Filesharing

Jason Healy, Director of Networks and Systems

Last Updated Mar 18, 2008

Contents

Chapter 1

Name of Project Here

Last updated 2008/03/18

1.1 Introduction

Suffield provides networked file server space for all of its users. This gives people a place to back up their important files, share files with others, and access their files from machines that aren't their own.

Additionally, users may create web pages in their file server accounts, which are automatically hosted on our internal webserver.

Finally, school-owned desktop and lab computers directly attach to file server storage when a user logs in. This way, a user's files "follow" them around from machine to machine, making access and backup simple.

This document describes how to set up a Mac OS X Server machine as a central file server. We cover configuration for Macintosh and Windows clients, as well as networked home directories for Macintosh and Windows. Finally, we'll discuss exporting files via NFS.

1.2 Initial Setup

Begin with a fresh install of Mac OS X Server 10.4. Note that you'll most likely want an **unlimited client license**, or you'll be severly limited in the number of connections your server will support.

Perform a standard installation. When running the **Server Setup Assistant**, you should be careful when choosing the **Computer Name**. This is the name that will be shown to users when they connect to the fileserver, so it should be something meaningful that they will understand.

When asked which services to start automatically, you should choose **Apple File Sharing**. Additionally, if you wish to let Windows users connect to the server, you should enable **Windows File Sharing**.

Once the base install is complete, run any pending software updates.

At this time, you should connect any external drives you plan to use for shared data. External disks, RAID arrays, or other media should all be connected, named, partitioned, and ready to use before continuing.

1.2.1 Open Directory Integration

If your network has one or more Open Directory servers, and you plan to authenticate file sharing logons using these servers, you'll need to set up directory authentication:

1. Open the **Directory Access** application in `/Applications/Utilities`.
2. If necessary, click the lock icon and authenticate.
3. Click on the item named **LDAPv3** and click the **Configure** button.
4. In the window that appears, *deselect* the **Add DHCP-supplied LDAP servers to automatic search policies** box.
5. Click the **New** buton.
6. Enter the name or IP address of your Open Directory server.
7. Ensure that the **Use for authentication** box is *selected*.
8. Click **Continue**.
9. Optionally, bind the machine to the OD server by entering the machine name and directory admin information. Click **Continue**.
10. In a similar fashion, add any backup Open Directory servers on your network.

Quit the **Directory Access** application when you are done.

1.2.2 Joining Kerberos

If you wish to gain the benefits of single-signon using Kerberos, you must first join your server to the OD server's Kerberos domain.

1. On the OD master server, open the **Server Admin** application.

2. Click on the **Open Directory** service listing.

3. Click on the **Settings** tab at the bottom of the window.

4. On the main settings screen, click the **Add Kerberos Record** button.

5. For the **Administrator Name** and **Password**, enter the master password for your OD domain.

6. For the **Configuration Record Name**, enter the name of the server you wish to join to the domain. The server must be bound to the domain, as described in the previous section. If you're unsure of the record name, look in **Directory Access** for the server you're trying to join. It should look something like "`cn=myserver,cn=computers,dc=suffieldacademy,dc=org`". Use the name part of this record (*e.g.*, "myserver").

7. For the **Delegated Administrators**, enter the name(s) of administrative users who will add the computer to the domain. These users must be in the OD domain (they cannot be local to the server).

8. On the computer you're adding to the domain, open **Server Admin**.

9. Click on the **Open Directory** service listing.

10. Click on the **Settings** tab at the bottom of the window.

11. Click the **Join Kerberos** button.

12. Enter one of the valid administrative usernames and passwords you specified on the OD server.

13. If no errors are reported, you're done!

1.3 AFP Sharepoints (Macintosh Clients)

AFP sharepoints are the native method for clients running Mac OS X. If you wish to share files to Macintosh clients, you should enable AFP sharepoints.

1.3.1 Server Admin Settings

In **Server Admin**, click on the **AFP** service entry.

Under the **Access** tab, *select* the **Enable Guest access** checkbox.

Under the **Logging** tab, enable any logs you wish to keep on the server.

Save your changes by clicking the **Save** button at the bottom of the screen.

1.3.2 Workgroup Manager Settings

Open **Workgroup Manager** and click on the **Sharing** icon at the top of the window.

From this point, you may add, modify, and delete share points on the server.

To add (or modify) a sharepoint:

1. Click on the **All** tab and navigate to the folder you wish to share.
2. Under the **General** tab, *select* the **Share this item and its contents** checkbox.
3. Under the **Access** tab, ensure the folder permissions are how you want them. Pay particular attention to the **guest** settings; if guests should not be allowed to access a share point, make sure they do not have rights to the folder.
4. Click **Save**. Move to the **Protocols** tab.
5. Move through each protocol section, and only enable those that you need for this share. See other sections of this document for information on the settings for Windows and NFS clients.
6. Again, check to confirm that you've enabled guest access only if you need it.
7. Save your changes and test your share point. You should be able to connect to the server with a valid name and password (or, with guest access if you've enabled it).

1.4 CIFS Sharepoints (Windows Clients)

CIFS sharepoints are most frequently used by computers running Windows, though UNIX, Mac OS X, and other clients are also cable of speaking the protocol.

CIFS shares may be enabled simultaneously with an AFP share, or it may exist on its own (*e.g.*, for Windows profile directories, which are not needed on the Mac).

1.4.1 Server Admin Settings

In **Server Admin**, click on the **Windows** service entry.

Under the **General** tab, set the **Role** of the server to **Domain Member**.

Enter the name and description of the machine, and set the domain to the proper value for your network (*e.g.*, `SUFFIELDACADEMY`).

Under the **Access** tab, decide if you wish to allow guests or not.

Under the **Advanced** tab, *deselect* the **Workgroup Master Browser** and **Domain Master Browser** checkboxes (we assume you have set up a valid Primary Domain Controller on another machine; if this is your PDC, leave the boxes checked).

If you're using WINS on your network, enter the IP address of your WINS server to register your computer's name.

You will probably want to enable **Virtual Share Points**, which allows users to connect directly to their home folder without needing the intervening path information.

Click **Save**. You will be prompted to enter a Open Directory Administrator password, which adds your computer to the domain.

1.4.2 Workgroup Manager Settings

Open **Workgroup Manager** and click on the **Sharing** icon at the top of the window.

Select a share point from the pane on the left, and click the **Protocols** tab on the right.

Choose **Windows** from the drop-down menu to edit the settings related to CIFS shares.

If you wish to share this folder to CIFS clients, *select* the **Share this item using SMB** checkbox. You may also *select* the **Allow SMB guest access** checkbox if you wish to allow guests.

Click **Save** to save your changes, and your share point should now be available to Windows clients.

1.5 Macintosh Network Home Directories

1.5.1 Enabling Local Home Directories

If you plan to let users log in to the file server directly (*e.g.*, via SSH), you'll find that the network home directories do not work, because they map back to the server.

To override this, we must tell the server to ignore the home directory attribute from the OD server, and replace it with a custom local value instead:

1. Open the **Directory Access** application, in `/Applications/Utilities`.
2. If necessary, click on the lock icon and authenticate.
3. Click on the item named **LDAPv3**, and click the **Configure** button.
4. For each of the servers in your search list, do the following:
   (a) Click on the **LDAP Mappings** popup menu, and choose **Custom**.
   (b) Click on the **Search & Mappings** tab at the top of the window.
   (c) Expand the **Users** section of the mapping list.
   (d) Find the attribute named **NFSHomeDirectory** and click on it.
   (e) In the right-hand pane, delete the current value, `homeDirectory`.
   (f) Click the **Add** button, and create a new value that stars with a pound sign (`#`) and contains the local path to your users' home directories. You may use the macro "`$uid$`" to add the user's login name. For example:

       ```
       #/Volumes/BigRaid/Users/$uid$
       ```

       If a user named `jbogus` logged in, the home directory would be set to `/Volumes/BigRaid/Users/jbogus`.
   (g) Click **OK**. Repeat the above steps for all bound OD servers.
5. Click **OK** on the main screen when you've completed your changes.

You can check your settings by logging in to the terminal and typing the following:

```
lookupd -d
```

This begins an interactive version of `lookupd`, which merges directory information on Mac OS X. Type the following command:

```
userWithName: jbogus
```

(Substitute a real username for `jbogus`.)

You should see a list of attributes for this user. Under the `home` attribute, you should see your new mapped value, rather than the network-mounted default.

1.6 Windows Roaming Profiles

1. Make sure the domain is set up properly (check domain WINS resolution).

2. Set perms on /etc/netlogon to 755 root:staff (copy in scripts and default profile)

3. Set perms on /Profiles to 770 root:staff

4. Set ACL on /Profiles to be "Suffield" (or whatever group all your users belong to), full read, create folder, this folder only.

5. Edit /etc/smb.conf, in Profiles section, set create mask to 0640 and dir mask to 0750.

6. Make fileserver version of file uchg (not necessary on PDC and BDC)

1.7 NFS Exports

NFS is the traditional file sharing mechanism for UNIX clients. It allows a machine to mount an entire directory and make it available to all of its clients, with proper permissions and ownership settings.

NFS does have its warts, however, including a bad security track record. Therefore, we only recommend enabling NFS for read-only, non-root exports. That minimizes exposure to security flaws that could corrupt your data.

1.7.1 Server Admin Settings

NFS is automatically enabled when share points are available for other machines to use. Thus, you do not need to explicitly start any services in **Server Admin**.

You may change a few parameters for the NFS daemon itself, but you should not need to do this unless you know what you are doing.

1.7.2 Workgroup Manager Settings

Open **Workgroup Manager** and click on the **Sharing** icon at the top of the window.

Select a share point from the pane on the left, and click the **Protocols** tab on the right.

Choose **NFS** from the drop-down menu to edit the settings related to NFS shares.

Because NFS is not a very secure protocol, we recommend restricting the export as much as possible.

If possible, use the **Client** or **Subnet** designation for the share point, to restrict which machines can connect to the share. Try to restrict it as much as possible, including only the hosts you trust to access the share.

If possible, export the share **read-only** to prevent clients from making changes.

If you need to preserve ownership of files for clients, *deselect* the **Map all users to nobody** checkbox. If you simply need to export all the files (and ignore ownership), leave this box *selected*.

You should *always* leave the **Map root user to nobody** box *selected*, unless you know what you are doing.