Troubleshooting Directory Services

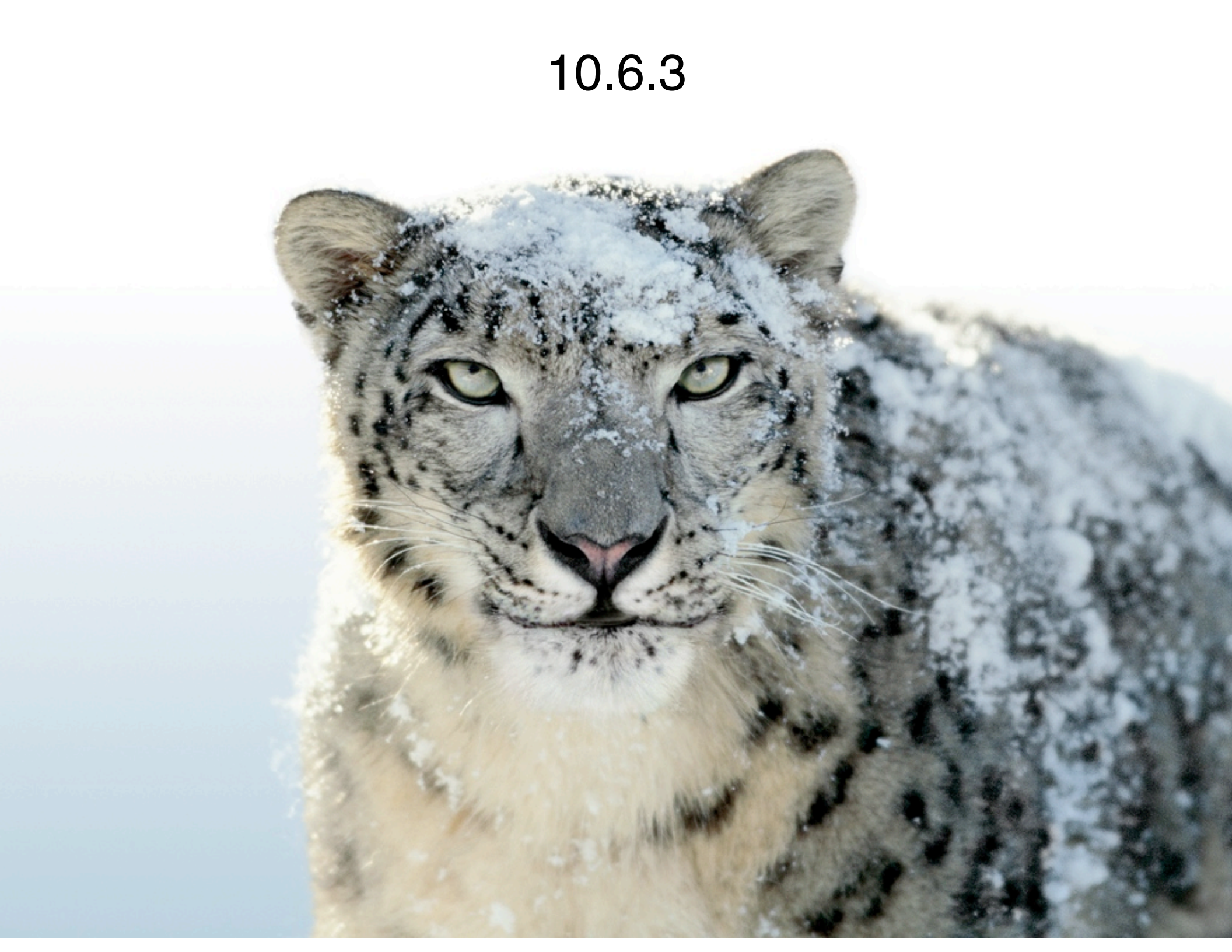
arek@arekdreyer.com

MacSysAdmin 2010

Careful Examination of Before and After

10.6.0

10.6.3



DS Troubleshooting

- Login process
- Logs
- Client Management focus
- Resources
- Changing Server hostname, IP

Logging In

- Identification
- Authentication
- Authorization
- (and client management)

Headshake Headache

- Likely reasons
  - Can't identify
  - Can't authenticate
  - Can't mount home folder
  - ACL disallows login

Login as local admin

- Verify
  - ID
  - Authenticate
  - Mount Home Folder

Identification

- `id username`

Authentication

- `dscl /Search -authonly \`
  `aduser01 thepass`
- No feedback = good password

Authorization

- Go > Connect to Server
  - try to mount home folder
- Automount could be problematic

Login with >console

- Immediate feedback if
  - can't identify
  - can't authenticate
- Network Home Folder error
- Logout

/etc/authorization

- See system.login.console

Terminal — vim — 90×31

```
                        <key>group</key>
                        <string>admin</string>
                        <key>shared</key>
                        <true/>
                        <key>timeout</key>
                        <integer>30</integer>
                </dict>
                <key>system.login.console</key>
                <dict>
                        <key>class</key>
                        <string>evaluate-mechanisms</string>
                        <key>comment</key>
                        <string>Login mechanism based rule.  Not for general use, yet.</st
ring>
                        <key>mechanisms</key>
                        <array>
                                <string>builtin:smartcard-sniffer,privileged</string>
                                <string>loginwindow:login</string>
                                <string>builtin:reset-password,privileged</string>
                                <string>builtin:auto-login,privileged</string>
                                <string>builtin:authenticate,privileged</string>
                                <string>loginwindow:success</string>
                                <string>HomeDirMechanism:login,privileged</string>
                                <string>HomeDirMechanism:status</string>
                                <string>MCXMechanism:login</string>
                                <string>loginwindow:done</string>
                        </array>
                </dict>
                <key>system.login.done</key>
                <dict>
"/private/etc/authorization" [readonly] line 846 of 1255 --67%-- col 4-32
```

Detect Smartcard

- `builtin:smartcard-sniffer,privileged`

Display Login Window

- `loginwindow:login`

PW Change Required?

- `builtin:reset-password,privileged`

Check for Autologin

- `builtin:auto-login,privileged`

Perform Authentication

- builtin:authenticate,privileged

Display progressbar

- `loginwindow:success`

Mount Home

- `HomeDirMechanism:login,privileged`

Update Progressbar

- `HomeDirMechanism:status`

MCX Dialogs

- `MCXMechanism:login`
  - Unlock filevault
  - Home folder sync

Dismiss Login Window

- `loginwindow:done`

Terminal — vim — 90×31

```
                        <key>group</key>
                        <string>admin</string>
                        <key>shared</key>
                        <true/>
                        <key>timeout</key>
                        <integer>30</integer>
                </dict>
                <key>system.login.console</key>
                <dict>
                        <key>class</key>
                        <string>evaluate-mechanisms</string>
                        <key>comment</key>
                        <string>Login mechanism based rule.  Not for general use, yet.</st
ring>
                        <key>mechanisms</key>
                        <array>
                                <string>builtin:smartcard-sniffer,privileged</string>
                                <string>loginwindow:login</string>
                                <string>builtin:reset-password,privileged</string>
                                <string>builtin:auto-login,privileged</string>
                                <string>builtin:authenticate,privileged</string>
                                <string>loginwindow:success</string>
                                <string>HomeDirMechanism:login,privileged</string>
                                <string>HomeDirMechanism:status</string>
                                <string>MCXMechanism:login</string>
                                <string>loginwindow:done</string>
                        </array>
                </dict>
                <key>system.login.done</key>
                <dict>
"/private/etc/authorization" [readonly] line 846 of 1255 --67%-- col 4-32
```

Moving On

- Looked at login process
- Next up: logs

PAM

- Pluggable Authentication Method
- /etc/pam.d

Using Logs

- syslog
- DirectoryService
- PasswordServer
- Kerberos
- MCX

Remote Monitoring

- SSH to client as admin user
- Watch logs
- Attempt login

syslog

- syslog -w
  - -w waits for syslog information
- sudo syslog -c 0 -d
  - log everything: Emergency to Debug
- syslog -c 0
  - check filter mask

DirectoryService

- USR1
- USR2

USR1

- `sudo killall –USR1 DirectoryService`
- toggles Debug Logging
- to /Library/Logs/DirectoryService/DirectoryService.debug.log

Deciphering USR1

- Compare against known good system

Filtering USR1

- Sample filter terms
  - "tory:" for "Active Directory:"
  - error
  - fail
  - get

Even More Details

- ```
  sudo defaults write /Library\
  /Preferences/DirectoryService\
  DirectoryServiceDebug   \
  "Debug Logging Priority Level" \
  -integer 7
  ```
  ```

Log at Boot

- `sudo touch \`
  `/Library/Preferences\`
  `/DirectoryService/.DSLogDebugAtStart`

sions
Why am I seeing S...
"Insufficient Pri...
Changing account ...
Item from another...
Which screensaver...

To set the Directory Service Debug Log Level to a higher level, open Terminal and execute the following command:

```
sudo defaults write /Library/Preferences/DirectoryService/DirectoryServiceDebug "Debug Logging Priority Level" -integer 7
```

To enable Directory Service logging manually (after log in), open Terminal and execute the following command:

```
sudo killall -USR1 DirectoryService
```

To enable Directory Service logging at restart, open Terminal and run the following command, followed by a restart of the machine:

```
sudo touch /Library/Preferences/DirectoryService/.DSLogDebugAtStart
```

To disable Directory Service logging, open Terminal and execute the following command:

```
sudo killall -USR1 DirectoryService
```

Note: If you enabled Directory Service logging on restart, delete the .DSLogDebugAtStart file from /Library/Preferences/DirectoryService so that Directory Service Debug Logging remains off should the machine be restarted.

The logs are saved to /Library/Logs/DirectoryService.

Additional Information

This logging is very verbose and should be disabled once troubleshooting is complete.

Rate this article: • • • • •

USR2

- `sudo killall -USR2 DirectoryService`
- API Logging
- toggles, default only 5 minutes

PasswordServer

- /Libary/Logs/ApplePasswordService/ApplePasswordServer.Server.log

Kerberos

- /var/log/krb5kdc
  - kadmin.log
  - kdc.log

MCX

- # defaults write /Library\
  /Preferences/com.apple.MCXDebug \
  debugOutput -2
- # chmod 666 /Library/Preferences\
  /com.apple.MCXDebug.plist
- # mkdir /Library/Logs/ManagedClient
- ManagedClient.log

Logs May Lie

- Example: SACL prevents SSH login
- secure.log:
  - `PAM: user account has expired`
- PasswordServer.Server.log:
  - `AUTH2:... succeeded`

Enough About Logs

- They'll rotate themselves
- Or keep collecting
- Next up: client management

Client Management

- When to Manage
- Management not honored

When to Manage

- Never
- Once
- Often
- Always

Never

- Really "Not at this level"
- Could easily be managed at another level

Once

- Timestamp
- Who changed setting last
  - directory record
  - user preference
- ~/Library/Managed Preferences

Often

- User can change for that session
- Reapplied at every login

Always

- Some things don't like Always
- /Library/Managed Preferences

Management Fail

- Marczark/Neagle book
  - Preferences not delivered?
  - Management not applied?

Not Delivered

- User
- Computer
- Computer Group
- Workgroup

Collecting MCX Info

- `mcxquery`
- `system_profiler`

mcxquery

- Terminal disallowed?
  - `mcxquery -user oduser01`
  - `mcxquery -user aduser01 -a`
- Doesn't composite Group information

system_profiler

- System Profiler from Apple Menu
- `system_profiler \ SPManagedClientDataType`
- Doesn't show Once sometimes

Delivered, Not Applied

- 3rd Party often best in Often
- Manager misunderstanding
- Bug?

Edge Cases

- Precreate home folder

Precreate Home Folder

- ```
  /System/Library/CoreServices\
  /ManagedClient.app/Contents\
  /Resources/createmobileaccount \
  -n tycho
  ```
  ```

Resources

- PDFs
- Books
- Videos
- Mailing Lists
- Web sites

PDFs

- images.apple.com/education/docs/Apple-ClientManagementWhitePaper.pdf
- http://images.apple.com/server/macosx/docs/L414857A-US_Local_Mgmt_Policy_White_Paper-3.pdf

Books

- Marczak/Neagle
- Edge/Hunter/Smith
- Apple Global Training

Videos

- www.apple.com/education/resources/information-technology.html

Mailing Lists

- MacEnterprise
- macos-x-server@lists.apple.com
- client-management@lists.apple.com

Web Sites

- afp548.com
- managingosx.wordpress.com
- Apple seminars

e.g

slot 0030: 0x4ac623546b8b4567000000230000001e _ldap_replicator 08/24/2010 01:17:09 PM

take the slot ID and the public key of the PWS (obtained by mkpassdb -key) and create the authenticationauthority string:

;ApplePasswordServer;0x4ac623546b8b4567000000230000001e,1024 35
1424571524061015083254016898004018289433991726500019224615493370856703081327
6226897752766650691756598860902321907564695824527912007153587565048650628852 2
6514894451255042732996739115447865361316899537697684684807336900223985208473 5
4010048390708840563818714291710166642934368167661989117255168588055389886409 7
43 root@server.example.com:192.168.2.254

Pop that into the AuthenticationAuthority section using the inspector in WGM

```
slapconfig -stopldapserver
slapconfig -startldapserver
```

on both the master and replica
and then monitor the slapd.log on both to see if the error persists. Check replication by creating a new user on the master, deleting a user on the master and editing a user on the master. All actions should immediately propagate to the replica(s)

Stu

Profile Email Quote

aread

Wednesday, August 25 2010 @ 10:20 pm MDT

Status: offline
Registered: 06/16/09
Posts: 2

Thanks very much for the response. Your directions were almost correct for us. Instead of making the _ldap_replicator user on the master and then copying the password to the slapd config file, I had to set up the replica and then use the password from the config file to create the user. Doing it the way Stu suggested resulted in the _ldap_replicator user not authenticating.

Thanks for the help,

Adam

Profile Email Website Quote

Managing OS X

Trials and Tribulations of an OS X Administrator

« Time Machine MenuExtra management MCX, dslocal, and the Guest account »

Managing Office 2008

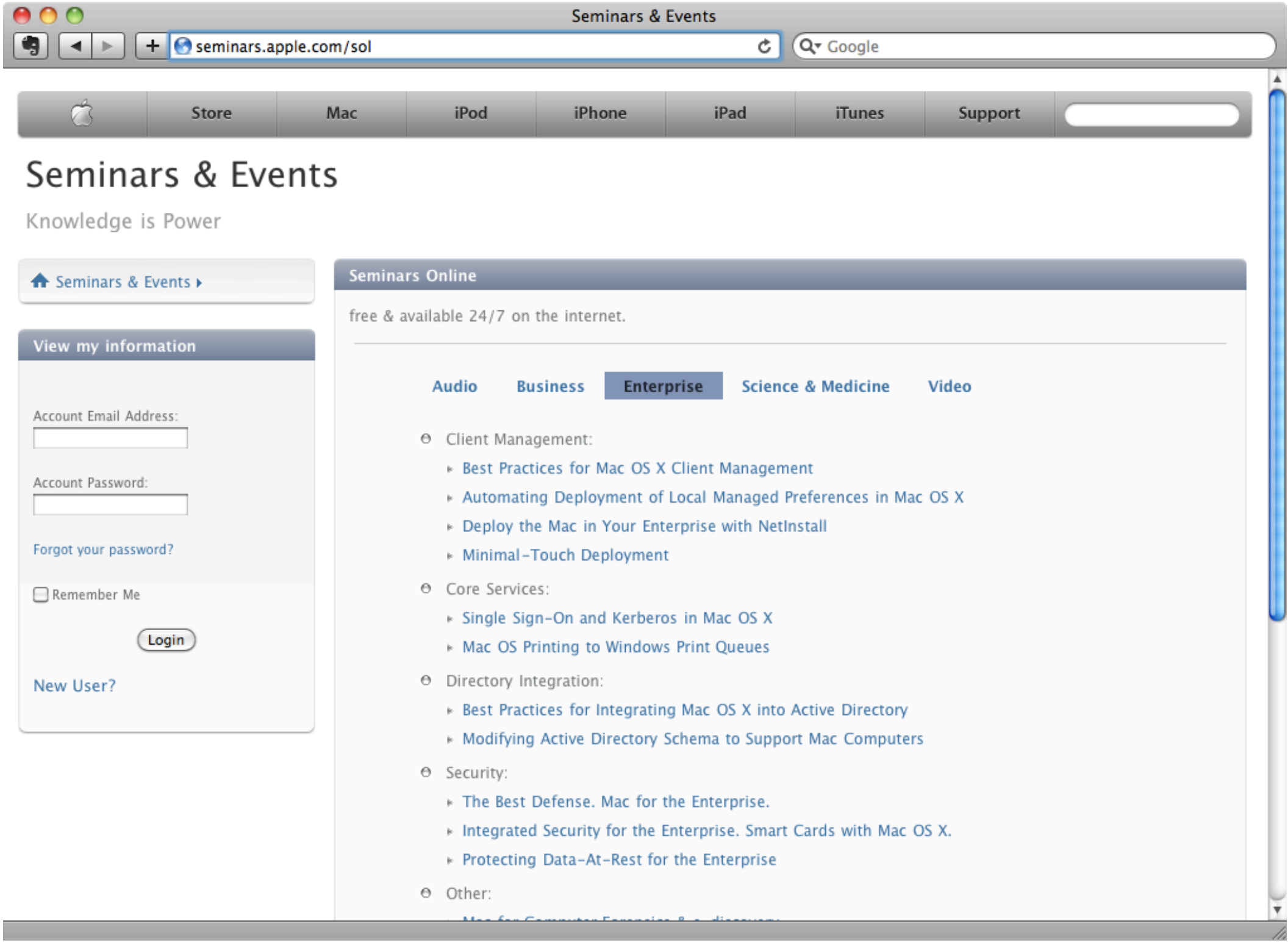
If you are thinking about deploying Microsoft Office 2008 in your environment, there are some preferences you should consider managing.

Microsoft has provided a high-level overview here. But it's short on details. Here's a few...

Many of the Office 2008 applications now use plist files to store their preferences. (A major exception is Entourage, which still stores a lots of its preferences in the monolithic Entourage Database.) Plist files mean we can use Workgroup Manager/MCX to manage many preferences.

Here's what I wanted to manage:

1. Set Microsoft AutoUpdate to check only manually.
2. Turn off the Office Setup Assistant.
3. Set the default save format for Word, Excel and PowerPoint to the Office 97-2004 format (as opposed to the new XML-based formats


Seminars & Events
seminars.apple.com/sol
Google
Store
Mac
iPod
iPhone
iPad
iTunes
Support
Seminars & Events
Knowledge is Power
Seminars & Events ▸
View my information
Account Email Address:
Account Password:
Forgot your password?
Remember Me
Login
New User?
Seminars Online
free & available 24/7 on the internet.
Audio
Business
Enterprise
Science & Medicine
Video
Client Management:
Best Practices for Mac OS X Client Management
Automating Deployment of Local Managed Preferences in Mac OS X
Deploy the Mac in Your Enterprise with NetInstall
Minimal-Touch Deployment
Core Services:
Single Sign-On and Kerberos in Mac OS X
Mac OS Printing to Windows Print Queues
Directory Integration:
Best Practices for Integrating Mac OS X into Active Directory
Modifying Active Directory Schema to Support Mac Computers
Security:
The Best Defense. Mac for the Enterprise.
Integrated Security for the Enterprise. Smart Cards with Mac OS X.
Protecting Data-At-Rest for the Enterprise
Other:

Server big changes

- `changeip`
- `changeDirData.pl`
- Notes on shortname, uid, GUID
- slapconfig -kerberize

change IP

- `# changeip`
- System Preferences > Network
- Reboot

changeDirData.pl

- Changes attributes
  - Great for changing server name
  - Won't change several attributes
- Only changes first instance of string
- Test before deploy!
- Notes: budurl.com/changedirdata

name, uid, GUID

- cannot import *user.name*
- Change shortname: delete/create user
  - POSIX uses uid (example: 1024)
- Preserve GUIDs for
  - SACLs
  - ACLs

Re-Kerberize

- Non-AD-integrated
  - `# slapconfig –kerberize`
- AD-integrated
  - unbind and rebind
  - `# dsconfigad –enablesso`

OD changes

- Decommissioning a replica
- http://docs.info.apple.com/article.html?path=ServerAdmin/10.6/en/od494c0a28.html
- Vestiges may still be around

DS Troubleshooting

- Login process
- Logs
- Client Management focus
- Resources
- Changing Server hostname, IP

Thanks

- Questions and Comments
- IM: arekd@me.com
- Email: arek@arekdreyer.com