

RED HAT :: NASHVILLE :: 2006

SUMMIT



**Identity: LDAP in the Real World, Migration &
Integration**

Satish Chetty

Agenda

- Legacy Migration - local files, NIS, local files (/etc/password)
- LDAP use with mixed OS environments
- LDAP and Windows (Samba, Windows Sync)
- LDAP and Web Applications



Migration

- /etc/passwd, /etc/shadow, /etc/group
- Tools supplied by <http://www.padl.com>, OS vendors
- LDAP must have correct (POSIX) schema – usually supplied by LDAP vendor or migration
- Mix POSIX schema with inetOrgPerson (See sample)



Migration (*Contd.*)

dn: uid=schetty, ou=People, dc=redhat, dc=com
objectclass: top
objectclass: person
objectclass: organizationalperson
objectclass: inetorgperson
objectclass: posixAccount
objectclass: shadowaccount
cn: Satish Chetty
sn: Chetty
uid: schetty
mail: schetty@redhat.com
telephoneNumber: +1 (650) 567 9039 x79203
title: Technical Support Account Manager
labeledUri: http://www.redhat.com

Contd...

businessCategory: GSS
homeDirectory: /home/schetty
uidnumber: 10203
gidnumber: 30400
manager: uid=mymanager, ou=People, dc=redhat, dc=com
l: MountainView
homephone: +1 650 555 6456
loginshell: /bin/bash
mobile: +1 650 555 6456
pager: +1 650 555 6456
street: 444 Castro Street
userpassword: {CLEAR}redhat
carlicense: CA 000000
facsimiletelephonenumber: +1 650 555 6456



Migration from local files

- Includes hosts, services, automount, aliases, etc.
- DNS: BIND can use LDAP
- Others: RFC 2307(bis), rfc822MailGroup schema required
- <http://www.padl.com> for migration scripts for most



NIS Migration

- Network Information Services (NIS) is widely deployed
- LDAP can model and serve this information
- LDAP approach
- Gateway approach



PAM/NSS

- Name Service Switch (NSS): controls which database apps use to look up data: files, NIS, LDAP, etc.
- Pluggable Auth. Modules (PAM): controls which database apps use for user auth.
- nss_ldap, pam_ldap are used to allow the OS NSS and PAM services to get data from LDAP



LDAP Integration with the OS

- Most modern Unix/Linux OSes support LDAP (AIX, Solaris, HPUX and RHEL)
- Need client configuration
- Be aware of protocol extensions, schema differences - even between versions of the same OS
- Support of non native LDAP clients may be possible



LDAP and Kerberos

- Kerberos is widely deployed intranet secure single sign on solution
- Authentication to LDAP using Kerberos ticket
 - uses SASL/GSSAPI on client
- Use LDAP for Kerberos data store



LDAP and Mail

- Type-down addressing in email
- Most address books can lookup in LDAP
- No common schema for address books – schema munging, rewriting proxies
- Need self service web apps for editing address book data



Samba

- Samba – Samba3 can be configured to use LDAP as it's data store
- Active Directory
 - Can support unix/linux clients directly
 - Use sync or meta directory
 - AD “look-alike” - Samba4, XAD, other products



Web Applications and Services

- Apache
 - mod_auth_ldap for authentication
 - mod_authnz_ldap for authorization
- Tomcat
 - JNDI with LDAP provider
 - Use JNDIRealm for auth and authz



Questions

