X World 2011

Managing and Hardening Snow Leopard:
Policies for Use in Education

Doug Brown
Redlands College

Overview

- Standard Operating Environment

  - Configuration Settings

  - Restrictions

- Deployment Issues

  - Adobe Suite

  - Logic and Final Cut Studio

AUC

XWII

Overview

- This workshop will be interactive and hands-on

- These slides should be used as reference materials

- For each topic, we will examine the code and see how it is applied

SOE Configuration Settings

Minor Settings

- Turn on SSHd

  - systemsetup -setremotelogin on

- Change umask

  - echo "umask 077" >> /private/etc/launchd-user.conf

- Enable Fast User Switching

  - defaults write /Library/Preferences/.GlobalPreferences MultipleSessionEnabled -bool 'YES'

Login Window Acceptable Use Policy

- defaults write /Library/Preferences/com.apple.loginwindow LoginwindowText "This machine is the property of REDLANDS COLLEGE, provided for educational purposes. Students may be requested to demonstrate a school-related activity for which they are using ICT resources to complete. Illegal, immoral, unethical, nuisance harmful or activities which contravene the College ethos are strictly forbidden. Users must report any physical problems of ICT equipment to a teacher and/or the IT Department as soon as it is noticed. Care must be taken when using or carrying a laptop. Movement of the machine should be kept to a minimum. For ICT related enquires, please call Help Desk on x555."

Login Window Background

- Create an organisational background picture

- Make a package to install your image to

    - /System/Library/CoreServices/ DefaultDesktop.jpg

- Be sure to check your image is the same pixel ratio as the original

AUC

XWII

Certificate Authority Distribution

- security add-trusted-cert -d -k /Library/Keychains/System.keychain /path/to/CA.der

- I have removed the "-p eap" flag between the '-d' and '-k /Lib…' flags because this way the certificate will be trusted for everything; rather than just eap authentication

- "-d trustAsRoot" is recommended after the '-d' flag, but it doesn't work for some reason

AUC

XWII

Apple Remote Desktop Settings

- /System/Library/CoreServices/RemoteManagement/ARDAgent.app/
  Contents/Resources/kickstart -activate -restart -agent -console

- /System/Library/CoreServices/RemoteManagement/ARDAgent.app/
  Contents/Resources/kickstart -configure -users administrator -access -
  on -privs -DeleteFiles -ControlObserve -TextMessages -
  OpenQuitApps -GenerateReports -RestartShutDown -SendFiles -
  ChangeSettings

- /System/Library/CoreServices/RemoteManagement/ARDAgent.app/
  Contents/Resources/kickstart -configure -allowAccessFor -
  specifiedUsers

AUC

XWII

System Proxy Settings

- Proxy must be set individually for each service, ie. Ethernet, AirPort, etc.

- Currently no API for proxy auto detect

- However pac file can be set using:

  - networksetup -setautoproxyurl servicename http://yourserver/your.pac

AUC

XWII

Custom LDAP Mappings

- If your organisation doesn't use OD or AD, you will probably have difficulties programmatically setting custom LDAP mappings

- This requires a bit of a hack, let's see it now...

Setting Users' Locale

- Use Apple's Login hook to execute:

  - su $1 -c 'defaults write "Apple Global Domain" AppleLocale "en_AU"'

  - Let's see this in action…

AUC

XWII

Standard Dock Items

- Use Apple's Login hook to execute:

  - cp /path/to/dock/default.plist /Users/$1/Library/Preferences/com.apple.dock.plist

  - killall -u $1 Dock

- Let's see this in action...

AUC

XWII

Password Change Distribution

- Some organisations have a static administrator account on all machines

- How can you distribute a change of password for this account in a more practical way than using ARD?

  - Let's see that now...

Roaming Apple Update URL

- This policy I use on startup and wake of client machines

- If the machine cannot contact the internal update server then it changes the Apple Update URL back to Apple

- Let's see this in action...

AUC

XWII

SOE Restrictions

noexec

- noexec is from UNIX

- It allows a file system to be mounted without the ability to execute binaries

- The noexec policy mounts all foreign file systems noexec

- Let's see the code...

System Preference Pane Lock

- Requires a password to unlock each System Preference pane

- security authorizationdb write system.preferences < /path/to/plist

- Let's see the plist file...

AUC

XWII

Deployment Issues

Adobe Suite

- Enterprise deployment difficulties

  - Size of package produced is huge

  - Installation process is very slow

    - Package duplicates built-in functionality of Apple packages with black-box binaries

Adobe Suite

- Enterprise deployment difficulties

  - Repackaging is very difficult as capture tools are unable to handle software suites of this size and complexity

AUC

XWII

Adobe Suite

- Enterprise deployment solution

  - logGen and pkgGen can capture and produce a fauxroot clone of installed components

  - Your favourite package making utility (like Iceburg) can then be used to produce the packages

Adobe Suite

- Enterprise deployment solution

  - Repackaging Adobe Suite results in:

    - Significantly smaller packages

    - Packages which install over network on average in 30 seconds

    - Individual components can be associated and installed with machines as required

AUC

XWII

Logic and Final Cut

- Each of the studio suites are 9 DVDs and approximately a 50GB install

- Installation typically takes hours

- Difficult to deploy in organisations with site licenses

AUC

XWII

Logic and Final Cut

- Deployment options

  - Producing a DMG image of each DVD and installing it from a firewire HDD OR

  - Combining the packages from all the DVDs into the first disk's metapackage on a firewire HDD

AUC

XWII

Logic and Final Cut

- How to produce a single meta package

  1. Copy LogicStudio.mpkg from first DVD to firewire HDD

  2. Copy all [meta]packages from install DVDs to LogicStudio.mpkg/Packages

  3. Modify meta package's .dist file

AUC

XWII

Logic and Final Cut

- Structure and modification of .dist file

  - <choice>

    - <pkg-ref>

      - Change all "x-disc://diskname/Installer/Packages/packagename.pkg" to "file:./Contents/Packages/packagename.pkg"

AUC

XWII

Logic and Final Cut

- How to automate .dist file modification

  - sed -i .original -e 'sl">x-disc:\/\/.*\/ Installer\/Packages\/l">file:\.\/Contents \/Packages\/l' -e 'sl">x-disc:\/\/.*\/ Installer\/l">file:\.\/Contents\/Packages \/l' -e 'sl">file:\.\.\/Packages\/l">file:\.\/ Contents\/Packages\/l' LogicStudio.dist

AUC

XWII

Questions?