Directory Services in an Education Network

Andrew Bartlett
Hawker College
Who Am I?

- Andrew Bartlett
- Samba Team
- Student Network Administrator
  - Hawker College, ACT
What is Hawker?

- 900 Students
- Year 11/12 High School, ACT
- Linux Centered
  - Samba, OpenLDAP, Heimdal Keberos
- Microsoft Clients
- Linux Clients
Directory Services

• Beyond the Buzzwords:
  - Single, Central source
  - Information on
    • Users
    • Computers
    • Printers
    • Assets
LDAP as a directory solution

- LDAP is a directory access protocol
- OpenLDAP is an implementation
- Everything talks to LDAP
  - well sort of...
- Many 'ideal world' documents abound
LDAP realities

• Different schemas
• Different expectations
• Plenty of cludges
• Still worthwhile
What we put into LDAP

- User Accounts
  - Students
  - Staff
  - Affiliates
  - System Accounts
What we put into LDAP (2)

- Machines
  - Boot records (macAddress)
  - Asset Details
  - Samba Trust account
What we need to drive

- 10 Linux servers
- 150 Windows Clients (or so)
  - WinXP
  - Win2000
- Dual-boot
  - LTSP
  - Linux Client (readonly NFS root)
How we use the Directory

• Single Sign on
  - One password for:
    • Windows
    • Linux (client and server)
    • Website
    • e-mail
    • Internet Proxy

• Controlled Booting
What we hook onto LDAP

- Samba DC
- Linux Clients (nss_ldap)
- Heimdal (Kerberos KDC)
- Internet Quotas
- DHCP+LDAP for controlled booting
The Good, the Bad and the Ugly

• Open Source is often not pretty
• Microsoft may be 'worse'
  - But this is no excuse
• Plenty of `perfect intergration'
pipedreams
  - Few administrators make it to the end
Really dancing the Samba

• 2 'Rudundent' Samba servers
  - Not hard to add more
  - Replicated netlogon

• Mandetory Profiles
  - Allows login systems to be rudundent
  - Even if home directory is still single-point-of-failure
Transparent NTLM Proxy Auth

- We wanted internet authentication
- We did not want extra prompts
- Squid + Samba's ntlm_auth + winbind
- Originally MSIE clients
- Now Firefox
Samba Load Center

- Samba is a 'load center' on our network
- Domain Logons
  - Over 2000 packets is reasonable for a login
- NTLM Authentication
  - Potentially one auth per page
Reducing the Samba Load

- Interesting progress on LDAP load issues
  - ldapsam:trusted = yes
- Work progressing to reduce:
  - round-trips to LDAP sever
  - excessive queries
OpenLDAP

- The 'standard' free directory solution
- Watch your versions closely
  - For x.y.z, maximize z
- OpenLDAP 2.1 and bdb don't mix
- I'm looking to OpenLDAP 2.2 on Debian Sarge
OpenLDAP Replication

• Still using push replication

• (Finally) have 'reset replication' scripts
  - Shut down master
  - Rsync to slaves
  - Restart master
  - Rebuild slaves
Schemas

- Hawker Custom Schema
  - hawkerAccount
  - hawkerDevice
DHCP+LDAP

- Mandatory registration of devices
  - Student wireless laptops
  - Workstations
    - Ensure we know what is on the 'net
- Controlled Dynamic DNS
  - More security on the dynamic names
DHCP+LDAP (technical)

• Patch to make DHCP read LDAP
  - Attach DHCP settings to existing entry
• Runtime configuration
  - No dhcp restart for many settings
• 'Does not play well with others'
  - I modified schema for more useful schema support
Kerberos Authentication

- Centralised Authentication System
- Long history, cryptographicly secure
- Internet Standard
- Typically hard to 'add' to a network
Heimdal hdb-Idap

- **Heimdal Snapshots**
- **Samba Intergration – Samba passwords**
  - Thanks to Microsoft actually...
- **ldapi://**
- **LDAP down error handling**
gq

- GUI LDAP Administration tool
  - X11 (I lothe web tools)

- Very useful
  - Easy queries

- Far from perfect
  - Occasionally Crashes
  - ... and takes the mouse
Internet Quotas

• Perhaps our biggest 'in house' script set

• LDAP
  - Controls the decrement of quota balance

• MySQL
  - Controls the allocation of quotas
Hawker and Linux Clients

- **LTSP**
  - Fedora Core 2
  - Setup for the benefit of the Linux Class
  - LTSP boot
  - VNC (On start menu, easy!)

- **Linux NFS Root**
  - Fedora Core 3
Questions

- abartlet@samba.org
- http://hawkerc.net/staff/abartlet/educationlinux2005-pres.sxi