FROM TO SOFTWARE UPDATES

How the Orchard infrastructure keeps OS X applications patched and secure, automatically

Ben Goodstein

Senior Systems Administrator NSMS Unix Services Team

ben.goodstein@it.ox.ac.uk

twitter: @fuzzylogiq github: fuzzylogiq

THE (GOOD OLD) BAD OLD DAYS

- Applications infrequently updated
- Physical media
- Security less of a concern for app developers and Mac admins
- Smaller catalogue of software to maintain
- · Yearly refresh with updated image with software manually updated was considered sufficient

THE CURRENT ZEITGEIST

- Agile development means important app updates released regularly
- Security of prime concern to app developers and, increasingly, Mac admins
- Apple themselves releasing OS updates more regularly with critical security fixes
- Customers expect and want new features faster

FIREFOX RELEASES 2003-2017

Phoenix	Firebird								Fire	efox						
		Firefax 0.8 Firefa	x 1.0 Fir	irefox 1.5 Fire	fax 2.0		Firefax 3.0	Firefox 3.5	Firefax 3.6		Firefox 4.0	Firefax 11.0	Firefax 18.0	Firefox 25.0	Firefax 32.0	Firefox 39.0
	0.6.1		1.0.1		2.0.0.1		1201	1254	3.6.2		4.0.1	12.0	18.0.1	25.0.1	32.0.1	139.03
10.3	10.7	0.9 0.9.1	1.0.2	11502	2.0.0.2		1302	3.5.2	3.6.3		150	13.0	18.0.2	26.0	32.0.2	140.0
0.2 0.3 0.4 0.5	0.7 0.7.1	0.9.2	1.0.3	1.5.0.2	20.03		1303	3.5.3	11	3.6.4	5.0 5.0.1	13.0.1	19.0	26.0.1	32.0.3	140.0.2
10.5	10.7.1	0.9.3	1.0.4	1.5.0.4	2.0.0.3 2.0.0.4		130.4	3.5	4	3.6.6	16.0	14.0	19.0.1	27.0	33.0	140.0.3
10.0		10.10	1.0.5	1.5.0.5	2.0.0.5		130.5	133	5.5	3.6.7	6.0.1	114.0.1	19.0.2	27.0.1	33.0.1	41.0
		0.10 0.10.1	11.0.6	1.5.0.6	2.0.0.6		30.6	10	3.5.6	3.6.8	6.0.2	115.0	120.0	28.0	33.0.2	41.0.1
		10.10.1	1.0.6 1.0.7	11.5.0.7	20	0.7	3.0.2 3.0.3 3.0.4 3.0.5 3.0.6	7	.4 5.5 3.5.6 3.5.7 3.5.8	3.6.9	170	14.0.1 15.0 15.0 16) 20.0 0.1 20.0.1	128.0	.1 33.0.3	40.0 40.0.2 40.0.3 41.0 41.0.1 41.0.2 42.0 43.0
			1	1.5.0.7 1.0.8 1.5	5.0.8	0.0.8	13.	0.8	3.5.8	3.6.10	7.0.1	116	6.0 21.0	28.0. 29	0.0 33.1	142.0
				117	1.5.0.9	2.0.0.9		3.0.9	3.5.9	3.6.11	18.0	116	6.0 21.0 6.0.1 22.0	0 12	9.0.1 33.1.1	143.0
					1.5.0.10	0.0.8 2.0.0.9 2.0.0.10		3.0.10	1:	3.5.10 3.6.12	la	0.1	16.0.2	23.0	30.0 34.0.5/34.	0 43.0.1
					1.5.0.11	2.0.0.11		3.0.11		3.5.11 3.6	.13	9.0	17.0	23.0.1	31.0 34.0.1	143 0 2
					1.5.0.12	2.0.0.12		3.0.12		3.5.12	3.6.14	9.0.1 10.0 10.0.1	17.0 17.0.1 17.0.2esr	24.0	35.0	43.0.2 43.0.4 44.0 1 44.0.1 2 44.0.2 3 45.0
						2.0.0.		3.0.12 3.0.13		3.5.13	3.6.15	10.0	17.0.2esr	24.1.0esr	35.0.1	43.0.4
						2.0.0		3.0.14		3.5.14	3.6.16	10.0.1	17.0.3esr	24.1.1esr	31.1.0esr 36.0	44.0
							2.0.0.15	3.0		3.5.15	3.6.17	10.0.2	17.0.4esr	24.2.0esr	31.1.1esr 36.0.	1 44.0.1
							2.0.0.16		3.0.16	3.5	.16 3.6.18 3.5.17 3.6.19	10.0.3esr	17.0.5esr	24.3.0es	sr 31.2.0esr 36.0	.2 44.0.2
							2.0.0.17		3.0.17		3.5.17 3.6.19	10.0.4esr	17.0.6	esr 24.4.	0esr 36.0	.3 45.0
							2.0.0.18		3.0.18		3.5.18 3.6.20	10.0.5esr			1.5.0esr 36.0).4
							2.0.0.19		3.0.19)	3.5.19 3.6.21	10.0.6e		17.0.8esr	37.0	0
							2.0.0.20				3.6.22	10.0).7esr	17.0.9esr	37.	0.1
											3.6.23	3 10	0.0.8esr	17.0.10esr		.0.2
											3.6.23 3.6 	5.24 10	0.0.9esr	17.0.11esr	24.6.0esr 31.3.0esr 3	38.0
												3.6.25	10.0.10esr	!	i i i	
													10.0.11esr			38.0.5
												3.6.27	10.0.12esr		24.7.0esr 31.4.0es	
												3.6.28			24.8.0esr 31.5.0	
															24.8.1esr	38.2.0esr
																5.2esr 38.2.1esr 5.3esr 38.3.0esr
																6.0esr 38.4.0esr
																31.7.0esr 38.5.0esr
																31.8.0esr 38.5.1esr
																38.5.2esr
																38.6.0esr
																38.6.1esr
																38.7.0esr
0000	0004	2025		20	0.7	2000	0000		10			10	2012	m11	2015	
2003	2004	2005	200	06 20	0/	2008	2009	20	10	2011	20	12	2013	2014	2015	2016

DOING IT ALL BY HAND

- Manual download
- · Manual packaging
- Copy to clients or bake into image
- Slow and frustrating

WHAT'S NEEDED?

- Inventory
- Packaging
- Testing
- Installation & Updating
- Automation

INVENTORY

- Needs to be regularly updated and accurate
- Needs to describe computer's location, ownership, hardware and software usefully
- · JSS, Sal, Absolute Manage, Filewave

PACKAGING

- Needs to be repeatable with predictable results
- GUI: Whitebox Packages, JAMF Composer
- Command line: The Luggage, autopkg, pkgbuild

INSTALLATION & UPDATING

- Needs to work closely with inventory to ensure it's always up-to-date
- · Must be aware of app versions and intelligently assess need for updates
- munki, JSS, Filewave, etc.

TESTING

- Updates can break functionality
- Need internal and user testing
- Various methods: testing/production, unstable/testing/stable etc.
- · JSS, munki, Google Experiments

ORCHARD INFRASTRUCTURE

- JSS (a.k.a. Casper) for inventory
- autopkg for packaging
- munki (the Orchard Software Centre) for installation & updating
- plus some magic to glue it all together



JSS (A.K.A. CASPER)

- · Great for inventory, MDM (mobile device management), settings management & imaging
- Easy to use web-based front end
- Comprehensive REST API



JSS (A.K.A. CASPER)

- Not so great for software packaging or patching
- No built-in concept of 'release channels' for staging and testing updates
- Laborious import process
- MYSQL string comparisons of application version numbers 😞



- Reliably and repeatably downloads and packages software using 'recipes'
- Open source
- · Recipes are reusable, configurable, extensible
- Large community
- · Command-line client GUI 'autopkgr' available



- Reasonably idempotent
- Integrates well with munki
- Flat file format (plists) allows easy Git collaboration
- Easy automation (hence the name!)
- Steep learning curve

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<pli><pli><pli>< version="1.0">
<dict>
    <key>Description</key>
    <string>Download recipe for Firefox. Finds and downloads a Firefox release.
Values for RELEASE correspond to directories here: http://download-origin.cdn.mozilla.net/pub/mozilla.org/firefox/releases/
Some useful values are: 'latest', 'latest-10.0esr', 'latest-esr', 'latest-3.6', 'latest-beta'
LOCALE corresponds to directories at http://download-origin.cdn.mozilla.net/pub/mozilla.org/firefox/releases/$RELEASE/mac/
Examples include 'en-US', 'de', 'ja-JP-mac', 'sv-SE', and 'zh-TW'
No idea if all Firefox builds are available in all the same localizations, so you may need to verify that any particular
combination is offered.</string>
    <key>Identifier</key>
    <string>com.github.autopkg.download.firefox-rc-en_US</string>
    <key>Input</key>
    <dict>
        <key>RELEASE</key>
        <string>latest</string>
        <key>LOCALE</key>
        <string>en_US</string>
        <key>NAME</key>
        <string>Firefox</string>
    </dict>
    <key>MinimumVersion</key>
    <string>0.2.0</string>
    <key>Process</key>
    <array>
        <dict>
            <key>Arguments</key>
            <dict>
                <key>product_name</key>
                <string>firefox</string>
                <key>release</key>
                <string>%RELEASE%</string>
                <key>locale</key>
                <string>%LOCALE%</string>
            </dict>
            <key>Processor</key>
            <string>MozillaURLProvider</string>
        </dict>
        <dict>
            <key>Arguments</key>
            <dict>
                <key>filename</key>
                <string>%NAME%.dmg</string>
            </dict>
            <key>Processor</key>
            <string>URLDownloader</string>
        </dict>
        <dict>
            <key>Processor</key>
           <string>EndOfCheckPhase</string>
        </dict>
   </array>
</dict>
</plist>
```



MUNKI (THE ORCHARD SOFTWARE CENTRE)



- Great for software installation and patching
- Open source (so customisable)
- · Repo is just a collection of packages and metadata on a web server



Munki (the Orchard Software Centre)

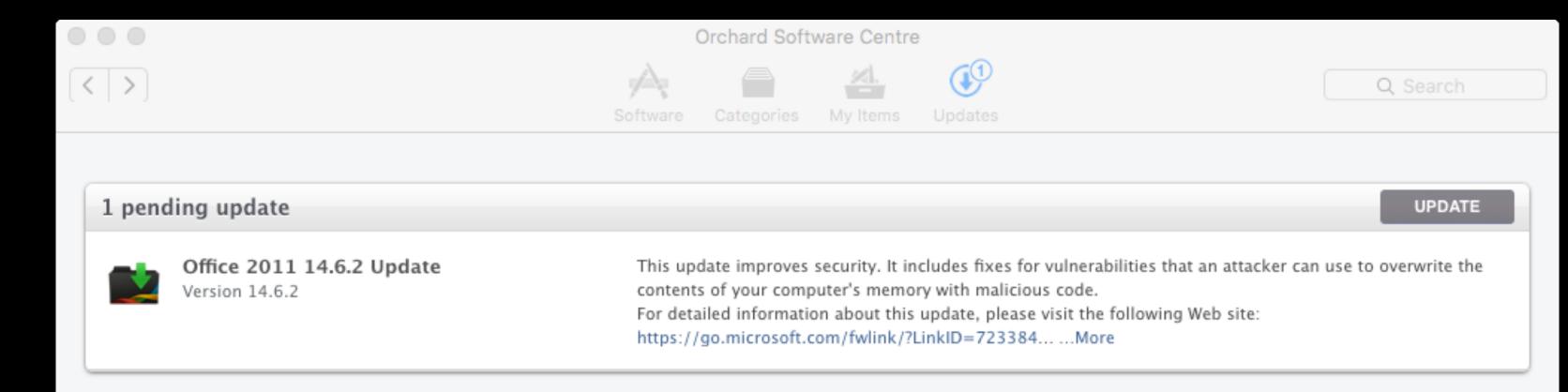


- · 'Magic' is done on client
- Catalogs and Manifests
 - · Catalogs list all software available to computer
 - · Manifests detail what should be installed from catalogs
- Familiar user interface for optional installs
- Many other useful features steep learning curve for the admin



Munki (the Orchard Software Centre)





BRINGING IT ALL TOGETHER

- manana to allow the JSS to inform munki's decisions
- munki-staging for automating testing stages

MANANA

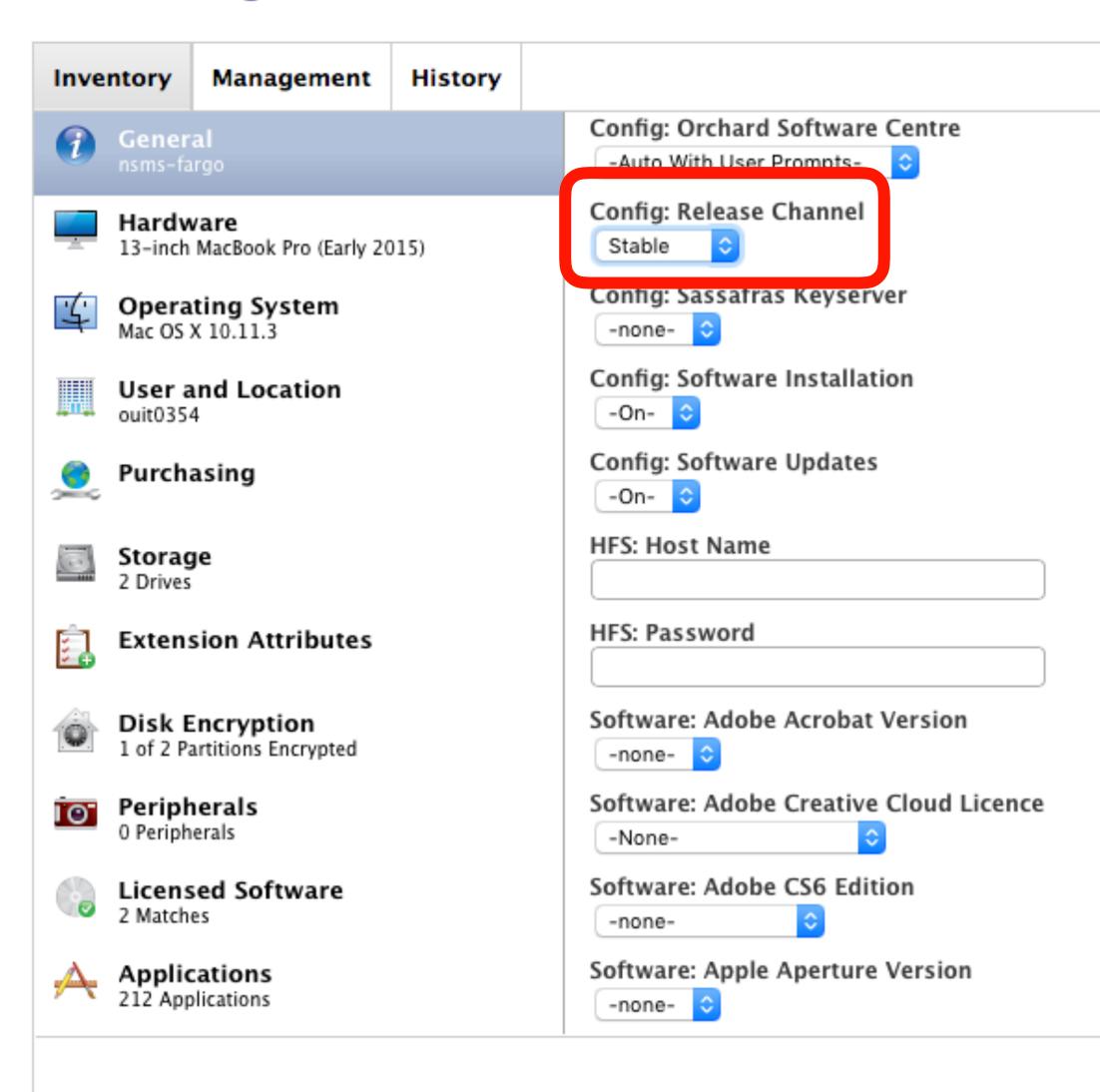
- manana dynamically changes munki manifest client receives from server based on JSS computer record
- deliver software based on inventory
- munki preflight/postflight ensures integrity with inventory

MANANA

	Computer Attribute Mapping
	If Group matches Location: Saïd Business School: Sainsbury Library then add manifest: sbs_library_customisations
	If Group matches BSG-ROQ-AV Mac Minis then add manifest: bsg_av_customisations
	Extension Attribute: If Config: Release Channel matches Unstable then add manifest: orchard_testing
	If Site matches IT Services - ITLP then add manifest: itservices_itlp_site_customisations
	If Site matches Department of Computer Science (DCS) then add manifest: dcs_site_customisations
	If Site matches NSMS then add package: Wireshark to optional_installs
	Extension Attribute: If Software: Adobe Creative Cloud Licence matches Orchard Device Licence then add manifest: adobe_creative_cloud_device
	If Group matches Settings: Management Option MMP (All OS) then add package: Office_2011_Update to managed_updates
	Extension Attribute: If Config: Release Channel matches Testing then add catalog: stable
	Extension Attribute: If Config: Release Channel matches Unstable then add catalog: stable
	Extension Attribute: If Config: Release Channel matches Unstable then add catalog: testing
	Extension Attribute: If Config: Release Channel matches Unstable then add catalog: unstable
0	Extension Attribute: If Config: Release Channel matches Testing then add catalog: testing
	Extension Attribute: If Config: Release Channel matches Stable then add catalog: stable

nsms-fargo





Done

History

Autorun Data

Delete

MANANA

Computer Attribute Mapping
If Group matches Location: Saïd Business School: Sainsbury Library then add manifest: sbs_library_customisations
If Group matches BSG-ROQ-AV Mac Minis then add manifest: bsg_av_customisations
Extension Attribute: If Config: Release Channel matches Unstable then add manifest: orchard_testing
If Site matches IT Services - ITLP then add manifest: itservices_itlp_site_customisations
If Site matches Department of Computer Science (DCS) then add manifest: dcs_site_customisations
If Site matches NSMS then add package: Wireshark to optional_installs
Extension Attribute: If Software: Adobe Creative Cloud Licence matches Orchard Device Licence then add manifest: adobe_creative_cloud_device
If Group matches Settings: Management Option MMP (All OS) then add package: Office_2011_Update to managed_updates
Extension Attribute: If Config: Release Channel matches Testing then add catalog: stable
Extension Attribute: If Config: Release Channel matches Unstable then add catalog: stable
Extension Attribute: If Config: Release Channel matches Unstable then add catalog: testing
Extension Attribute: If Config: Release Channel matches Unstable then add catalog: unstable
Extension Attribute: If Config: Release Channel matches Testing then add catalog: testing
Extension Attribute: If Config: Release Channel matches Stable then add catalog: stable

nsms-fargo



Inver	ntory Management	History				
0	General nsms-fargo		Config: Orchard Software Centre -Auto With User Prompts-			
Ţ	Hardware 13-inch MacBook Pro (Early 20	015)	Config: Release Channel Unstable			
4	Operating System Mac OS X 10.11.3		Config: Sassafras Keyserver -none- ≎			
	User and Location ouit0354		Config: Software Installation			
	Purchasing		Config: Software Updates			
<u></u>	Storage 2 Drives		HFS: Host Name			
	Extension Attributes		HFS: Password			
0	Disk Encryption 1 of 2 Partitions Encrypted		Software: Adobe Acrobat Version			
0	Peripherals 0 Peripherals		Software: Adobe Creative Cloud Licence -None-			
	Licensed Software 2 Matches		Software: Adobe CS6 Edition -none-			
Ą	Applications 212 Applications		Software: Apple Aperture Version -none-			

Done History

Autorun Data

Delete

```
<pli><pli>st version="1.0">
<dict>
  <key>catalogs</key>
  <array>
    <string>unstable</string>
    <string>testing</string>
    <string>stable</string>
  </array>
```

DEMO

MUNKI-STAGING

- · python script relies on a Trello board
- Manual or automatic staging of packages
- Drag and drop or 'due dates'

USEFUL LINKS

- Casper/JSS http://www.jamsoftware.com
- munki https://github.com/munki/munki/wiki
- munkiadmin https://github.com/hjuutilainen/munkiadmin
- munkiwebadmin https://github.com/munki/mwa2
- autopkg https://github.com/autopkg/autopkg/wiki
- autopkgr http://www.lindegroup.com/autopkgr
- munki-staging https://github.com/ox-it/munki-staging
- manana https://github.com/ox-it/manana
- · Orchard autopkg recipes https://github.com/ox-it/orchard-recipes