

# OS X – Here We Go Again

Scott E. Hanselman  
Ringling School of Art  
2700 N Tamiami Trail  
Sarasota, FL 34234  
(941) 359-7633  
shanselm@ringling.edu

Luis Hernandez  
Ringling School of Art  
2700 N Tamiami Trail  
Sarasota, FL 34234  
(941) 359-7633  
lhernand@ringling.edu

Divyangi Anchan  
Ringling School of Art  
2700 N Tamiami Trail  
Sarasota, FL 34234  
(941) 359-7633  
danchan@ringling.edu

Mahmoud Pegah  
Ringling School of Art  
2700 N Tamiami Trail  
Sarasota, FL 34234  
(941) 359-7633  
mpegha@ringling.edu

## ABSTRACT

Due to the positive response of our fall 2002 OS X deployment and our desire to provide the campus community with the latest and greatest tools, we upgraded our instructional computer laboratories to Jaguar, Macintosh OS X version 10.2 in the fall of 2003.

This paper will outline the procedures we implemented our second time around. We shall discuss the items we did differently such as LDAP authentication, font management, application support, user training, login and logout hooks, printing, and peripheral support. We will share with our colleagues the issues we came across and provide the solutions that so many of us in a support role strive to provide.

A new local file system was designed and integrated into Jaguar by The Ringling School Institutional Technology (IT) staff. Login and logout hooks were implemented to ensure usability and to call several maintenance-type functions. Issues such as file corruption on the desktop and user quota encroachment were handled in a unique and elegant manner and will be detailed in our paper. Jaguar provides support for SMB file services and was a welcome addition that allowed users to seamlessly share files with their colleagues on other platforms.

The summer of 2003 was a busy time for Ringling School's IT staff and we are proud of the results we achieved and hope that others can benefit from our trials and tribulations.

## Categories and Subject Descriptors

K.6.1 [Project and people management]: Life cycle, Management techniques, Strategic information systems planning, Systems analysis and design, Systems development, Training

## General Terms

Management, Documentation, Performance, Reliability, Security, Human Factors, Standardization.

## Keywords

Macintosh OS X, Migration, Fonts, Network, LDAP, NFS, SSH, Login Hooks, Logout Hooks

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

*SIGUCCS'04*, October 10-13, 2004, Baltimore, Maryland, USA.  
Copyright 2004 ACM 1-58113-869-5/04/0010...\$5.00.

## 1. INTRODUCTION

The fall semester of 2003 saw our academic Macintosh computer labs as well as faculty and staff machines upgraded to OS X version 10.2 or Jaguar. The advent of Jaguar brought LDAP version 3 support as well as enhanced SMB and hardware support [2]. We will address the things we learned the second time around and the adjustments we made from what we learned the first time from our fall 2002 OS X deployment. We shall also discuss the new challenges we faced as we adapted our schema to the new features of this generation of OS X.

## 2. ISSUES

### 2.1 File Inconsistencies

When Macintosh OS X files are copied to and from HFS (Hierarchical File System) and HFS+ file systems to a UFS file system, the Finder attribute and or the resource fork can become inconsistent. The Finder attribute is closely coupled with the resource fork and contains similar data [5]. Finder attributes can become inconsistent for a number of reasons including:

- User has encroached their disk quota
- Application failure or crash
- Downloading issues

When a file becomes inconsistent many issues can arise:

- User cannot log in if file resides on Desktop
- User cannot access any Folder or Directory that file resides in
- File will not open with relevant software application

### 2.2 NIS and Other Security Concerns

NIS identification and authentication security concerns [8] as well as NetInfo security needed to be addressed. Software copyright laws and network security dictated that measures be taken in order to protect our resources.

### 2.3 Housekeeping Chores

- Removal of local user cached items to ensure confidentiality
- Preparation of user's networked home space to provide consistent starting point for all users as well as point to return to if needed
- Address Print Center inconsistencies when printers were deleted or added improperly by users
- Enable ATS Font server mechanism
- Provide for unavailability of network file servers

## 2.4 Hardware Issues

- Scanning with old SCSI scanners not supported under OS X
- Needing to provide slide scanning capabilities
- Printing with new color laser printers with color consistency and accuracy

## 2.5 Software Issues

All applications were installed on a distributed image and run locally. The issues with applications this time around generally was in their functionality after installation. Please note that these functionality issues may have been due to our installation and customization procedures but some have been wide spread and are known issues with the vendor.

### 2.5.1 Third Party Applications

- Adobe Photoshop print issues when improper format chosen
- Adobe Illustrator save for web feature non functional due to write access needs
- Macromedia Flash MX initialization and first run non-functional due to improper "Case" of filenames

### 2.5.2 OS X System Issues

- Removal of OS X cached items of over 3GB in some instances
- Nightly machine reboot and user warning prior to reboot so data loss could be prevented
- Provision of ample local disk space for user for compute intensive applications such as digital media
- Mount point for optical media when size of media encroached on remaining disk space
- Roaming Profiles for consistent user experience across all academic laboratories

## 3. ADDRESSING THE ISSUES

### 3.1 File Inconsistencies

We had over 100 instances of users with corrupted files on their desktop which prevented them from logging in. The locking of the Desktop directory alleviated many help desk calls and prevented frustration on the part of the users. The means of locking this directory was straightforward and done by first changing the ownership to root and then omitting write permission to the user. The identification of the inconsistent files in non-accessible directories was achieved by using the Terminal application. Generally, files with dates askew or with a size of 18K were the standard indicators of file abnormalities. Troubleshooting the problem was done by moving the file to another location and then accessing the problematic directory in the Finder to see if the issue had been resolved.

The solution of locking the Desktop directory brought its own issue that was foreseen before its release. The default location for screen grabs is the Desktop. To circumvent this problem a solution was found and introduced at the same time as the Desktop locking. To take a screen grab it was necessary to place the image on the clipboard [4] by pressing the control key in

conjunction with the normal key combination of shift+apple+3 or 4.

If a file had lost its application association, it was on occasion addressable by adding the correct extension to the end of the file.

## 3.2 NIS and Other Security Issues

### 3.2.1 LDAP

NIS identification and authentication security issues were addressed by our migration to LDAP version 3. This migration was planned and implemented in the summer of 2003 and was the subject of our SIGUCCS'03 publication "Regaining Single Sign-On – Taming the Beast." The server setup can be found there and is beyond the scope of this paper. Once the LDAP server setup was complete it was necessary to configure the client's Directory Services. The setup for LDAP is done using Directory Access in the Utilities directory of Applications. The steps that follow outline how we configured our clients to include LDAP as the authentication entity.

- Open Directory Access and select 'LDAPv3' check box and use 'configure' to enter values.
- Select 'New' and enter the required information for 'IP Address' and 'Configuration Name.'
- Select 'RFC 2307 UNIX' as the 'LDAP Mappings' drop box.
- Use the search base for your LDAP server in the 'search suffix base' box. For example, we use 'dc=rsad, dc=edu' as our suffix base.
- Select the 'Search and Mappings' tab.
- Select 'Users' and ensure that the 'Search Base' box at the bottom reflects the correct base as entered before (e.g. dc=rsad,dc=edu). In the right hand side pane, ensure that 'Users' maps to the following 'objectclasses': posixAccount, inetOrgPerson, shadowAccount, extensibleObject, and apple-user. Other 'objectclasses' can be included as required. Expand the 'Users' tree and use the following attributes map to correctly map the Directory Access attributes to the LDAP attributes:

Table 1.

Directory Access Attribute	LDAP Attribute
RecordName	Uid cn
RealName	Cn uid
UniqueID	UidNumber
userPassword	userPassword
loginShell	loginShell
authAuthority	authAuthority
PrimaryGroupID	gidNumber
NFSHomeDirectory	homeDirectory

- Select ‘Groups’ and ensure that the ‘Search Base’ box at the bottom reflects the correct base as entered before (e.g. dc=rsad, dc=edu). In the right hand side pane, ensure that ‘Groups’ maps to the following ‘objectclass’: posixGroup. Expand the ‘Groups’ tree and use the following attributes map to correctly map the Directory Access attributes to the LDAP attributes:

**Table 2.**

Directory Access Attribute	LDAP Attribute
GroupMembership	MemberUid
Member	MemberUid
PrimaryGroupID	GidNumber

- Select ‘Mounts’ and ensure that the ‘Search Base’ box at the bottom reflects the correct base as entered before (e.g. dc=rsad, dc=edu). In the right hand pane, ensure that ‘Mounts’ maps to the following ‘objectclasses’: mount. Expand the ‘Mounts’ tree and use the following attributes map to correctly map the Directory Access attributes to the LDAP attributes:

**Table 3.**

Directory Access Attribute	LDAP Attribute
VFSType	mountType
VFSOps	mountOption
VFSLinkDir	MountDirectory

- Save the configuration using ‘OK’.

Select the ‘Authentication’ tab and add the LDAP server in the authentication path by using ‘Search → Custom path → Add.’ Save the configuration by using ‘Apply’.

### 3.2.2 Other Security Issues

In any open lab environment, security must be at the forefront of thought for any administrator. Physical security is maintained with a combination of cables and locks and a mandatory count of all equipment by lab monitors on a nightly basis.

Software and network security are also of major importance and very closely mimic the schema we introduced last year. Open Firmware Password [3] is a very important feature to include on every workstation as it prevents the machine from being booted by any other device than the one chosen by the administrator. If the machine were to be booted from the install CD for instance, the user could change the root password and have complete access to the system. Booting the machine from another device would also negate the font protection schema outlined later in this paper.

We once again disabled the Terminal application to avoid prying eyes by changing the executable permissions and hiding the

application by preceding its name with a dot. We also disabled Network utilities to avoid unnecessary traffic by the use of the tools provided to run traceroutes, portscans, and pings. Access was also limited to many of the utilities such as NetInfo, Directory Access, and other administrative applications. Remote administration was enabled via ssh and made secure via the /etc/sshd\_config file by adding an “AllowGroups” entry for those approved to login remotely.

Third party software licensing and security were addressed through the use of KeyServer [7]. KeyServer is a software application license metering package that limits launches of keyed applications to a particular number, location, or user. When an application is keyed it must have contact with the key server in order to run. If the server is not available the application will not function therefore rendering software pilferage fruitless.

## 3.3 Housekeeping Chores

### 3.3.1 Login Hook

The implementation of a Login hook allowed us to perform many tasks upon user login to ensure usability under all foreseeable circumstances. Login hooks took care of many “housekeeping” chores to set up the system with the users personal preferences and files. Essentially, the login hook prepares the users home space for transparent access, makes fonts available for the user, resets printer preferences, and alerts users of pending quota limits or unavailable network resources.

#### 3.3.1.1 Default User Library

In order to provide a consistent profile upon first login and to install a few desirable preferences such as a Dock with oft accessed applications, we created a default Library to distribute to all users. We implemented a flag check in the Login hook that if not present would trigger a download from a network location and unpack the default Library into the users network home directory. The benefit of this mechanism was twofold, it allowed for a default starting point for all users and a way to revert back to the default Library in case of preference corruption.

#### 3.3.1.2 The Local File System

One of the issues we ran into last year that rendered the client machine inoperable was when network file services were not available. OS X necessitates that each user has write access to a location to write preferences, generally their Library. When network file services are not available which includes the users home directory, there is no Library the user has write access to. In this case, the machine would lock up and refuse the user access to any application or function whatsoever. To combat this we implemented a local file system that would provide for a local home space should the user’s network space be unavailable.

This local file system is a set of symbolic links except for the Desktop folder that point to the users network home space. In the event that the network home space is not available, this local store allows the user to utilize the computer and all its resources by becoming the default home space that the user has write access to. Upon user login, the hook checks to see if a local store exists for the user and if it does it must be deleted in case the users network home space location has changed. If there is no local store, or one has just been deleted, the hook then creates a current local store

with all the necessary links. Figure 1 depicts an image of the directory tree of the local store:

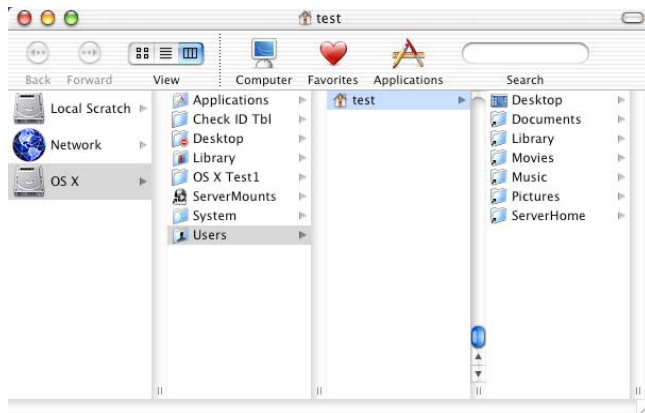


Figure 1.

The omission of the Desktop link was planned due to the lessons learned from the previous year. As mentioned earlier, the provision of the users Desktop directory caused many issues as several users overloaded this directory. The login hook also creates a link to the users “ServerHome” which is their actual network home space. The link is there to enforce the idea that the other links are local and are not their permanent home directory. An applescript executable in the login hook places the default Home icon of the users network home for easy access to their permanent home directory.

### 3.3.1.2.1 Training For Local File System

Our faculty at The Ringling School of Art and Design demand the best from their students and the best environment in which to instruct these future artists. When deploying an upgrade in a system like OS X, familiarizing our faculty members with the new features of the system as well as our customizations was paramount. By educating the faculty who have contact with the student body on a daily basis, they, in a sense, become the technical liaisons between the IT department and the students.

The new local file system was an area that needed to be addressed so that the users knew what we did and why. The items discussed with the faculty were also posted on each machine in printed form and posted on the IT web site.

### 3.3.1.3 Fault Tolerance and Alerts

The login hook allows for a large level of fault tolerance. Should the directory server or network home space not be available, the login hook is able to continue cleanly with its execution. If the directory server is unavailable, the login hook will default access to local users so that the administrator may troubleshoot the system. If network home spaces are unavailable, users are alerted of the situation (see figure 2) and their local home links are directed to temporary local storage so that the user may log in and work from the system.



Figure 2.

Another alert will activate when users reach ninety percent of their quota limit.



Figure 3.

In both situations, users are informed with audible and the visual messages shown above to contact technical support services. The alerts have decreased the amount of frustration on the part of our users and have increased the speed at which we respond to technical issues since the alerts let users know exactly what the issue is before they contact technical support.

### 3.3.1.4 Printer Configuration

The nature of the Print Center allows for users to add and delete printers. While this is not ideal, it was deemed necessary to leave this functionality to ensure that the users could manage their print jobs and access print queues. Problems arose when users deleted printers and added printers improperly. To circumvent this issue we implemented our PrintFix script in the login hook to ensure that at login the user has a correctly configured Print Center. The following is our Perl script verbatim but for the DNS name of our printers.

```
sub printFix()
{
    ### Declare variables
    my $cupsdExec = "/usr/sbin/cupsd";
    my $killExec = "/usr/bin/killall";
    my $cpExec = "/bin/cp";
    my $sleepExec = "/bin/sleep";
    my $lpadmExec = "/usr/sbin/lpadm";
    my $touchExec = "/usr/bin/touch";
```

```

### Clear out improperly added printers by replacing .conf file
### with empty file
`$touchExec/etc/cups/ORIG.printers.conf`;
`$cpExec/etc/cups/ORIG.printers.conf/etc/cups/printers.conf`;

###Killing cups daemon to reload printer configuration
`$killExec -9 cupsd`;
`$cupsdExec`;

### Must wait for process to start before we can add printers
`$sleepExec 3`;

### Add printers
`$lpadmExec -p BlackAndWhite -E -v lpd://PrinterDNS -m "HP
LaserJet 8150 Series";
`$lpadmExec -p Color -E -v lpd://PrinterDNS -m "Xerox Phaser
7300N";

### Assign the default printer
`$cpExec /etc/cups/ORIG.lpoptions /etc/cups/lpoptions`;
}
1;

```

This script worked flawlessly for us but there is some preparation involved in order for it to work. A lot of sweat equity went into bringing it to fruition so we hope this helps someone. The lpadmin command dictates that the ppds for the printers be located not in their usual default location but in /usr/share/cups/model and must be spelled exactly as defined in the lpadmin command. The last line is where the global default printer location is stored and contains the description "BlackAndWhite" also as defined in the lpadmin command. The nature of the Print Center is to use the last printer accessed as the default and we wanted the black and white laser to be the default.

### 3.3.1.5 Fonts

Working for an Art and Design College, the importance of fonts, their variety, the licensing, and their cost is of major interest. Commercial font management tools available today secure fonts by burying them several layers deep in the hierarchy. It has been experienced however that no number of layers can keep out the curiosity seekers.

Fonts have been inherently insecure since the advent of OS X and the loss of ATM support. The methodology of the ATS font server in the previous release of OS X was to read the fonts at boot time from the /Library/Fonts directory and hold them in memory. In Jaguar, the ATS font server reads the fonts when an application is launched and calls for them. This created an issue for us and the login hook came to the rescue.

In order to protect the font licensing agreement we placed the fonts in a hidden directory that the user cannot see in the Finder which prevents the copying of fonts through the GUI. The login hook creates a link to this hidden directory in the /Library/Fonts

directory and removes the link after the font list has been read. Upon login, an applescript is called that launches the console which calls the fonts into memory. This link creation and removal in the login hook allows the font server to provide all available fonts to the user with an added layer of security.

### 3.3.2 Log Out Hook

The logout hook provides some minor house keeping by moving the local cache to another location and changes the permissions for nightly cleanups. This function prevents the subsequent user from viewing the previous users Internet and other caches.

## 3.4 Hardware

Scanning which had been so problematic in the past was addressed with the purchase of new Epson 3200 flatbed scanners. These new scanners have templates for film and slides negating the need for a third party utility to support our SCSI slide scanners. With Jaguar and these new scanners we were able to use PhotoShop once again to import images as well as use the scanning utility provided by the hardware vendor.

We provided training for the use of the new color laser printers deployed in seven academic labs. The printer workshops included swatches, proper media, and general usage of the new equipment.

## 3.5 Software

### 3.5.1 Third Party Applications

#### 3.5.1.1 Macromedia

Macromedia Flash proved to once again be problematic in our installation, this time was version MX. Upon first launch, Flash writes over 15mb of preferences to the user's Library. The problem occurs when the application tries to access files within its own directory, in this case a particular file it cannot find. The reason that it cannot find the file is that it's looking for a file called Html when the file is actually named HTML. Case counts in OS X where it didn't in OS 9.

#### 3.5.1.2 Adobe

We ran into a couple of issues with Adobe products, most notably Illustrator and PhotoShop. The save for web function in Illustrator in our installation was non-functional for a non-administrative user because write access is necessary in a particular directory. The file that needs to be written to is called Recently Used Optimizations.irs and is located in the directory /Applications/Adobe Illustrator 10.0.3/Presets/Save for Web Settings. The issue with PhotoShop was with printing. Unless you choose Print with Preview and set the preference to ASCII instead of Binary [6], gibberish will be printed on numerous pages to the printer with no end in site. This preference stays with the user and need only be set once.

### 3.5.2 OS X System Issues

In the Ringling campus academic laboratories we try to provide ample space for the users to work locally. This is necessary due to the nature of some of the digital video applications. To provide this feature we divide the hard drive into two partitions, one named OS X for the system software and applications, and one called Local Scratch. Due to the increasing sizes of software applications the size of Local Scratch has been diminishing over time. Our present base image is currently over 5GB and with the digital video applications the image surpasses 20GB.

The size in and of itself is not an issue, other than image distribution that we will get into later. Making the correct decision when choosing partition sizes is of great importance. To provide the largest Local Scratch and still provide ample space for the operating system and application updates we increased the size of the OS X partition to 5GB beyond the image size. This may seem like overkill but you will see shortly that it is not large enough.

OS X harbors many levels and quantities of caches. In our multi-user networked environment OS X has cached in excess of 3GB in /Library/Caches which includes the desktop pictures of every user that has logged into the machine. If you take that 5GB of extra space, subtract 3GB of cache and then try to mount a blank DVD for burning in a Super Drive equipped machine, you will most likely see the problem. There is not enough space to mount the disk in the scenario above and a descriptive error message tells you so. The solution to this is to find the location where media is mounted. Media mounts in the directory /tmp which can be problematic if not enough disk space is available. The trick is to take advantage of the large Local Scratch partition by pointing the mount point to /Volumes/Local Scratch/tmp by creating a symbolic link in /tmp.

To remove the 3GB of cache we schedule a cron job once every week. A cron job was also scheduled to remove some cached items from the local file system mentioned previously. We reboot the machines also via a cron job at 2:30am which was not problematic until the end of the fall semester drew near and the lab hours were extended to 3am. In order to avoid data loss we implemented another cron job to alert the user via an applescript that the machine was scheduled to reboot. We gave the user a five-minute warning to save all open documents. The alert was verbal and textual.

In order to provide a consistent user experience on all of the Macintosh computers across campus we once again leveraged the NFS automount feature of OS X. Automounting lets the user seamlessly and transparently access their network home space and all of the files within, including preferences regardless of the users physical location.

#### 4. IMAGE DISTRIBUTION

It has been the passion of the IT staff to distribute images via an OS X server with the use of NetInstall. Unfortunately this did not pan out as expected due to time considerations. Images were distributed using the tried and true method of Apple Software Restore (ASR) in conjunction with FireWire drives.

ASR has been ultra reliable and an indispensable tool to have in our toolbox. One limitation of ASR however is image size. The image for our labs equipped with digital video software approached 20GB and ran into this size limitation. The fix was to use ASR via the command line in OS X as opposed to the OS 9 GUI version.

#### 5. WHAT'S NEXT

Panther is on the agenda for the fall semester of 2004. The images will be distributed and updated via Radmind [7] in conjunction with NetInstall which we have tested thoroughly this past year. New G5s will be installed in some of our academic labs along with new firewire interfaced scanners. We have found OS X server 10.3 to be a suitable vehicle for a CUPS print server and are testing it using Pykota [1] for accounting and quota enforcement. FontBook and some of the other new features of Panther are a welcome addition as we move the Ringling Academic computing labs forward.

#### 6. ACKNOWLEDGEMENTS

The authors would like to thank the Ringling School of Art and Design Academic Affairs department for their continued support of our quest to bring the best technology to the Ringling campus. Apple computers has been a long standing and valued partner at Ringling and their continued support is appreciated. We would also like to thank ACM SIGUCCS for their interest in our project and for providing the vehicle for us to share with our colleagues.

#### 7. REFERENCES

- [1] A full featured, free centralized and extensible Print Quota and Accounting Software [http://www.librelogiciel.com/software/Pykota/action\\_Features](http://www.librelogiciel.com/software/Pykota/action_Features)
- [2] Apple – Mac OS X – New Features <http://www.apple.com/macosx/newfeatures/>
- [3] Apple – Support - Downloads – Open Firmware Password 1.0.2 <http://www.apple.com/support/downloads/openfirmwarepassword.html>
- [4] Mac OS X: Shortcuts for Taking Pictures of the Screen <http://docs.info.apple.com/article.html?artnum=61544>
- [5] Mac OS X: System Overview: The Finder and File Operations [http://developer.apple.com/documentation/MacOSX/Conceptual/SystemOverview/Finder/chapter\\_9\\_section\\_6.html#apple\\_ref/doc/uid/20000987/BCIIICII](http://developer.apple.com/documentation/MacOSX/Conceptual/SystemOverview/Finder/chapter_9_section_6.html#apple_ref/doc/uid/20000987/BCIIICII)
- [6] Multiple Pages of Garbled Characters Print from Photo Shop 7.0 in Mac OS X <http://www.adobe.com/support/techdocs/2db2e.htm>
- [7] Sassafras Software K2 KeyAuditor/KeyServer <http://www.sassafras.com/k2.html>
- [8] Research Systems Unix Group: radmind <http://rsug.itd.umich.edu/software/radmind>
- [9] Securing NIS <http://www.eng.auburn.edu/users/doug/nis.html>