The AD-OD Sandbox

A quickstart guide for setting up Active Directory and Open Directory in your test environment

Mac OS X 10.5 Leopard Edition

1.4

The Sandbox..... 3

Installation of Windows Server 2003..... 4

Setting up Active Directory..... 5

Check DNS using nslookup..... 9

File sharing on Windows Server 2003..... 10

User creation in Active Directory..... 14

Testing file services connections..... 15

Specifying an account for the binding process..... 16

Binding Mac OS X 10.5 to Active Directory..... 18

Import Users into Active Directory..... 19

Active Directory group membership..... 22

Bringing Open Directory into the mix..... 24

Now, the easy way (optional)..... 27

Binding the client to both directories..... 27

Managed Client for Mac OS X (MCX) and AD together..... 28

Hosting the home folders on the Open Directory server..... 30

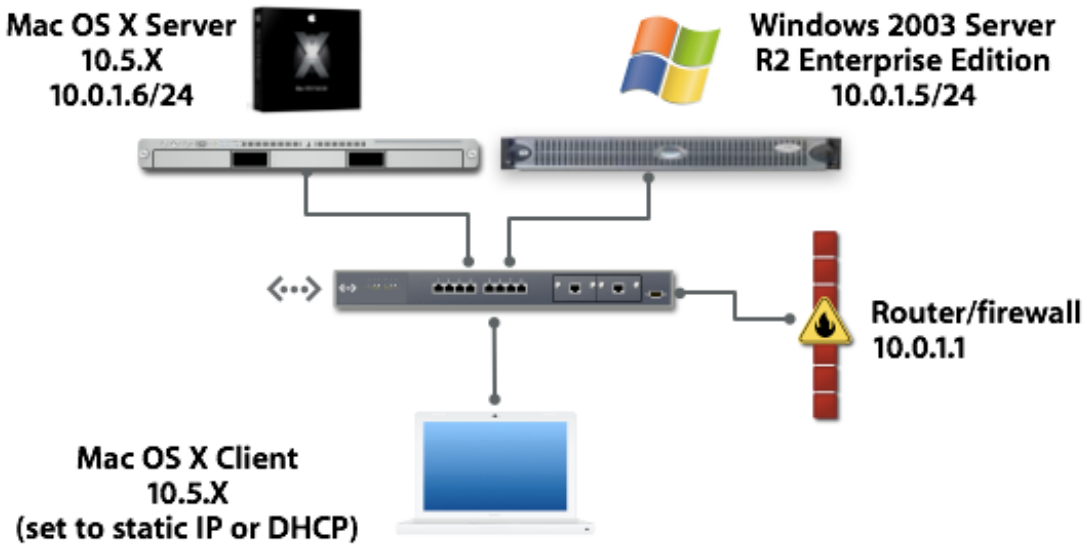
The Sandbox

The reason this document was built is to bring the pieces of the puzzle together in a simple and step-by-step fashion. There are plenty of online articles, whitepapers, and listserve archives that talk about Active Directory and Open Directory integration, but there wasn't one document that graphically walked people through the steps of setting up Active Directory from scratch and then tying Mac OS X and Mac OS X Server into that. Hopefully this document will help people get a sandbox environment up and running in less than a few hours and eliminate frustrating snags and confusing steps that are missing from most guides out there today.

What this document is not intended for is for setting up Active Directory and Open Directory in any production environment. The advanced guides found on Apple's website, as well as afp548.com and macenterprise.org fill in those gaps very well. Where this guide can really help you is to simply get familiar with the two directories, set up user accounts and learn how the integration works. Once your comfortable, then apply what you've learned to your production environment after a great deal of testing.

What this setup consists of is a Windows 2003 Server, a Mac OS X Server and a Mac OS X client. DHCP services can be provided by a router or either of the two servers used in this document. DHCP setup knowledge is assumed, so that service will be up to you to configure for your sandbox. When configuring, use a range that's within the 10.0.1.1/24 range, such as 10.0.1.10 through 10.0.1.20 (or up to 253 if you wish). The software versions used, at the time this document was written, are:

- **Windows Server 2003 R2 Enterprise Edition** (with SP2 and all patches applied)
  - *Used for Active Directory, DNS and File Services*
- **Mac OS X Server 10.5.2**
  - *Used for Open Directory and File Services*
- **Mac OS X 10.5.2**



Installation of Windows Server 2003

During installation, it asks you to name the computer and provide an administrator password. This is an important step in regards to how you want your AD server to be named when it has a fully qualified domain name. In my environment, I want my AD server to be **ad.apple.edu**, therefore I name the computer **AD** (host name of what it will resolve as when DNS is set up). Set the password to whatever you like. Since password policies are enforced during installation, you'll have to mix the case and include a number.

When prompted to enter network information, enter the static IP address and appropriate settings. In the environment for this document, I'm using the following:

IP address:	**10.0.1.5**	
Subnet mask:	**255.255.255.0**	
Router:	**10.0.1.1**	
DNS Primary:	**10.0.1.5**	(should match IP address so that DNS setup goes smoothly)
DNS Secondary:	**10.0.1.1**	(typically your home router so that you can run Windows update)

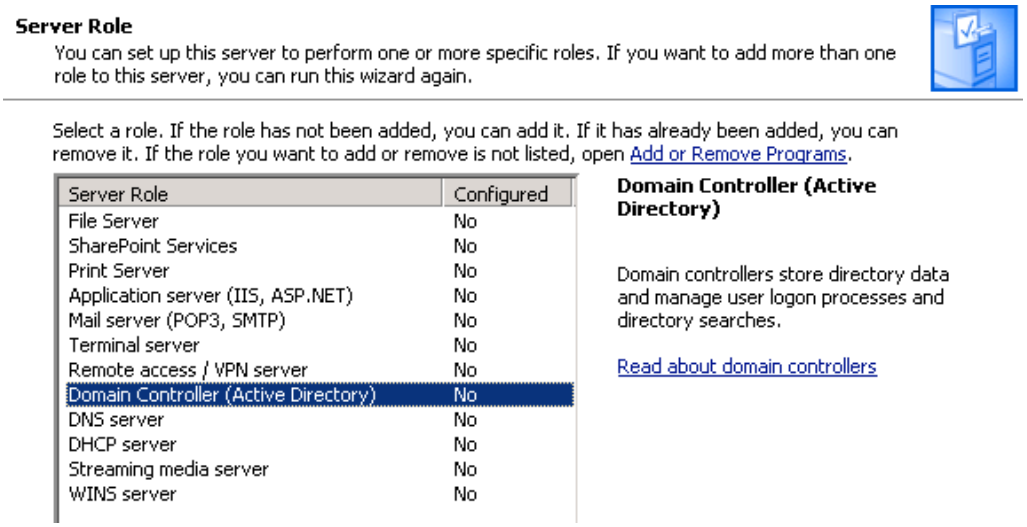
When installation is finished, reboot and log in to the server. Run Windows update to ensure that you have SP2 and all other patches installed (not all are necessary, such as IE 7).

To take advantage of the included files to import DNS entries and user accounts, you will need to install the Support Tools. On your Windows Server 2003 Disc 1, navigate to **:\SUPPORT \TOOLS** and launch **SUPTOOLS.MSI** to install.

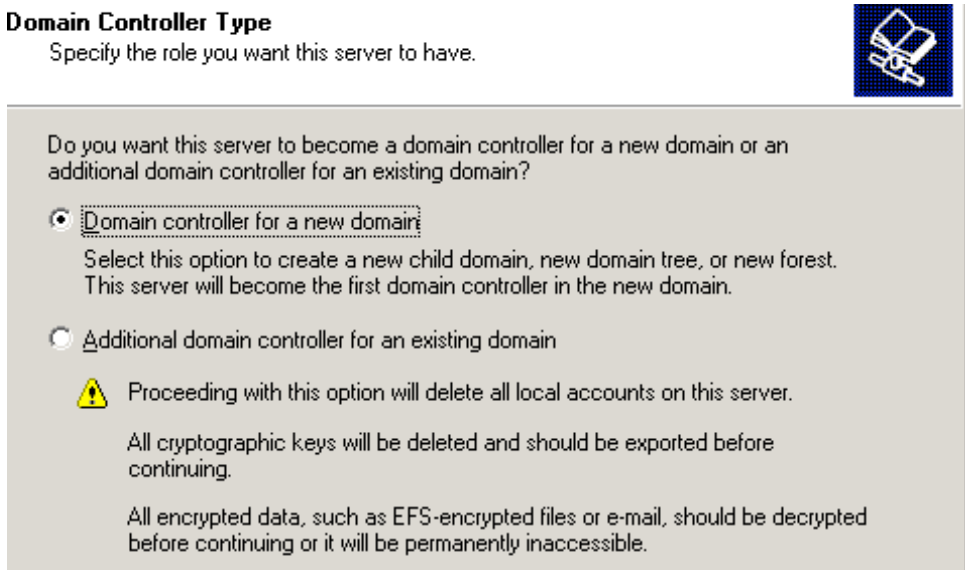
Setting up Active Directory

1. Click on the **Start** menu and select **Manage Your Server**.
2. In the Manage Your Server app, click on the link to **Add or remove a role**.
3. Select **Domain Controller (Active Directory)** and click **Next**.

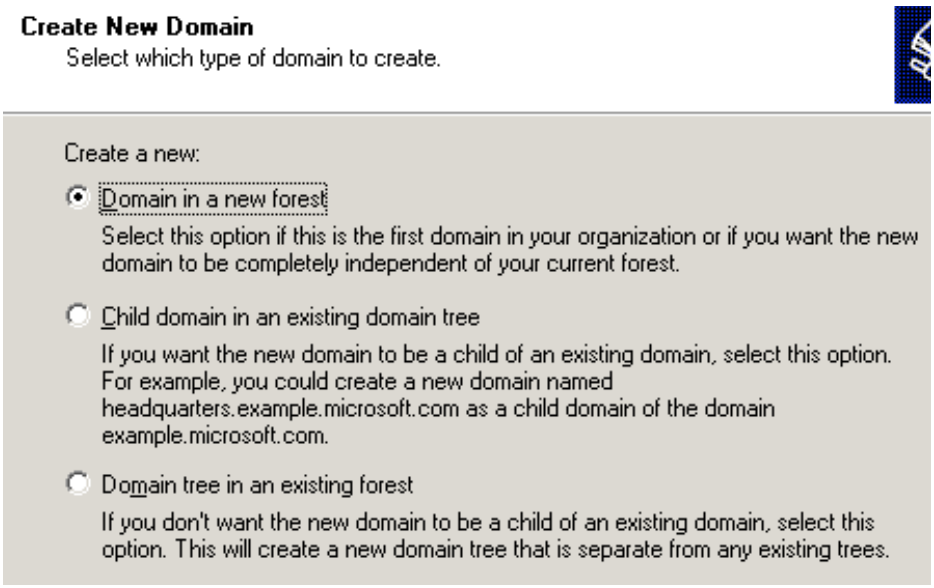
   NOTE: Be sure that you're not utilizing the automatic setup that comes with Windows 2003 Server. Instead, this document will walk you through setting up Active Directory, which will also prompt you to add the DNS service (which you'll do). Then file services will be added later.



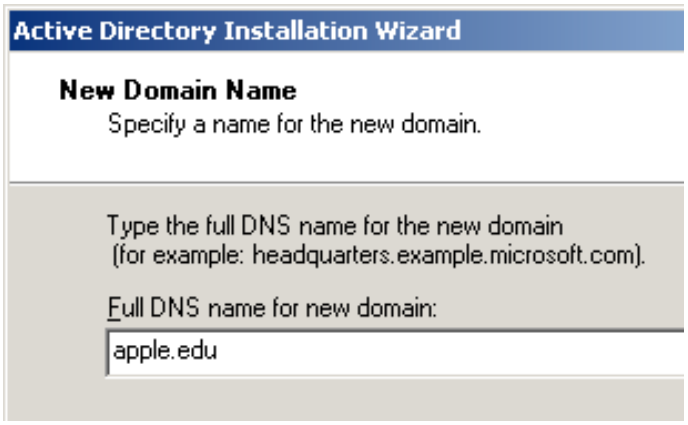
4. Set the domain controller type for a **new domain**.



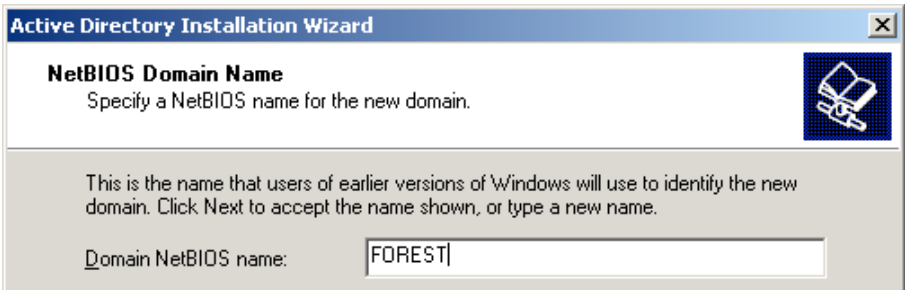
5. Create a new **Domain in a new forest**.



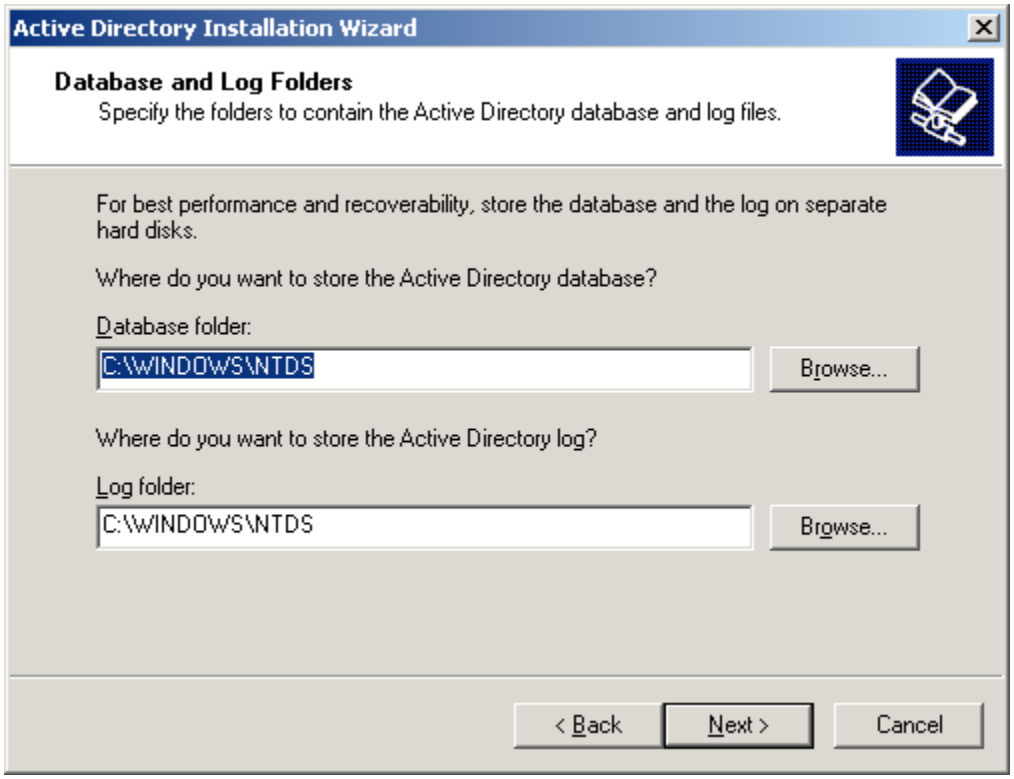
6. Naming the new domain is a critical step to ensure that your AD server resolves as you expect. With a desired fully qualified domain name of **ad.apple.edu** for this server, you must set this as **apple.edu**, as shown below and click **Next**. The fact that it asks for the "Full DNS name" can be a bit misleading.

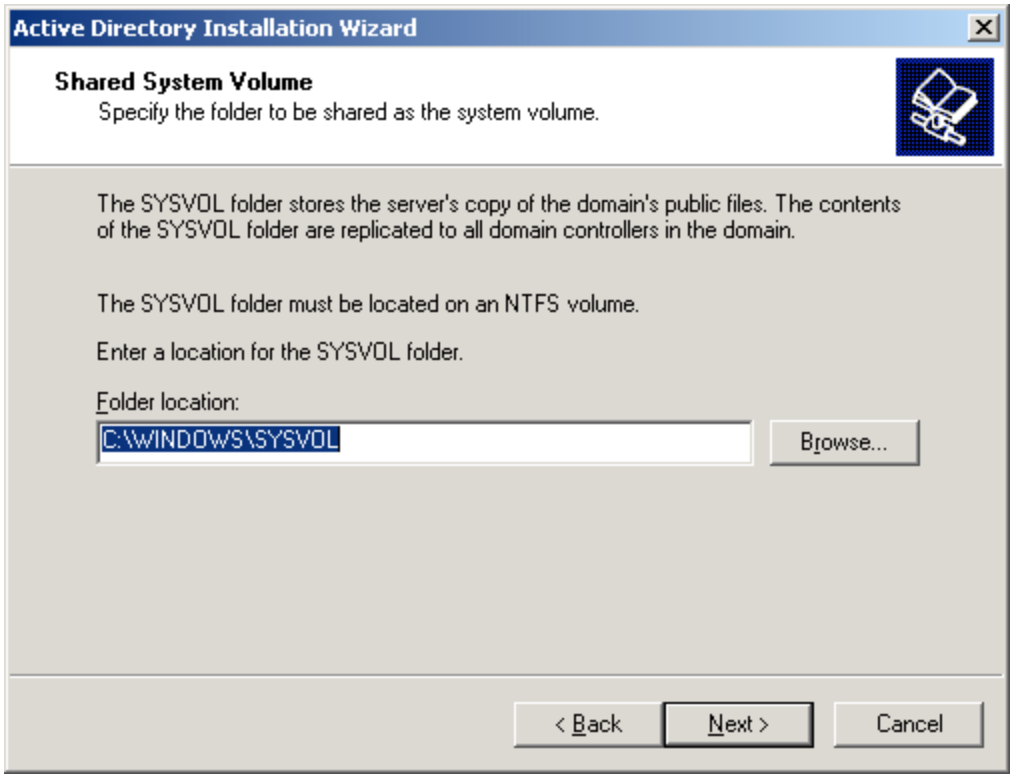


7. A common assumption for the Domain NetBIOS name is **AD**, but you've already used AD for your computer name. You can enter whatever you like here. This document is using **FOREST**.

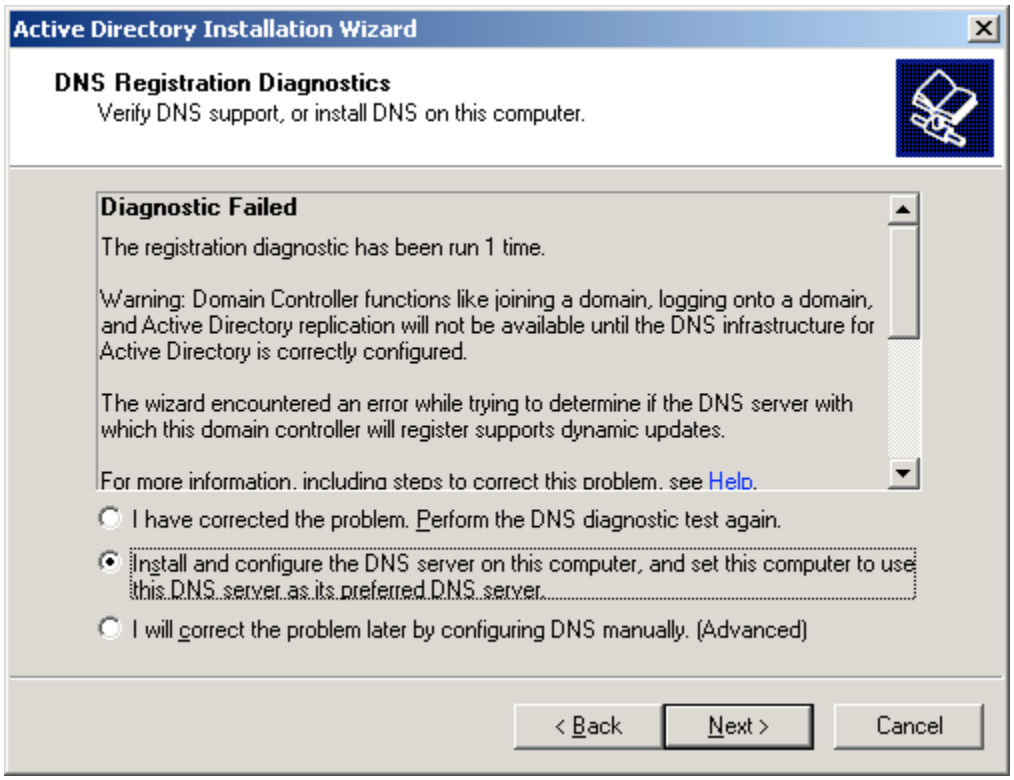


8. Choose the default locations for the database, log and SYSVOL data.

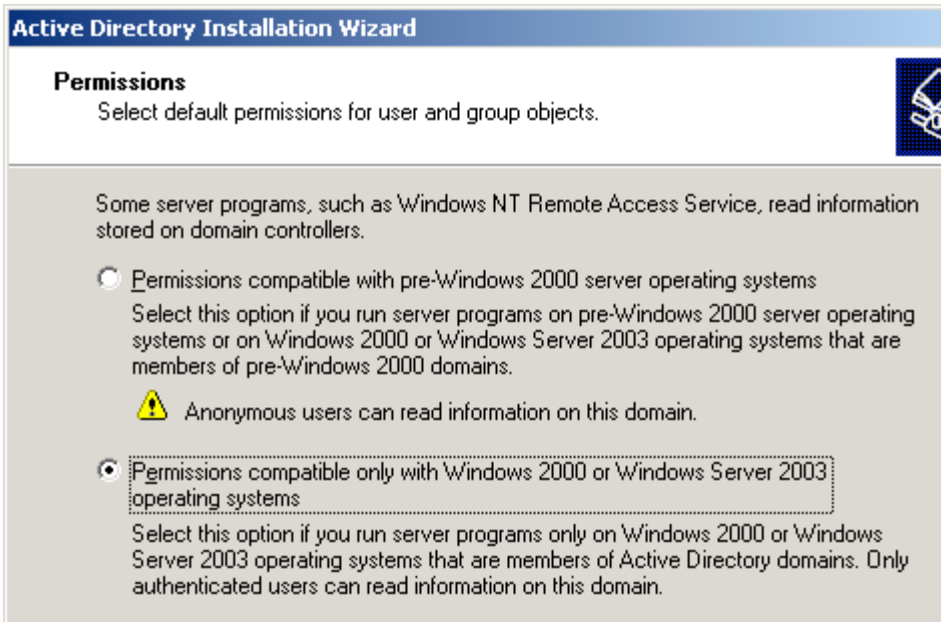




9. At this point, DNS wants to come along for the ride. Choose the **middle option at this step so that DNS is installed along with Active Directory**. Based on your computer and domain names that you previously set, this will do the right thing (for now).



10. Default permissions (**compatible with Windows 2000 and newer**) should be used.



11. Type in a restore password and click **Next**.

12. Confirm your settings and finish. Upon completion, restart the AD server.

Check DNS using nslookup

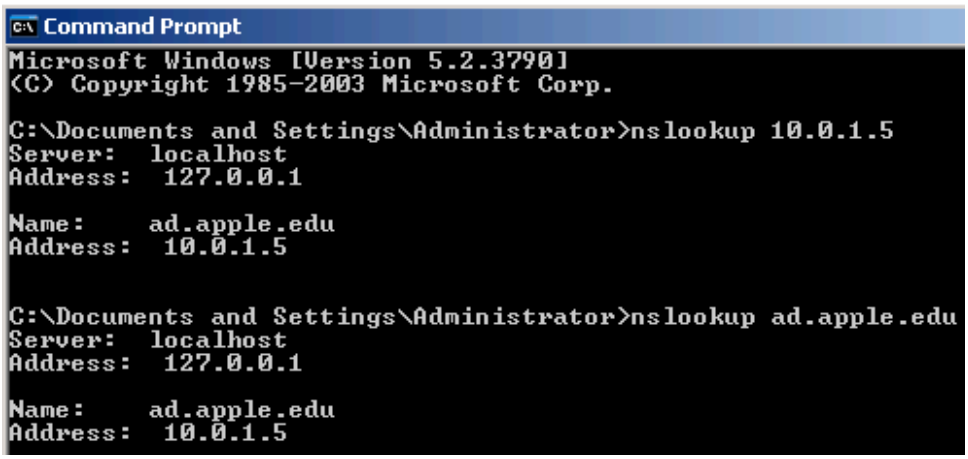
Now we'll use the nslookup command (similar to what the host command does for us in Mac OS X) to check DNS.

1. Click **Start** and select **Command Prompt**.
2. Type **`nslookup 10.0.1.5`** and press **return**. You should find that it doesn't resolve because there are no forward or reverse records in your DNS zones.
3. Locate the **dns.bat** file that is associated with this document and copy it to your Windows server. Here are the contents of that file.

```
PATH=c:\Program Files\Support Tools;C:\Documents and Settings
\Administrator\Desktop
dnscmd . /ZoneAdd 1.0.10.in-addr.arpa /DsPrimary

dnscmd apple.edu /RecordAdd apple.edu od A 10.0.1.6
dnscmd apple.edu /RecordAdd 1.0.10.in-addr.arpa 6 PTR od.apple.edu

For %%A In (10 11 12 13 14 15 16 17 18 19 20) Do (
    dnscmd apple.edu /RecordAdd apple.edu host%%A A 10.0.1.%%A
    dnscmd apple.edu /RecordAdd 1.0.10.in-addr.arpa %%A PTR host%
%A.apple.edu
)

dnscmd apple.edu /RecordAdd apple.edu ad A 10.0.1.5
dnscmd apple.edu /RecordAdd 1.0.10.in-addr.arpa 5 PTR ad.apple.edu

exit
```

4. Edit this file to meet your needs by right-clicking on it and selecting **Edit**. Be sure that the path to your support tools location is correct, and notice to change the Administrator name if you chose something different. You'll see that this .bat file puts in forward and reverse records for **ad.apple.edu** (10.0.1.5) and **od.apple.edu** (10.0.1.6). It also creates records for hosts 10.0.1.10-20 as **host10.apple.edu**, **host11.apple.edu**, etc.. Edit this script to meet your needs
5. When the script has the right information on it, close and save it.
6. Double-click on the **dns.bat** file to run it. It will put in the records you define.
7. Go back to the command prompt and press the **up arrow** to show the last command.
8. Press **return** and see that DNS resolves successfully.

9. Type **`nslookup ad.apple.edu`** and that should resolve as well.



10. If your requests aren't resolving correctly, visit **http://tinyurl.com/ysqqb7** for an excellent document that covers DNS setup in details for Windows 2003 Server.

File sharing on Windows Server 2003

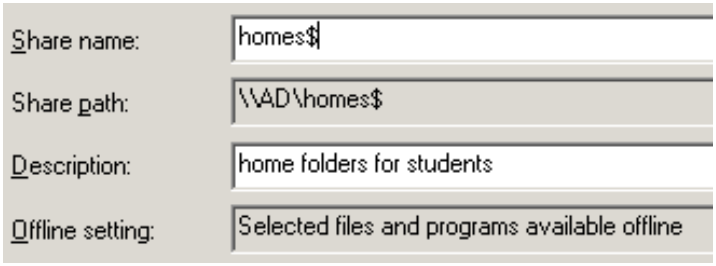
Before hosting home directories on the Mac OS X Server, let's go through the steps of having the AD server host it first...just for fun.

1. Click **Start** and select **Manage Your Server**.
2. In the management window, click **Add or remove a role**.
3. Choose **File Server** and click **Next**.
4. When the File Server installation wizard runs, do **not** choose any **optional components**. This is how most setups are configured, and we want to imitate that as closely as possible.

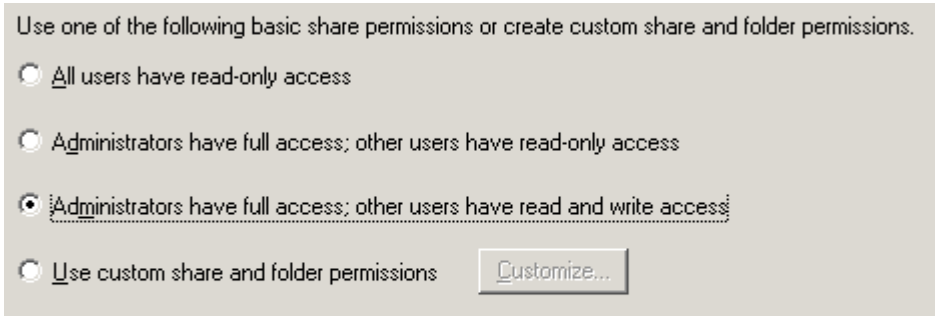
5. Let the server restart upon completion.
6. Using the **Manage Your Server** application, you now see the File Server as an active role. Click on the link to **Add shared folders**.

7. You can browse to or just put in the path **C:\homes**. If that folder isn't there, it will ask to create it for you.

8. The next step is to name the sharepoint. Name the folder **homes$**. The reason for doing this is because the trailing dollar sign keeps the sharepoint hidden from file server browsing. Users can get to the sharepoint if they know the name of it, but they cannot browse to find it. Since it's fairly common for Windows Server admins to do this, this document will as well.

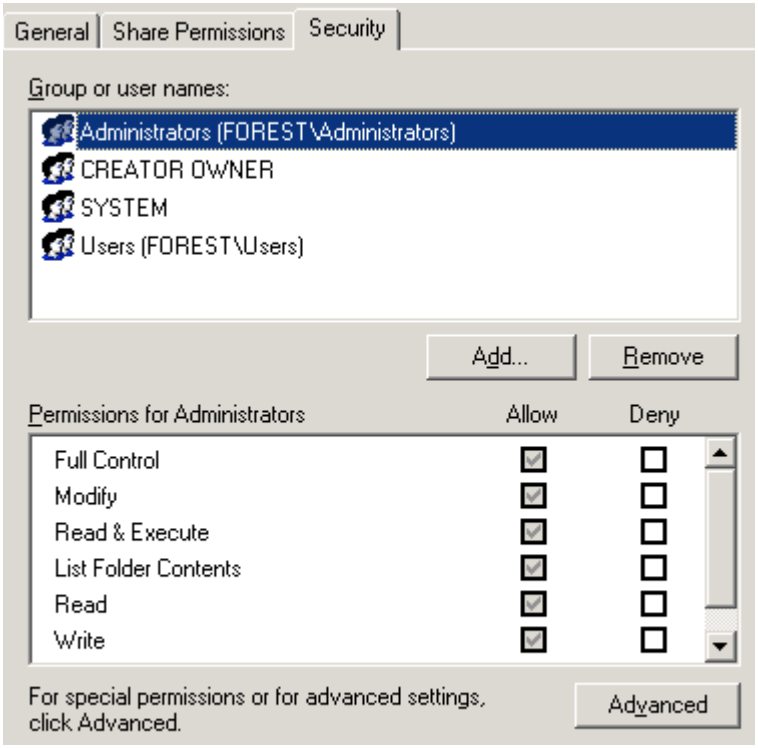


9. Set the permissions so that Administrators have full access and other users have read and write access.

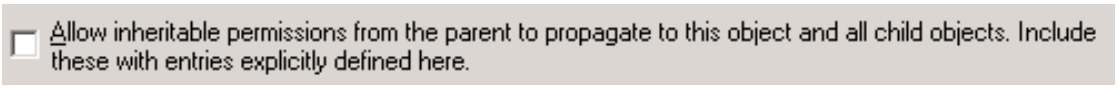


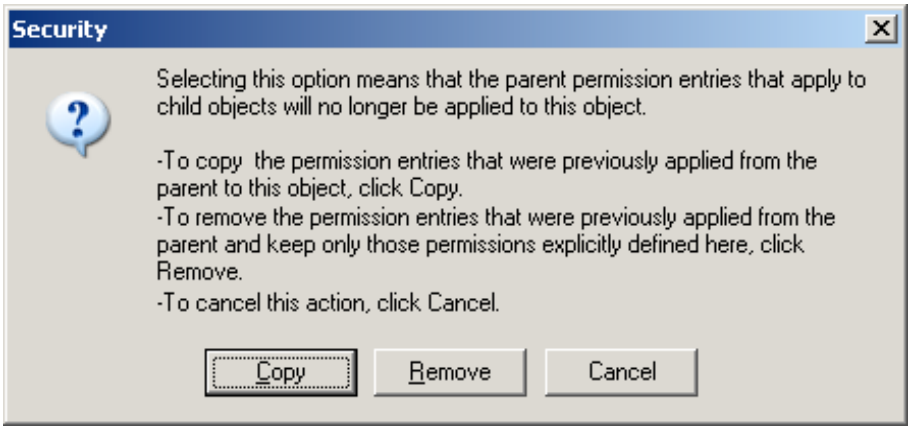
10. Your summary should look like this.

11. If you leave the default permissions alone, your first AD authentication attempt from Mac OS X will be successful, but you won't be able to write to the H: drive for any particular user. Follow these steps after creating that new homes$ sharepoint to avoid any headaches.
12. In the **Manage Your Server** application, click on **Manage this File Server** to open the File Server Management application.
13. Right-click on your new **homes$** sharepoint and select **Properties**.
14. Click on the **Securities** tab, and then the **Advanced** button.

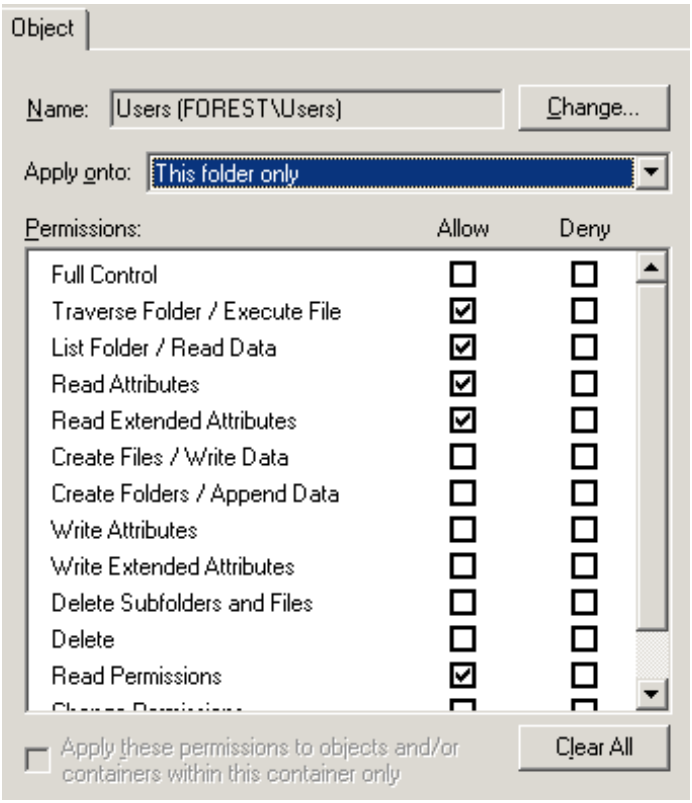


15. Uncheck the **Allow inheritable permissions...** checkbox and click **Copy** when the dialog box pops up.





16. Highlight the last entry of **Special** permissions for the **Users** group and click **Remove**.
17. Highlight the new last entry of **Read & Execute** for the **Users** group and click **Edit**.
18. Change the **Apply onto** field to **This folder only**. Taking this step will prevent users from viewing the contents of other user's home directories.



19. Click the **Apply** and then the **OK** button.
20. Click the **OK** button again to finish the changes.

User creation in Active Directory

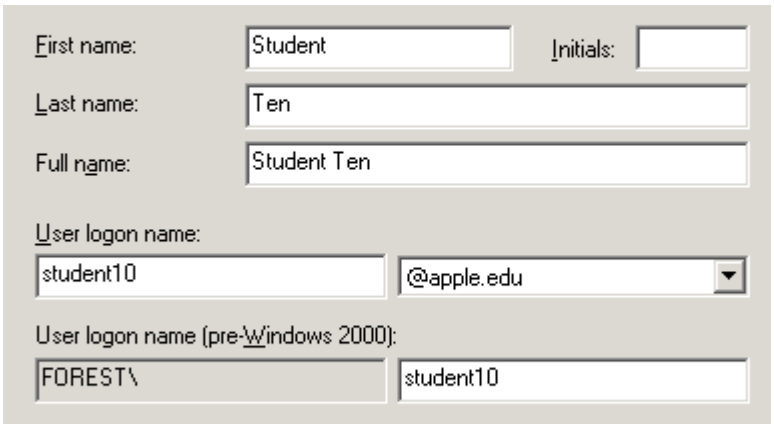
Now we'll create a user in AD and later use a script to import users more efficiently. There's many methods and opinions when it comes to importing users into AD. One of the more frequently used methods is outlined in this Microsoft knowledge base article.

http://support.microsoft.com/kb/555636/en-us

We'll tackle user import in a different section of this document. For now, we'll manually create a user and test out connectivity.

1. In the **Manage Your Server** window, click on the link to **Manage users and computers in Active Directory**.
2. Expand the **apple.edu** Directory and select the **Users** folder.

3. Select the **Action** menu and choose **New** -> **User**.
4. Create a user with first name **Student** and last name **Ten**. Username should be **student10** and password should be **Apple12**.



5. Once finished, right-click on the new **Student Ten** account and choose **Properties**.

6. Click on **Profile** and point their home directory to **H:** and **\\ad.apple.edu\homes$ \student10**. This screen shot doesn't show the **10** on the end of the path, but it's there. Be sure to put the full path.

7. Click **Apply**.

Testing file services connections

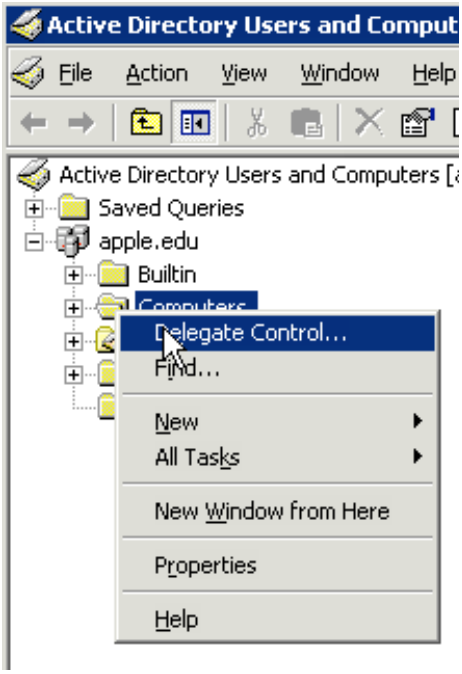
8. If you have a Windows XP or Vista client in your test environment (steps for Windows XP are used here), point that XP client to your AD server for DNS. Click **Start**, then **Run** and connect to the sharepoint by typing in **\\ad.apple.edu\homes$\student10**.
9. When prompted, type in the username **student10** and password **Apple12**.
10. Create a new folder in the student10 folder to ensure that permissions are as expected.
11. Move to your Mac OS X client, running 10.5.1 or newer, and set your network preferences to point to the AD server for DNS. Also, set **apple.edu** in the search domain.

12. Launch Terminal and type **`host 10.0.1.5`** and confirm that it resolves to **`ad.apple.edu`**.
13. Type **`host ad`** and confirm that it resolves to **`10.0.1.5`**.
14. In the Finder, press **cmd-k** to Connect to Server and type **smb://ad.apple.edu/homes$/ student10**. A window will open showing the empty sharepoint. You should see the folder you made when connected via your XP client. Create a new folder and name it **Made in Mac OS X**. You've successfully connected to Windows file sharing from Mac OS X 10.5 and Windows XP at this point.

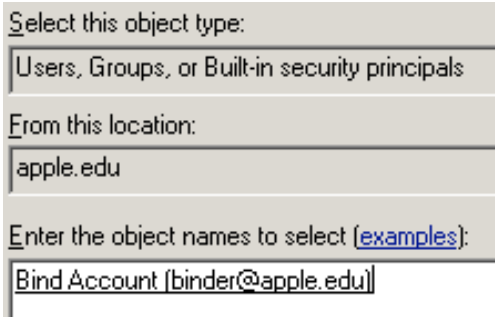
Specifying an account for the binding process

Before going any further, we'll first want to set up an account that will be solely responsible for binding computers to AD. It is a common practice to specify an account, that is not the AD administrator, to do the lone task of binding computers to the domain.

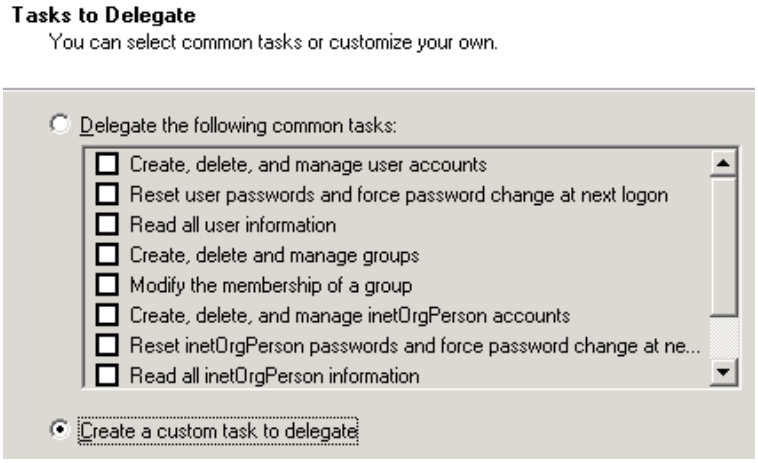
1. In the Manage Your Server application, again click on the link to **Manage users and computers in Active Directory**.
2. Expand the **apple.edu** directory.
3. Select **Users** and create a new user like you did in the previous section.
4. Give the user a first name of **Bind** and a last name of **Account**.
5. Give the user a logon name of **binder**, a password of **Apple12** (or anything else that you wish) and click **Apply**. You don't need to set a profile location for this user.
6. Right-click on **Computers** and choose **Delegate Control**.



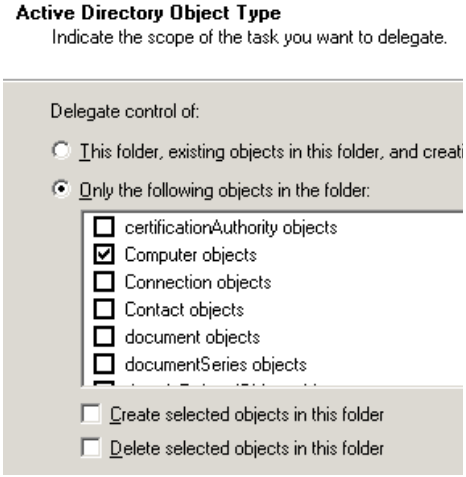
7. Click to Add a user and search for **binder**. Click **OK**.



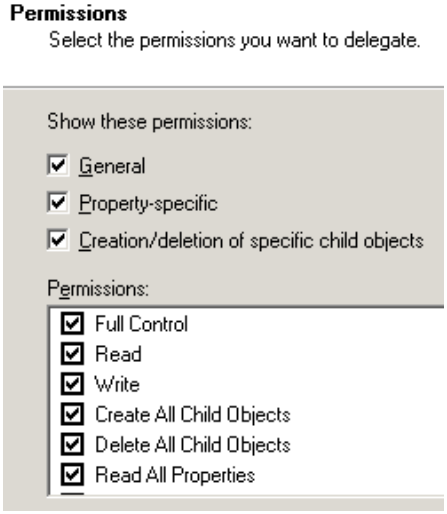
8. Choose to **Create a custom task to delegate** and click **Next**.



9. Choose **Only the following objects in the folder** followed by **Computer objects**. Click **Next**.



10. Check **Full Control** and all boxes will automatically check as well.

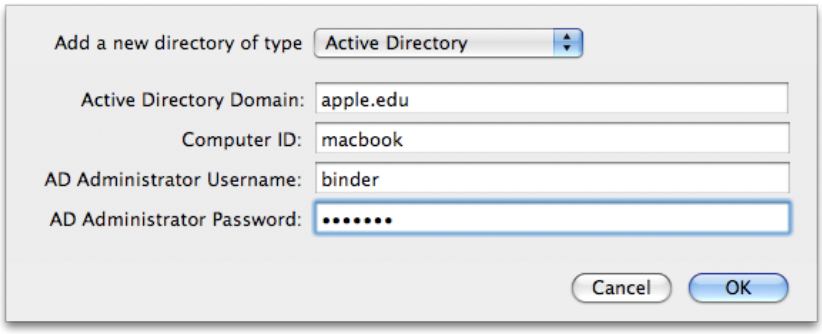


11. Click **Next**, then **Finish**.
12. You can now use the account **binder** with the password **Apple12** when binding clients to the AD domain.

Binding Mac OS X 10.5 to Active Directory

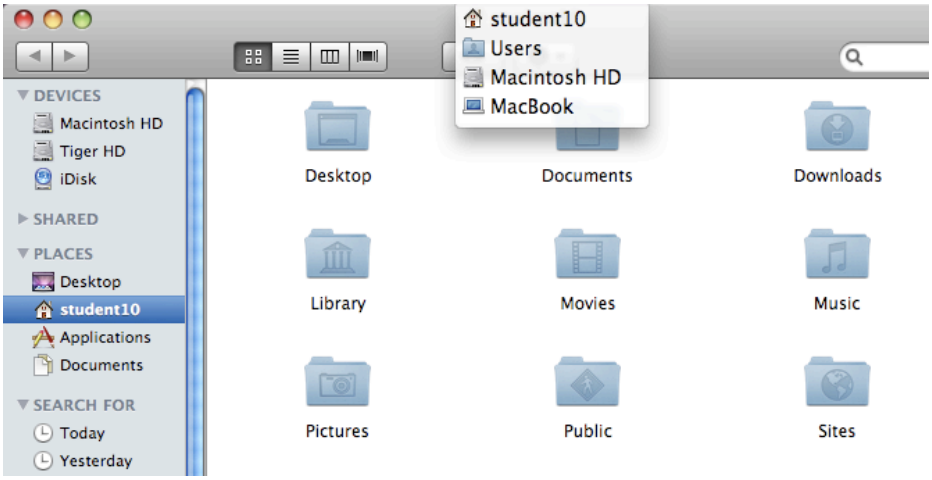
We'll now bind a Mac OS X 10.5 client computer to Active Directory for authentication and access to it's home folder via SMB. Double check that the Mac OS X client is pointed to your AD server for DNS.

1. Open /Applications/Utilities and launch **Directory Utility**.
2. Click on the **plus** sign to add a new Directory Server.
3. Change the directory type to **Active Directory** and fill in the blanks as shown below.



4. It should show in the list as responding normally.

5. Logout and the log back in as **student10**.
6. You'll see that authentication is successful, you have a forced local home directory on the startup disk, and your network home location is mounted for you automatically via **SMB**.



7. These are the results you see when simply binding and authenticating to AD and using the default settings in Directory Utility. While you've been given a local home directory in **/Users** on the Macintosh HD, your **H:** drive in AD is conveniently brought to you in the Dock.

8. If you create a folder and it immediately disappears, logout and then log back in again. There is a GUI glitch of some sort where logging in when the home directory location is empty can cause this to happen. When logging in a second time, folder creation sticks and you can immediately see your results. When importing users in the next section, the vb script we'll use eliminates this issue by pre-populating each user home directory with a Documents folder.

Import Users into Active Directory

This is the part where you get slightly angered when you see how easy a vb script can do all of the work that you've been running through. While going through the steps helps to see how it all comes together, it's also helpful to see how most AD admins (I'm not one, by the way) probably get this done more efficiently.

1. On your AD server, browse to **C:\homes** and select any home folders that are present for student users you've created.

2. Right-click on them and select **Delete**.

3. Confirm the dialog box that prompts you in order to remove the home folders.

4. Go back to the **Active Directory Users and Computers** app and delete the **student10** account and any other student account you created. **DO NOT** delete your **binder** account.

5. In the downloaded zip file should be two files named **import.csv** and **import.vbs**. If you haven't copied them to your AD server, do that now. They can reside anywhere as long as the two files are in the same location.

6. Right-click on the **import.csv** document and select **Edit**. Here are the contents of the file.

```
Ten,Student,student10,Apple12
Eleven,Student,student11,Apple12
Twelve,Student,student12,Apple12
Thirteen,Student,student13,Apple12
Fourteen,Student,student14,Apple12
Fifteen,Student,student15,Apple12
Sixteen,Student,student16,Apple12
Seventeen,Student,student17,Apple12
Eighteen,Student,student18,Apple12
Nineteen,Student,student19,Apple12
Twenty,Student,student20,Apple12
```

7. This is simply a comma-delimited file that breaks down the last name, first name username and password of each user being imported.

8. Right-click on the **import.vbs** file and select **Edit**. Here are the contents of the file.

```
'CSV FORMAT lastName,firstName,userName,password

Option Explicit

Const ForReading = 1

Dim objDomain, objUser, fso, tsInputFile, strLine, arrInput, homeServer, homeShare
Dim fldUserHomedir, wshShell
homeServer="ad.apple.edu"
homeShare="homes$"

Set objDomain = GetObject("LDAP://CN=Users,dc=apple,dc=edu")
Set fso = CreateObject("Scripting.FileSystemObject")

'************************************************************
'Open the text file as a text stream for reading.
'Don't create a file if users-to-create.txt doesn't exist
'************************************************************
Set tsInputFile = fso.OpenTextFile("import.csv", ForReading, False)

While Not tsInputFile.AtEndOfStream

     strLine = tsInputFile.ReadLine
     arrInput = Split(strLine, ",")

     Set objUser = objDomain.Create("user","cn=" & arrInput(1) & " " & arrInput(0))
     objUser.Put "sAMAccountName", arrInput(2)
     objUser.Put "userPrincipalName", arrInput(2) & "@apple.edu"

     '************************************************************
     'Write the newly created object out from the property cache
     'Read all the properties for the object, including
     'the ones set by the system on creation
     '************************************************************
     objUser.SetInfo
     objUser.GetInfo
     objUser.SetPassword arrInput(3)
     '************************************************************
     'Set the properties
     '************************************************************
     objUser.AccountDisabled = False
     objUser.givenName = arrInput(1)
     objUser.sn = arrInput(0)
     objUser.IsAccountLocked = False
     objUser.PasswordRequired = True
     objUser.DisplayName = arrInput(1) & " " & arrInput(0)
     '************************************************************
     'Set the drive that you'll map to
     '************************************************************
     objUser.HomeDirectory = "\\" & homeServer &"\" & homeShare& "\" & arrInput(2)
     objUser.Put "homeDrive", "H:"
     objUser.SetInfo
```

```
      '*********************************************************
      'Create a home directory for the imported users
      'and populate each home directory with a Documents folder
      '*********************************************************
      If Not fso.FolderExists("\\" & homeServer &"\" & homeShare& "\" & arrInput(2))
Then
      Set fldUserHomedir = fso.CreateFolder("\\" & homeServer &"\" & homeShare& "\" &
arrInput(2))
      fso.CreateFolder("\\" & homeServer &"\" & homeShare& "\" & arrInput(2) &
"\Documents")
      End If

      '*********************************************************
      'Set full rights for the user to the home directory and
      'propagate those rights through the contents of each home directory
      '*********************************************************
      Set wshShell = WScript.CreateObject("Wscript.Shell")
      wshShell.Run "cacls \\" & homeServer & "\" & homeShare & "\" & arrInput(2) _
            & " /T /e /g " & arrInput(2) & ":F", 1, True

      '*********************************************************
      'Stop referencing this user
      '*********************************************************
      Set objUser = Nothing
Wend

'Close the file
tsInputFile.Close
```

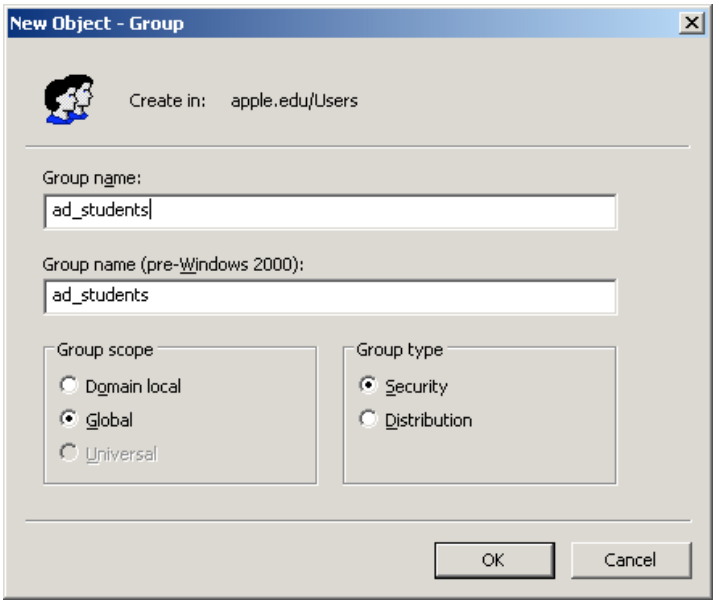
9. You can see what each section accomplishes in this script. It calls the csv file you have and imports users into AD. Then, it sets their profile and maps to the proper home directory. Finally, it populates each home directory with a Documents folder and propagates the permissions.
10. Double-click the **import.vbs** file to run that script.
11. Login as **student20** with the password **Apple12** from the Mac OS X client as soon as the script completes (it shouldn't take more than 3-5 seconds).
12. Authentication, home directory mapping and file permissions should all check out.

Active Directory group membership

1. On your AD server, open the **Active Directory Users and Computers** application.
2. Open the **apple.edu** domain and select **Users**.

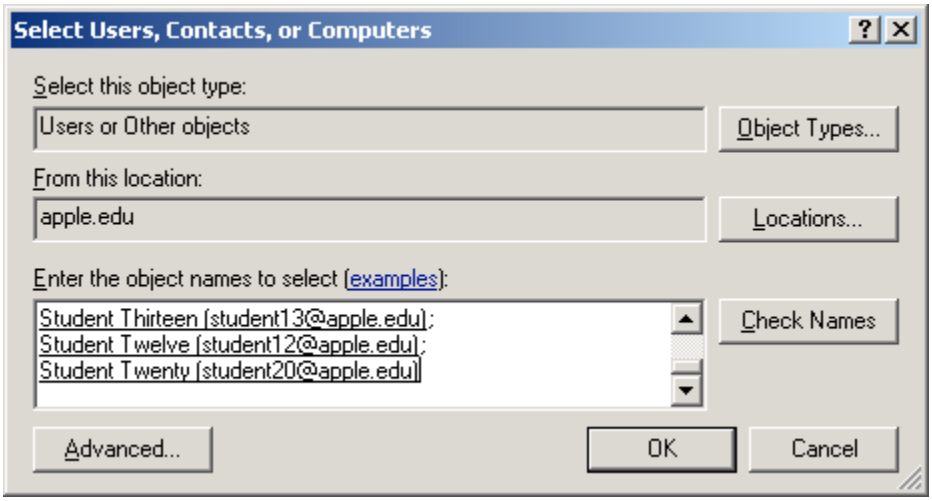
3. Click on the **New Group** button or .use the **Action** menu to create a new group.

4. Name the group **ad_students** with the default settings unchanged, as shown below. Click **OK**.

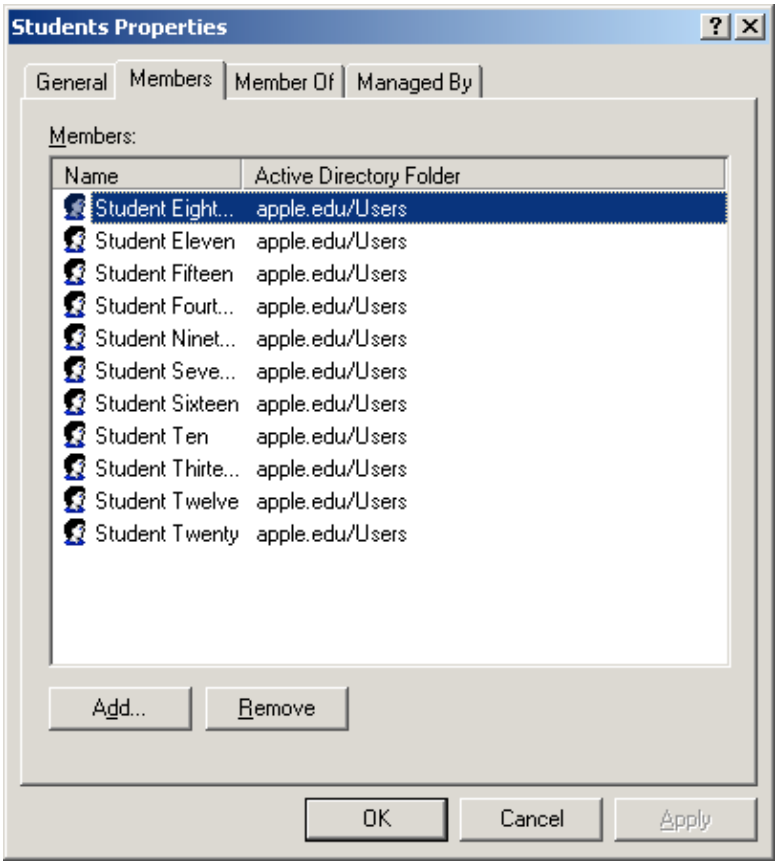


5. Locate your new ad_students group. **Right-click** on it and select **Properties**.

6. Select the **Members** tab and click on the **Add** button.
7. In the **Object names to select** window, type **student** and click on the **Check Names** button.
8. Use the **control-a** keys to select all of the student users you imported earlier and click **OK**.
9. Click **OK** again.



10. In the membership window, click **Apply** and then **OK**.



Bringing Open Directory into the mix

Why would we do this? The whole point of bringing AD and OD together is to give the Mac user (and IT administrator) the best of both worlds in a heterogeneous environment. IT benefits from having a single directory to maintain, but can also leverage managed client for Mac OS X (MCX) to manage the Macs in their environment.

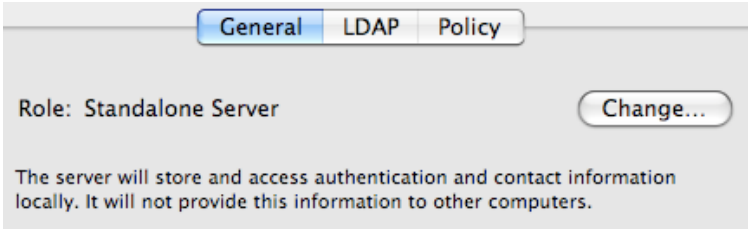
At this point we'll fire up Leopard Server (or install it for the first time). When installing, follow these guidelines during the setup assistant.

- Use the **Advanced** mode. We're not doing Standard or Workgroup in this setup.
- For the examples used in this document, the Administrator account will be **Server Admin** with **sadmin** as the short name.
- Leave the Directory setup to **Standalone**. We'll change it later when binding to AD.
- Set the IP address to the following

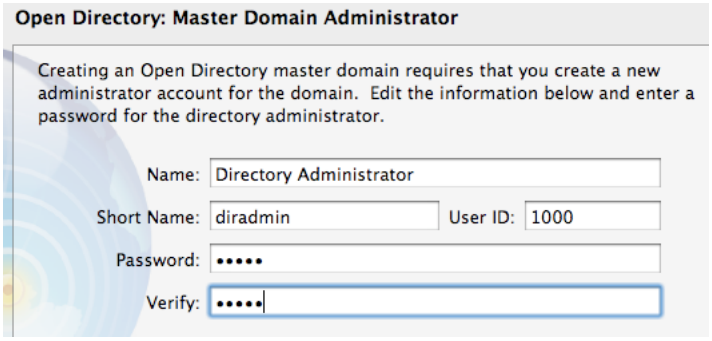
IP address:	**10.0.1.6**
Subnet mask:	**255.255.255.0**
Router:	**10.0.1.1**
DNS Primary:	**10.0.1.5** (should match IP address of your AD server)
DNS Secondary:	**10.0.1.1** (typically your home router so that you can run Software Update)

- Server name should be set to **od.apple.edu**, or whatever matches the DNS record you entered on your AD server.
- Computer name can be set to whatever you like, so we'll leave it at **od** for the purpose of keeping this document as simple as possible.

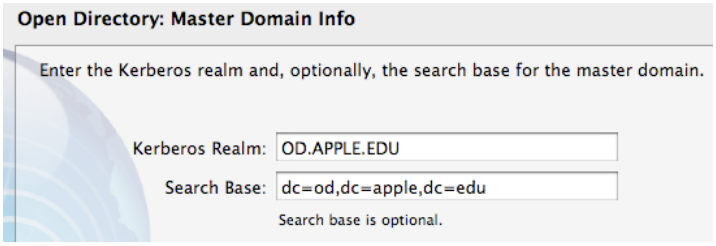
1. In **Server Admin**, select your new OD Server and click on **Settings**, then **Services**.
2. Enable the **Open Directory** service and click **Save**.
3. Select the **Open Directory** service and choose **Settings**.
4. Click the **Change** button to change the role of the server. This will launch the configuration assistant.



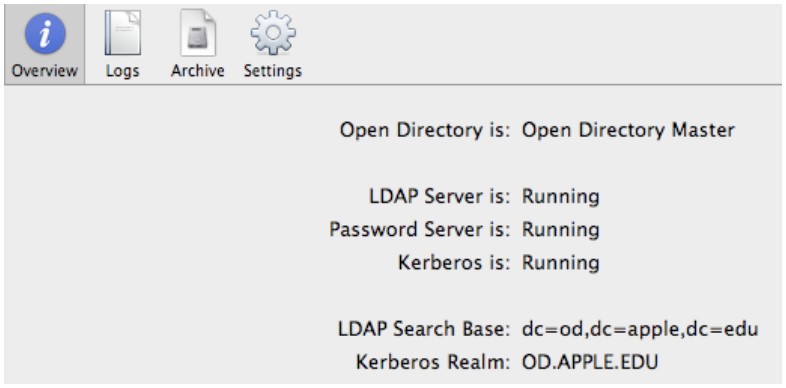
5. Choose **Open Directory Master**.
6. On the following pane, you must confirm a Directory Administrator account and password. Feel free to leave the **diradmin** account as it is set by default, and choose a password.



7. Confirm the Kerberos realm info and click Continue.



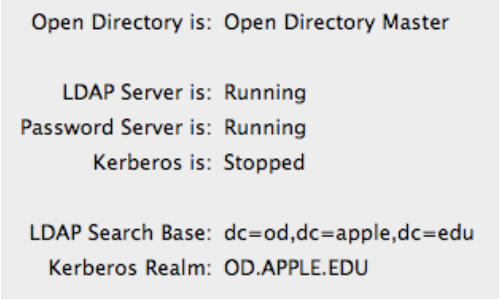
8. The final pane confirms the settings. Click on the **Close** button.
9. You now have an ODM working as a Kerberos key distribution center (KDC). In Server Admin, you'll see in the Open Directory overview that all is running as expected.



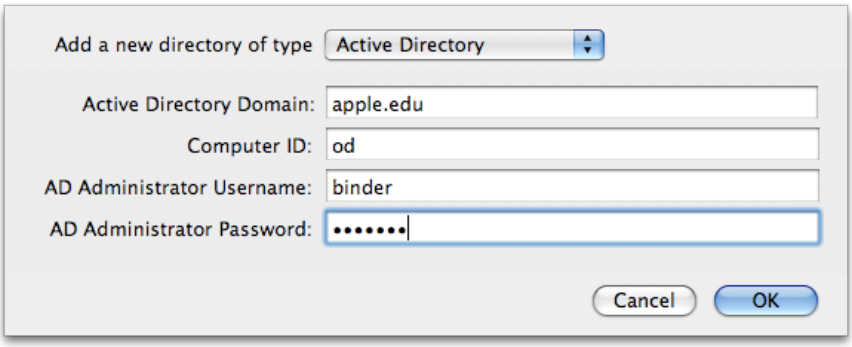
10. Now that you've set up the ODM so that we can manage Macs in our Active Directory environment, we need to stop Kerberos on the ODM and join the Kerberos realm of the AD server.
11. Open **Terminal** and type the following command and press return.

    `sudo sso_util remove -k -a sadmin -p password -r OD.APPLE.EDU`
    (replace **`password`** with your own password used for the sadmin account)

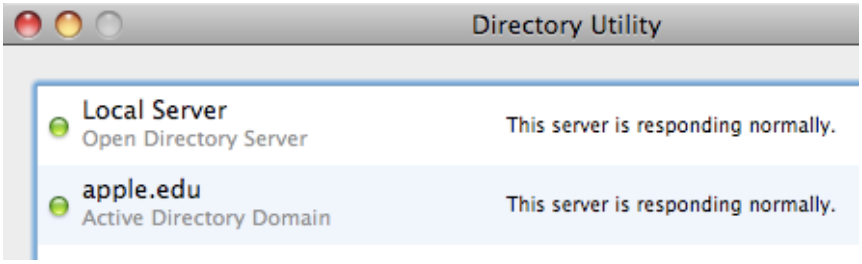
12. Once completed, you can go back to Server Admin and refresh the overview page. You'll see that Kerberos is stopped.



13. Launch **Directory Utility** and click on the **plus** sign to add a new Directory Server. Change the directory type to **Active Directory** and fill in the blanks as shown below. You can use the **binder** account for this step, just like when you bound a client workstation to AD earlier.



14. It will show that the AD and OD servers are responding normally. Quit Directory Utility.



15. Return to Terminal and type the following command to join the AD kerberos realm.

```
sudo dsconfigad -enablesso
```

Now, the easy way (optional)

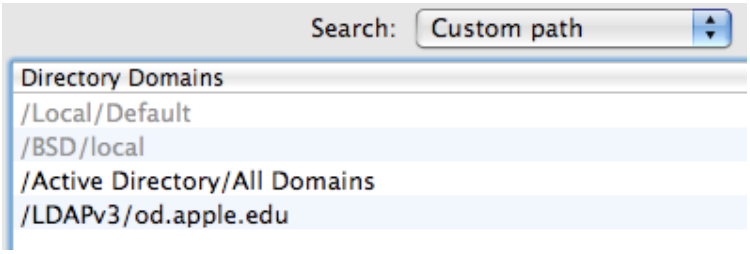
This document just walked you through the steps that you need to follow for both 10.4 and 10.5 server when bringing AD and OD together. Now that you know the hard way of doing it, here's the easy way. You can simply demote your server to standalone and then promote it back using these steps, or format and reinstall completely if that's your thing. These steps are quick and easy, assuming that you now know your way around the server.

1. Demote your server to **Standalone** in **WGM -> Open Directory -> Settings**.
2. With DNS resolving properly at every turn, like you should have established by now, bind your OD server (now at Standalone) to Active Directory using **Directory Utility**.
3. Return to **Server Admin** and promote your server to an **Open Directory Master**.
4. While looking at Open Directory in Server Admin, click on the **Overview** button and you'll notice that the Kerberos service is **Stopped**.
5. Launch **Terminal** and type **`sudo klist -kt`** followed by **Return**.
6. You'll see the proper entries listed, and the principles will end with **@APPLE.EDU**. That shows you've joined the AD Kerberos realm, represented by **APPLE.EDU** instead of **OD.APPLE.EDU**. If you hadn't bound your OD server to AD first, you would've created your own Kerberos realm based on **OD.APPLE.EDU**.

It's very cool how Leopard Server just does the right thing. Let's move on.

Binding the client to both directories

1. On your Mac OS X 10.5 client, open **Directory Utility**.
2. Click on the **plus** sign to add a new Directory Server.
3. Leave the directory type on **Open Directory** and add the **od.apple.edu** server.
4. Click on the **Show Advanced Settings** button and select the **Search Policy** button.
5. If the Active Directory entry is not above Open Directory, click and drag it above to set it that way (as shown below).

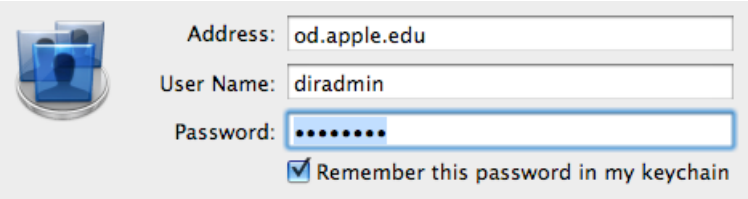


6. Log out.
7. Login as the **student10** user with the password **Apple12**.
8. You've logged in with an AD account while bound to OD as well. "So what?!" you say?

Managed Client for Mac OS X (MCX) and AD together

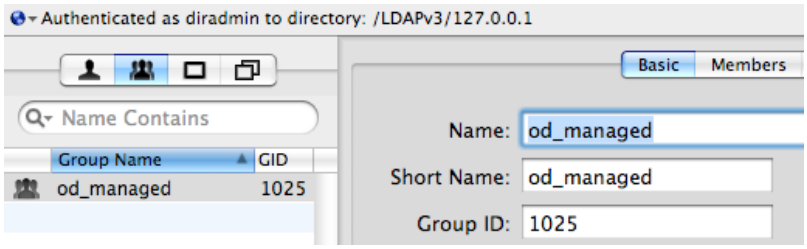
This is what we've been building towards. AD authentication with group management and MCX policy enforcement for our Mac users. The user gets the computer they want. They IT folks get the management they require.

1. On your ODM, launch WGM and login with the **diradmin** account.



2. Ensure that you're working with the **/LDAPv3/127.0.0.1** directory.

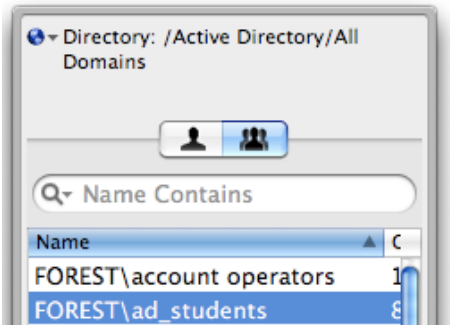
3. Create a new group and call it **od_managed**.

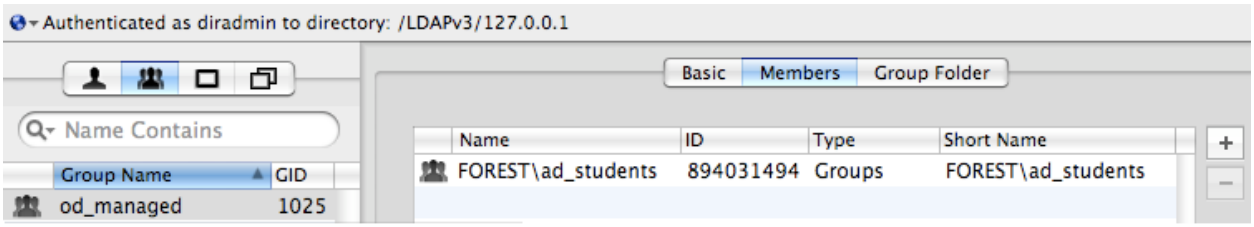


4. Click on the **Members** tab and again on the **plus** sign.

5. Use the pull-down menu in the side bar to switch the directory to **/Active Directory/All Domains**.
6. Select the **groups** tab to show AD groups.

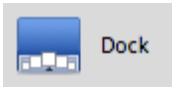
7. Drag the **ad_students** group into the Members window of your new **od_managed** group.



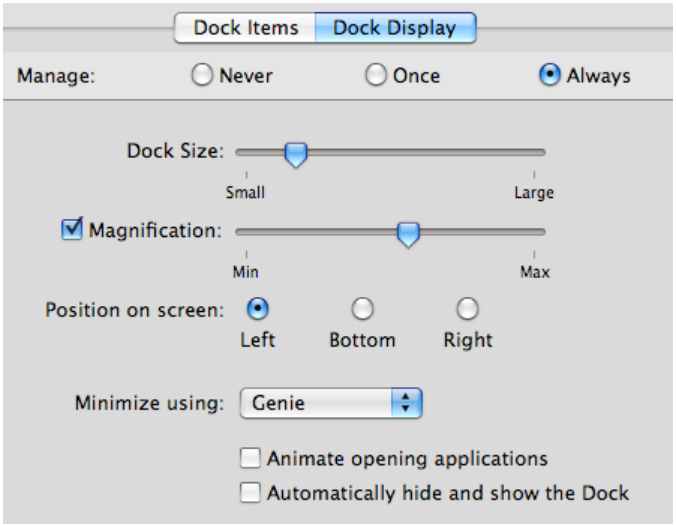


8. Click **Save**.

9. With the **od_managed** group still highlighted, click on the **Preferences** button.Select the **Dock** preference since that's what we'll manage.

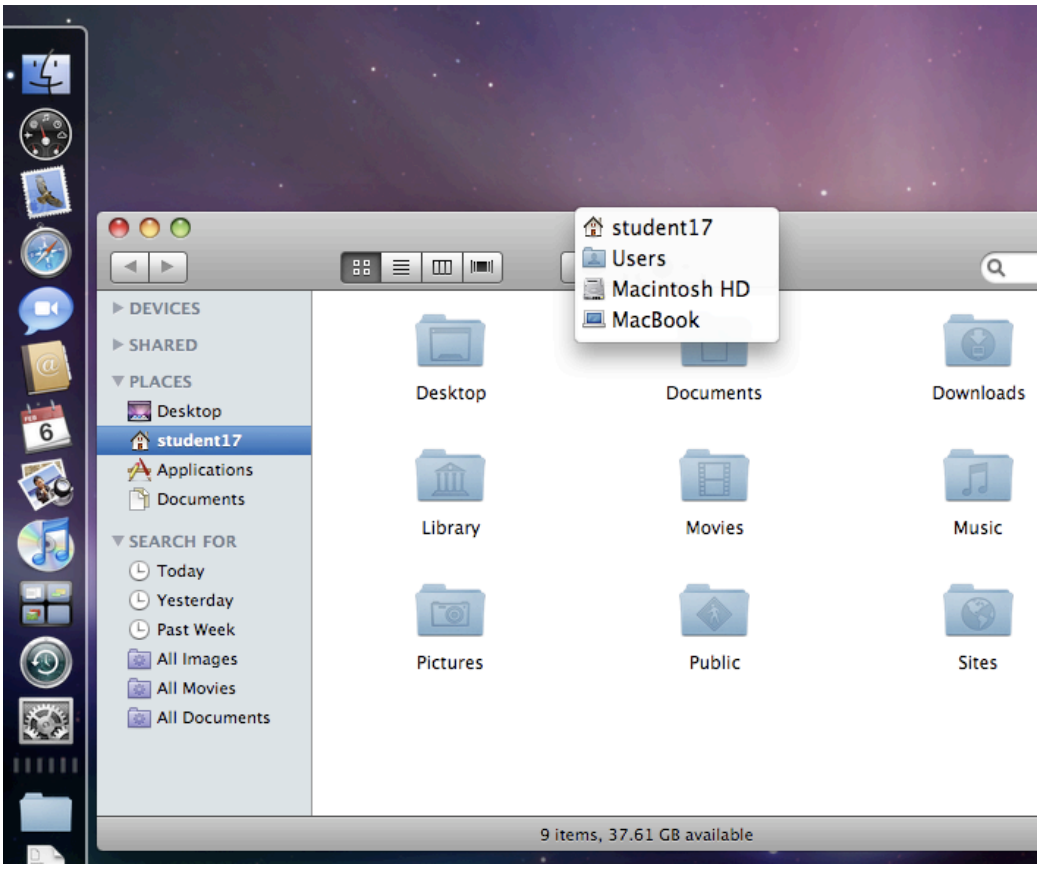


10. Click on the **Dock Display** tab and set it however you wish. So that I can easily tell my management is working, I always move the dock to the left side.



11. Click **Apply**, then **Done**.

12. Logout of your Mac OS X client and then back in as any of the **student10-20** users. What you see is an AD account, mapped to their home on a Windows server with MCX policies enforced.

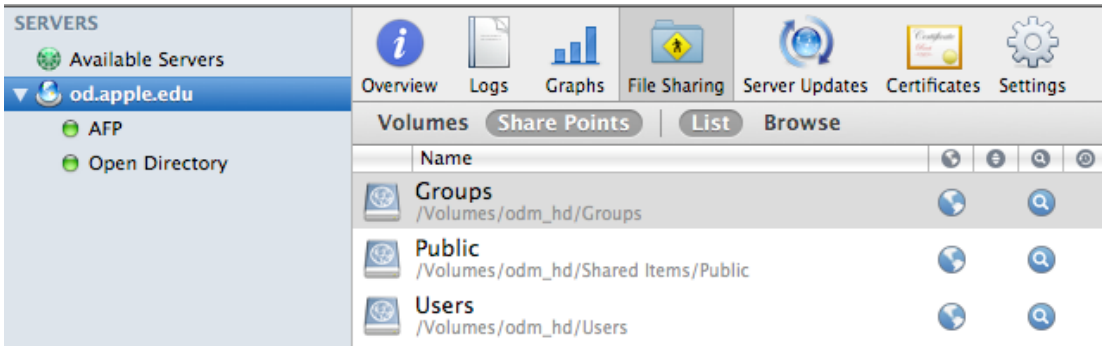


Hosting the home folders on the Open Directory server

What if you want AD in the picture only for authentication? No problem. Let's put that Xserve to work.

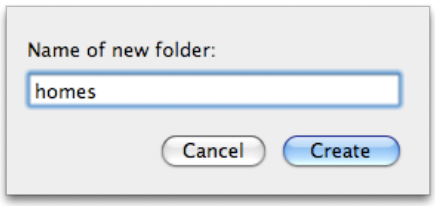
1. On your ODM, launch **Server Admin** and enable the **AFP** service.
2. Highlight the **AFP** service on the left, and click the **Start AFP** button in the lower left of the Server Admin window.
3. Highlight the **od.apple.edu** server on the left, and click on **File Sharing** in the tool bar.

4. Click on the **Share Points** button and disable each of the three default shares by using the **Unshare** button on the far right. You have to click the **Save** button after each one.

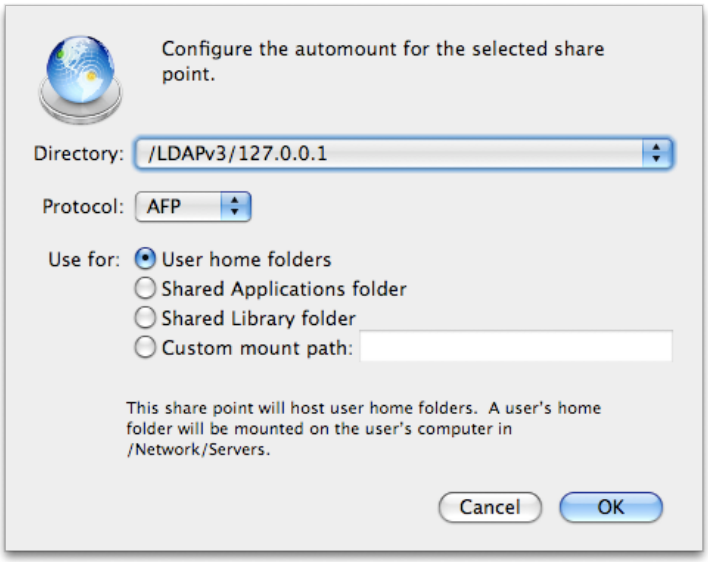


5. Select the **Volumes** button, followed by the **Browse** button.

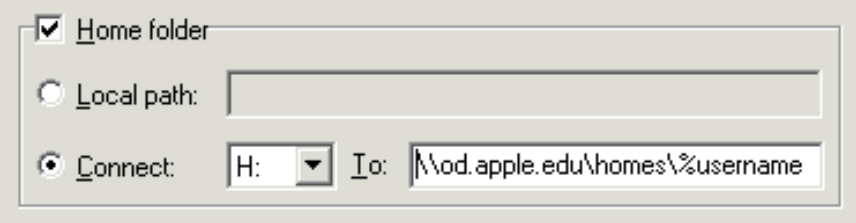
6. Click on **New Folder** to create one at the root of one of your server hard drives.
7. Call the folder **homes** and click the **Create** button.



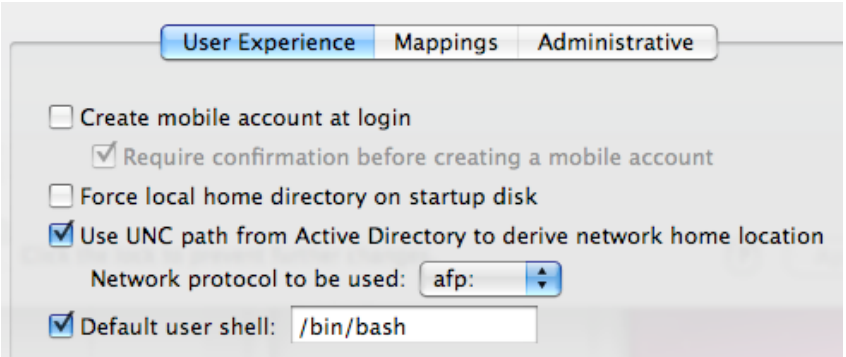
8. Select the new folder and share it using the **Share** button.
9. The sharing options are shown in front of you. Click the **Enable Automount** button.
10. When prompted, choose the **LDAP directory**, **AFP** and **User home folders** options.



11. When prompted, type in your **diradmin** credentials and click **OK**.
12. Click **Save**.
13. Move to your AD server.
14. In the **Active Directory Users and Computers** application, select your **student10** account.
15. Right-click on it and choose **Properties**.
16. Click on the **Profile** tab and check the **Home folder** box.
17. Select the **Connect** button and set the **H:** drive to **\\od.apple.edu\homes\%username%**. The screen shot doesn't show the trailing **%**, but it's there.



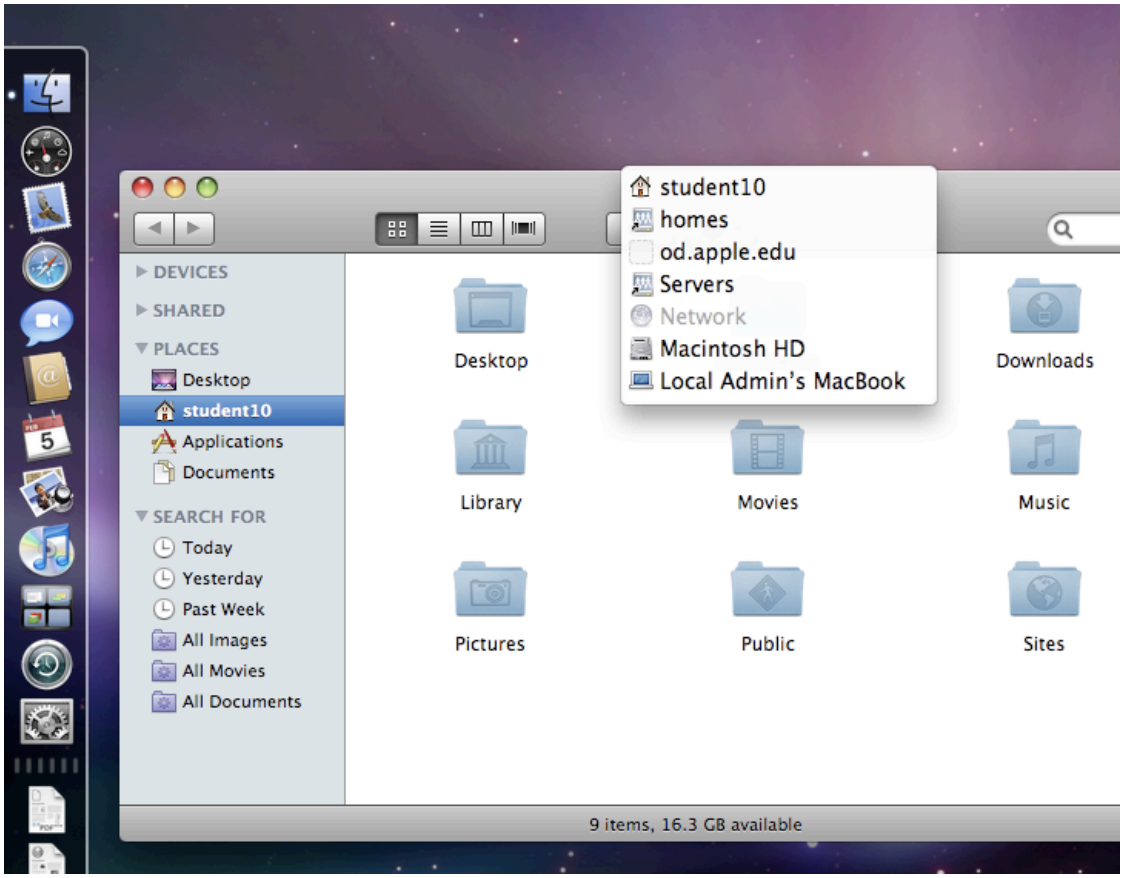
18. Ignore any errors or warnings that may pop up when you click **Apply**.
19. Move to your Mac OS X client and open **Directory Utility**.
20. Unlock the padlock in the lower left-hand corner and authenticate.
21. Click on the **Show Advanced Settings** button.
22. Click on **Services** and then double-click on the **Active Directory** plugin.
23. Click on the triangle next to **Show Advanced Options** and match the settings as shown below.



24. **Force local home...** should be unchecked, and the network protocol should be changed from the smb protocol to the **afp** protocol.

25. Logout of the Mac OS X client and log back in as **student10**. You may need to wait a few seconds for network accounts to become available again or possibly even reboot the client.

26. We now have a managed dock, an AFP-based network home directory hosted on an Xserve, all while AD is handling the authentication.



There are literally hundreds of directions that this document could go, from nesting AD groups within OD, to extending the AD schema, to using Centrify for policies. This document was simply created to help you get a test environment up and running quickly in order to understand the initial setup and go through a few common practices.

Special thanks got to Jeff Walling and Jeff Ochsner for helping me verify the steps and processes. Mike Bombich also gets credit since he wrote the dns.bat file that I barely modified for this document. A real big thanks goes to Matt Riley for cooking up the AD import script and helping me with the permissions details. Comments and corrections for this document can be sent to me at carson@mac.com.