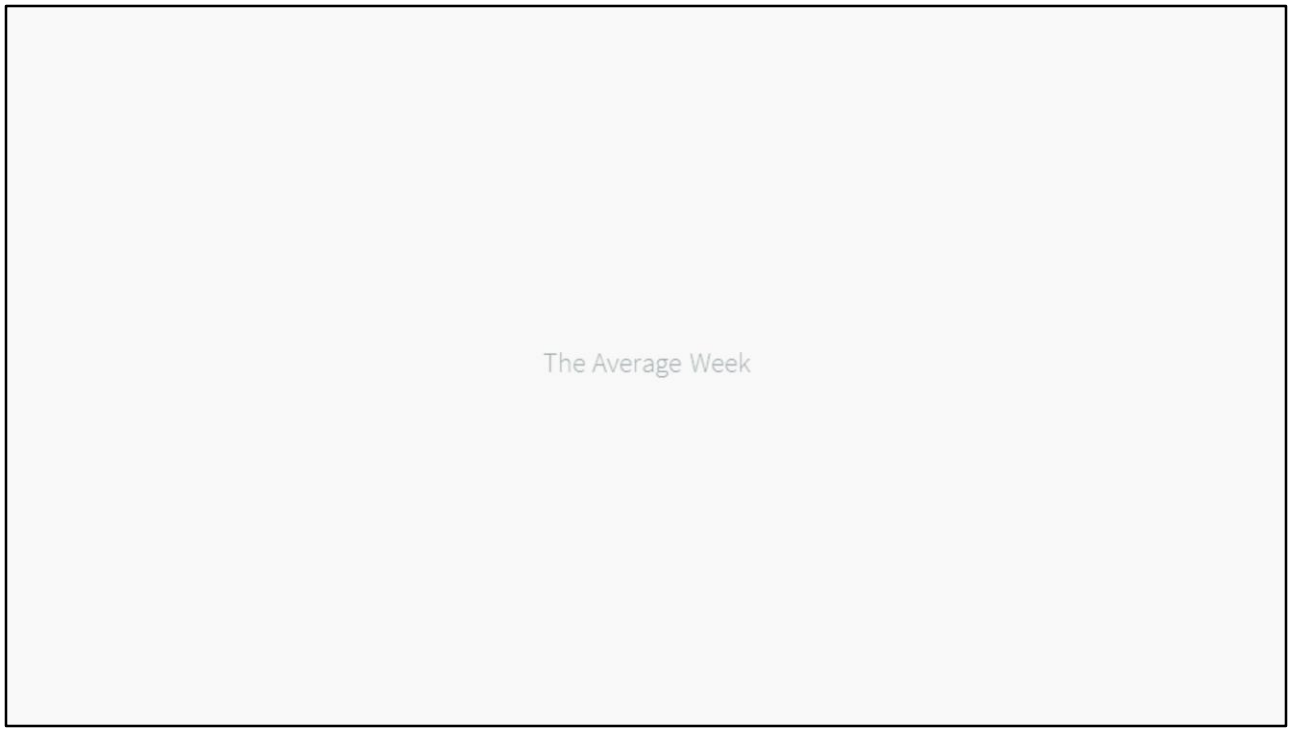
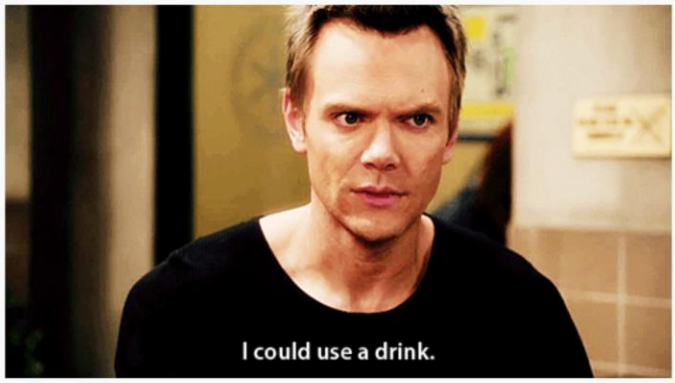
Death by .local

Or: How I became an Alcoholic


The Average Week

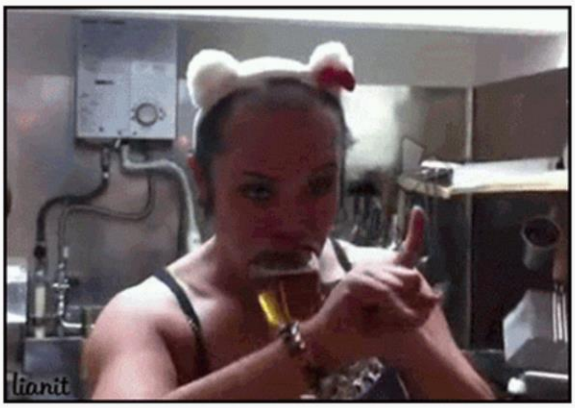
Monday



Tuesday

Wednesday

Thursday

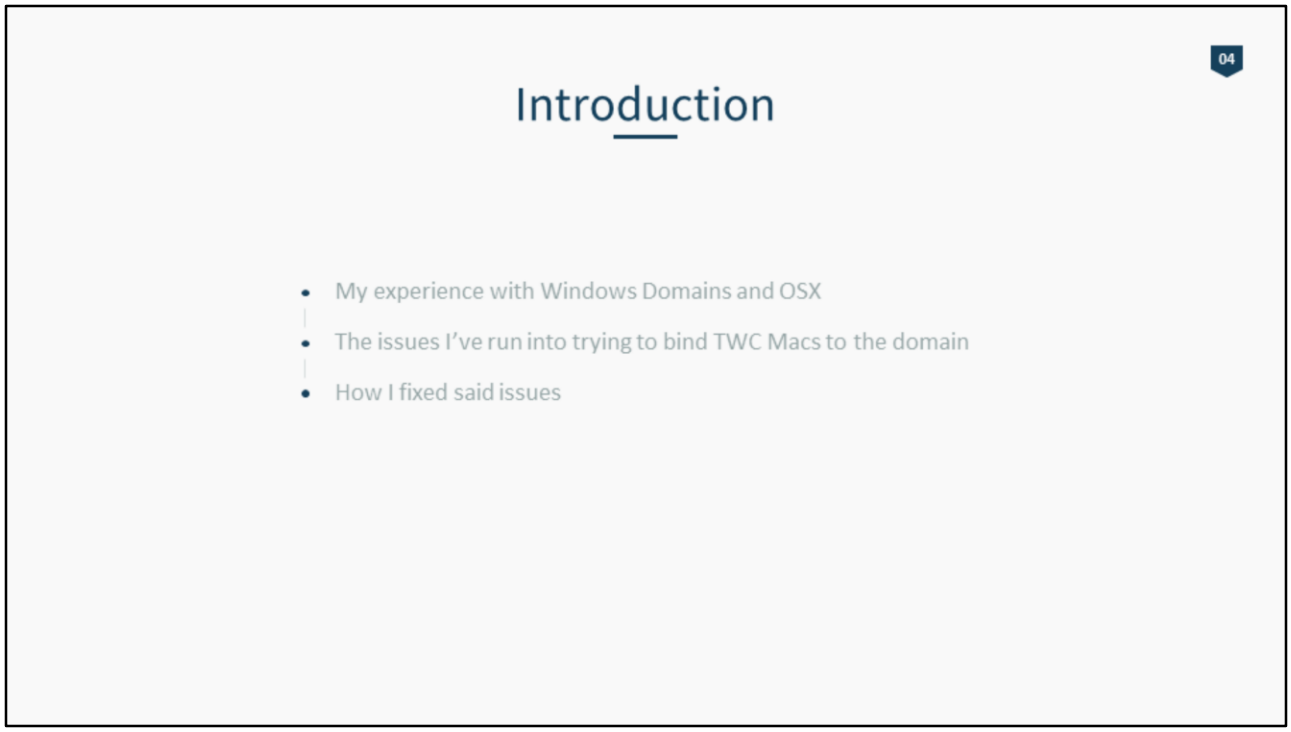

lianit

Agenda

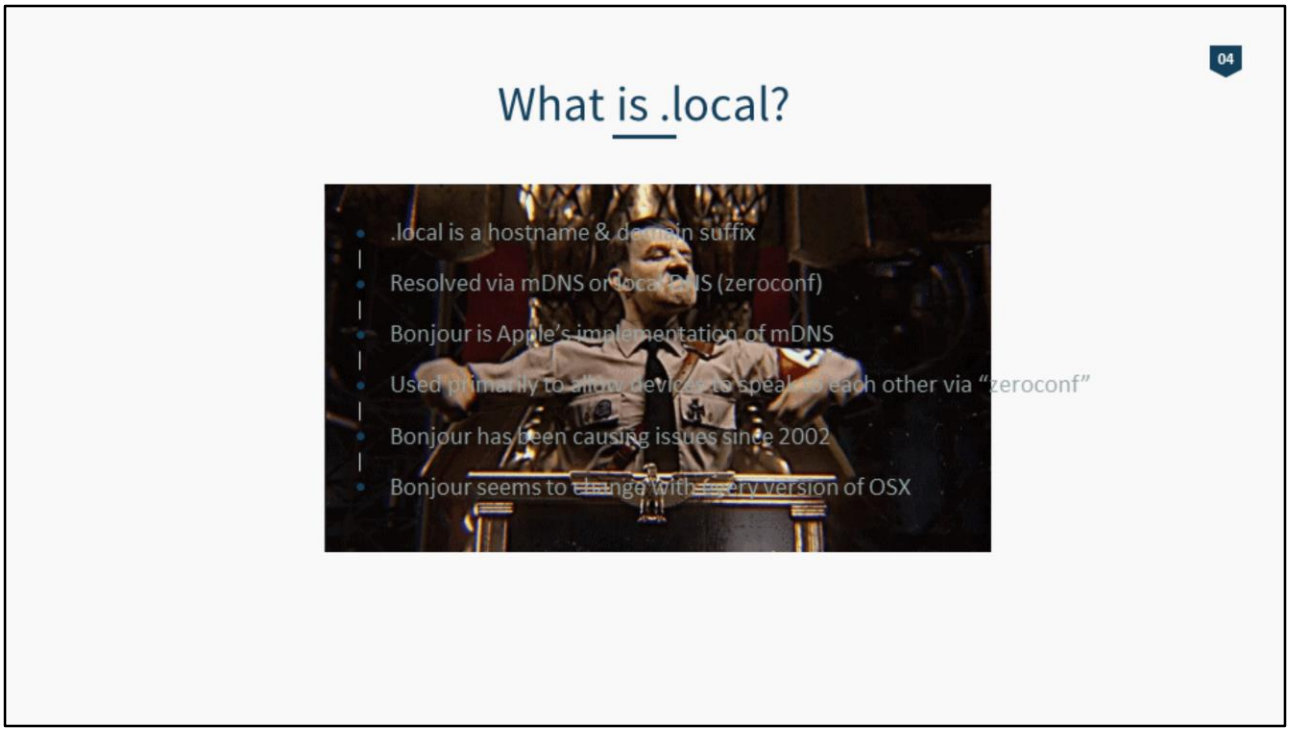
Otherwise known as "topics"

- Who am I?
- Introduction
- What is .local?
- Why is .local so bad?
- The real issue...
- MacGyver time!
- Issues + The Future

Multichannel Retailer selling bedding, towels, clothing, kid stuff (the huge bear is called Ralph) and home stuff for making your outside area look like that



5 years of doing Mac support in Windows environments
3 of those being a 1st line newb deleting plists, resetting keychains etc



Literally hitler

.local only on private networks

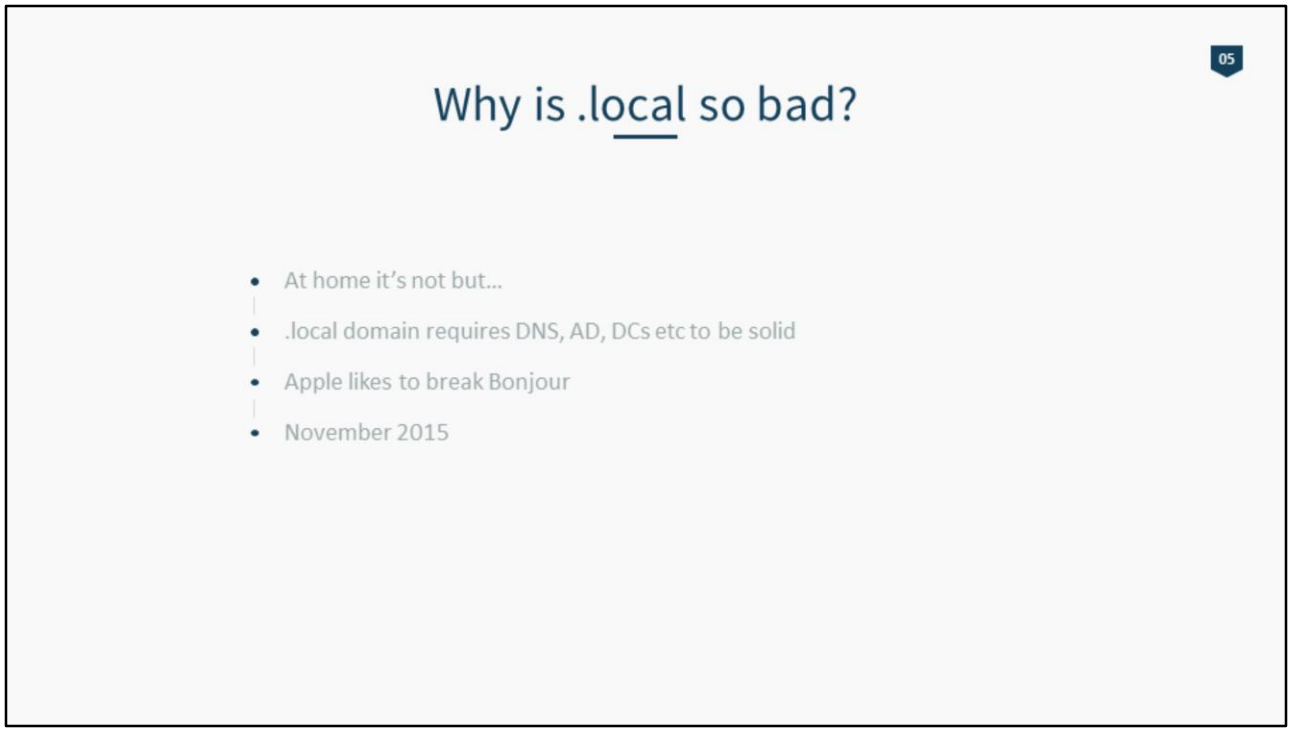
Each computer knows its own name and responds to requests for that name automatically via IP multicast which is cool for home.

But it means no DNS/DHCP server(s) required; doesn't work in an Enterprise; come onto that later.

Bonjour is on OSX and iOS out of the box; some printers use it, can install an agent on Windows

Caused issues in 2002 by being called Rendezvous and Apple had a lawsuit filed against it (in 2003).

From the documentation I can find on Apple.com, they have changed how Bonjour works every version from 10.4 onwards (all host names that ended with .local were resolved by default with mDNS needed to be added to search domain, 10.5 added hostnames containing two or more labels are resolved using server but changes may have needed to be added to search list, 10.6 worked fine as long as you had a functioning DNS server. mDNSresponder swapped with discoveryd



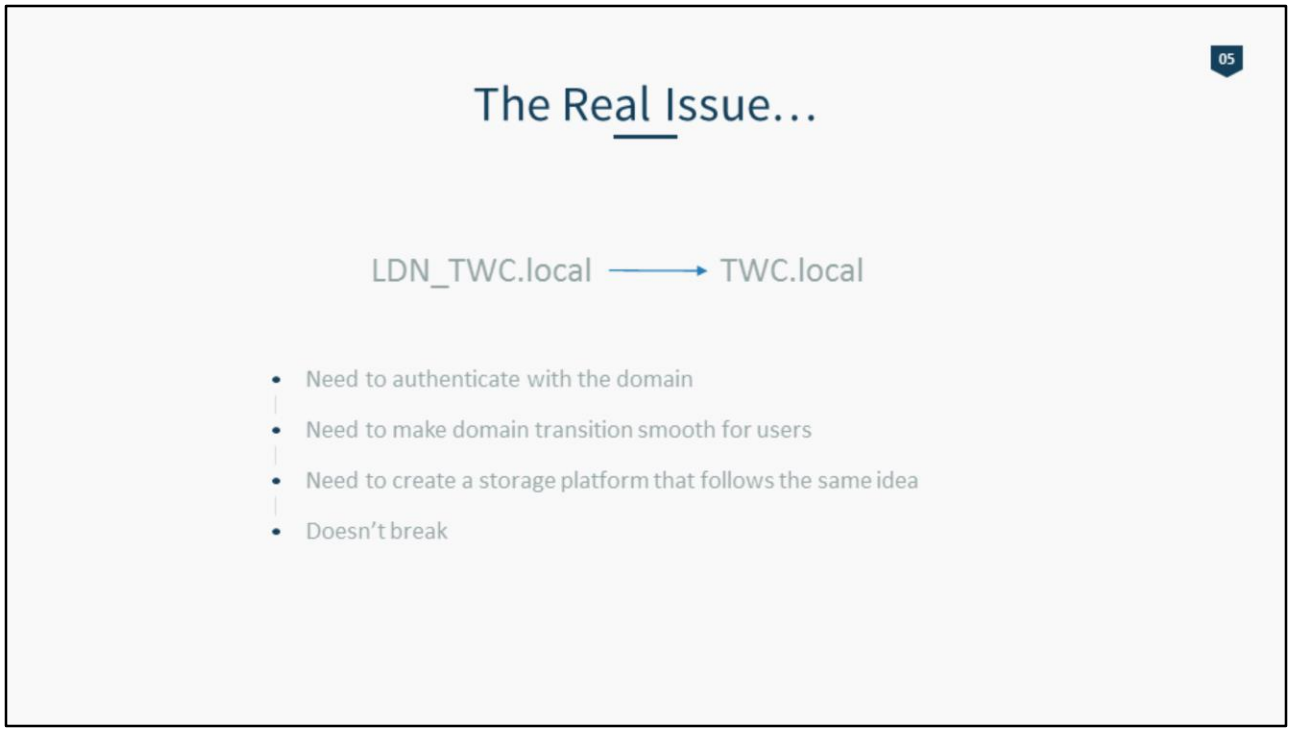
Additionally, Mac OS X v10.6 automatically detects when the local network operator has set up a name server that will answer name requests for a domain ending in ".local". It does this by checking to see if there is a Start Of Authority (SOA) record for the top level domain "local", which is how a DNS server indicates that it claims to have authority over a part of the DNS namespace. As long as the DNS server is properly configured with the required SOA record, Mac OS X v10.6 will detect this SOA record and automatically use this server to look up all host names in the domain.

1st November 2015 is when Certificate Authorities stop issuing certificates for .local and all CA issued .local certificates will at the latest expire on that date.

Although the underscore character is valid in hostnames, it is not a valid component in a DNS domain name. If the Active Directory domain being bound to contains an underscore in the domain name, binding and services will not function as expected (i.e. it won't bind).

RFC1123 from 1989 states as much but I suspect the domain was created in the Windows 2000 days where underscore was allowed.


TRON
FUCK YOU



Small project to get Macs managed properly

Needed to allow users to log into their Mac using domain credentials rather than having a different password for local login and server login

We can't bind to LDN_TWC.local using the Apple AD plugin; and the Apple AD plugin doesn't support cross domain trust relationships so we can't put them on the new domain

New storage platform as part of that project
New servers are being bound to TWC.local so needs to support cross domain trust

Centrify plugin allows binding to an underscore

It supports cross domain trust relationships so we can authenticate against TWC for the storage server

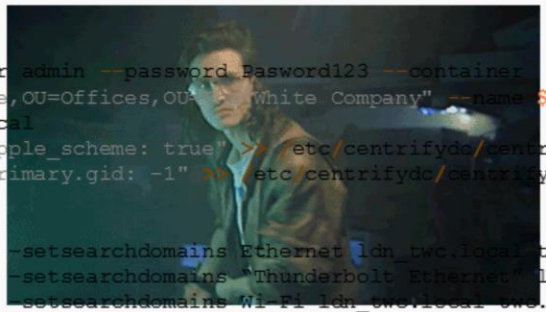
We can script it

And it's is free

Thanks to Greg Neagle for the suggestion; I think he just wanted to shut me up

05

MacGyver Time!



```
#!/bin/sh
/usr/sbin/adjoin --user admin --password Password123 --container
"OU=Macs,OU=Head_Office,OU=Offices,OU=[illegible] White Company" --name $DS_HOSTNAME --
workstation LDN_TWC.local
echo -e "auto.schema.apple_scheme: true" >> /etc/centrifydc/centrifydc.conf
echo -e "auto.schema.primary.gid: -1" >> /etc/centrifydc/centrifydc.conf
/usr/sbin/adreload
/usr/sbin/adflush
/usr/sbin/networksetup -setsearchdomains Ethernet ldn_twc.local twc.local
/usr/sbin/networksetup -setsearchdomains "Thunderbolt Ethernet" ldn_twc.local twc.local
/usr/sbin/networksetup -setsearchdomains Wi-Fi ldn_twc.local twc.local
```

Script we used in binding via deploystudio

This will tell the Centrify agent to use the same UID generation algorithm as the Apple plugin (Rather than use the traditional Centrify method of calculating it off of the user's SID).
This way your existing AD users can continue logging into their Mac systems without any further configuration needed when we swap from Centrify to Apple AD.

Networksetup to add domain to search domains (we don't have local set as a SOA).

Bound the Mac server doing the sharing to ldn_twc.local or twc.local, and the SMB service just crashes and requires a restart. Confirmed issue with Centrify, but using Express so it would have to be a forum post.
Setup temporarily a single user with access to the storage – bad but best we can do in short term
Users don't understand the keychain despite documentation being sent their way; so ADPassMon to the rescue: https://yourmacguy.wordpress.com/adpassmon/
Windows computers couldn't connect to the mac server; we had a over eager GPO setup to restrict NTLM authentication types for the Computer OU in AD; created a new OU and moved all PCs that needed access to the server to that OU (temporary while we move domains and create new GPOs for the new domain).
Centrify has a line in its conf that controls password expiry, if the AD account has password never expire enabled then it will ask to update the password and then muck up the keychain by updating network passwords. Fixed by disabling that setting for all users

Plans for Mac environment at TWC
Script the adleave and join process to join twc.local
Figure out a way to script UID using dscl or whether it's better just to create new accounts
Install ESXi on the Mac Pro we have as the server; install drivers needed for the Pegasus RAID boxes to work with ESXi and then migrate all the things to linux/docker
Make software install hands off with Salt + ServiceNow i.e. User requests software on ServiceNow, ServiceNow uses Salt to add the software to their manifest and then tell Munki to update on the Mac

Feel free to say hi!

We are friendly and social (and spam /giphy).

macadmins.org

Also who uses IRC anymore?

05

Resources

- Centrify Express http://www.centrify.com/express/
- Kung Fury https://www.youtube.com/watch?v=bS5P_LAqiVg
- IRC ##osx-server on irc.freenode.net
- ADPassMon https://yourmacguy.wordpress.com/adpassmon/