Directory Services Integration with Third Party Directories

Utilizing methods to integrate Open Directory with other systems

Session M251
Macworld San Francisco 2005

Michael Bartosh

4AM-Media

Apple Certified Trainer, ACSA 10.3

Apple Certifications for 10.3.x

Course Names	Certification Level	Length (days)
Mac OS X Help Desk Essentials	ACHDS	3
Mac OS X Server Essentials	ACTC (with Help Desk Essentials)	4
System Administration of Mac OS X Clients	Apple Certified System Administrator	5 days each course
System Administration using Mac OS X Server		

train.apple.com • 800-848-6398

Open Directory II

Agenda

- AD Plug-In basics
- ADMitMac
- AD Plug-in vs. LDAPv3
- Troubleshooting

Panther: The Active Directory Plug-In

- Client-Side Features
  - Accesses AD like a PC would (machine account, kerberized LDAP)
  - HomeDirectory is mounted, but not used as home
  - UniqueID: derived from guid or specify an attribute
  - local caching of user (similar to other mobile accounts)
  - Map local administrators to AD group
  - Great Kerberos support! (just like a PC client)

Where is PDC?

- Samba PDC is a big step forward for Apple (but)
- Most sites have existing Windows infrastructures
- It doesn't support secure authentication (NTLMv2 or kerberos)
- There's already a large body of knowledge around maintaining it due to its open source roots.

Panther: The Active Directory Plug-In

- Architecture
  - /Library/Preferences/DirectoryService/ActiveDirectory.plist
    - Contains base64 Computer Pass
  - winbind.conf and ntlm_auth
  - dsadconfig

Panther: The Active Directory Plug-In

- Joining AD:
  - dsconfigad and authorization
  - loginhook (this is a hack)

ADMitMac

- Third Party Product: Thursby
- Support for DFS, clustering, Packet Signing

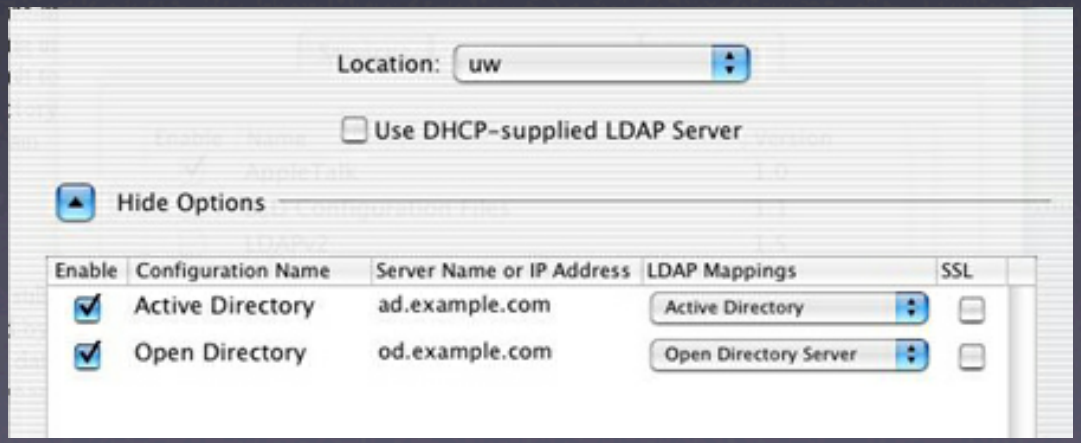
Troubleshooting

- /Library/Preferences/DirectoryService/SearchNodeConfig.plist
- be systematic! use ldapsearch, tcpdump, lookupd -d
- Ports for joining: dns, ldap, kerberos, kpasswd, 3269
- killall -USR1 DirectoryService

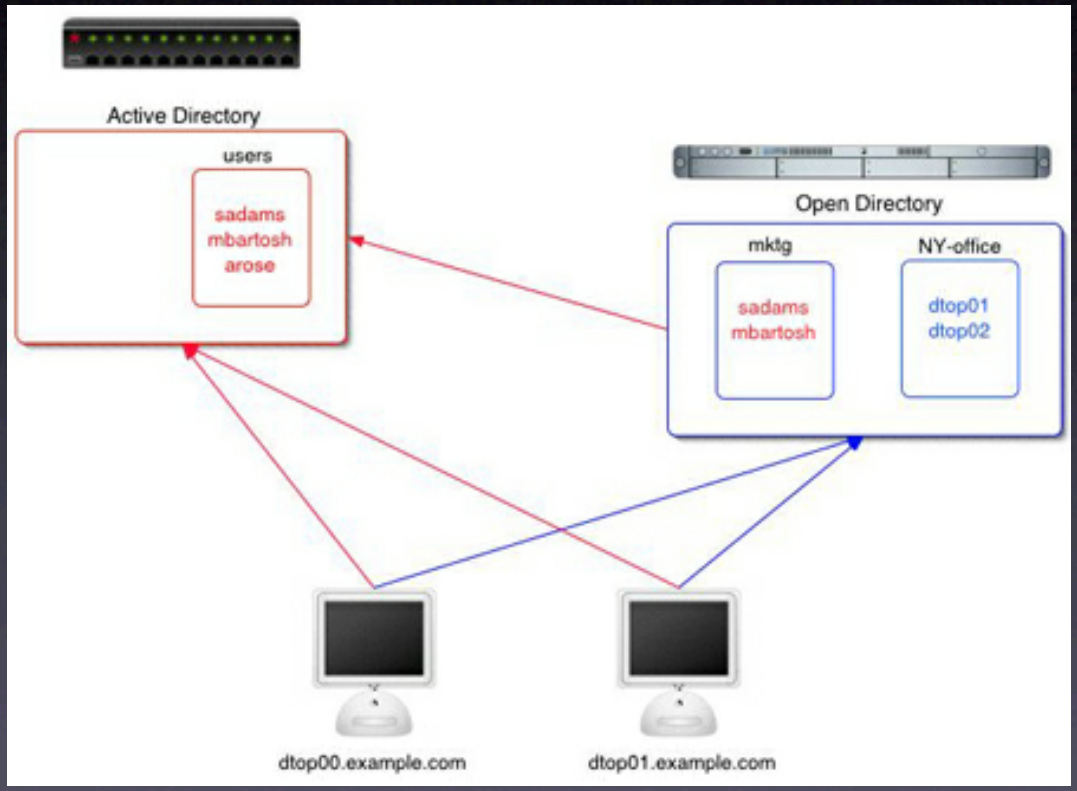
Using Multiple Directories

- It's often politically inadvisable to add a bunch of Mac-specific data to the directory
- This strategy is applicable to both AD and LDAPv3 Plug-Ins
- User principals live in AD
- Mac-specific data lives a Mac Directory
- Delegates Mac-specific management to Mac-specific personnel

Using Multiple Directories



Using Multiple Directories



Integrating Server Services

- Active Directory Plug-In will do pass-through (but that's not single sign on)
- AFP Kerb
  - Join AD
  - create windows user to map principal to
  - use ktpass on windows to generate service principal and keytab
    - ktpass -princ afpserver/server.example.com@ADS.EXAMPLE.COM -mapuser afp -out krb5.keytab
  - copy keytab to Mac OS X Server
  - Enable kerberos authentication

Integrating Server Services

- smb
  - security = ads
    - secure single sign-on for the masses
    - AD Plug-In will do pass-through NTLMv2 (lmcompatibiliy=4 server-side)
      - requires re-authentication
      - see winbindd config in /Library/Preferences/DirectoryService

Integrating Server Services

- smb: setting up security = ads
  - easiest with standalone server
  - edit smb.conf (much friendlier in Panther)
    - workgroup, usespnego = yes, security = ads, realm = ADS.EXAMPLE.COM
  - command: kinit Administrator@ADS.EXAMPLE.COM
  - command: net ads join
  - Configure AD Plug-In

Thank You!

Directory Services Integration with Third Party Directories

Utilizing methods to integrate Open Directory with other systems

Session M251
Macworld San Francisco 2005

Michael Bartosh
4AM-Media
Apple Certified Trainer, ACSA 10.3