Directory Services on Mac OS X and Mac OS X Server

Understanding Apple’s Open Directory Architecture

Session M241
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 1

Agenda

- Guiding principals
- What is a directory
- What is Open Directory
- Open Directory Server

Guiding Principals

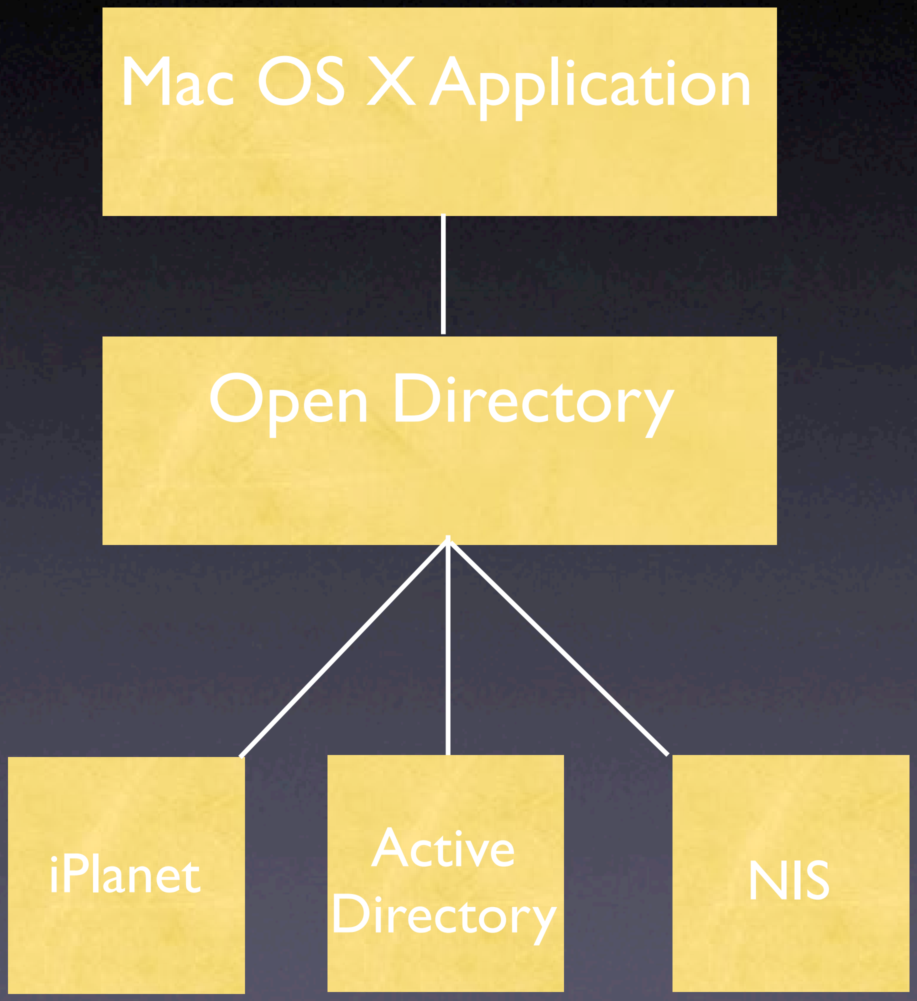
- Solutions should minimize impact on existing infrastructure.
- We should strive to help IT do more efficiently what it's doing today.

What is a directory?

What is Open Directory

- Mac OS X’s Directory Services Architecture
- Client-Side processes and libraries providing access to directories
- Server-Side: LDAP Server (OpenLDAP), MIT KDC (Panther), Password Server

Open Directory Architecture



Mac OS X Application

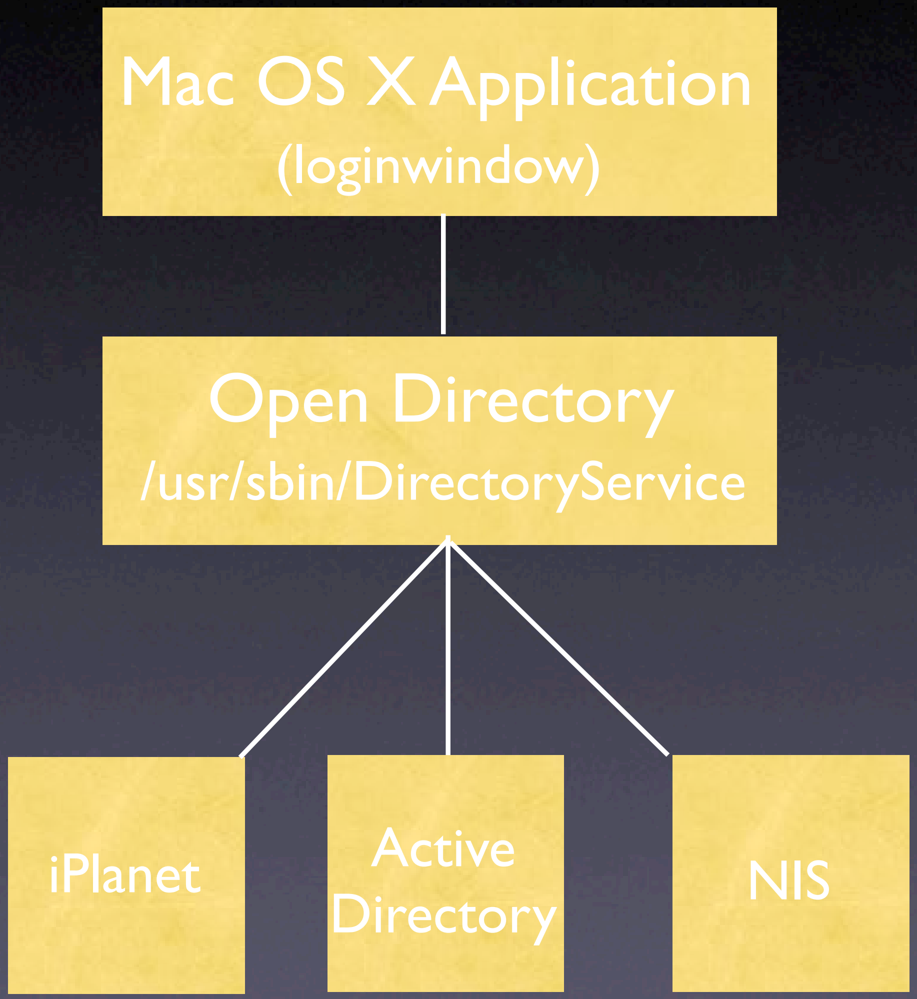
Open Directory

iPlanet

Active Directory

NIS

Open Directory Architecture



Mac OS X Application

(loginwindow)

Open Directory

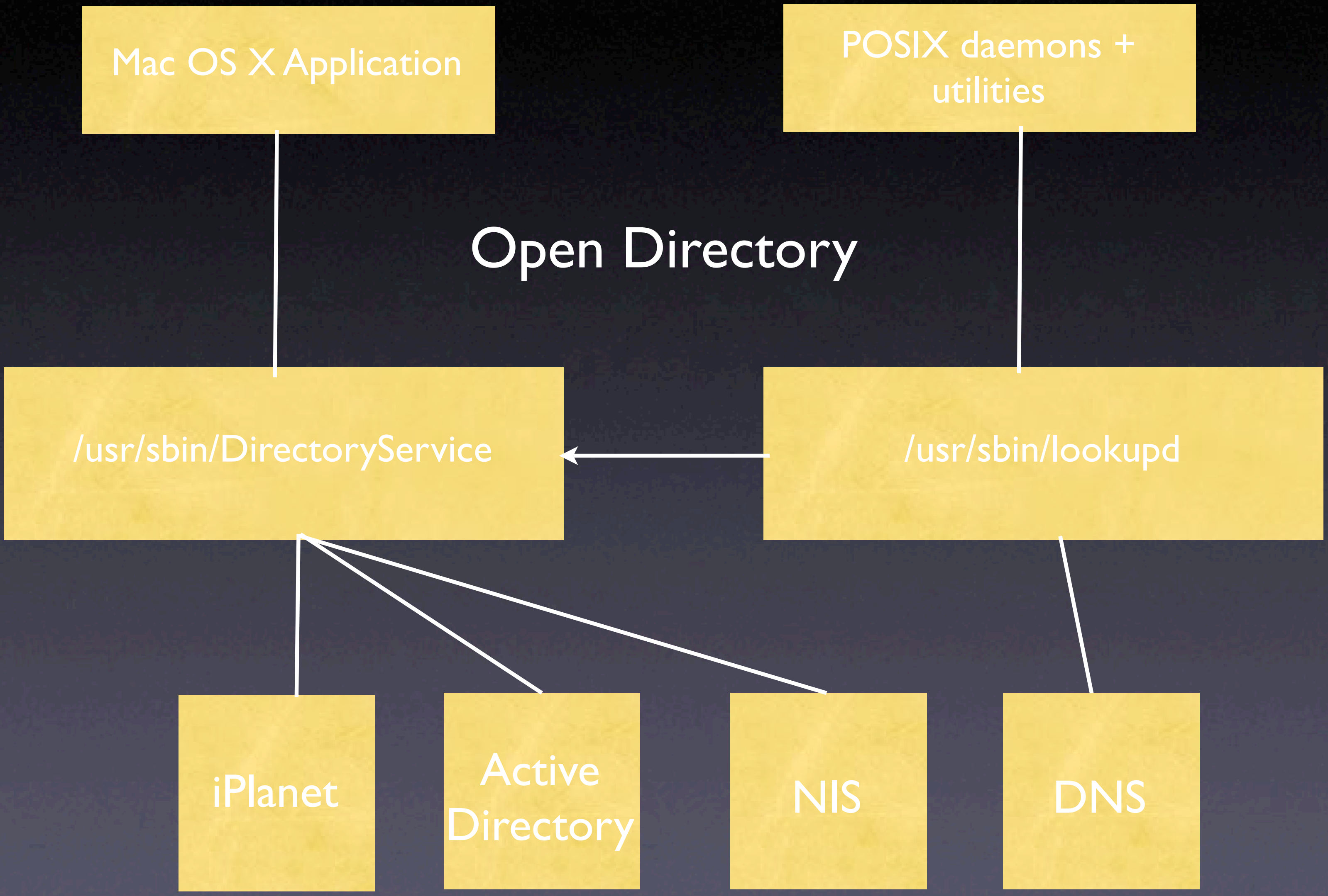
/usr/sbin/DirectoryService

iPlanet

Active Directory

NIS

Open Directory Architecture



Mac OS X Application

POSIX daemons + utilities

Open Directory

/usr/sbin/DirectoryService

/usr/sbin/lookupd

iPlanet

Active Directory

NIS

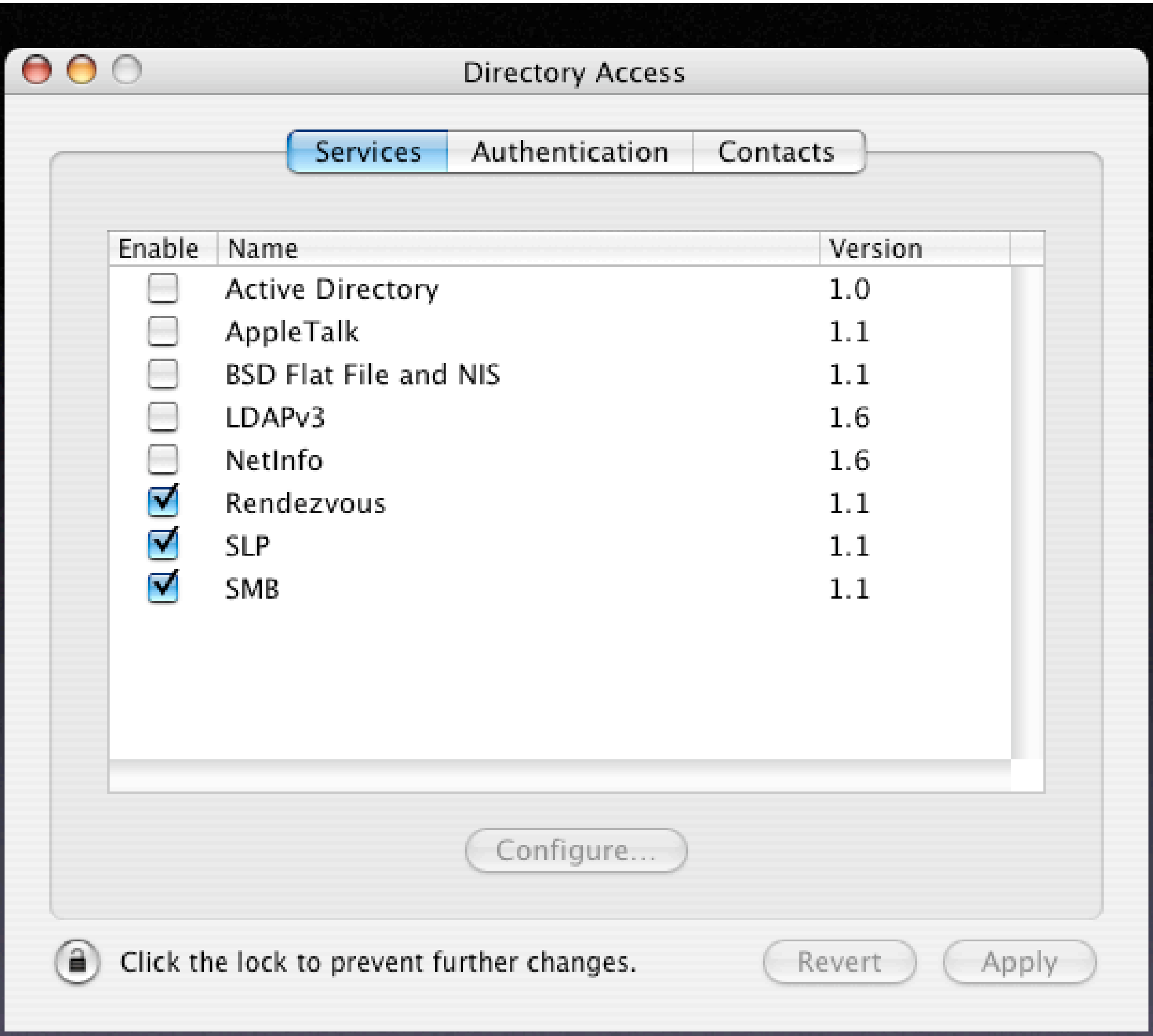
DNS

DirectoryService Architecture

- Plug-Ins: DirectoryService is extensible
  - Jaguar: LDAPv3, LDAPv2, NetInfo, NIS (10.2.5), BSD Configuration files
  - Panther: adds Active Directory, combines NIS and BSD FF, deprecates LDAPv2
- Configuration: Directory Access application writes to files in /Library/Preferences/DirectoryService
  - Panther adds /usr/sbin/dsconfigad for configuring AD Plug-In

DirectoryService Architecture

- Authentication in Panther
  - password hashes are no longer stored in NetInfo
    - instead they're in a root-readable shadow file
  - password hashes are no longer crypt()
    - NTLM and SHA-1 is used instead



Enable	Name	Version
□	Active Directory	1.0
□	AppleTalk	1.1
□	BSD Flat File and NIS	1.1
□	LDAPv3	1.6
□	NetInfo	1.6
☑	Rendezvous	1.1
☑	SLP	1.1
☑	SMB	1.1

Click the lock to prevent further changes.

Demo: Directory Access

The LDAPv3 Plug-In

- Platform Agnostic LDAP support
  - supports SSL, objectClass filters
- Supports static mapping of attribute values
- Panther: adds support for static mapping with variables
  - /Users/$sAMAccountName$ becomes /Users/jdoe
  - 10.3.3
- Jaguar Plug-ins with this support are available at http://homepage.mac.com/dansinema

Open Directory Server

- OpenLDAP with back-bdb
- MIT KDC
- Password Server
- Fully Replicated

Open Directory Server

- Authentication vs. Identification
  - Airport: ID (authentication), Airline Database (identification)
  - loginwindow: username is identified, then authenticated. 2 seperate processes.
  - Different protocols are used for each.

Open Directory Server

- OpenLDAP with back-bdb
  - configuration: /etc/openldap/slapd.conf
  - ...and slapd_macosxserver.conf
  - back-bdb is a high performance data store
  - see slapcat and slapadd commands
  - Access Controls

Open Directory Server

- Password Server
  - /usr/sbin/PasswordService
  - PWS is authoritative
  - legacy (non kerberos) protocols
    - NTLMv1, LANMAN, CRAM-MD5, APOP, WebDAV Digest, MS-CHAP2, DHX

Open Directory Server

- Password Server: Neat Tricks
  - AuthenticationAuthority (Demo)
    - password admins
  - NeST -hostpasswordserver admin pass
  - Unix password maintenaince utilities now can deal with PWS (via the DirectoryService api)

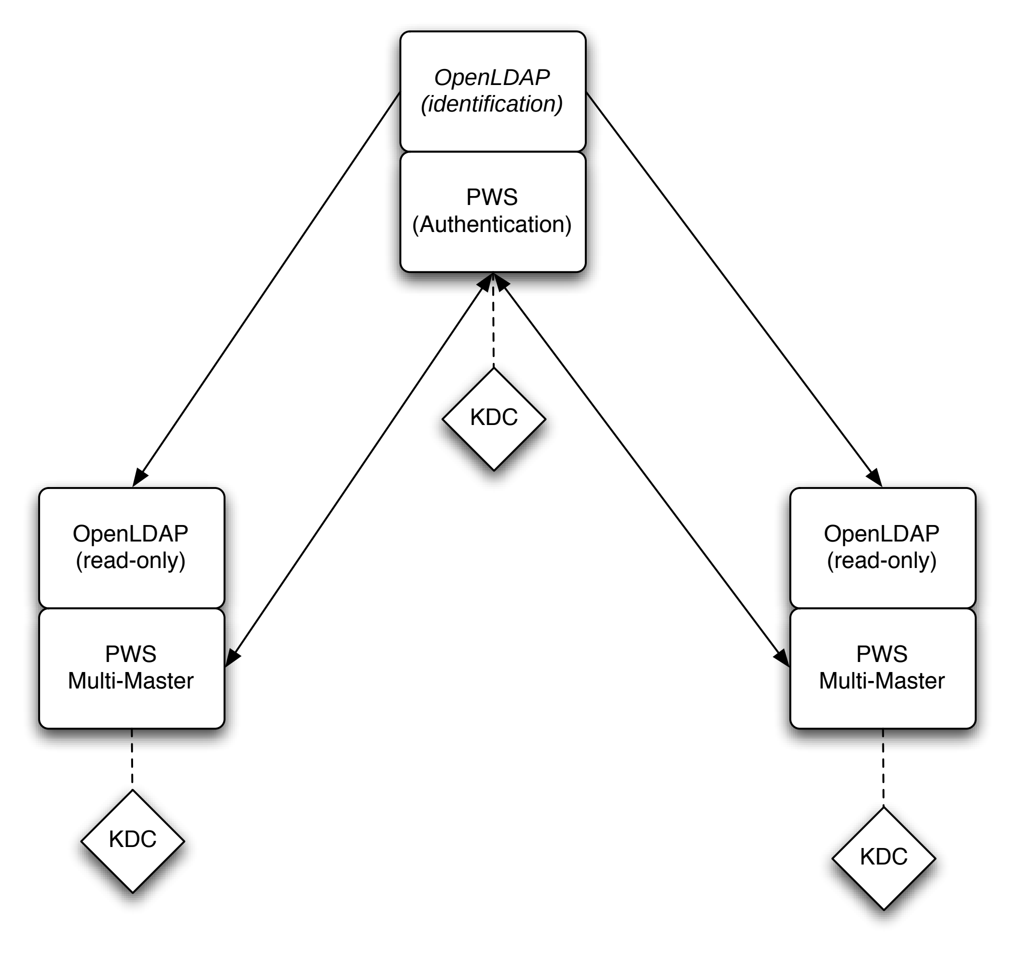
Open Directory Server

- Kerberos: MIT KDC (key distribution center)
  - Standard MIT distribution
  - PWS calls kadmin.local to keep password sync'd (KDC leverages PWS replication)
  - Key to single sign-on

Open Directory Server

- Troubleshooting
  - slapconfig and its log
  - DNS DNS DNS
  - admin user namespace issues

Open Directory Replication



Open Directory Replication

- Clients discover replicas in several ways:
  - Cached value
  - Record in Directory Service
  - Rendezvous
  - Network address in Authentication Authority

Thank You!

Directory Services on Mac OS X and Mac OS X Server

Understanding Apple's Open Directory Architecture

Session M241

Macworld San Francisco 2005

Michael Bartosh

4AM-Media

Apple Certified Trainer, ACSA 10.3