Managing Public Area Macs (OS X)

James Partridge (OUCS) 24 June 2004

What will this talk cover?

- Overview of integrating OS X into Directory Services
- Client Management
- Application Management

States States

- Essential Tools
- Security

Why talk at all?

- Still many preconceptions about MacOS X dating from OS 9 days
- Macs are very well suited to Help Centres
- More detailed courses (esp. on Directory Service integration) will be offered

Directory Service Integration

□ AD

eDir

Should I use an OS X Server?

Active Directory

- □ We aren't even at the testing stage yet
- IO.3 native authentication uses the AD plug-in in Directory Access.app
- ADmitMac (Thursby) is popular. Thursby's comparison of ADmitMac and the native 10.3 AD method is available at: http://www.thursby.com/products/ admitmac-vs-panther.html
- IO.3 native plug-in good for smaller environments; ADmitMac better for larger ones
- Useful scripts at http://shukwit.com/ and other documentation on Macosxlabs site

eDirectory

0		Directory Access	
	Services	Authentication	Contacts
Enable	Name Active Directory AppleTalk BSD Flat File and LDAPv3 NetInfo Rendezvous SLP SMB	NIS	Version 1.0.3 1.1 1.1 1.6.3 1.6 1.1 1.6 1.1 1.6.3 1.6 1.1 1.1
		Configure	
Click th	e lock to prevent fu	urther changes.	Revert App

No native eDir plug-in (yet!!)

Must extend eDir schema to accommodate Macs

Use LDAPv3 and custom mappings on the client

Netware 5.1	Netware 6	Netware 6.5	
Native File Access pack must be installed	Native NFAP or can be added	Native NFAP or can be added	
AFP 2.2	AFP 2.2	AFP 3.1	
NDS RSA + Simple password	NDS RSA + Simple password	Universal password	
≤ 8 character passwords on Mac	≤ 8 character passwords on Mac	≥ 8 character passwords on Mac (in SP2?)	

eDir Authentication Summary

- Extend schema (LDIF files are available for NW6 and NW6.5)
- Set user attributes
- Create mounts object
- Import server public certificate (for SSL connections) onto client Mac (convert from .der to .pem format)
- Directory Access for LDAP mappings

States and

Diagnose problems

Server Public Certificate

- Copy RootCert.der file from SYS:PUBLIC directory on NW server into folder on client Mac
- Open Terminal.app, navigate to folder and type: openssl x509 -inform DER -outform PEM -in RootCert.der -out RootCert.pem
- Create directory 'certs' in /Library, then sudo cp [path] / RootCert.pem /Library/certs
- cd /Library/certs, then: sudo chown root:wheel RootCert.pem and sudo chmod 400 RootCert.pem

Sector States

Add the following line to /etc/openIdap/ldap.conf: **TLS_CACERT** /Library/certs/RootCert.pem

Netware Troubleshooting

SDIDIAG to check only one SDI key for Tree

Monitor LDAP activity with DSTRACE:

DSTRACE SCREEN ON

DSTRACE -ALL

DSTRACE +LDAP

Pipe DSTRACE activity into a file with DSTRACE FILE ON (defaults to SYS: \System)

Netware Troubleshooting

Monitor NMAS activity with NMASMON:

NMASMON * sys:\public\nmaslog.txt

Turn it off with UNLOAD NMASMON

AFP activity: AFPLOG ON / AFPLOG OFF
 Creates log file afptcp.log in SYS:\ETC

Should I use OS X Server?

IO or unlimited client versions are available

Doesn't require an Xserve to run - any reasonable Mac will do

LDAP integration into existing Directory Services

Excellent client management (OS X & OS 9)

Many other uses

OS X Client Management

ARD
Radmind
Casper
OS X Server

States and

Apple Remote Desktop 1.2

Current version

Good for monitoring and troubleshooting

Quite secure: AES-128 bit encryption; uses UDP 3283

Uses Apple's own ARD protocol

Can be started remotely with the 'kickstart' utility: sudo '/System/Library/CoreServices/ARD Agent.app/ Contents/Resources/kickstart' -restart -agent

See http://www.apple.com/support/remotedesktop for more details

Apple Remote Desktop 2

New version ARD 2 (available in July)

Sector States

- Greatly enhanced management capabilities
- Single and multiple software installs (can be scheduled)
- Greatly enhanced inventory db (PostgreSQL) & reporting
- Uses VNC (so can view Linux and Windows too); Java viewer also built in
- Execute Unix shell scripts or commands on 1 or more Macs
- ...and many more! (comparison chart at http:// www.apple.com/uk/remotedesktop/upgrade.html)





- Powerful CLI Unix tools (a Tripwire system, in effect)
- Open Source

States and

- http://rsug.itd.umich.edu/software/radmind/
- Several webcasts on the Macosxlabs site: http: //www.macosxlabs.org/webcasts/index.html
- Widely used in academic institutions, but has a relatively steep learning curve



Several Parts:
Casper Admin
Casper
Composer
Recon

2 - Starson



http://www.jamfsoftware.com/index.html

Casper Admin

0	Cass	er Admin				_	
	6 203	299	RDMI	v			
Configurations		Gr	oups				1
Package Repository	All (95 Packages)						
OS X Standard	Classic Apps						
OS 9 Standard	Classic Multimedia						
OS X with Classic	Classic OS						
	Communications						
	Fonts						
	Graphic Design						
	Package Name *	Size	Format	Group	Priority	FUT	
	InDesign 2.01.package	144.24 M8	Read Write (OS X)	Graphic Design	10	Yes	
	Intellimouse.img	267.03 KB	Read Only (OS X.	Classic Apps	10	Yes	
	iPhoto 2.0.package	35.45 MB	Read Only (05.X)	MultiMedia	10	Yes	
	Sync 1.0.package	5.47 MB	Read Only (OS X)	Utilities	10	Yes	
	Sync 1.1.package	6.83 M8	Read Only (OS X)	Utilities	10	Yes	
	Ralian.pkg	7.22 M8	Apple Package	Languages	10	Yes	
	(Tunes 4.1.package	7.1 MB	Read Only (OS X)	MultiMedia	10	Yes	
	Japanese.pkg	7.03 M8	Apple Package	Languages	10	Yes	
	Korean.pkg	6.71 M8	Apple Package	Languages	10	Yes	
	LexmarkPrinterDrivers.pkg	42.32 MB	Apple Package	Print Drivers	10	Yes	
	Mac OS 10.3.1.package	638.13 M8	Read Only (OS X)	Operating Syste	1	No	
	Mac OS 10.3 package	634.77 M8	Read Only (OS X)	Operating Syste	1	No	
	Mac OS 9.2.2.img	109.71 M8	Read Only (OS X.	Classic OS	2	No	
	MacOSXUpdate10.3.1.pkg	713.15 KB	Apple Package	OS Updates	10	Yes	
	Media Player 7.1.img	3.56 MB	Read Only (05 X.	Cassic Multimedia	10	Yes	
	Microsoft Frontpage 1.0.img	10.91 M8	Read Only (OS X.	Classic Apps	10	Yes	
	Microsoft Outlook 2001.img	12.7 M8	Read Only (OS X.	Classic Apps	10	Yes	
	MS Office vX 10.1.5.package	122.39 M8	Read Only (05.X)	Standard Applica	10	Yes	
	MS Office vX Value Pack.package	186.81 MB	Read Only (OS X)	Standard Applica	10	Yes	
	MSUAM.package	175.21 KB	Read Only (OS X)	Utilities	10	Yes	

New Config] [New Group

1 Unknow

Application packages can be bundled together into groups (e.g., Web browsers).

Packages and Groups can be bundled together to make Configurations (e.g., for specific Colleges or Departments)



Casper

000 c	asper
CERE	200
Install Location: Macir	ntosh HD 🗧
🗹 Erase volume "M	acintosh HD"
Configuration: OS X	Standard 🗧
	Easy Install
Installs the latest build o standard applications.	f Mac OS X and all of our
Computer Name: Dem	onstration
🗹 Reboot When Done	Create Install Log
Take Snapshot For Ba	ickup
	nstall

Client-side application for deploying packages to client machines

Can be run from local FireWire drive or from an OS X server hosting NetBoot images

Can push packages to remote machines (over SSL)

Can be used for deploying a standard OS X image



Recon

0	Recor	n for JAMF Demo	
, ree	3N >		
ase fill out the inform	nation about your comput	er below	
User's Name:	Benny	Computer Name:	Benny's Computer
Phone Number:		Asset Tag:	387624
Email Address:	benny@email.com	Position:	Assistant
Department:	Development 🗧		
Building:	Fleming Hall	Room:	100a
Monitor Make:	Apple	Monitor Model:	
Monitor Size:	21"		
Monitor Asset Tag:	387625	Monitor Serial #:	
PO Number:	100345	PO Date:	02 ; / 22 ; / 2003
Vendor:	Apple	Warranty Expires:	02 1 / 22 1 / 2006

Communicates with Jamf Software Server to upload hardware & software inventory



Composer

000) Com	ooser
S	COM	203302
	Snapshot Type:	✓ Please Choose
	Take Snapshot	New Files New and Modified Files
	Install and configu	ire your software
	Package Name:	
	Build Package	
	Verify Contents)
	Package Type:	Please Choose 🛊
	Finish Package	Delete Temp Files

Builds packages for deployment by Casper

Takes before and after snapshots of an install





Jamf Software Server

- Web interface to Casper
- Apache Tomcat / MySQL backend
- Can be installed and configured in a few minutes
- Combines Casper, Casper Admin, Recon and Composer

OS X Server

000	Workgroup Manager: xserve-1.oucs.ox.ac.uk	0
Admin Sharing Accounts Prefe	a c Connect Disconnect Refresh New Window	
€ + Authenticated as admin to loca	l directory: /NetInfo/root	۲
	Preferences	
Q.	Select one or more items from the list and click on a preference below to make changes.	
Name ID		
Administrator501102	5 Applications Q Classic Dock	
	Finder 🚱 Internet 🙆 Login	
	Media Access 🔶 Mobile Accounts 📑 Printing	
	System Preferences 🕢 Universal Access	
1 of 2 users selected		
		ALCONTRACTOR D

Application Management

Installers
CLI
Licensing

Contraction and

Application Installers

- Read the new white paper on the Macosxlabs site: "Mac OS X Enterprise Application Management: Best Practices"
- Utah University have a very helpful site: http: //www.macos.utah.edu/crappyApps.html
- Understand different types of Application install in OS X

Application Bundles

Many OS X apps are, more correctly, application *bundles* or *packages*. Actually, they're folders.

Bundle contents can be seen by control-click on app name, then selecting 'Show Package Contents'



.plist files (~/Library/Preferences)

 .plist files are XML files containing all User or Application preferences. Think of them as configuration files

User-defined .plist files in ~/Library/Preferences can be deleted or edited fairly safely. Check for syntax errors with sudo plutil -s ~/Library/Preferences/*.plist

can be read (e.g., defaults read -app Safari) or edited (e.g., defaults write com.apple.Safari IncludeDebugMenu 1) in terminal.app. See man defaults for more info.

Com.apple.print.defaultpapersize.plist

 $\Theta \Theta \Theta$

New Sibling Del	ete	Dump
Property List	Class	Value
▼Root	Dictionary	🗘 1 key/value pair
DefaultPaperSize	String	iso-a4
xml version="1.0" encoding="UTF-8"?"</th <th>></th> <th><u>^</u></th>	>	<u>^</u>
plist PUBLIC "-//Apple Comp<br <plist version="1.0"> <dict></dict></plist>	uter//DTD PLIST 1	1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<key>DefaultPaperSize</key> <string>iso-a4</string>		

.plist files (/Library/Preferences)

These will override preference files in ~/Library/ Preferences if the same

	📄 com.apple.sharing.firewall.plist			
New Sibling	Delete		Dump	0000000
Property List	Class	Value		- 8
▼ Root	Dictionary	3 key/value pairs		100
▶ allports	Array	1 ordered object		3
▼firewall	Dictionary	\$ 9 key/value pairs		
FTP Access	Dictionary	4 key/value pairs		
▶iChat Rendezvous	Dictionary	4 key/value pairs		
iTunes Music Sharing	Dictionary	4 key/value pairs		100
Personal File Sharing	Dictionary	4 key/value pairs		
Personal Web Sharing	Dictionary	4 key/value pairs		100
Printer Sharing	Dictionary	4 key/value pairs		
Remote Apple Events	Dictionary	4 key/value pairs		
Remote Login - SSH	Dictionary	4 key/value pairs		
editable	Number	\$ 0		
enable	Number	‡ 1		
▼ port	Array	1 ordered object		
0	String	\$ 22		
row	Number	\$ 3		
Samba Sharing	Dictionary	4 key/value pairs		
state	Boolean	Yes	\$	

Uninstalling

- In most cases, simply drag app to Trash
- .plist files may be left in ~/Library/Preferences but these are tiny and harmless and can be deleted or left
- Some apps are messier. DesInstaller is a big help (but use with caution). Download it from http://krugazor.free.fr/ software/desinstaller/DesInstaller.php (free)
 - DesInstaller reads the Package Receipts in /Library/ Receipts
 - The lsbom tool shows the same info (man lsbom)
- Management apps such as Radmind can do this too

DesInstaller

DesInstaller	
Package names	
Safari_1.2.pkg	
SecUpd2004-04-05Pan.pkg	
SecUpd2004-05-03Pan.pkg	
SecUpd2004-05-24Pan.pkg	
SecurityUpd2003-06-09.pkg	
SecurityUpd2003-07-14.pkg	
SecurityUpd2003-08-14.pkg	
SecurityUpd2004-01-26Pan.pkg	
SimplifiedChinese.pkg	
SoftwareRestore.pkg	
Snanish nko	▼
Overall progress	
/System/Library/OpenSSL/misc/c_name	
/System/Library/OpenSSL/misc/der_chop	
/System/Library/OpenSSL/openssl.cnt /System/Library/OpenSSL/private	
/private	
/private/etc	
/private/etc/cups /private/etc/cups/cupsd.conf	
/usr	
/usr/bin	
/usr/bin/c_rehash	
/usr/bin/xml2-config	

Tools

Carbon Copy Cloner
 FW Drive

2 - States States

Carbon Copy Cloner

Mike Bombich is highly respected in the Mac community Fantastic tool: use for backup and restore of clean installs Use for cloning and distributing known systems Clone volume before repartitioning drive Free for Education (otherwise donation ware)

http://www.bombich.com/software/ccc.html



FireWire

Two speeds: 400 and 800 Mbps

New drives have both + USB2

Cheap cables are frequent cause of problems - buy good ones

Always dismount drives cleanly before unplugging (%e)

Check devices in System Profiler

Section Contraction

Blue & White G3 Macs *cannot* boot from FireWire drives, most others can

Essential Software

Install CDs
Alsoft Disk Warrior
CCC (Carbon Copy Cloner)
TechTool Pro
Norton Utilities



Major OS X Disk Utilities



- DiskWarrior 3.0 (with CD updater)
 - http://www.alsoft.com/DiskWarrior/index.html



- FrechTool Pro v.4
 - http://www.micromat.com/



Norton Utilities 8.0

Section States

http://www.symantec.com/nu/nu_mac/index.html

Maintenance tools:



Onyx: http://www.titanium.free.fr/english/onyx/index.html



Xupport: http://www.computer-support.ch/Xupport/index.html





TinkerTool/TinkerTool Pro: http://www.bresink.com/osx/index.html



Cronnix: http://www.koch-schmidt.de/cronnix/

Also Rans: **Panther Cache Cleaner** (http://www.northernsoftworks.com/ panthercachecleaner.html) **MacJanitor** (http://personalpages.tds.net/~brian_hill/macjanitor.html)



2 . States and

Open Firmware



For Macs in a public area it's a good idea to password protect the Open Firmware. This prevents:

Startup from CD (c)

Startup from Network (n)

Startup in Target Disk Mode (t)

Startup in Single User (#s) or Verbose (#v) Mode

Blocks a PRAM reset (% \pr)

Access to Open Firmware (% \of) blocked without password

☐ Password required for Startup Manager (∖)

Anti-Virus Software

- You need it, even though there are still NO OS X viruses or worms (proof-of-concepts aside)
- Sophos client [update July 2004]
 - New 10.2+ client no longer requires mounted volume on desktop
 - New 10.2+ client updates automatically from CID
 - Can't be managed by Savadmin

States States

AFP-enabled sharepoint on Windows server necessary for EM Library