Mac OS X Enterprise Directory Integration

By
Darren R. Davis
Student Computing Labs
Presentation Overview

- Enterprise Directories
  - What are they?
  - Why do I need one?
  - Who makes them?
- Server Setup
- Client Setup
  - Apple’s Directory Tools
- U of U Case Study
Enterprise Directories

- What are they?

- A Directory is essentially a special use database designed for quick searching and retrieval of information. Think of a phone book where you look up a name and get phone number, or quick reverse search by looking up phone number and getting name.
Many Directory Services

- X.500 (Original Standard)
  - Used DAP (Directory Access Protocol)
- NIS
  - Sun’s Network Information Services
- Apple Netinfo
- Novell’s NDS (Novell DAP)
- Note: LDAP is not a Directory
  - Access Protocol (Lightweight DAP)
Structure (Schema)

- Data is organized in Key and Value pairs.
  - What is that? Think of...
    - Key of Name - Value of Darren Davis
    - Key of Phone - Value of 801.585.9811
    - Key of EMail - Value of drdavis@scl.utah.edu
    - Key of Password - Value of (yeah like I would tell)
Enterprise Directories

• Why do I need one?

• Uses of a Directory
  – Storage of user identities
  – Authentication
  – Authorization
  – Phone Book (Searching)
  – Storing Common or Network Configuration Information
  – Network Services Discovery and Location
Enterprise Directories

• Where is it?

- Enterprise Directories are Network resources accessed like any typical network service located on a server.
Enterprise Directories

- Who makes them?

- Just about Everyone
  - Apple Open Directory
  - IBM
  - Microsoft Active Directory
  - Novell eDirectory
  - OpenLDAP
  - Oracle
  - Sun ONE (Formerly iPlanet)
Enterprise Directories

- How do I access them?
  - Directory Client
  - Uses standard protocol
    - X.500 had DAP (Directory Access Protocol)
    - DAP was way too heavy...
    - U of Mich. developed LDAP (Lightweight)
      - First implemented as a Gateway to DAP
      - Now becoming primary access method
Server Setup

- Depends on who’s directory you use.
  - Follow setup instructions

- OpenLDAP (Open Source Directory)
  - Apple includes as part of it’s Open Directory.
Client Setup

- Use a directory client
  - Built-In to Mac OS X
  - Now built in to most UNIX Systems
  - OpenLDAP
  - Oh yeah, Windows have them too...
Apple’s Directory Tools

Directory Access

Services  Authentication  Contacts

Enable  Name  Version

AppleTalk  1.0
BSD Configuration Files  1.1
LDAPv2  1.5
LDAPv3  1.5.3
NetInfo  1.5.1
Rendezvous  1.0.1
SLP  1.0
SMB  1.0

Configure…

Click the lock to make changes.

Revert  Apply

UNIVERSITY OF UTAH
STUDENT COMPUTING LABS
Demonstration

- Setting Up Mac OS X Client
- Apple Directory Access
  - Located in Applications:Utilities
University of Utah Case Study

U
Definitions

- **Authentication**
  - The process of verifying the identity of a user.

- **Authorization**
  - Determining what the user can access.

- **Kerberos**
  - A network authentication protocol

- **LDAP**
  - A directory access protocol
University of Utah Case Study

• We use Kerberos for Authentication

• We use Active Directory for user information storage.
  – Why Active Directory?
  – Because we needed it to manage Win 2K clients. So, if we already have a directory, we should just use it.
Setting up Active Directory

- Install Win 2K Server
- Patch and Patch and Patch
  - It’s Win 2K double check your patches ;)
- Setup Domain Controller
  - Starts AD
- Use AD4UNIX to extend schema
  - MKSADExtPlugins.msi
- Add users (Perl Script)
Why Extend the Schema?

  - So, we needed it to represent Mac OS X (basically just another UNIX) information.
  - So, we added schema information to have standard UNIX information stored in AD.
What is stored in AD?

- User ID
- UID (UNIX ID #)
- GID (Group ID #)
- Home Directory

- We DO NOT store passwords in AD
This Presentation is a Work in Progress...

This will be finalized at the joint Apple and U of U seminar “Integrating Mac OS X on Campus” on May 1st.
Resources

- www.macosxrlabs.org
- web.mit.edu/kerberos/www/
- www.netcom.utah.edu
  - NID
  - ANA
- www.openldap.org