Client Management Fundamentals

MacWorld SF 2007 **Session IT851**



Who?

- Administrative staff?
- Faculty?
- V.I.P.'s?



What?

Applications?

System settings?

Look and feel?









System Preferences

Why?

- Efficiency?
- Lack of staff?
- Maximizing uptime?



Three types of managed environment

- Fully Managed (Kiosk)
 - Users have little or no control of their environment
 - Machine is always in a known state on reboot
- Mostly managed (Desktop/Laptop)
 - Users do not run as administrators
 - Users can control their environment
 - Machine is in a fairly known state
- Mostly unmanaged (Student laptop,
 - Users have full control of the box
 - Box is always in an unknown state

ment t

Options for great flexibility

(Without Workgroup Manager)

/etc/authorization

- Allows equivalent of "power-user"
- Rights can be granted/denied based on group
- Fine grained control of some administrative rights

riahte









Another example

<key>system.preferences</key> <dict> <key>allow-root</key> <true/> <key>class</key> <string>user</string> <key>comment</key> <string>This right is checked by the Admin framework when making changes to the system preferences.</string> <key>group</key> <string>admin</string> <key>shared</key> <false/> </dict>

Another example

<key>system.preferences</key> <dict> <key>allow-root</key> <true/> <key>class</key> <string>user</string> <key>comment</key> <string>This right is checked by the Admin framework when making changes to the system preferences.</string> <key>group</key> <string>admin</string> <key>shared</key> <false/> </dict>

File authorization

authopen provides authorization-based file opening services. In its simplest form, authopen verifies that it is allowed to open filename (using an appropriate sys.openfile.* authorization right) and then writes the file to stdout. If -w is specified, authopen will read from stdin and write to the file.

authopen is designed to be used both from the command line and programmatically. The -stdoutpipe flag allows a parent process to receive an open file descriptor pointing to the file in question.

Before opening filename, authopen will make an authorization request for a right of the form:

sys.openfile.[readonly|readwrite|readwritecreate]./fully/qualified/path. .readonly' rights only allow for read-only file descriptors.

`.readwrite' rights allow for read/write file descriptors.

`.readwritecreate' rights allow for read/write descriptors and the creation of new files.

Let's dig in!

Sudo!

Granularity in sudo: aliases

User_Alias	FULLTIMERS = millert, mikef, dowdy
User_Alias	PARTTIMERS = bostley, jwfox, crawl
User_Alias	WEBMASTERS = will, wendy, wim
Runas_Alias	OP = root, operator
Runas_Alias	DB = oracle, sybase
Host_Alias	<pre>SPARC = bigtime, eclipse, moet, anchor :\</pre>
	SGI = grolsch, dandelion, black :\
	ALPHA = widget, thalamus, foobar :\
	HPPA = boa, nag, python
Host_Alias	CUNETS = 128.138.0.0/255.255.0.0
Host_Alias	CSNETS = 128.138.243.0, 128.138.204.0/24, 128.138.242.0
Host_Alias	SERVERS = master, mail, www, ns
Host_Alias	CDROM = orion, perseus, hercules
Cmnd_Alias	<pre>DUMPS = /usr/bin/mt, /usr/sbin/dump, /usr/sbin/rdump,\</pre>
	/usr/sbin/restore, /usr/sbin/rrestore
Cmnd_Alias	KILL = /usr/bin/kill
Cmnd_Alias	PRINTING = /usr/sbin/lpc, /usr/bin/lprm
Cmnd_Alias	SHUTDOWN = /usr/sbin/shutdown
Cmnd_Alias	HALT = /usr/sbin/halt
Cmnd_Alias	REBOOT = /usr/sbin/reboot
Cmnd_Alias	SHELLS = /usr/bin/sh, /usr/bin/csh, /usr/bin/ksh, \
	/usr/local/bin/tcsh, /usr/bin/rsh, $\$
	/usr/local/bin/zsh
Cmnd Alias	SU = /usr/bin/su

Granularity in sudo: defaults

Defaults Defaults>root Defaults:FULLTIMERS Defaults:millert Defaults@SERVERS

syslog=auth !set_logname !lecture !authenticate log_year, logfile=/var/log/sudo.log

Examples:

operator	<pre>ALL = DUMPS, KILL, SHUTDOWN, HALT, REBOO sudoedit /etc/printcap, /usr/oper/bin/</pre>
joe	ALL = /usr/bin/su operator

pete		HPPA = /I	usr/bin/passwd	[A-z]*,	!/usr/bin
aaron	shanty =	= NOEXEC:	/usr/bin/more,	/usr/bi	n/vi

T, PRINTING,

/passwd root

Stock sudo on Macintosh OS X

ALL=(ALL) ALL root

%admin ALL=(ALL) ALL



Refining sudo permissions

root ALL=(ALL) ALL
singleuser ALL=(ALL) ALL

Managed Preferences



Three types of management

- Users
 - Applications, Dock, Login
- Groups
 - Same as Users
- Computers
 - Ability to manage Energy Saver is added
 - Login scripts are added as well
 - Ability to restrict machine to specific set of groups

How?

- Open Directory Server for authentication and management
- "Triangle" method
- Local management

Open Directory Server



00			Wo	rkgroup Man	ager: oban.its.y	yale.edu			
Admin Sharing	Network Accounts	Preferences	New User Delete	Connect Disc	Connect Refresh	New Window S	earch		
€ - Authenticate	ed as cracky to directo	ory: /LDAPv3/12	7.0.0.1						۲
0-1	1	₽ 0		Prefer	ences)	
Name						0	verview Details)	
J Directory	Administ 1000			Se	lect one or more i	tems from the lis	t and click on a prefere	nce below to	make changes.
					Application	ons	Classic		Dock
					4 Finder	(Internet		Login
					Media Ac	cess	Mobility	0	Network
					Printing	(Software Update	[s 🍏	System Preferences
					Universal	Access			
				C	Preference is be Preference is be	eing managed for eing managed for	r the selected items r some of the selected i	items	
0 of 1 user se	elected								

One example

😝 🖯 💮 Workgr	roup Manager: oban.its.yale.edu	\bigcirc
Admin Sharing Network Accounts Preferences	S S Connect Disconnect Refresh New Window Search	
↔ Authenticated as cracky to directory: /LDAPv3/127.0.0.1		۲
	Login Items Scripts Login Window Options	
Q	Manage: Never Once Always	
Name Image: Guest Computers Image: Windows Computers Image: All Computers Image: Test	Hide Item Kind Hide Item Kind Mount item with user's name and password Mount item with user's name and password Drag items to specify the order in which they open. To hide an application after login, click its Hide checkbox. Remove Add Add network home share point ✓ User may add and remove additional items ✓ User may press Shift to keep items from opening	
1 of 4 lists selected	✓ Merge with user's items (Mac OS X v10.4 and later) Done Revert	Now
1 of 4 lists selected		1

Access

\varTheta 🖯 💮 Workgro	oup Manager: oban.its.yale.edu	\odot					
Admin Sharing Network Accounts Preferences New Computer List Del	ete Connect Disconnect Refresh New Window Search						
↔ Authenticated as cracky to directory: /LDAPv3/127.0.0.1	+ Authenticated as cracky to directory: /LDAPv3/127.0.0.1						
 Authenticated as cracky to directory: /LDAPv3/127.0.0.1 All Computers All Computers Test 	List Access Cache Inspector All groups can use the computer Restrict to groups below Name ID -						
	Allow users with local-only accounts Local-only accounts pick workgroups from the above list (OS 10.4 clients and la Allow computer administrators to disable management (OS 10.4 clients and la	ter only) ter only)					
1 of 4 lists selected	Presets: None Revert S	ave					

Cache settings

\varTheta 🕘 🕘 Workgro	oup Manager: oban.its.yale.edu	\bigcirc				
Admin Sharing Network Accounts Preferences New Computer List Del	Ete Connect Disconnect Refresh New Window Search					
€ + Authenticated as cracky to directory: /LDAPv3/127.0.0.1	Authenticated as cracky to directory: /LDAPv3/127.0.0.1					
List Access Cache Inspector						
Q-	Update the preferences cache every 17 days					
Nume Image: Computers Image: Windows Computers Image: Computers Image: All Computers Image: Computers Image: Test Image: Computers Image: Computers Image: Computers Image: Computers	Update Cache					
1 of 4 lists selected	Presets: None Revert Sav	e				

The "Triangle"

Active Directory













Caveats

- Standard behavior is to have Active Directory first in Authentication path in Directory Services
- DNS resolution is important and can cause managed preferences oddities
- Need to remove or disable OD kerberos config to prevent conflicting authentication information
 - Alter Kerberos attribute
 - Remove kdc

Applying mcx locally



What?

- No need for OS X server
- Management is "point-in-time"
- User and group settings work, computer settings may not

How?

Connect Connect Recent	жк ▶
Disconnect	•
New Workgroup Manager Window	ЖN
New Computer List Delete Selected Computer List	Ω₩Ν
View Directories	ЖD
Close Window	жw
Import Export	



This is not a server directory node.

Some functionality may not work.

Do not show this warning again



😝 🖯 😁 Workgroup M	lanager: Local 🔘
Admin Sharing Network Accounts Preferences	nnect Refresh New Window Search
€ - Authenticated as pr26 to local directory: /NetInfo/DefaultLocalNode	۲
	Dock Items Dock Display
Q N	anage: ONever Once ONevays
Name ID Demo Group 1025 Idap 1026 mbp 502 nagios 503 pr26 501 zimbra 504	Dock Size: Small Magnification: Min Min Max Position on screen: Image: Cenie Image: Cenie <
1 of 6 groups selected	

Preference management



Light touch

Energy Saver

Manage:	OS: Mac OS X Never Settings apply to Mac	Once OS X v10.2.4 and late	⊙ Alwa r.	ays
Manage:	Never Settings apply to Mac	Once OS X v10.2.4 and late	● Alwa r.	ays
Custom Minim Energy	Settings apply to Mac	OS X v10.2.4 and late	r.	
Custom Minim Energy	ı	I.		
Custom Minin Energy	num			1
5	Usage			Maximum Performance
	Settings: Sleep	•		
Put the compute	r to sleep when it is i	inactive for:		
_				_
1 m	in 15 min	1 hr	3 hrs	Never
🗹 Put the disp	lay to sleep when th	e computer is inac	tive for:	
_				_
1 m	in 15 min	1 hr	3 hrs	Never
🗹 Put the hard	disk(s) to sleep whe	en possible		
Done			Revert	Apply



System Preferences





Loginwindow

Login I	tems Scripts	Login Window	Options			
Manage:	O Never	Once	💽 Always			
🗌 Login Window	message:					
Display Login Wi	ndow as: ONar	ne and nassword t	ext fields			
Display Login Wi	List	of users able to u	se these computers			
	2	Show local users				
Show network users						
	✓ 9	Show computer's a	dministrators			
	N	show other users				
🗹 Show Restart I	button in the Lo	gin Window				
🗹 Show Shut Do	wn button in the	Login Window				
Show passwor	d hint after 3 at	tempts to enter a p	assword			
🗹 Enable Auto L						
	ogin Client Setti	ng				



Software updates

Manage:	💽 Never	⊖ Once	Always
Software Update serv	ver to use:		
Specify a URL	of the form: http://s	omeserver.apple.com	1:8088/



Middle ground

Printers

Manage: 💽	Never	Once	Always
(Printer List	Access	
Available Printers	_	User's Pr	inter List
hp color LaserJet 5550 [HP LaserJet 1200 ir3300	Add to I Remov	_ist /e	
Open Print ✓ Allow user ✓ Allow prin	r to modify the ters that conne	rch for additional p printer list ect directly to us	rinters. er's computer
Require	e an administra	tor password	





Application management

•	User can only o	open these application	ons
Õ	User can open	all applications exce	ept these
Item		Kind	
Activity Monitor		Application	le la
📔 Address Book		Application	4
adium 👌		Application	
🕐 Adobe Help Cent	er	Application	
🛃 Adobe Reader Do	ownload Manager	Application	
🏷 Adobe Updater		Application	
AirPort Admin Ut	ility	Application	
🔣 AirPort Setup As:	sistant	Application	
🔕 Aperture		Application	2
🖼 Apple Loops Util	ity	Application	
	Remove	Add	
	open all applic	ations on local volue	mos



Manifest inspector

Preferenc	:es				
		Overvie	w Details		
Se	lect an item fro e the Add butto	m the list and cl on to add items r	ick on Edit b not in the lis	pelow to make o st.	changes or
	Name	*	Preference ID		
C	Add			Remove	Edit
Clie	ck "Add" to selec	t an application or	a preferences	document.	



An example

	com.apple.Quick1	lime
New Key Delete)	Set Default Del
Name	Type Value	
▼ Once	dictionary empty	
▼ Often	dictionary 1 item	
▶ Pro Key	dictionary 🗘 3 items	
▼Always	dictionary empty	
	^	
Done		Revert



Possible candidates

com.apple.desktop.plist

com.apple.iWork.plist

com.apple.screensaver.*

Type dictionary dictionary string dictionary	Value empty 1 item /System/Library/Scree empty	Set Default Delete Unmatched
Type dictionary dictionary string dictionary	Value empty 1 item /System/Library/Scree empty	en Savers/Flurry.saver
dictionary dictionary string dictionary	empty 1 item /System/Library/Scree empty	en Savers/Flurry.saver
dictionary string dictionary	1 item /System/Library/Scree empty	en Savers/Flurry.saver
string dictionary	/System/Library/Scree empty	en Savers/Flurry.saver
dictionary	empty	
	^	
		Revert Apply Now
		Cherent Chepping How

Login scripts

\varTheta \varTheta 🕙 Workgroup	Manager: oban.its.yale.edu	0
Admin Sharing Network Accounts Preferences New Computer List Delete	Connect Disconnect Refresh New Window Search	
↔ Authenticated as cracky to directory: /LDAPv3/127.0.0.1		۲
	Login Items Scripts Login Window Options	
Q- Name contains	Manage: Never Once Always	
Name Image: Computers	Settings apply to Mac OS X v10.4 and later.	
 All Computers Test 	□ Login Script: Select ✓ Also execute the client computer's LoginHook script	
	□ Log-Out Script: Select ✓ Also execute the client computer's LogoutHook script	
	 Selected scripts will execute only if (1) The preference "EnableMCXLoginScripts" is set to true in the root user's com.apple.loginwindow defaults domain on the client computer. (2) The client computer binds to its directory service using trusted directory binding. Please see the OSX Server Guide for more information. 	
1 of 4 lists selected	Done Revert Apply I	low)

Possible login items to script?

- Microsoft Word settings?
- Printers?
- Dock specific settings?
- IMPORTANT: Must set key on client workstation

Network Directories

a.k.a. Portable Home Directories



Advantages

- Preferences are consistent across multiple machines
 - Language settings
 - Printers
 - System Preferences
- Central backup of user data can be done at the server level
- Machines become expendable (labs, offices)



Disadvantages

- Some applications are not 'network-friendly' – Office, Adobe CS Suite, etc.
- Disk intensive applications will not perform well - iMovie, Final Cut Pro, et al.
- Requires a fairly robust hardware/network combination
- No quota reporting

Troubleshooting



MCX diagram



MCXCacher

/System/Library/CoreServices/mcxd.app/Contents/Resources/MCXCacher

MCXCacher -U usershortname [-h homepath] Creates (or overwrites an existing) mobile account on the current machine for user "usershortname" with optional home path "homepath"

MCXCacher Performs the pre-login checks and refreshes cache if required.

MCXCacher -u usershortname Performs the post login checks and refreshes caches -- does everything that "MCXCacher" does plus caches the current user's mcx_settings

MCXCacher -f Flushes the cache (Mobile accounts not removed; but system is unmanaged)

MCXCacher -d Dirties the cache so that it will be refreshes at the next login ("MCXCacher" call by mcxd)

MCXCacher -f will put the machine into an unmanaged state until the next time it reconnects to the management server, so it's a rather drastic thing to do. From memory, if you run this command, Mobile Users won't be able to login at the loginwindow unless the machine can connect to the management server at that time.

MCXCacher -d does the right thing in the vast majority of cases, and as John DeTroye just pointed out to me, runs at login/logout and restart.

Compositor.plist

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!DOCTYPE plist SYSTEM "file://localhost/System/Library/DTDs/</pre>
PropertyList.dtd">
```

```
<plist version="0.9">
```

<dict>

<key>PreLoginAllowBundles</key>

<array>

<string>com.apple.loginwindow</string>

<string>com.apple.MCX</string>

<string>com.apple.mcxloginscripts</string>

<string>com.apple.SoftwareUpdate</string>

</array>

</dict>

</plist>

CinchDefaults.plist

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://</pre>
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>excludedAlways</key>
   <array>
     <dict>
       <key>comparison</key>
       <string>fullPath</string>
       <key>value</key>
       <string>~/Library/Mirrors</string>
     </dict>
```

Debugging

- Two caches
 - computer
 - user
- Turning on debugging
 - defaults write /Library/Preferences/com.apple.MCXDebug debugOutput 3

Real World:

Ventura County Star





Before:

- Mac OS 9
- MacAdministrator
 - User folder of files preserved and copied
 - No preferences copied
 - All control panels locked
- AppleShare IP 6.3
- Windows NT 4.0 (some 2000)



After:

- Mac OS X
- AD-OD Integration (golden triangle)
- Mobile accounts with portable home directories
 - Entire user environment preserved and moved
 - But with exceptions (cache, etc.)
 - Limited access to system preferences
- XServe G5 Open Directory Master
- Bound to AD for authentication

es /ed



What Happened:

- First time system was loaded:
 - 15-20 minute boot times
 - Random syncing errors:
 - "Your AFP home cannot be synchronized right now because it is on an SMB or AFP home." Pardon?
- Additional load placed on system:
 - Network failed (lesson: make sure your infrastructure is sound, ahead of time)





?artnum=300765



Lessons Learned

- Take your time
- Don't lose your notes
- ARD is your friend
- Scour the Library for cache files to exclude

0	0		_		Workgr	oup Manager: vcxse	rve01.ad.ewsad.net	\odot
Admin	救 Sharing	Network A	Accounts	Preferences	+ New Gre	oup Delete Connect	Disconnect Refresh New Window Search	
⊗ + Auth	enticated	as dispatch	n1 to dire	ctory: /LDAPv3,	127.0.0.1			۲
		1 2	D 0				Synchronization Rules	
Q-Na	ame cont	ains				Login &	Logout Sync Background Sync Options	
Na 1	me	A	ID 1025		Ξľ	Manage:	Once Olways	
						Settings a	oply to mobile accounts on Mac OS X v10.4 and later.	
						Synchronize at log	in and logout:	
						Folder	+	
						~		
							_	
						Skip items that ma	atch any of the following:	
						Match	String, file, or folder	
						Full Path	¢∼/.Trash	
						Full Path	🕈 ~/Library/Caches/ 🔰 🗕	
						Full Path	* ~/Library/Application Support/Adobe/Bridge/	
						Full Path	* ~/Library/Application Support/Photo Mechanic 🐺 🛄	
						Merge with use	r's settings	
						Ends with	 Ippi Ibrary/Preferences/PyHost 	J
						Full Path	 ~/Library/Preferences/Dynost ~/Library/Preferences/Mirrors 	
						Full Path	 A logation 	
						Name contains	, ipopulon	
						Name contains	• .istemp	
					(Done	(Revert) (Apply N	(wol
1 of 1	aroup se	lected						/



To do:

- Manage Network views - What it looks like now
- Creating a view in WGM

● ● ●	Workgroup Manager: vcxserve01.ad.ewsad.net	\bigcirc
Admin Sharing Network	eferences New Network View Delete Connect Disconnect Refresh New Window Search	
↔ Authenticated as dispatch1 to directo	ry: /LDAPv3/127.0.0.1	
Network Views		
VCS View	Name: VCS View Enabled	
	Layout Settings	
	Clients:	
	Computer Name Address	+
	Oc:0d:93:42:b7:76	
		-
		/
	Clients check for changes every 10 hours	
	Client Finder will: O add to Network view	
	replace Network view	
	Teplace Network view	
	(2) (Revert) (Sav	



 $\Theta \Theta \Theta$

4.1

iDisk

Utilities

 \sim

0



To do:

- Migrate OD Master to Intel XServe
- Move!



