

Leveraging Open Source & Freely Available Software to Streamline Operations and Lower Operational Costs

Joseph J. Viscomi
Brehm Preparatory School

Areas of focus

- Inventory
- Imaging & LDAP
- Service configuration
- Software Installation and Distribution
- System Updates
- Server Configuration Changes & Tracking / Blame
- E-Mail
- Firewall / Content filtering / Bandwidth / Virus Scanning / LDAP ...

Inventory

- Starts the deployment process, should be done when the computer is received.
 - Computer model
 - Serial
 - Wired & wireless MAC address
 - Organizational inventory tag
 - Computer is added to DNS
 - This is automated because we have a standard way of assigning hostnames based off of serial number of the machines.
- **OCS Inventory** - <http://www.ocsinventory-ng.org/en/>
 - OpenSource
 - Automated discovery and resource monitoring
 - Web based interface

Imaging



Imaging

- **DeployStudio** (<http://www.deploystudio.com>)
 - OpenSource
 - Network based Imaging & deployment for **Macintosh** and **PCs**
 - Advanced computer reconfiguration
 - Fully automated
 - Lets operators define custom workflows
 - Scripting integration
- **InstaDMG** (<http://code.google.com/p/instadmig/>)
 - Creates clean, never booted ASR images for deploying OS X.



Imaging (cont)

- Imaging Guidelines
 - Goal is to push out a small standardized image as fast as possible.
 - Base image should only include the base Operating System that is fully patched at the time of the image creation, * we disable mDNS on client machines.
 - Image should also contain all of the most stable drivers this system will need at the time of image creation.
 - * We include Munki, Puppet, Chrome & Sophos Antivirus on our base image. Chrome is set to auto update on the stable branch.
 - * We run Monolingual before image creation to remove unnecessary files.
 - Test, test, test ... and test an image before it is used in production.
 - * We create a new base image for each major computer system we use, and update them every 6 months.



Imaging (cont)

- Post image configuration by **DeployStudio**
 - **DeployStudio** fetches the configuration for each inventoried machine.
 - **DeployStudio** sets the machine's hostname, IP address, location name.
 - **DeployStudio** binds the computer to appropriate domain and places the computer in the appropriate group in LDAP.
- Machine reboots ...

- Inventory
- Imaging

Questions ?

System Updates

- **Reposado** - (<https://github.com/wdas/reposado>)
 - OpenSource version of Apple's Software Update Server, doesn't have the headaches SUS.
 - You can host this services on any hardware / os of your choice, you are not forced to use OS X Server (* **We use virtualized Gentoo servers to handle our updates**).
 - Easily implement an unstable / testing / release workflow for Apple software updates.
 - Allows you to continue to offer "deprecated" updates, this is not possible with Apples update server.
 - * We use **Munki** to distribute them, NOT the Apple Software Update program, but this is not a requirement.

Service Configuration Software Distribution

An army of puppets

- Puppet - (<http://puppetlabs.com>)
 - Declarative language allows for easy reproduction of configurations, even in a heterogeneous environment.
 - Simulates and tests changes without disruption to your infrastructure.
 - Automatically enforces your desired system state, correcting any drift.
- Node level
 - Puppet allows you to compose and define your configurations as modules using simple human language.
 - You can schedule deployments inside Puppet or, with Puppet's **MCollective**, deploy to any node.
 - You can re-use configurations across multiple nodes.
 - Puppet has the ability to install pkg or mpkg packages, and keeps track of them.
 - After imaging Puppet automatically does all the system configurations and service setups on both clients and servers.



Even a Munki can do it

- **Munki** - (<http://code.google.com/p/munki/>)
 - Is a set of tools that, used together with a web server-based repository of packages and metadata, can be used by OS X administrators to manage software installs and removals on OS X machines. (WPKG is similar for windows based environments: <http://wpkg.org/>)
 - Manifests can easily be controlled by LDAP computer group membership, automating the software that goes out to different client types.
 - **Simian** - (<http://code.google.com/p/simian/>) Project offshoot by google for very large deployments.
- **MunkiReport** - (<http://code.google.com/p/munkireport/>)
 - Gathers reports from clients, quickly showing you errors and current activity, and lets you view detailed reports on individual clients.

- Inventory
- Imaging

- Software Updates
- System Configuration
- Software Distribution

Questions ?

Change Management

- Dealing with managing changes in configurations on servers.
- How do you know when something broke due to a configuration change, who made the change, and what what the configuration before the change was made?
- **Subversion** provides a simple transparent solution to this problem.
 - Originally designed for code development.
 - <http://subversion.apache.org/>
 - <http://svnbook.red-bean.com/en/1.7/svn-book.pdf>
- All server configuration files are checked into a subversion repository, each server has it's own.
- Allows you to track when the change was made what it was before the change and who changed it. Offers a very good audit log!
- Can rollback to any previous state with one command.
- Works with Linux, OS X, Unix, and Microsoft operating systems.
- Provides remote storage of a server's configuration files in case of data loss or corruption.

E-Mail

Google Apps for ED

- Google Apps for Education - (<http://www.google.com/apps/intl/en/edu/>)
 - Free!
 - 25 GB of storage for each users account.
 - Hosted remotely, less to manage.
 - Easy integration for Single Sign-on in an LDAP (OpenLDAP,AD, OD) environment.
 - Has all the major features you would expect for an enterprise level e-mail system.
 - Focus IT energy on activities that add value instead of worrying about e-mail uptime.
 - No software to install, no hardware to buy.

GAPPS Integration

- Simple integration with OpenDirectory can be done using [googlePasswordSync](https://github.com/jjviscomi/googlePasswordSync) - (<https://github.com/jjviscomi/googlePasswordSync>).
- Complex integration with OpenDirectory can be done using both of [googlePasswordSync](#) and [Google Apps Directory Sync](#) (GADS - <http://www.google.com/support/a/bin/answer.py?answer=106368>) tools together.
- Simple or complex integration with OpenLDAP or Active Directory can be done with just using [Google Apps Directory Sync](#).
- Very large deployments also have the option to use SAML Single Sign-On for Google Apps.
 - This actually eliminates the need to login to integrated services.
 - This is realtime compared to a syncing schedule.
 - Most complicated to get working.

- Inventory
- Imaging

- Software Updates
- System Configuration
- Software Distribution

- Change Management
- Email

Questions ?

Firewall / Content Filtering

Firewall

- **NETFILTER/IPTABLES** - (<http://www.netfilter.org/>)
 - Stateless & stateful packet filtering
 - Network address and port translations
 - Packet manipulation (mangling)
 - Build sophisticated QoS and Policy routers
 - Very complicated to learn - Large companies have dedicated expertise for iptables.
- **SNORT/IDS/IPS** - (<http://www.snort.org/services>)
 - Adds signature, protocol, and anomaly-based inspection.
 - Industry de facto standard
 - Lots of available help and info, creating new packet signatures should be left to the pros.

VPN

- **OpenVPN** - (<http://openvpn.net/>)
 - Any OS
 - Client - to - Site
 - Site - to - Site
 - Tunnel any IP subnetwork or virtual ethernet adapter over a single UDP or TCP port.
 - Configure a scaleable, load balanced, VPN server farm using one or more machines.
 - Leverages the OpenSSL library.
 - Real time adaptive link compression and traffic shaping to manage bandwidth.

Content Filtering

- **DansGuardian** - (<http://dansguardian.org/>)
 - Filters the actual content of the pages
 - Phrase matching
 - PICS filtering
 - URL filtering
 - It dose **NOT** purely filter based on banned lists of sites
 - It can be as draconian or unobtrusive as you want
 - Default settings are what you might find at most primary schools
 - Runs on any linux / unix POSIX compliant based server
 - Truly a **CONTENT FILTER**
- **OpenDNS** - (<http://www.opendns.com/>) : 40,000 Schools

Optimizing Web Delivery

- Squid - (<http://www.squid-cache.org/>)
 - Caching proxy for the Web
 - HTTP
 - HTTPS
 - FTP
 - ...
 - Reduces **BANDWIDTH**
 - Improves response time
 - Runs on most operating systems, including windows server.

BANDWIDTH

- **Linux Bandwidth Arbitrator** - (<http://www.bandwidtharbitrator.com/>)
 - This is what the commercial NetEqualizer system uses.
 - Influences traffic coming in and going out of your network.
 - Adjusts traffic flows every 1/2 second.
 - Allows low powered hardware to run it.
 - Layer 7 Bridge
 - Does not introduce enough delay to adversely effect packet transmission.

The cost

- Netfilter, Snort, DansGuarding, Squid, and Bandwidth Arbitrator take a talented and certain level of expertise to get working reliably together and to troubleshoot should anything ever go wrong.
- Our solution was developed on approximately 130 man hours.
- We spend around 20 man hours a year updating and maintaining these systems.
- Simple IU servers that have RAID 1 and quad core 8 GB RAM support ~ 500-750 concurrent users.
 - netfilter and snort run on a box
 - squid and danguardian run on a box

Easy Alternative

- **Untangle** - (<http://www.untangle.com/>)
 - Integrates netfilter, snort, network level virus scanning, squid, OpenVPN, URL based content filtering, and much more into a VERY easy to install Server OS distribution with a easy to use web management portal.
 - Has paid modules that offer even more powerful features with a very simple to use virtual rack interface.
 - Very detailed reporting to the user level.
 - Less than an hour from start of installation to actively using it on your network.
- **SmoothWall Express** - (<http://www.smoothwall.org/>)
 - More suited to less than 200 connections.
 - Very easy to install and manage.
 - Lots of pluggins available to gain the exact same results.

- Inventory
- Imaging

- Software Updates
- System Configuration
- Software Distribution

- Change Management
- Email

- Firewall
- VPN
- Content Filtering
- Bandwidth

Questions ?

LDAP



OpenLDAP

- OpenLDAP - (<http://www.openldap.org/>)
 - OpenSource implementation of LDAP.
 - Easy to integrate with open standards.
 - Large support group.
 - Adopted world wide.
 - Kerberos & SASL integration.
 - Supports Windows/Linux/Unix/OS X client environment

Thank You

Joseph J.Viscomi (jviscomi@brehm.org)- TABS Annual Conference, 2011 Boston.