Implementing Active Directory
Hurdles, Obstacles, and the Finish Line

Jim McDonough
Samba Team
IBM Linux Technology Center

April 6, 2004

IBM Interest

- Alternative to Active Directory
- Common request from customers
- File and Print is not enough
- Truly standards based...or close enough
- Pick and choose components
- Question: what will it take?

Project Approach

- Gather more data
- Need a visible demonstration
- Essential task
- “Can't Do” with NT-style system
- Involve core components
- Join a Domain and Find a Printer

What Do We Need?

- Samba (RPC)
- LDAP
- Kerberos
- Let's find out...

DNS Configuration

- SRV records
- Supported in any fairly recent bind (named)
- Locate a specific service on a specific protocol in a domain or site
- Example: *_kerberos._tcp.msdcs.mcd.home.test*
- By the way, MS doesn't pay attention to the protocol part
- Easily done (but a bit tedious)

DCLS

Domain Controller Location Services

- Find DC
- Services offered: KDC, LDAP, GC, Time
- Which Site
- Find the “best” DC for a client
- MS uses a variant of LDAPv3 over udp (no standard exists at all), and OpenLDAP requires -D flag (not a ./configure option)

DCLS

- What we have done so far:
  - Extend mailslot SAMLOGON response
  - Standalone MS-CLDAP server (coming in Samba 4.0 nmbd)
  - Create a basic response: fields are fixed
- What we still need to do:
  - Allow multiple sites
  - Allow forests
  - Very easy, but no point yet

Kerberos

- rc4-hmac, arcfour-hmac
  - In MIT 1.3, Heimdal 0.6+
  - Not critical, but it makes life easier
- PAC
  - Lot of hype, but not critical
  - Timesaver...reduce number of trips to DC

Kerberos

- Minor details
  - Realm names
  - Service Principal Names
    - cifs/hostname.domain.com = HOSTNAME$
  - Password change
- Synchronization
  - Heimdal/LDAP provides basis
  - Andrew Bartlett patches
- Bigger issues:
  - Cross-realm
- We decided to wait a bit...

LDAP

- GSS-SPNEGO SASL support
  - AD servers offer GSSAPI for compatibility, but clients don't like it
  - Need NTLMSSP: ntlm_auth!
  - Cooperation between IBM, Volker, and Andrew Bartlett (lorikeet)
- New syntaxes and matching rules
  - Easy to add with SLAPI...and native OpenLDAP api...

LDAP

- New RootDSE attributes, e.g.:
  - ldapServiceName: static attribute easily added in schema files with OpenLDAP 2.2
  - currentTime: computed attribute added via SLAPI
- ObjectGUID:
  - Generates domain GUID
  - Different format than OpenLDAP's entryUUID
  - Done by OpenLDAP: operational
  - SLAPI plugin

LDAP

- Point of Synchronization
  - Create user via RPC, set password via Kerberos, modify attribute via LDAP
  - Can be done with SLAPI and/or modifications to Samba and Kerberos
  - Easy to make a mistake
- Again, we decided to wait...

Endpoint Mapper

- Advertises RPC services over transports (SAMR, NETLOGON, LSA, SPOOLSS)
- Maps from UUID:Version:Protocol to location where service is available: e.g., IP address/port, named pipe
- Available through tcp port 135 or named pipe /PIPE/EPMAPPER
- Client code in rpcclient
- Started standalone server, decided to wait for Samba 4.0

Strange Brew

- Finally, success?
  - Disable Directory Services in DCLS response
    - Eliminate need for LDAP and EPM
  - Heimdal KDC modified to handle realm cases
  - Samba using tdbsam!
  - Samba gives service principal name (cifs/host.domain.com)
  - Machine joins!
  - On boot, doesn't work...it “knows better”, looks for alternate principal name, and really really wants LDAP and RPC directory services

Why Are We Running This Race?

- Why do my customers want AD?
  - Marketing
    - “We need it”
    - “It's the latest”
    - “It's our company policy”
    - “I don't know”
  - Technical
    - Kerberos
    - Single sign-on
    - Group policies
    - Delegation/distribution of administration
    - Automatic/transitive trusts

Where Is the Finish Line?

- How compatible do we want it?
  - Will we keep chasing? Does this lock us in?
- Which features do we really need?
  - What does "Active Directory" mean to you?
- How long can we wait?
- How many projects need to be involved?
  - Can we get them to play along?
  - How much glue (and baling wire and duct tape)?