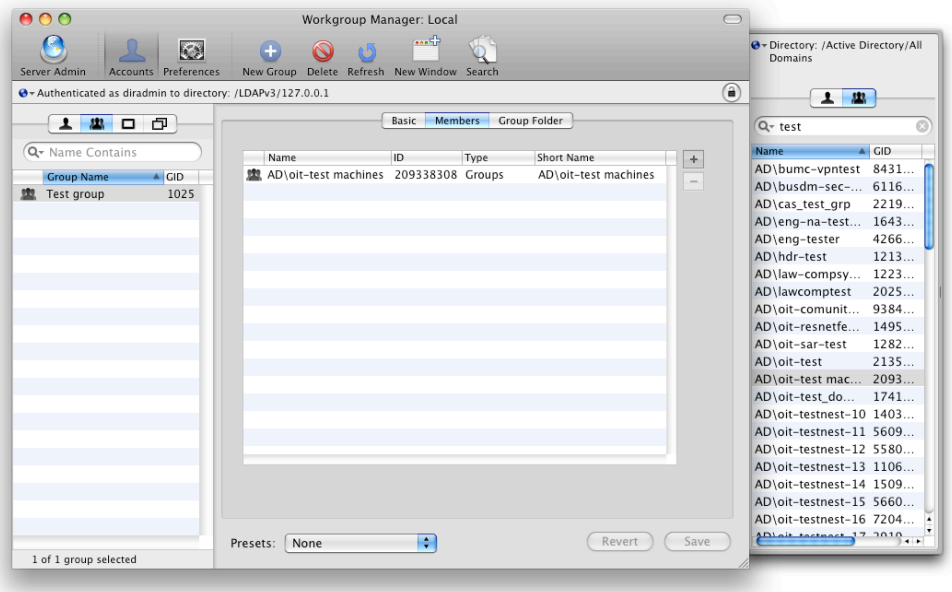
Next, install and configure a Mac OS X Server. As with the client, the server **must be patched to at least 10.5.3 *before* beginning this process**. If the server is a new installation (which is the recommended process for the purposes of this document) it should be set to “Advanced” rather than “Standard” or “Workgroup” and it should simply be left as “Standalone” during the setup assistant: binding to AD must be done at a later time. **A static IP address and hostname are required, and should be obtained before trying to configure the server environment**. The server will prompt to configure services upon first boot; this should be delayed until after the patches are all applied and AD binding is complete. For the binding process, the steps are almost identical to those for binding a client: the difference is that it is not necessary to leave any boxes checked on the “User Experience” tab; rather, these settings can be configured on the client workstations or applied via Workgroup Manager. Similarly, it is unnecessary to specify administrative rights for AD groups unless you need multiple accounts to have administrative rights on the server console. The server must be added to the same special AD group as the clients.

Once the server has been bound to Active Directory, launch Server Admin. Choose which services to configure–most of these are optional, and this document will touch only briefly on services which are not required for integrating AD. The one service you must configure is Open Directory. Once Open Directory is enabled, select it from the list of services. On the General tab, click the Change button to promote the server to an Open Directory Master. Selecting this option after binding a server to AD will automatically detect that status and pass through Kerberos authentication to the Active Directory rather than to the local directory. To verify that single sign-on is properly configured, launch Terminal, and issue the command `sudo klist -kt`. The results should indicate that each service has a Kerberos

principle in the form of *servicename/servername.ad.bu.edu@AD.BU.EDU*. It is normal for each service to have three identical entries. Finally, 0pen the Terminal application and enter the command sudo slapconfig -setmacosxodpolicy -binding required

The next step is to bind the client workstation(s) from the first section to the Mac OS X Server. On the client system, open Directory Utility, authenticate as a local administrator, and click the "+" then add the Mac OS X Server. You will be prompted for a user name and password, at which point you should provide those of the Directory Administrator account on your Mac OS X Server. You may notice that any hyphens in the client's name are converted to underscores: **do not change them back**. Open Directory does not work well with object names which contain hyphens. The end result of this is that the machine will have a different name on the OD server than it had locally or in AD, but this should have any effect on the usability of the server and its services. Next, click Show Advanced Settings and then the Search Policy button, and ensure that AD is above the Mac OS X Server in the list.

At this point, the client system should be bound to both AD and OD. To verify this, try managing some settings via the Mac OS X Server. Open Workgroup Manager, click the "Viewing directory" drop-down, and ensure that it's set to /LDAPv3/127.0.01–you may need to select the "Other" option to allow this to be selected for the first time. Next, authenticate as the local Directory Administrator ("diradmin", by default) and switch to the Groups tab. Create a new group, then click the Members tab, and click the "+". In the drawer, click the drop-down menu at the very top and select "/Active Directory/All Domains." Switch to the group tab in the drawer as well, type the name of a group of users into the search box, and wait for the results to appear. This may take several minutes, during which there will be no indication of progress. Once the group has appeared, drag the group into the Members list, and click Save. The next screenshot illustrates these last few steps, and should serve as a reference for how Workgroup Manager should appear at this stage.



Next, click the Preferences button in the toolbar and configure a preference. Dock settings are readily noticeable, so this is a good category to test. Change the position of the Dock, or enable hiding, and apply the changes. Log in to the workstation with an AD account that is a member of the group you selected and verify that the Dock's settings reflect the settings configured in Workgroup Manager. It is possible to manage settings based on user groups, as in this example, or based on computers. Note that if you are using computer-based management, and one of the managed machines has its account reset and subsequently re-bound, you will need to remove it from the group in Workgroup Manager and re-add it.

Troubleshooting and Tips

If something doesn't work, first verify the steps above.

It may be useful to log in with a local account, then open Terminal, then try to authenticate as an AD account via the login command. If login works, issue the id command, and verify that the account's correct global UID is displayed, and that the correct AD groups are enumerated. If either condition is not met, verify or ask your OU admin to verify for you that the machine account in AD is indeed a member of your OU's privileged Mac group. If the information does display correctly, open Directory Utility and toggle "Force local home directory" off and then back on, then reboot and try again.

If something is still not working, disconnect the workstation from the network and remove the Active Directory entry in Directory Utility, then delete the /Library/Preferences/DirectoryService folder and the /Library/Preferences/edu.mit.kerberos file. Reboot and try again. If these steps still don't solve the problem, reinstall and try again, or try from a different test system.

If you don't need Bonjour (aka Rendezvous, aka Zeroconf), you can disable it and potentially reduce login time; log in to the client system as an administrator, and issue the commands

```
sudo launchctl unload -w /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist
```

and

```
sudo launchctl unload -w \
/System/Library/LaunchDaemons/com.apple.mDNSResponderHelper.plist
```

It is possible to view, renew, and destroy Kerberos tickets via /System/Library/CoreServices/Kerberos.app or via the command line utilities (klist, kinit, kdestroy, and so on). Kerberos authentication is not available for off-campus systems.

If you are unable to resolve a problem, you can request assistance via e-mail to ad-admin@bu.edu or ithelp@bu.edu. The former is most appropriate for Active Directory problems, the latter for Mac-specific problems. At times this distinction may not be clear, but the two groups work closely and will redirect your inquiry as necessary. Suggestions and requests for additional topics may be sent to ithelp@bu.edu for consideration.

When connecting to a network share, the "Connect to..." dialog automatically populates the username box with the full name of the current account. To override this behavior, log in as an administrator and launch Terminal then run the following command:

```
defaults write /Library/Preferences/com.apple.NetworkAuthorization UseShortName -bool YES
```

If your Macs are off campus frequently, or are shut down or put to sleep at night, they may sometimes spontaneously lose their bindings. This happens because the machine account in Active Directory defaults to requiring an update every two weeks. If the client machine

misses one of these updates, the AD will no longer communicate with it correctly. To prevent this, you can open Terminal on the client, and issue the following command:
sudo dsconfigad -passinterval 0
this updates the binding information such that the password is never updated.

If you deploy your Macs from a master image, and you use a Mac OS X Server, you must run a command to remove the local KDC before capturing the image file. If you do not, the Mac OS X Server will report that each client is a duplicate as it is added, and it will be impossible to bind more than one of the clients successfully at the same time. To prevent this, run:
sudo dscl /Local/Default delete /Config/KerberosKDC

Additional references

The following documents may provide additional information on Active Directory/Open Directory integration:

Building an AD/OD Sandbox
http://www.afp548.com/filemgmt/visit.php?lid=69

Leveraging Active Directory on Mac OS X *
http://www.bombich.com/mactips/activedir.html

AD-OD Integration Whitepaper *
http://www.afp548.com/filemgmt/visit.php?lid=12

Apple's Mac OS X Server resources
http://www.apple.com/server/macosx/resources/

The following sites may have additional useful information for integration and/or lab management topics:

http://www.afp548.com
http://www.bombich.com
http://www.macwindows.com

* These documents were written for 10.4.x, but may still contain useful information.