Preparing for the Next macOS: Testing in Your Environment, and What's New!

Feedback: https://bit.ly/psumac2019-382

@roberthammen @hammen

Robert Hammen

Robert Hammen has been managing Macs for a long time - since before Apple shipped a Unix-based client OS. Robert was a long-time consultant to K-12 as well as small, medium, and enterprise organizations, but, for the past three years, has worked at the National Institutes of Health in suburban Washington DC, helping deploy, secure, and support Macs. Robert has numerous Apple and Jamf IT certifications, going back to OS X 10.4 and Jamf Pro 6.

2019 MACADMINS CONFERENCE

@roberthammen @hammen

Ground Rules & Tips

- Please silence all mobile devices!
- Take calls in the hall.
- Take a bathroom break if needed.
- Please hold questions until the end.
- All slides and speakers notes will be available for download.

Why Test Catalina Now?

- Provide feedback to Apple
- Find bugs/issues, potentially exclusive to your environment
- Be ready to support as close to release as possible

Why Support Right Away?

- Previously: Benfer's Maxim: "Woe is me, if I deploy before .3"
- Security model has changed
- Gone from a slow, methodical change management approach…
- …to an Agile software development methodology, with development sprints and regularly-scheduled releases

Education, I Feel You

- Timing of Apple OS releases not great for most edu customers, at least in North America
- Adopt when you are ready

Regularly-Scheduled…

- Mac Office Team: monthly releases
- Adobe: Patch Tuesday (unless critical vulnerabilities)
- Apple: new major macOS in fall, .1 release after 30 days, then point releases every 45-60 days
- Apple Spring Release has new features/surprises (if you're not paying attention)

Security!

- Unofficially (not documented anywhere, but SOP): Apple provides patches for current OS and previous 2, i.e. N-2
- Read the Apple Security Updates KB: https://support.apple.com/en-us/HT201222
- Not all fixes are back-ported to the previous OS (see: Spectre/Meltdown initial response, ZombieLoad/FallOut only fully patched on 10.14.5): https://support.apple.com/en-us/HT210107

Security!

- If you want to have the most secure Mac, you must be running the latest (N) macOS (with the latest app updates, of course)

Ch-ch-ch-ch-changes…

- Turn and face the strange...

2019 MACADMINS CONFERENCE

@roberthammen @hammen

Rate of Change is Increasing

- macOS 10.13: APFS (end of imaging), User-Approved MDM, User-Approved Kernel Extension Loading
- macOS 10.14: PPPC (Privacy Preferences Policy Control), Notarization
- macOS 10.15: Read-Only Boot Volume, expansion of PPPC and notarization, no more 32-bit processes, KEXTs deprecated, and much more…

Apple is Playing Chess

- If you pay attention, you can see the pieces moving
- Read-only boot volume and separated user apps/data? Where might this be going?

2019 MACADMINS CONFERENCE

@roberthammen @hammen

The Game Plan?

- Step 1: Move iOS security concepts/model to Mac (TouchID, Secure Enclave, T2 chip, SecureBoot, always-(hardware) encrypted storage)
- Step 2: Allow iOS apps to easily be ported to Mac (Project Catalyst)
- Step 3: (More) Profit?!?

“Difficult to see.
Always in motion is the future.”

2019 MACADMINS CONFERENCE

@roberthammen @hammen

How Can You Obtain macOS Catalina?

- Developer Seed - $99/yr - https://developer.apple.com/programs/
  Probably still a good idea if you create installer packages and need to sign/notarize them - available immediately
- Public Beta - https://beta.apple.com/sp/betaprogram/
  not available right away

How Can You Obtain macOS Catalina?

- AppleSeed for IT - this is what most people should be using. Previously required you to ask/nag your Apple SE or AE, now allows access to Managed AppleID's (i.e. the ones you use to log into https://business.apple.com or https://school.apple.com)

How Can You Obtain macOS Catalina?

- installinstallmacos.py - https://github.com/munki/macadmin-scripts

```
sudo python installinstallmacos.py --seedprogram=DeveloperSeed
```

- seedutil - https://derflounder.wordpress.com/2018/01/06/setting-your-mac-to-receive-macos-beta-updates-using-seedutil/

```
sudo /System/Library/PrivateFrameworks/Seeding.framework/
Versions/A/Resources/seedutil enroll DeveloperSeed
```

How Should You Test?

- Early Betas - Virtual Machines (VMware Fusion, Parallels)
- How to install macOS Catalina on VMware Fusion 11.1.0: https://planetvm.net/blog/?p=64552

General VMware Testing Tips

- Tools like the previously-mentioned installinstallmacos.py, AutoDMG (not yet publicly Catalina-compatible) https://github.com/MagerValp/AutoDMG and vFuse https://github.com/chilcote/vfuse will allow for automated VM creation

General VMware Testing Tips

- Testing Device Enrollment with VMware Fusion
  https://www.rderewianko.com/how-to-create-a-vm-thatll-work-with-dep-on-vmware-fusion/
- If enrolling VMs in Jamf Pro, be sure to allocate 2 CPU cores to ensure MDM is functional
  https://www.jamf.com/jamf-nation/discussions/23549/reality-check-mdm-capability-with-virtual-machine#responseChild142635

General VMware Testing Tips

- Disable TouchID/authentication spins on TouchID Macs:

```
board-id.reflectHost = "FALSE"
```

- Useful shortcuts in Setup Assistant

  https://chris-collins.io/2018/03/15/Using-Terminal-At-macOS-Setup-Assistant/

- Force DEP nag:

```
sudo profiles renew -type enrollment
```

Install on Real Hardware

- Secondary Mac, i.e. not your daily driver
- Any data on it must be backed up
- If upgrading an already-provisioned Mac, you should probably uninstall all security software
- Sign out of iCloud:

  https://ulysses.app/blog/2019/07/a-word-about-apples-os-betas/

2019 MACADMINS CONFERENCE

@roberthammen @hammen

Notes About Testing Subsequent Betas

- Don’t expect the App Store to be fully functional/reliable
- Don’t expect Software Update (i.e. beta 2->beta 3) to work
- Be prepared to nuke and pave, or at least reinstall
- If you find a bug, reproduce on a VM, other hardware, or nuke-and-pave and reproduce before reporting

Resources Available On AppleSeed

- Test Plans
- Discussion Forums
- The awesomely-well done “What's New for Enterprise and Education” PDF

Betas Keep Coming…

- Approximately every 2 weeks or so
- Avoid the temptation of updating your primary Mac
- At least wait until mid-August 😀

Betas Keep Coming…

- You will most likely be waiting for your MDM vendor to release Day Zero support (not Zero Day support, that's something entirely undesirable)
- If you need to *test* new MDM functionality ahead of time, Profile Manager in macOS Server Beta is available…

Documenting your Provisioning Process

- Do you have a runbook that documents what applications/ settings/profiles/configuration changes are made as part of your provisioning process?
- If the answer is **No**, time to create one

Testing Your Provisioning Process

- Device Enrollment (via Apple Business Manager/Apple School Manager) on a non-T2 Mac
- Same, but on a T2 Mac

What Makes a T2 Mac Special?

- One computer, two OSes - macOS and bridgeOS
- bridgeOS gets updated when macOS does
- External boot disabled by default (Boot Security)

Testing on a T2

- With external boot disabled by default, if the beta OS goes south, you may have a problem
- Suggest creating a new APFS container, and either installing Catalina on it, or installing Mojave on it as a backup, and upgrading your current OS to Catalina
- That way, you should still be able to Option-boot into a known-good OS.

Test Your Apps

- Do they launch? Do they function correctly?
- RoaringApps - https://roaringapps.com/apps?platform=osx
- Template for Technical Readiness - https://www.modtitan.com/2019/06/template-for-macos-core-application.html

Application Name	Application Owner	Min. Version Required	Catalina Ready?	Notes
Google Chrome	Mac Eng	TBD	☐	20190619 - Version 75.0.3770.100 functions as expected, unsure about notarization requirements (@EKW)
"AV Software"	@Security Person		☐	20190618 - Version 1.2.3 appears to be functioning normally, waiting on confirmation of support from $vendor
"Random Internal App"	@Developer Person	RIP ☠️	☐	It's dead, Jim
etc. ...			☐	

Test Your Scripts

- Scripting languages may not be included in the OS - more on that later
- Default Unix shell has changed - more on that later

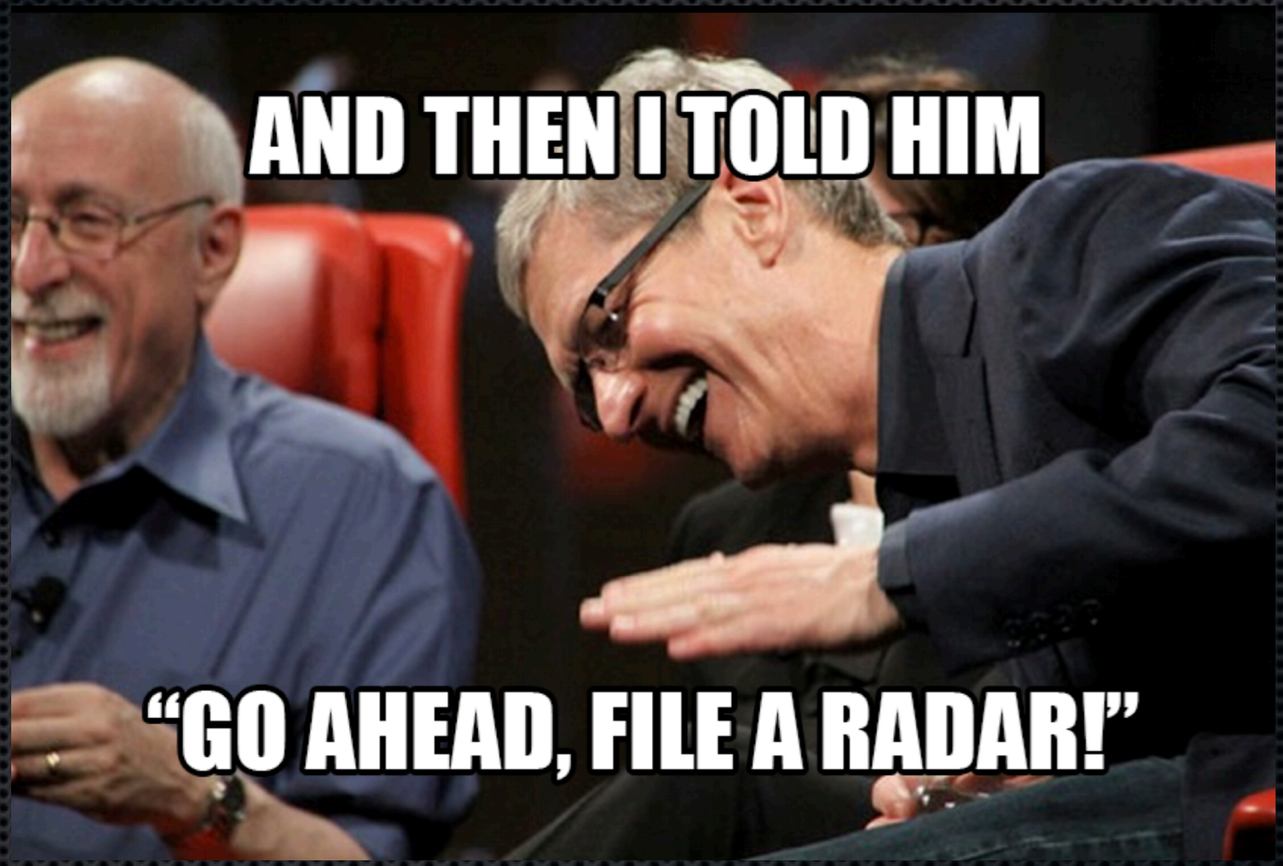
Test Your Security Tools

- Like your MDM vendor, you'll probably need to wait until Catalina goes Golden Master, or close to it, for compatible security tools
- If Catalina is shipping, but your security vendors aren't ready, and won't be ready any time soon, time to change vendors

Early Adopters

- You need them
- Identifying good ones is an art, not a science

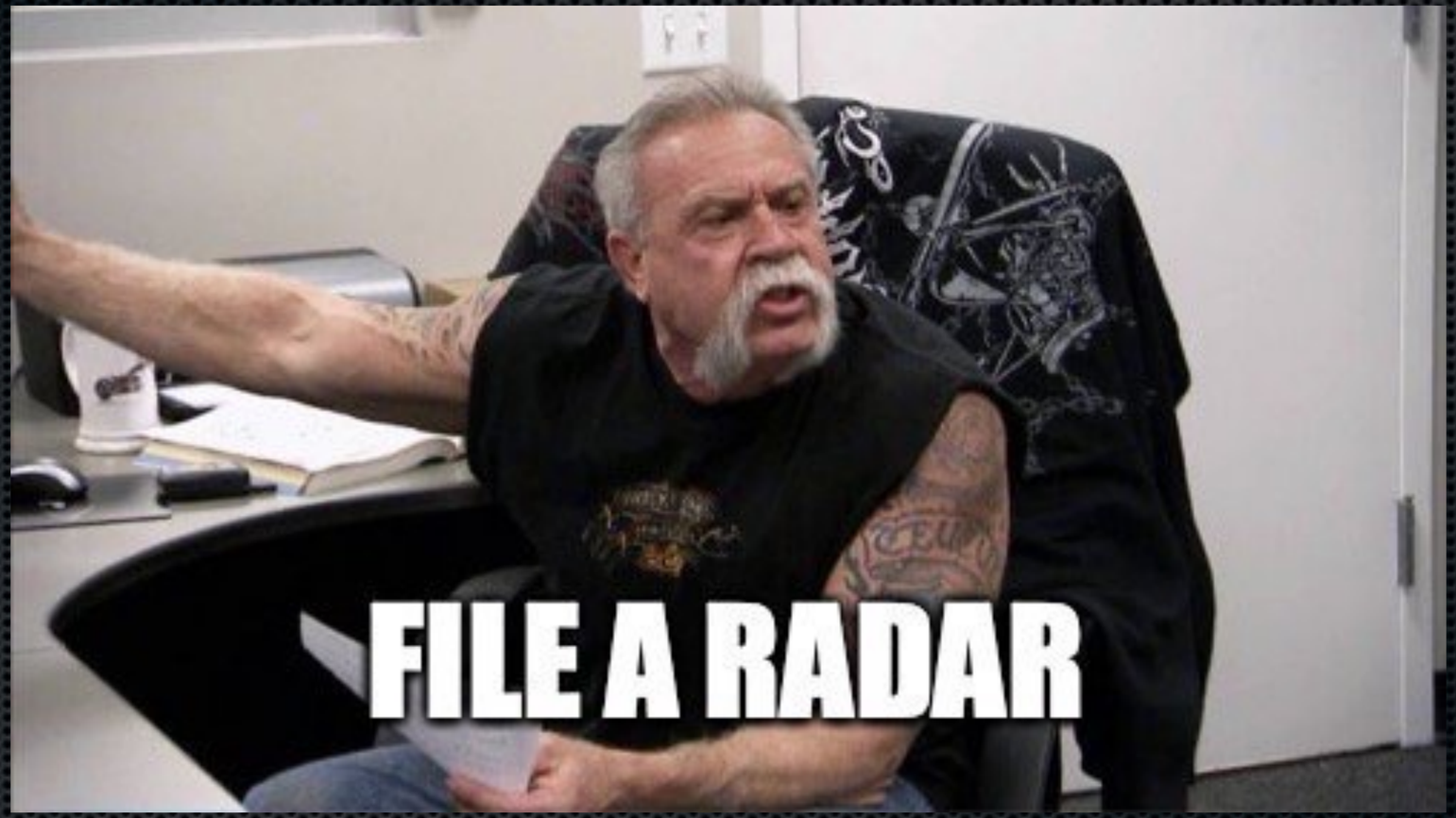
Reporting Bugs to Apple



2019 MACADMINS CONFERENCE

@roberthammen @hammen

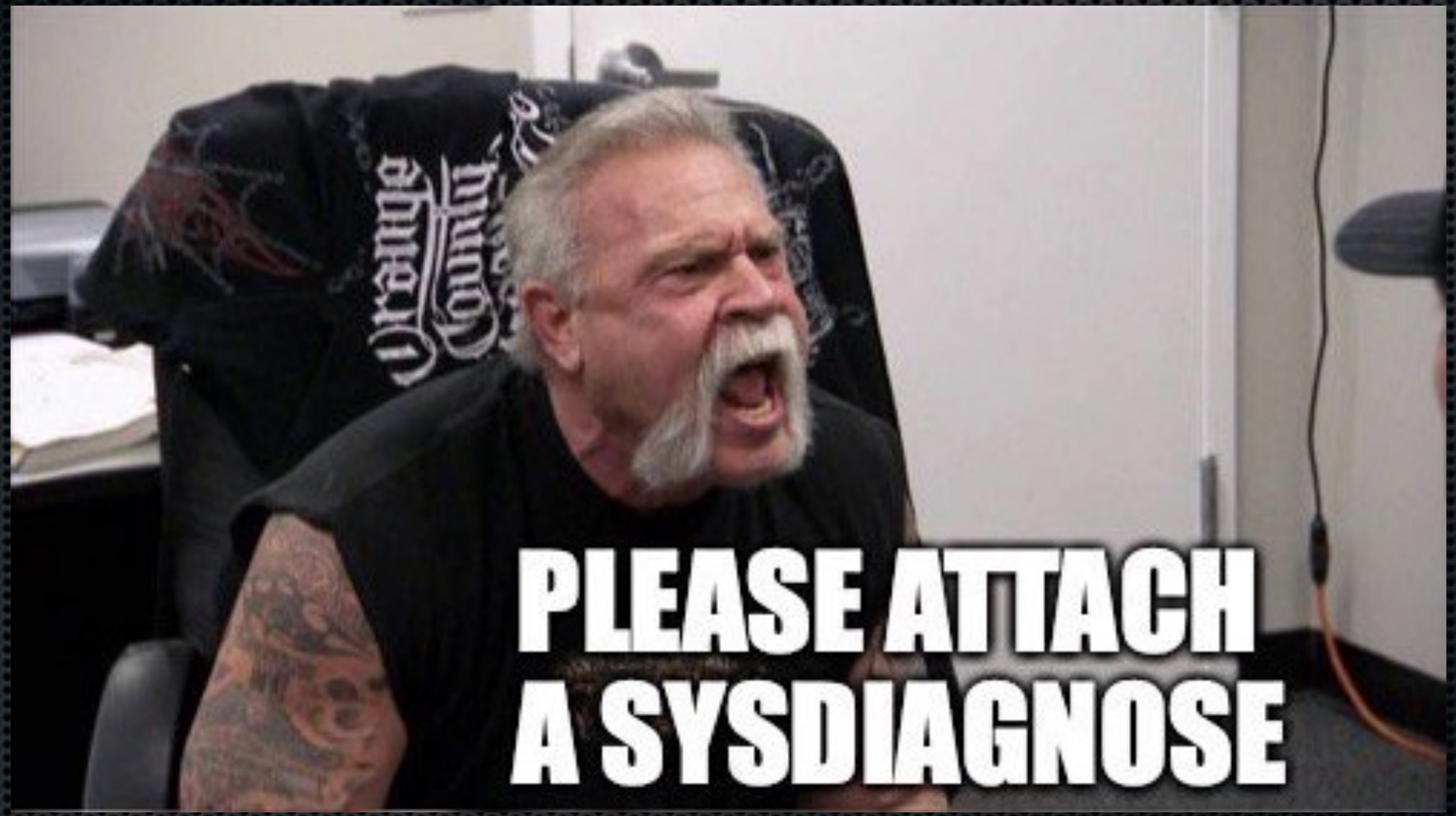
Circle of a Bug Report's Life



2019 MACADMINS CONFERENCE

@roberthammen @hammen

Circle of a Bug Report's Life



2019 MACADMINS CONFERENCE

@roberthammen @hammen

Circle of a Bug Report's Life

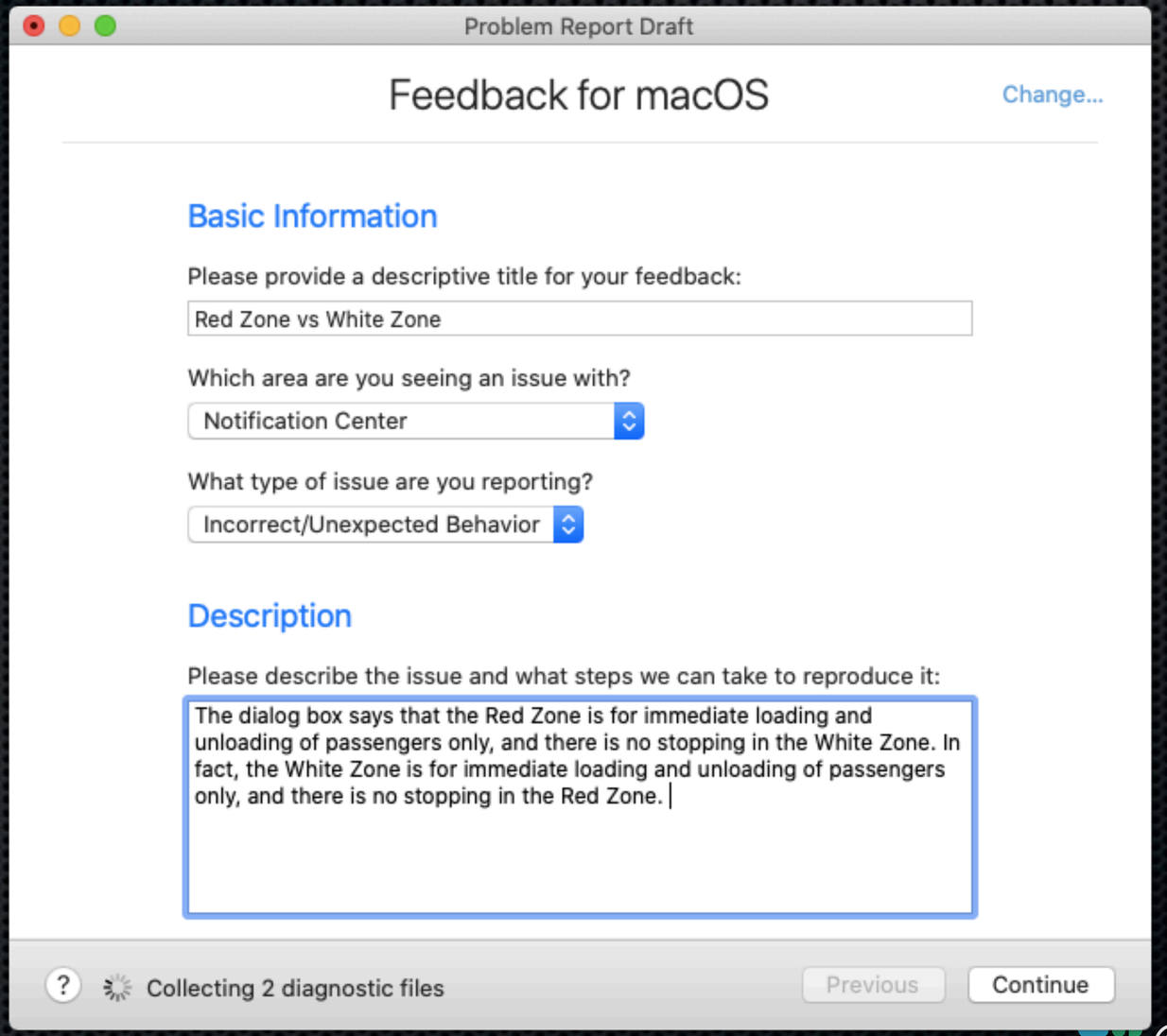
2019 MACADMINS CONFERENCE

@roberthammen @hammen

R.I.P. BugReporter

- New method of reporting bugs to Apple is Feedback Assistant (on both macOS and iOS)
- Located in /System/Library/CoreServices/Applications
- History of previous bugs maintained in app or at https://feedbackassistant.apple.com

Feedback Assistant



2019 MACADMINS CONFERENCE

@roberthammen @hammen

How To Write a Good Bug Report

- Provide an accurate title/subject
- What are you trying to accomplish?
- Please write an explicit description of the issue.
- Is it a new problem, or something that used to work?
- Can you reproduce it? What are the steps to do so?

How To Write a Good Bug Report

- Include any screen shots or videos of the issue
- Sample scripts, sample code, test cases
- Any error messages, in full
- What the expected results were, versus the actual results
- Any workarounds you were able to identify
- Explain the impact/how many potential systems this affects

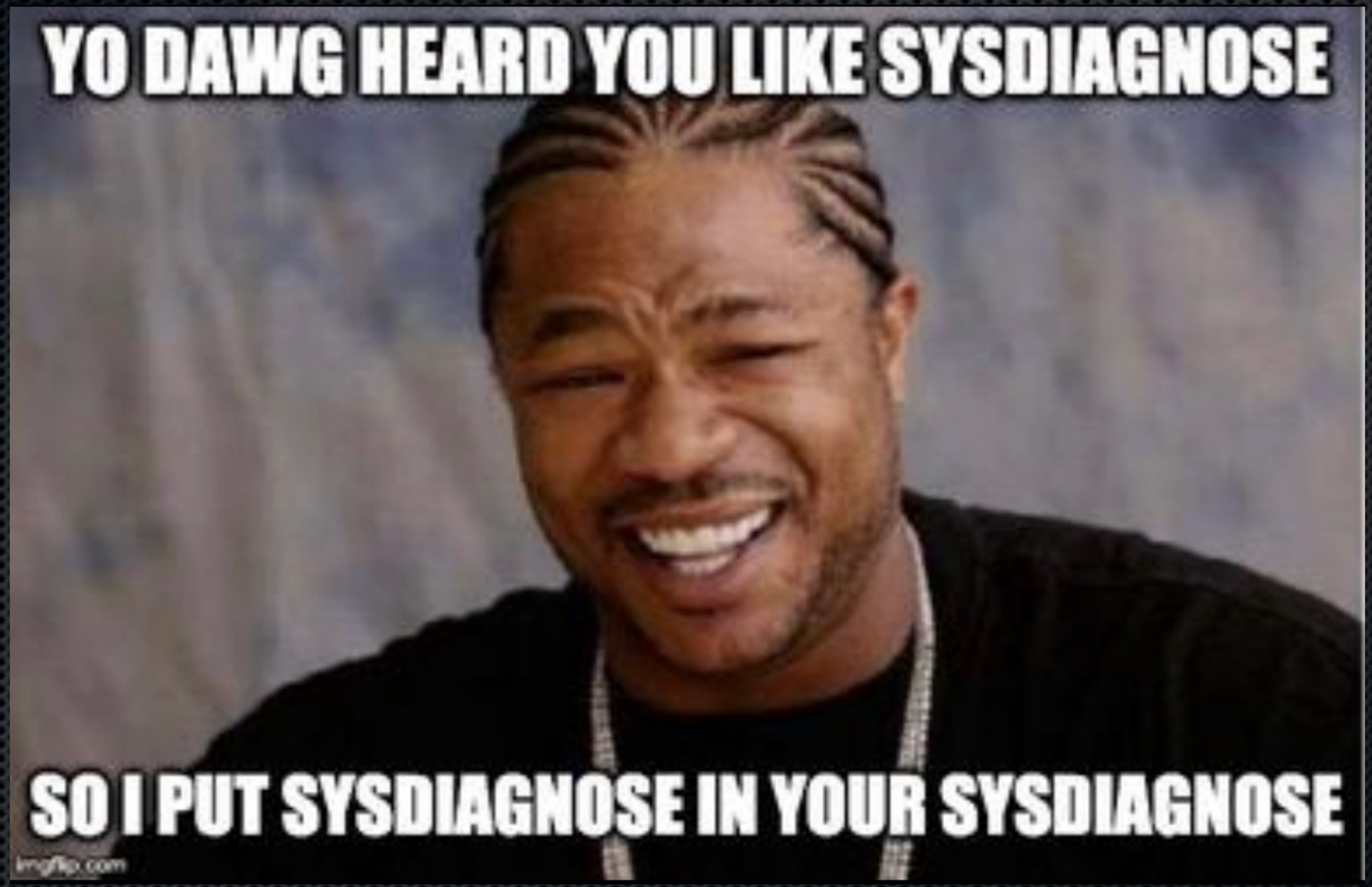
@roberthammen

@hammen

sysdiagnose

- command-line tool to gather system diagnostic information, logs, etc.
- Invoked by **sudo sysdiagnose** or Control-Option-Command-Shift-period
- Automatically performed when submitting a report via Feedback Assistant
- High-security environments may not be able to use this tool

Sysdiagnose



2019 MACADMINS CONFERENCE

@roberthammen @hammen

If It's A Critical Bug

- Be sure to file it using a Managed AppleID from Apple Business Manager/Apple School Manager (goes to a different queue)
- Open an AppleCare Enterprise Case
- Email both the Feedback ID and the AppleCare Enterprise Case numbers to your SE
- SE's have an escalation path for serious issues

Bug Report Links

- Profiles and Logging instructions for Apple technologies: https://developer.apple.com/bug-reporting/profiles-and-logs/
- SysDiagnose Logging Instructions: https://download.developer.apple.com/OS_X/OS_X_Logs/sysdiagnose_Logging_Instructions.pdf

What's New in Catalina (that might affect you)

2019 MACADMINS CONFERENCE

@roberthammen @hammen

Changes to the FileSystem

- New boot/system volume is created during installation, and is made read-only afterwards
- Existing "Macintosh HD" is renamed to "Macintosh HD-Data"
- New APFS feature called "firmlinks" allows Finder and Unix shell to show unified Applications folder, even though apps are dispersed between R/O system (Apple) and data volume (third-party)

Changes to the FileSystem

- Explicit paths/locations of files have changed
- Have seen some scripts and commands show inconsistent or inaccurate results
- Fun troubleshooting boot issues with not knowing where exactly the problematic LaunchDaemons, KEXTs etc. are, or if the volumes are mounted read/write
- NFS mounts at / not possible right now, will be in future

Changes to the FileSystem

- Erase and Install today will wipe both OS and data volume
- Will that behavior continue in a future OS?
- In the future, will OS updates be installed, or copied? We have .ipsw files for iOS, could there someday be a similar approach for macOS? Stay tuned.

Supervision now possible in macOS

- Will only happen if Mac is in Automated Device Enrollment via Apple Business Manager/Apple School Manager, not manual
- (User Approved) MDM - UAMDM Macs cannot be supervised
- Happens automatically during Catalina upgrade
- Verify via System Profiler app or system_profiler command

Activation Lock

- T2 Macs only
- Mac must be in Automated Device Enrollment via Apple Business Manager/Apple School Manager, not manual (User Approved) MDM - UAMDM
- Supervision is Required
- Manageable via MDM (must support Activation Lock)

Activation Lock

- If "Find My Mac" is enabled in iCloud System Preferences, it will be turned on by default (if above requirements met), and user is signed in to iCloud
- Can block FMM via macOS Restrictions profile
- Must still sign out the user before upgrading (and deploying restrictions profile disables the interface to do so)

Privacy Preferences Policy Control Updates

- Desktop
- Documents
- Downloads
- Trash
- Cloud Storage (iCloud Drive, Dropbox, Box, etc.)
- Removable/External Drives

2019 MACADMINS CONFERENCE

@roberthammen @hammen

Privacy Preferences Policy Control Updates

- Camera
- Microphone
- Input Device Monitoring
- Screen Capture
- Speech Recognition
- Network Shares - beware Jamf Distribution Points!

2019 MACADMINS CONFERENCE

@roberthammen @hammen

KEXTs are dead! Sort of...

2019 MACADMINS CONFERENCE

@roberthammen @hammen

Not dead, just... resting

- Kernel Extensions = run at kernel level
- Can have significant performance and stability effects on the OS (current environment: 7 mandatory agents and a poor user experience)
- macOS 10.15 Catalina is the last version where KEXTs will run without compromise

What Replaces KEXTs?

- System Extensions, aka SEXTs

On Second Thought…

- System Extensions, aka sysx's
- Part of new DriverKit
- Runs in User Space, not Kernel
- Typically part of an app bundle, not dispersed across the filesystem

DriverKit

- Endpoint Security Framework - like previous Hypervisor and VPN Frameworks included in the OS
- Designed to provide functionality to security tool vendors
- On macOS Catalina, after installing a KEXT, it does not load until after a restart

Gatekeeper and Notarization

- Signature checks each time an app is launched, not just the first time
- Notarization (automated malware scanning like VirusTotal) added in macOS Mojave
- 10.14.5 required KEXTs signed after a certain date, or apps signed by new developer IDs, to be notarized in order to load
- 10.15 has some additional notarization requirements
- Tom Bridge's session right after this one (same room)

Default Unix Shell Changed

- zsh in lieu of bash (for new users, existing can change)
- bash still shipping as part of the OS, existing scripts will run
- https://github.com/rothgar/mastering-zsh
- Scripting OS X has an 8-part series on moving to zsh: https://scriptingosx.com/2019/06/moving-to-zsh/

Removal of Scripting Languages

- Reduces attack surface - does your dad really need a Python interpreter on his Mac?
- Python 2.7 deprecated, EOL in January 2020
- Python3 installation-on-demand (similar to Xcode command-line tool installation/prompts)
- Ruby and Perl may be removed from a future version of macOS

Removal of Scripting Languages

- Similar to when Apple stopped including Java and XQuartz
- Scripting and automation on macOS is not going away

BootStrap Tokens

- Enables FileVault unlock/granting of SecureTokens via MDM
- Requires Automated Device Enrollment, not manual/User Approved MDM
- Currently has some workflow limitations/considerations

Zero Touch Improvements

- Enrollment customization with web sheet
- Acceptable Usage Policy/consent text, branding, multi-factor authentication
- Enrollment continues after web sheet complete
- MFA Authentication via various cloud identity providers

Single-Sign On (Replacing Enterprise Connect)

- Apple-provide Kerberos Extension for Single-Sign On
- Local account, but gets a Kerberos ticket to log into websites, printing, etc.
- Managed via MDM/config profile (link to example profile in References section)
- Still room for third-party tools like Jamf Connect, etc.

Miscellaneous Changes

- 32-bit apps are truly dead, will not run/display an error dialog
- **fdesetup** command will prompt user for approval
- Installation of profiles via the **profiles** command-line tool will be deprecated in a future release of macOS.

Miscellaneous Changes

- Requirements for trusted certificates in iOS 13 and macOS 10.15: https://support.apple.com/en-us/HT210176
- “Printer drivers are deprecated and will stop working in a future version of CUPS.”

Printers…

2019 MACADMINS CONFERENCE

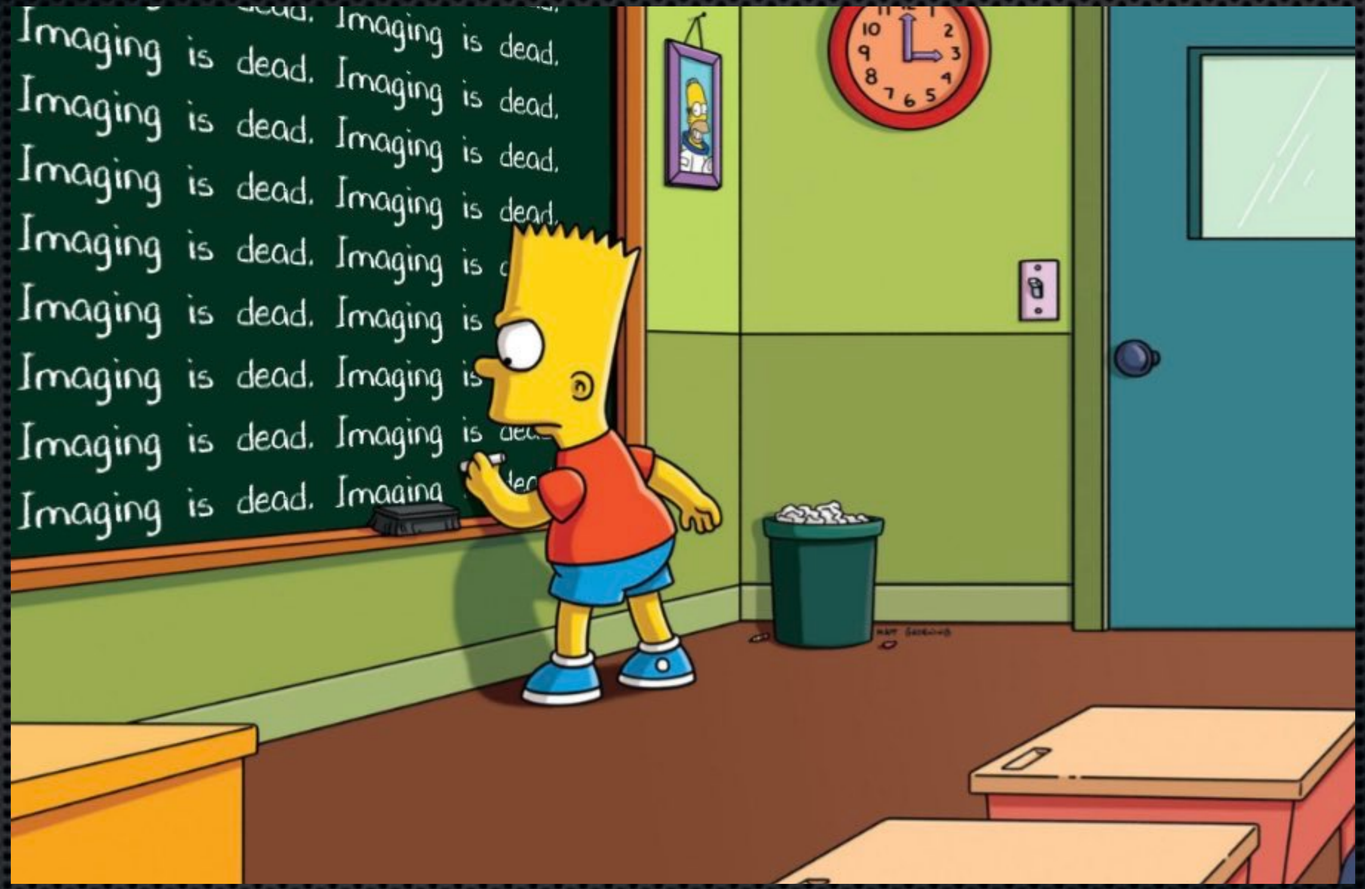
@roberthammen @hammen

Imaging Isn't Dead?

2019 MACADMINS CONFERENCE

@roberthammen @hammen

Meanwhile, at Apple Park…



2019 MACADMINS CONFERENCE

@roberthammen @hammen

Waving the Green Flag

- Tom Bridge wrote a great blog post: https://tombridge.com/2019/06/04/waving-the-green-flag/
- Change can be good
- Time to get to work!

Questions?

Feedback: https://bit.ly/psumac2019-382

2019 MACADMINS CONFERENCE

@roberthammen @hammen

References

- https://developer.apple.com/documentation/macos_release_notes/macos_catalina_10_15_beta_3_release_notes
- https://medium.com/@hammen/significant-changes-in-macos-10-15-catalina-of-interest-to-mac-admins-fbc3865c055e
- https://mrmacintosh.com/macos-10-15-catalina-updated-index-of-need-to-know-changes-links/
- https://developer.apple.com/documentation/devicemanagement/extensiblesinglesignonkerberos/extensiondata
- https://macadmins.slack.com/archives/C066MCBT2/p1562790283096900?thread_ts=1562790283.096900

2019 MACADMINS CONFERENCE

@roberthammen @hammen