Using NetRestore to Deploy OS X Labs

- or -

A Unix Curmudgeon tries to keep some Macs in line

Thomas L. Kula
Iowa State University
Information Technology Services
Introduction

• How Macs netboot
• Using that to run NetRestore
• Automating/Provisioning NetRestore
• Tricks to managing systems
• Pitfalls and things to watch for
The Most Important Advice

• Read www.bombich.com
• Memorize it
How Macs netboot

• Send out a BSDP packet
• Get a reply that tells it
  – where to find a boot loader
  – which kernel to load
  – which options to pass the kernel
How Macs netboot

- Firmware loads the boot loader using tftp
- Boot loader loads the kernel using either nfs or (10.4 or later) http
- Kernel uses passed options to mount a disk image either via nfs or afp and uses that as its system partition
BSDP Problems

• BSDP is a protocol akin to DHCP
  – In fact, it is simply DHCP that asks for some extra client options

• Works only within a broadcast domain
  – Unless a helper passes the packet on to the BSDP server
  – On campus, those helpers pass it on to the campus DHCP servers
BSDP Workarounds

• You can supply the information directly
• On Intel Macs:

```bash
bless --netboot --booter
    tftp://ser.ver.ip.addr/NetBoot/NetBootSP0/NetInstallImageName.nbi/i386/booter
--kernel
    tftp://ser.ver.ip.addr/NetBoot/NetBootSP0/NetInstallImageName.nbi/i386/mach.macosx
--options
    "rp=nfs:ser.ver.ip.addr:/private/tftpboot/NetBoot/NetBootSP0:NetInstallImageName.nbi/NetInstall-Restore-Image.dmg"
```
BSDP Workarounds

• On PPC macs:

```bash
nvram boot-device =
enet:ser.ver.ip.addr,NetBoot\NetBootSP0\NetInstallImageName.nbi\booter
```

```bash
nvram boot-file =
enet:ser.ver.ip.addr,NetBoot\NetBootSP0\NetInstallImageName.nvi\mach.macosx
```

```bash
nvram boot-args =
 rp=nfs:ser.ver.ip.addr:/private/tftpboot/NetBoot/NetBootSP0:NetInstallImageName.nbi/NetInstall-Restore-Image.dmg
```

• Phew
Using NetRestore to Deploy OS X Labs

BSDP Workarounds

• Fortunately, if you use some of the hints later, sending these commands to a whole lab of machines is trivial

• If your OS X server is on the same local network as your machines, you simply need to tell the Macs to NetBoot

• It is safe to run a BSDP server *IF* you also do not run the DHCP service on the campus network
We've NetBooted, Now What?

- You could, if you were so inclined, run the machines entirely NetBooted.
- You can run an installer image
NetRestore

• NetRestore allows you to restore an image to a drive
  – The image can supplied via NFS, AFP, a locally mounted disk, or via multicast
  – It is built on top of Apple System Restore

• NetRestore Helper helps you create disk images
  – It can create the actual image you apply to the machines
  – It will also create a bootable installer image
NetRestore

• You could, if you were so inclined, shuffle around with a firewire drive, touching each machine and using NetRestore individually

• Combined with NetBooting, NetRestore has some hooks in it that allow you to do fairly comprehensive automation
NetRestore Automation Outline

- NetBoot a NetRestore installer image
- NetRestore is configured to pull its configuration from a webserver
- Pre- and post-install scripts also pull from a webserver
Web NetRestore Configuration

- NetRestore can be configured to send a query to a web server to get returned a plist that tells it where to find the restore image and how to apply it.
- Supplied script uses PHP and a MySQL database.
- I threw together one that uses Python and flat text files.
- The query supplies the hardware address of the first ethernet interface on the system.
Using NetRestore to Deploy OS X Labs

Pre- and post-scripts

• NetRestore looks in a couple well-defined locations for pre- and post-scripts
• Can be written in shell or perl
• Pre: partitioning and formatting of drives
• Post: installation of after-the-fact packages
• My pre- and post-scripts borrow the NetRestore configuration model, and query a webpage with the hardware address to get per-machine pre- and post-scripts
Image Source

• NetRestore can pull an image from a locally mounted disk, via NFS or AFP, or from an Apple System Restore multicast stream

• The first three options are useful for one-off restores

• Multicast is useful for an entire lab of images
  – Requires a well functioning network
  – Requires coordinating with ITS Netcomm
Post-install Management

• ssh with keys
  – Create a local administrative user
  – Drop in one or more ssh public keys
  – Use ssh with those keys to remotely run commands

• Passwordless sudo
  – Allow the local administrative user to run commands via sudo with no password
  – Security considerations
Post-Install Management

• Apple Remote Desktop
• Has shortcomings
• Still fairly useful
• At the very least, set up VNC to operate over an ssh tunnel so you can help users remotely
Post-Install Management

• All of my local customization (startup scripts, nightly cleanup, login/out hooks) are in a management package
• Apple PackageMaker
• There are other ways of doing this as well
Caveats

- or -

Things that will fill you with the rage of a thousand burning suns
launchd undeterminability

- Launchd allows you to schedule recurring events
- pmset allows you to configure a machine to wake up or power on at a certain time
- Launchd stops counting time whenever the machine is asleep
- If your machine has slept for, say, two hours that day, your launchd events happen two hours after they are supposed to
Apple Remote Desktop Problems

• ARD uses ssh for all of its actions
• If the user ARD uses to connect also has a ssh key set up, ARD doesn't know how to handle that
• Have to create another user without a shared ssh key pair
Apple Remote Desktop Problems

• One Thing At A Time
• If ARD is doing something to a group of machines that is all it does
• Can not say “copy this file, then run this script, then ....” --- no grouping of actions
Stupid Applications

- Non-scriptable installers
- Applications that require per-install license keys
  - “You want to install this on 28 machines? You must touch each of the 28 machines.”
Conclusions

• NetRestore, combined with some additional glue, provides a scalable way to deploy groups of OS X machines

• Tools like ssh and sudo allow for easy remote management of machines, in an automatable fashion

• Various bits of this pie still suck, and serious work need to be done to make OS X deployment not be stuck in the “one machine, one user” frame of mind
Conclusions

• Read www.bombich.com
• Memorize it
Using NetRestore to Deploy OS X Labs

- or -

A Unix Curmudgeon tries to keep some Macs in line

Thomas L. Kula

Iowa State University

Information Technology Services