Building NetRestore Images

Jason Healy, Director of Networks and Systems

Last Updated Mar 18, 2008

Contents

Chapter 1

Building NetRestore Images

Last updated 2008/03/18

1.1 Introduction

We repair and set up hundreds of machines each year at Suffield Academy. To help us with this process, we have set up several pre-made **system images** that we use to reformat computers. Each image contains an operating system and common applications.

This document describes how to build a new image for computers running Mac OS X. It is intended for someone who has experience installing applications on Macs, and who has a general familiarity with the applications used at Suffield. No system administration experience is necessary.

Note: this document describes how to create images that will be installed on user machines (erasing and replacing whatever is there). We also use a special *rescue image* for booting machines and running diagnostics. If you need to know how to create a rescue image, please see our NetBoot documentation on rescue image creation.

1.1.1 Prerequisites

When building an image, always start with a clean machine. If possible, restore the computer using the restore CDs (or DVD) that came with it. Otherwise, erase the hard drive and perform a full install of the operating system from installation media.

Use the newest model of computer available when you build your image. Try to find one with as many "extra" features in it (such as DVD burners, large screens, etc). Images built on the best machines tend to work well on all other machines. Images built on "average" machines, however, do not tend to work well on better machines.

Try to build images for "classes" of machines. For example, if you're building an image that will primarily be used for laptop computers, build it on the best laptop you can find. If you're building an image for a group of machines in a lab that are all the same, choose the best machine from the lab. And if you're building an image for desktop machines, choose the best desktop machine available.

1.2 Preparing the Operating System

1.2.1 Initial Setup

We're assuming that you're starting with a machine that has a fresh install of the OS on it. The Apple Registration program should launch on start, and ask you the basic configuration questions.

Register the computer to `Suffield Academy`, and provide the school's address and phone number for the registration form.

When asked to create a user account, use `Suffield Academy` as the name, and `suffieldacademy` as the short name. Use `1833` as the password if this is a personal machine (*e.g.*, a laptop), or the proper master password for shared machines. If you do not know which password to use, consult the Network Administrator.

Continue through the rest of the setup program, setting up the network, date and time, and other settings.

When you're done with the registration program, the computer should boot to a default desktop, and be ready to use.

1.2.2 Boot Images

Suffield uses a custom background picture so we can tell which computers have been restored with our system image. These images reside on our file server. To get them, connect to the fileserver and mount the **Groups** partition. Then, open the **Tech Repair** folder. There is a folder called **Boot Pictures** that contains the pictures we need.

The **Desktop** folder contains a series of background images for use on the machines. Choose the one for the type of machine you're setting up. In general, `Laptop Aqua Blue.jpg` is used for personal machines, and `Suffield Aqua Blue.jpg` is used for machines that the school owns (such as office machines). Select the correct image and copy it to your desktop.

This copies the default background. Open Terminal and type the following commands (when prompted, enter your administrative password):

```
cd /System/Library/CoreServices/
sudo cp DefaultDesktop.jpg DefaultDesktop_original.jpg
sudo cp ~/Desktop/Laptop\ Aqua\ Blue.jpg DefaultDesktop.jpg
```

When you're done, you may quit `Terminal.app` and remove the images from your desktop.

1.2.3 Software Updates

Run Software Updates on the computer until there are no updates left to run. This may require multiple installations and reboots.

1.2.4 System Preferences

Now enter the System Preferences application. For each preference pane listed below, follow the instructions given.

Sharing

In the **Computer Name** field at the top of the screen, enter `unregistered`.

Date & Time

Find the **Set Date & Time Automatically** checkbox, and make sure it is *selected*. In the input box, type `ntp.suffieldacademy.org`.

Click on the **Time Zone** tab and confirm that the computer's time zone is set to an appropriate time zone (*e.g.*, **Boston**).

Network

We need to teach the laptop about the wireless networks available on campus. Click on the **AirPort** icon, and then click on the **Advanced** button.

Under **Preferred Networks**, click the plus sign to add a network. Choose "Suffield Auth" as the network. Do not enter any name or password; just add the network.

1.2.5 Certificate Trust

Connect to the **Installers** and move into the **Suffield Installers** folder. Double-click the *Suffield Academy Network Certificates* file. Enter your administrator password if prompted.

1.3 Installing Applications

Suffield has licenses for several commonly-used applications. You must install these applications before building the image so that they are immediately available when a computer is re-imaged.

1.3.1 Common Applications

The applications in this section should be installed on all computers at Suffield Academy. We have unlimited licenses for them, and they are used by nearly everyone on campus.

FirstClass 9

Install the FirstClass 9 client from the file server (you can find it in the **Suffield Installers** folder).

Once installed, FirstClass automatically launches. Quit the program immediately.

Run the "Install FirstClass Settings" script from the same folder.

Re-start FirstClass and ensure that the settings are now correct (*e.g.*, the server listed is `fc.suffieldacademy.org`).

Add the FirstClass client to the dock.

Sophos Anti-Virus Install

Run the Sophos Anti-Virus Installer off of the file server (you can find it in the **Suffield Installers** folder).

Microsoft Office

Run the Microsoft Office installer from the file server (you can find it in the **Suffield Installers** folder). When prompted to register the program, use `Suffield Academy` as the name, and leave all other fields blank. Click **Install** to complete the installation.

After installation, Office will run its auto-update tool. Install any pending updates before quitting.

iWork '09

Install from the server, and register with the given serial number.

iLife '09

Install from the server if iLife was not included as part of the default OS install.

Adobe Creative Suite Design Premium

Run the Adobe installer from the file server (you can find it in the **Suffield Installers** folder). Perform a default install of the application, but **skip** the "Version Cue" server.

When installation is complete, launch **Photoshop** and complete the product registration process (enter the serial number if necessary).

Run the Adobe Updater (in **Utilities**) and all updates (may need to run multiple times to get all updates).

Launch Acrobat, and make sure to say "don't ask again" when prompted for file-opening preferences.

For multimedia lab machines, download and install the Canon CanoScan drivers for our scanners (see the **Scanners** folder on the server).

Fetch (FTP Client)

Install from the **Network** folder on the server. Register with the name "Suffield Academy" and the serial number in the name of the disk image.

FireFox

Download the latest off the web and install.

Video Players

On the file server, in the **Multimedia** folder, find and open the folder called **Video**.

Install **VLC**.

Install **Perian** by double-clicking the Perian prefPane. Choose **Install for all users of this computer**. When the preference pane loads, *uncheck* **Automatically Update**.

Fonts

On the file server, in the **Multimedia** folder, find and open the folder called **Fonts**. Copy the contents of this folder into the `/Library/Fonts/` folder on the computer's hard drive.

1.3.2 Network Workstation Software

The following software should be installed on machines that are owned by Suffield (network workstations)

Remote Desktop

In the **Network** folder, install the **Suffield Remote Desktop 3** package. This allows us to connect to computers and remotely manage them.

Network Settings

Networked machines should force the user to authenticate before they can use the machine.

Open **System Preferences** and click on **Accounts**.

Click the lock to make changes (if necessary) and authenticate.

Click the **Login Options** button.

In the preference pane that appears, make sure **Automatically log in as:** is **deselected**. Also, set **Display login window as:** is set to **Name and password**. Finally, make sure **Enable fast user switching** is **deselected**.

1.3.3 Printers

On the **Installers** section of the file server, open the **Printing** folder.

Canon Copier Software

Run the **PS Installer** in the **Faculty Room Copier** folder.

Run the **UFR II Installer** in the **Library Copier** folder.

1.3.4 Faculty Applications

The following applications should only be installed on computers for Faculty and Staff.

FileMaker 9

Open the **Faculty and Staff** folder on the file server. Then find and open the **FileMaker** folder.

Run the FileMaker Pro 9 installer. If asked to register, choose **Already Registered**.

Once installation is complete, you'll need to copy a few more files onto the computer. Copy one or more of the FileMaker launch scripts (*e.g.*, `Open-o-Rama` or `Portal`) onto the desktop.

GradeKeeper

Open the **Faculty and Staff** folder on the file server. Then find and open the **Gradekeeper** folder.

Run the installer with the default options. When the installer is done, launch the application.

The application will prompt you to register the product. Click the **Enter Code** button. The registration information is contained in a text file in the same folder as the application.

Once the application is registered, you can quit it.

1.4 Final Preparations

Before building an image out of this computer, we need to make sure and "tidy up" any other aspects of the system.

1.4.1 Customize the Dock

Make sure the dock has all of our standard applications on it. You may wish to remove unused applications (such as Mail and Address Book) to create more space.

1.4.2 Hard Drive Cleanup

Look at the root level of the hard drive and delete any temporarly log files left over from the installation of software.

1.4.3 Reset Safari

Open Safari and choose **Reset Safari...** from the **Safari** menu. Check all the boxes and reset, then quit.

1.4.4 User Profile Customization

Any changes we've made to the User's desktop must now be saved so that when the computer is re-registered the user gets the same settings.

Open `Terminal.app` (in `/Applications/Utilities`) and type the following:

```
sudo -s
```

You will be asked for the administrator's password. Once you have correctly authenticated, your prompt will begin with a hash (#).

If you changed the background image and want that to stick for new users, copy the background preferences to the global prefs:

```
cp "/Users/suffieldacademy/Library/Preferences/com.apple.desktop.plist" \
"/Library/Preferences/"
```

We need to provide some default settings for new user accounts:

```
cd "/System/Library/User Template/"
```

That moves you to the folder where the user settings are kept. Before we do anything else, make a copy of the existing settings:

```
cp -pR Non_localized Original_Non_localized
```

Now we're ready to copy settings from our current user into the default settings for the machine. Each of the commands below has been split into two lines. You may enter each command on two lines (as shown), hitting the **return** key after the backslash. Alternately, you may omit the backslash entirely and type the commands all on a single line.

Since we modified the dock to hold our new applications, we'll move that over as well:

```
cp "/Users/suffieldacademy/Library/Preferences/com.apple.dock.plist" \
"Non_localized/Library/Preferences/"
```

We'll copy the modified FirstClass settings:

```
cp -R "/Users/suffieldacademy/Library/firstclass" \
"Non_localized/Library/"
```

If you've installed Gradekeeper on this computer, you'll need to copy the registration preferences over:

```
cp "/Users/suffieldacademy/Library/Preferences/Gradekeeper.plist" \
"Non_localized/Library/Preferences/"
```

If you've installed FileMaker on this computer, and you've copied the Suffield Opener script to the desktop, you'll also want to add those files to the default. Note that the scripts must be on the user's desktop for this line to work:

```
cp "/Users/suffieldacademy/Desktop/"*.fp? \
"Non_localized/Desktop/"
```

1.4.5 Deleting All Users

If you wish to return the computer to a "factory default" state, where the user must register the machine and create a new admin user, you can do so. We recommend copying the machine to a disk image, and then opening the disk image and making the changes. In the example below, the disk image has been mounted at `/Volumes/Macintosh HD`.

```
sudo /usr/bin/dscl -f \
/Volumes/Macintosh\ HD/private/var/db/dslocal/nodes/Default \
localonly -delete /Local/Target/Users/suffieldacademy

cd /Volumes/Macintosh\ HD/private/var/db/dslocal/nodes/Default/groups

for g in *.plist; do group=${g%.plist}; echo $group
sudo /usr/bin/dscl -f \
/Volumes/Macintosh\ HD/private/var/db/dslocal/nodes/Default \
localonly -delete \
/Local/Target/Groups/$group GroupMembership suffieldacademy
done

sudo rm \
/Volumes/Macintosh\ HD/private/private/var/db/dslocal/nodes/Default/config/SharePoints/Suffield*.plist

sudo rm /Volumes/Macintosh\ HD/private/var/db/.AppleSetupDone
```

Those lines remove the user from the directory, remove it from all the groups, drop any shares associated with the user, and finally, remove the AppleSetup flag (which forces re-registration).

1.4.6 Networked Users

For **networked workstations** (not laptops), we tell the machine to allow anyone with a valid network name and password to log on.

Open **System Preferences** and click on the **Accounts** icon.

Unlock the preference pane, if necessary.

Click on the **Login Options** icon at the bottom of the screen.

There will be a button to **Join** a network directory system. Click this button.

If not already filled in, use "ldap.suffieldacademy.org" as the server.

1.4.7 Local Admin Group

For **networked workstations** (not laptops), we add a special group so that we can easily administrate the computers with our own usernames and passwords.

In the terminal, type the following:

```
dscl /Search -read /Groups/helpdesk GeneratedUID
```

That will give you the UID of the group you'd like to nest (use something else instead of "helpdesk" for your group name).

Now:

```
dscl . -append /Groups/admin NestedGroups GENERATED-UID-OF-NETWORK-GROUP
```

Substitute the UID you got from the first step.

That adds our OpenDirectory "helpdesk" group to the local administrators group, granting us the rights to make administrative changes on the machine.

1.4.8 Printer Group Changes

On **networked workstations** (not laptops), we add our networked groups to a special group so that any user can add or delete printers on the system.

In the terminal, type the following (all on one line):

```
dseditgroup -o edit -n /Local/DEfault -u suffieldacademy -p -a
suffield -t group lpadmin
```

This authenticates as user "suffieldacademy" and adds our "suffield" network group to the "lpadmin" group, effectively allowing all our networked users to modify printer settings.

1.5 Building the Image

Netboot the master machine.

Start DeployStudio.

Choose the "Create master from hard drive" option.

1.6 NetRestore Configuration

Once you've built a NetRestore image, you have to make NetRestore aware that it exists. A quick configuration file change allows NetRestore to "see" the new image and make it available for restoring.

Note: The reader is assumed to have some general experience with NetRestore; we do not provide an in-depth discussion of what NetRestore is or how it works. For more information on NetRestore (including documentation), please see the NetRestore web site.

1.6.1 Updating an Existing Image

If you're building an image that replaces an existing one, you simply need to copy the new image onto the NetBoot server and replace the existing image. Currently, all images on the NetBoot server reside on the **Images** drive, filed away by image type.

You may wish to move the existing image to a temporary location before deleting it, in case the new image does not work as expected.

Once the image is copied, make sure it has the proper permissions. You can easily do this from the command line by running the following commands:

```
sudo chown netrestore_access:netrestore_admin ImageFile.dmg
sudo chmod 464 ImageFile.dmg
```

Replace `ImageFile.dmg` with the full path to the image file you copied.

Once this is done, the change should take effect immediately. NetRestore should begin using the new image without needing any further configuration.

1.6.2 Adding a New Image

In some cases, you may want to add a new image type to NetRestore. First, follow the instructions above for adding an image to the server and setting its permissions. In this case, however, do not replace an existing image; rather, pick a new name for the image that reflects what it does.

Next, you will need to update the `netboot-configurations.plist` file on the server. Currently, that file lives on the **Images** volume, in a folder called **WebConfig**. When our NetBoot image runs NetRestore, it loads this folder over the network and reads the configuration file found there.

The easiest way to add an image is to copy an existing stanza from this file and customize it for a new image. Here is a skeleton stanza you might want to use:

```
<key>Image Name</key>
<array>
    <string>afp</string>
    <string>veronica.suffieldacademy.org</string>
    <string>Images</string>
    <string>Path/To/ImageFile.dmg</string>
    <string>netrestore_access</string>
    <string>password</string>
    <string>Description of Image</string>
</array>
```

Assuming you store the image on the **Images** volume, you only need to customize the `Image Name` to give a short title to the image, the `Path/To/ImageFile.dmg` field to include the relative path to your image (relative to the **Images** volume), the `password` line to include the password to the server (ask the Network Administrator if you don't know it), and the `Description` field to define what the image does.

Once this file has been saved, the changes take effect immediately for clients accessing the settings via the web. Launch **NetRestore** and verify that the information is correct.

1.7 Resources

Mike Bombich is the creator of Carbon Copy Cloner (to create disk images) and NetRestore (to reimage the machines). His main web site is www.bombich.com, and it contains a wealth of information on building images and managing large numbers of computers.