Post Image Automation

MacWorld SF 2009
Session IT863

Presentation Logistics

Post Image Automation

- Q&A managed with Google Moderator
  - http://tinyurl.com/633v6e
  - Sign in using your personal Google account
  - Find session matching IT863
  - Submit or vote on questions for this session
- Download PDF of this presentation
  - Join Wireless MW09_PRESENTATION_DOWNLOAD
  - Open web browser for automatic redirect

About the Presenters

Who are these guys?

- Dave Pooser

  Alford Media Services:
  Manager of Information Services

- Kevin M. White

  Owner: Macjutsu, Inc.

  Author:
  Apple Certified Training - Mac OS X Support Essentials
  Apple Certified Training - Mac OS X Deployment

Agenda
Post Image Automation

- What Needs to be Unique?

- System Configuration

- Directory Service Configuration

- Automating Your Configuration

- Examples! Examples! Examples!

- Suggested Tools

What Needs to be Unique?

Every Mac is special in its own way

What Needs to be Unique?

Every Mac is special in its own way

- System configuration for many network settings, even with DHCP

- Any setting that touches the firmware

- Any authenticated directory service needs to run from each computer

- Mac OS X 10.5 LKDC may need to be reset for proper authenticated binding

- Any unmanaged user specific settings

About This Session

Post Image Automation

- This session isn't about GUI tools...

- ... it's about the technology beneath those GUIs that actually does the work

- This session covers:

  - The UNIX configuration tools beneath the GUI

  - The automation technology in Mac OS X

  - Example first run script ideas

Learn to Script!

Real administrators script their own solutions

- Most command line tools are easily automated in a shell script

- Simply create a text file:

  - Give it a useful name: *myscript.sh*

  - Make the first line: `#!/usr/bin/env bash`

  - Enter the commands you want separated by full returns

  - Make it executable: `$ chmod u+x `*myscript.sh*

  - Secure the script: `$ chown root:wheel `*myscript.sh*

  - Run the script: `$ sudo ./`*myscript.sh*

System Configuration

Name your baby... Mac

System Configuration Tools

Make your Mac unique

- General settings: `$ systemsetup`
  - Date and time
  - Power management
  - Enable remote login
- Network settings: `$ networksetup`
  - Any network setting found in Network Preference
  - Computer name
  - AirPort settings as well

System Configuration Tools

Make your Mac unique

- Power management: `$ pmset`
  - Advanced sleep settings
  - Power management scheduling
  - UPS (battery backup) configuration
- ARD configuration: `$ /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart`
- Printer configuration: `$ lpadmin`

Set Firmware Password

- No built-in command for enabling and setting the firmware password

- OFPW from MacEnterprise.org:

  - Free downloadable binary

  - Works on PPC & Intel / Mac OS X 10.4 & 10.5

  - `$ sudo OFPW -pass `*`cleartextpassword`*

  - `$ sudo OFPW -mode 1`

Directory Service Configuration

Directory services is kind of a big deal

Fix the Local KDC

Every Mac hosts its own Kerberos!?!

- Yes... in Mac OS X 10.5 every Mac hosts its own local Kerberos KDC (aka LKDC)

- Provides secure authentication for ad-hoc file and screen sharing

- Provides unique identifier for trusted LDAP

- Cloned system images will have problems

- Apple kbase: #TS1245

Fix the Local KDC

Every Mac hosts its own Kerberos!?!

- On your system image delete the KDC pair in the System keychain

  - No useful command line tool for this... grrrrr!

  - Use Keychain Access before you clone system

- `$ sudo rm -fr /var/db/krb5kdc`

- `$ sudo /usr/libexec/configureLocalKDC`

- Note: This will delete any existing user's principal entry in the LKDC! Use tool of choice and reset the users password to fix.

Bind to a Directory Server

Post Image Automation

- Trusted LDAP and AD require each client Mac bind to the service

- This process is several steps

  - Enable the LDAPv3 or AD plug-in: `$ defaults`

  - Bind to directory server using
    `$ dsconfigldap` or `$ dsconfigad`

  - Add the server to the DS search path: `$ dscl`

  - Configure Kerberos: `$ kerberosautoconfig`

Automating Your Configuration

Let the computer work for you

Launchd Runs Everything

One process to rule them all

- Legacy but still supported: /etc/rc.local

- Better form is to create your own launchd configuration file (.plist)

  - Place in /Library/LaunchDaemons

  - Only a few required keys in the configuration file:
    Label, ProgramArguments, and KeepAlive

  - To run at first boot use RunAtLoad key

- To disable the launchd item after first run:
  ```
  $ sudo launchctl unload -w pathtoscript
  ```

Login/Logout Hooks for Users

A little automation for the users

- Scripts that run when any user logs in or out

- Executed by the loginwindow process

- User's shortname passed to script as variable $1

- Best practice is to use MCX to enable hooks

- Locally you can simply configure loginwindow:

  - `$ sudo defaults write com.apple.loginwindow LoginHook ` *`pathtoscript`*

  - `$ sudo defaults write com.apple.loginwindow LogoutHook ` *`pathtoscript`*

Suggested Tools

To make life a bit easier

Suggested Tools

Post Image Automation

- Apple Training Series books!

- Automation Freeware:

  - PSU Blast Image Config

  - http://www.bombich.com

  - http://www.macenterprise.org

- Lingon for managing launchd

Presentation Logistics

Post Image Automation

- Q&A managed with Google Moderator
  - http://tinyurl.com/633v6e
  - Sign in using your personal Google account
  - Find session matching IT863
  - Submit or vote on questions for this session
- Download PDF of this presentation
  - Join Wireless MW09_PRESENTATION_DOWNLOAD
  - Open web browser for automatic redirect

Post Image Automation

MacWorld SF 2009
Session IT863