Linux and LDAP authentication

Birmingham LUG

Richard Wallman
richard@bossolutions.co.uk

LDAP in brief

- Hierarchical system – a tree of entries
- Entries are collections of classes
- Classes have attributes
- Attributes have one or more values
- Unique identifier: 'Distinguished Name' (DN)

Advantages of LDAP authentication

- One place to create/remove accounts
- Same username/UID across all computers
- Single password for multiple services (login, email, database, websites, etc.)
- Can be used as an address book by email clients
- Supports replication (for performance/ availability)

Setting up

- Server side
  - Install OpenLDAP
  - Create user entries
    - posixAccount for simple logins
    - shadowAccount for password aging etc.
- Client side
  - Install LDAP PAM module (libpam_ldap)
  - Install name service module (libnss_ldap)
  - Install Name Service Cache Daemon (nscd)

How it works

- The user enters their login name and password
- PAM checks local accounts (/etc/shadow) first
- If no match, LDAP is searched for user
  - **Hashed token is sent to the client!**
- Token (if found) used for authentication
  - Token includes hash method, e.g. {CRYPT}f97VVNc1IjyxI

People who looked at this also looked at...

- Kerberos
  - Users obtain 'tickets' from auth servers
  - Tickets can be reused by services - single sign on
- NFS
  - Central storage of files
    - Particularly home directories
  - Can be combined with Kerberos or IPSec for transport-layer security