AD Integration & Home Folders

2015
MACADMINS
CONFERENCE
AT PENN STATE

David Acland

Technical Director at Amsys

@davidacland

Amsys

2015 MACADMINS CONFERENCE AT PENN STATE

ACSE

Training

Projects & Support

What the heck's AD?

AD… mastered!

Uh-oh

Amsys

2015 MACADMINS CONFERENCE AT PENN STATE

What I'll be talking about

- AD Integration
  - Troubleshooting
  - Tweaks
  - Scripting
- Home folders
  - Mounting options
  - Finder integration
  - Troubleshooting
  - Syncing
  - Other options

Integrating with Active Directory

Amsys

2015 MACADMINS CONFERENCE
AT PENN STATE

Objectives

- Login Window Authentication
- Certificate enrollment
- Single username & password for services

Getting Connected

- GUI
- Casper or DeployStudio directory bind
- Script
  - `dsconfigad -add domain.com -computer $computer -username aduser -password yourpw`
  - `-ou “CN=Computers,DC=domain,DC=com"`
- Third Party Tool
  - Centrify Express

What if you can’t connect?

Amsys

2015 MACADMINS CONFERENCE
AT PENN STATE

Troubleshooting

Client

- Are other Macs affected?
- Was this Mac previously working?

Network

- Where is the affected device?
- Should it work from that location?
- Try from a known working location / port / switch

Server

- No devices can communicate with DC
- Can other Macs write to that OU using that username & password?

Troubleshooting

- Has this configuration ever worked?
- Get back to a minimal system to establish a baseline

What Causes It To Break?

- AD Permissions
- DNS
- Service Reachability
- Date & Time
- Computer Name Length
- Corrupt client files
- opendirectoryd

Troubleshooting

- Client?
  - Check DNS
    - `host -t SRV _ldap._tcp.yourdomain.com`
  - Check the clock
  - Check what DC the client is using
    - /Library/Preferences/OpenDirectory/DynamicData/Active Directory/DOMAIN.plist
  - Delete any local files from previous bindings
    - /Library/Preferences/OpenDirectory
  - Set a preferred DC
    - `dsconfigad -preferred dc01.domain.com`

Troubleshooting

- Network?
  - Check port reachability
    - `nc -z dc01.domain.com 389`
  - Firewall
  - Rule out physical issues

Troubleshooting

- Server?
  - Usually someone else
  - Handover as much useful information as possible
  - Test with a domain admin account
  - Test with a pre-created computer object
  - Test writing to a different OU (or default Computers container)

Great, we're connected, but there are some issues…

Troubleshooting

Issues after binding

- Slow logons
- Failed reconnects
- Computers “dropping off the domain”
- Macs crashing 50% through boot up

dsconfigad Advanced Options

```
-sharepoint disable
-useuncpath disable
-passinterval 0
-mobile enable
-mobileconfirm disable
-force
```

e.g. `dsconfigad -force -sharepoint disable -passinterval 0 -mobile enable -mobileconfirm disable`

Amsys

Slow Logons

- Restrict scope of search to specified domain
  - `dsconfigad -alldomains disable`
  - `dscl /Search -delete / CSPSearchPath "/Active Directory/YOURDOMAIN/All Domains”`
  - `dscl /Search/Contacts -delete / CSPSearchPath "/Active Directory/YOURDOMAIN/All Domains”`
  - `dscl /Search -create / SearchPolicy CSPSearchPath`
  - `dscl /Search -append / CSPSearchPath "/Active Directory/YOURDOMAIN/domain.com”`
  - `dscl /Search/Contacts -create / SearchPolicy CSPSearchPath`
  - `dscl /Search/Contacts -append / CSPSearchPath "/Active Directory/YOURDOMAIN/domain.com"`
- Specify a particular DC
  - `dsconfigad -preferred dc01.domain.com`
- Set timeout value
  - `defaults write /Library/Preferences/com.apple.loginwindow DSBindTimeout -int <seconds>`

Failed Reconnects

- For classrooms, shutdown at night, only put display to sleep during the day

- Mac wakes from sleep and doesn't reconnect to the DC
  - Reboot
  - Restart opendirectoryd
    - `sudo killall opendirectoryd`
  - Script kdestroy and ask user to re-enter password

- Mac fails to reconnect when returning to the office
  - `dsconfigad -passinterval 0`

Computers “dropping off” the domain

- Don’t trust `dsconfigad -show`

- Add a “self-heal” script or policy to the Mac
  - Check client is on the right network
  - Check DC is available
  - Check client can read its own computer object
  - Retry in 2 mins if it fails
  - 2nd failure triggers a re-bind

- Check with Windows administrator

Macs crashing 50% through bootup

- After a crash, a hard reboot, or just when it feels like it
- Affects 10.10.0 - 10.10.2
- `/usr/sbin/BootCacheControl jettison` *(triggered by /etc/rc.server)*
- Update to 10.10.3

.local

- Expect issues!
- Add .local to your search domains
- Lower the mDNS timeout
  - `defaults write /System/Library/SystemConfiguration/IPMonitor.bundle/Contents/Info mdns_timeout -int 1`

Stress Testing

Use ARD to login multiple Macs at once…

```
osascript -e 'tell application "System Events" to keystroke "username"' \
osascript -e 'tell application "System Events" to keystroke tab' \
osascript -e 'tell application "System Events" to delay 0.5' \
osascript -e 'tell application "System Events" to keystroke "password"' \
osascript -e 'tell application "System Events" to keystroke return'
```

Home Folders

Amsys

2015 MACADMINS CONFERENCE
AT PENN STATE

What is a home folder?

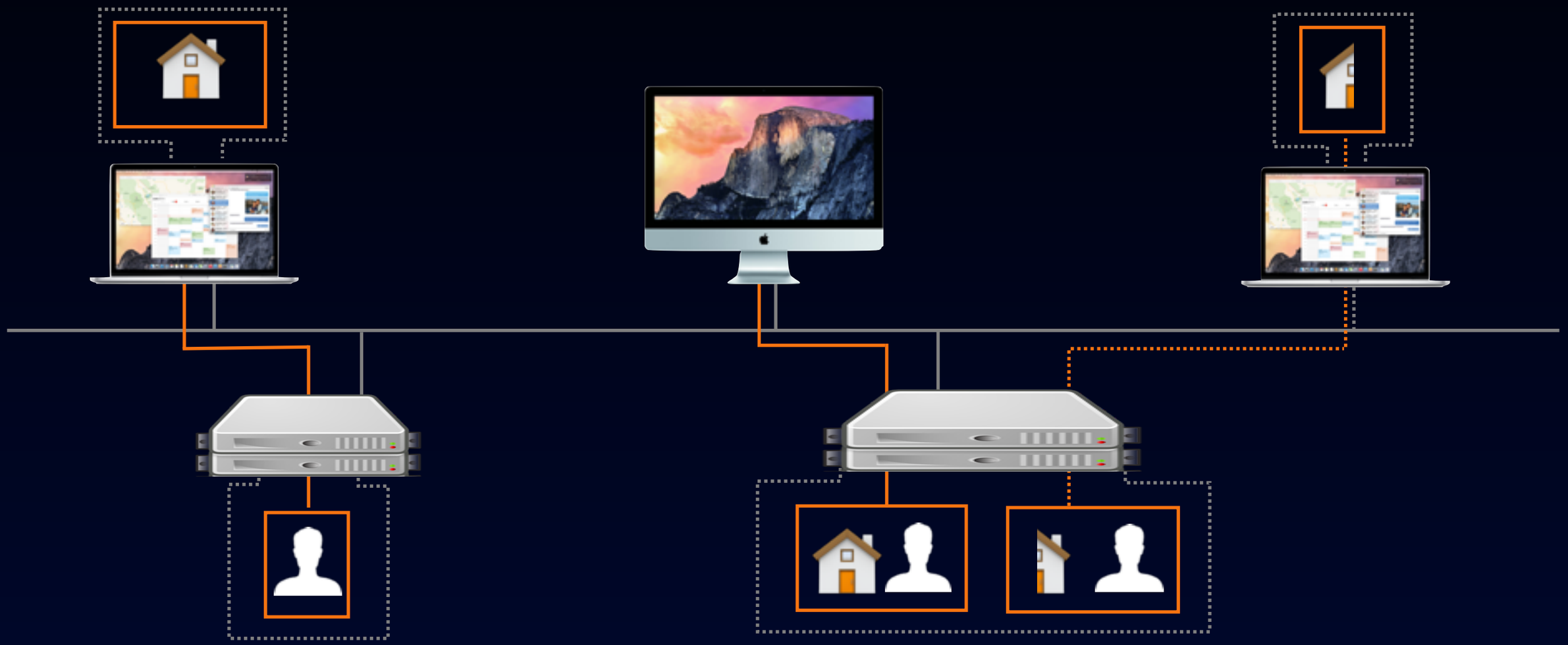
- Data store
- User level settings and resources

Types

Local Home

Full Network Home

Split / Re-directed Home Folder

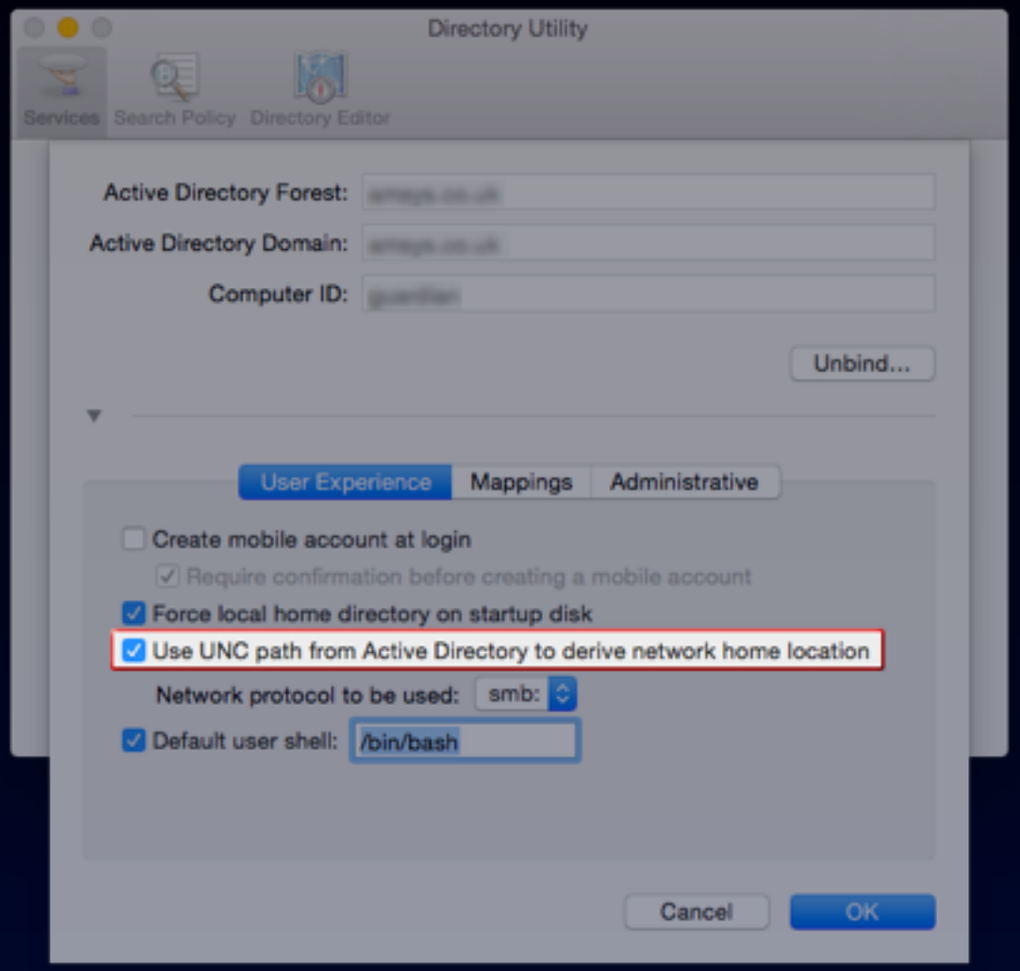


Objectives

- Providing personal network storage for the users
- Backing up user data
- Hot-desking

Mounting Options

- Use UNC path (SMBHome)
- Mounts top-level share
- Tries to add shortcut to the Dock
- Causes a lot of logon failures

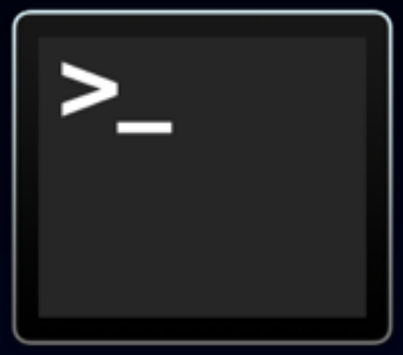


Amsys

2015 MACADMINS CONFERENCE AT PENN STATE

Mounting Options

- Logon Script
- User initiated script
- Directory Automount



Script to mount the network home

- Determine the user's network home folder path

```
ShortDomainName=$(dscl /Active\ Directory/ -read . | grep SubNodes | \
sed 's|SubNodes: ||g’)

adHome=$(dscl /Active\ Directory/$ShortDomainName/All\ Domains -read \
/Users/$USER SMBHome | sed 's|SMBHome:||g' | sed 's/^[\\]*//' | \
sed 's:\\:/:g' | sed 's/ \/\///g' | tr -d '\n' | sed 's/ /%20/g’)
```

`sed ‘s|SMBHome:||g'` – Strip off the “SMBHome: “ part of the string
`sed ’s/^[\\]*//'` - Remove the first two backslashes
`sed ’s:\\:/:g'` - Turn any remaining backslashes into forward slashes
`tr –d ‘\n'` - Remove a carraige return if the path is wrapped onto two lines
`sed 's/ /%20/g’` - Replace a space with %20 if its found in the path

Script to mount the network home

- Check the attribute has a value

```
case "$adHome" in
 "" )
    echo "ERROR: ${USER}'s SMBHome attribute does not have a value
set.  Exiting script."
    exit 1  ;;
 * )
    echo "Active Directory users SMBHome attribute identified as
$adHome"
    ;;
esac
```

Script to mount the network home

- Mount the home value

```
# Mount the network home
    mount_script=`/usr/bin/osascript > /dev/null << EOT
    tell application "Finder"
    activate
    mount volume "smb://${adHome}"
    end tell
EOT`
```

Interacting with the Finder

- Adding to the Dock

```
dockutil --add $SMBHome --label 'Network Docs' --position beginning – \
no-restart /Users/$USER
```

- Adding to the Sidebar

```
changeSidebarListsCasper.py --first /Volumes/$USER

 - first
 - last
 - after
```

Syncing

- Goals
  - Hot-desking
  - Centralised backups
- Do the users really need it?
- Cost

OS X Home Sync

- Why don’t we use it?
  - 2 way sync
  - Unreliable
  - No central reporting

Rsync?

- We use Rsync
  - We're in full control of what gets synced and when
  - We can have a central reporting system for failures
  - We can adjust and develop it over time
- We have spent a number of years refining the scripts
- Error capturing and handling is very important

Core components

- Check capacity and amount to copy before syncing
  - `dataSize$(rsync -n source destination) | grep "total size" | awk '{ print $4; }' | sed 's/M//g' | awk '{printf("%d\n",$1 + 0.5)}'`
  - `networkhomecapacity=$(df -hm $syncDest | awk 'NR==2 {print $4}’)`
  - `if [ $syncsize -lt $networkhomecapacity ]; then…`
- Loop through sub-folders to get more granular logging
  - `ls $syncSource | grep "[A-z 0-9]" | head -$counter | tail -1`
- Use a filter file
  - `--filter='merge /path/to/exclusionfile/syncup_filter_exclude'`

Core components

- Capture errors in a temp file
  - `rsync command 2>> /tmp/${USER}syncerror`

- Email issues to IT
  - `sendMail -f $fromAddress -t $toAddress -u $subject -m "$message" -s $mailServer -xu $username -xp $password`

- Other rsync options
  - `# u - Skip files that are newer on the receiver`
  - `# z - Compress file data during the transfer`
  - `# r - Recurse into directories`
  - `# l - Copy symlinks as symlinks`
  - `# v - Increase verbosity`

When do we run it?

- Every 15 minutes while logged in
- At logout

User Trigger

- Applescript saved as an application
  - `set myScript to POSIX path of (path to resource "LogoutSync.sh")`
  - `do shell script myScript`
- Lets user run the script when they want

Thanks

https://github.com/amsysuk/psu