Linux-based Server Appliance Deployment in an Educational Setting

Jim McDonough
IBM Linux Technology Center
Samba Team
SambaXP 2005
Network Overview

My Office Network

- hi-speed interweb connexion
- Sisko rowder
- Blinkenlighten switchen
- super-skrit fearwall
- ups from ebay
- Dell Windoze swerver
- 133t lunix swervers
- swever cabinet
- dirty webcam
- free web
- 100meg network switcharoo
- my lunix desktop
- my personal swever
- other stuff

LAN

lusers 'doze pееceеs

Courtesy of Nicholas Drouet
Environment

- UK County-wide school system
- Highly distributed
- Varied site size (200-1600 users)
- Large total deployment
  - 400 sites
  - 300K users
- Some centralized management and monitoring
- Some localized management
Requirements

- Support Windows desktops
- Logon with lockdown
- Shared files
- Printing system with quotas
- Web content filtering
- Proxy (web and streaming media)
Restrictions

- Mix of central and local hardware
- Certain proprietary software already in place
- Minimize unsupported software
- Function with unreliable WAN
- Highly available with basic Future infrastructure considerations
Software Components

- IBM Tivoli Directory Server 5.2
- Samba 3.0
- PyKota
- Linux-HA (heartbeat/mon/drdb)
- Squid
- Identd
- SquidGuard / Websense
- Helix
Directory Server

- IBM WebSphere and SecureWay already in place
- Need local ability to manage even when WAN is down
- Explored possibility of OpenLDAP with syncrepl
- Decided on IBM Tivoli Directory Server 5.2
Directory Structure

- Data Center
  - Partnership
    - School
      - o=county,ou=partnership,ou=school
Directory Structure

- Management and Policy information for WebSphere and Tivoli are used at Data Center level
- Partnership level is for future plans with policy and management (e.g. budgeting and quotas)
- Most server appliance apps are based out of school-level DN
Subtree Replication

- Each school DN is the root of a peer-replicated subtree (Datacenter is the peer)
- Enables school apps to run/manage with local directory server while allowing data center to maintain central control
- Small directory size (and hardware) at schools
ITDS Issues

- Initial setup was difficult
- Schema format slightly different than OpenLDAP
- Peer replication does not resolve conflicts (not multi-master)
  - Use access controls on attributes to minimize conflict potential
  - Policy must be in place to handle conflicts
Samba 3.0

- **Domain Controller**
  - LDAP passdb backend
  - Desktops locked down via policies

- **File shares**
  - Home directories
  - Class directories
  - Applications
  - CD sharing

- **Print serving**
Samba 3.0 Issues

- Schema updates for ITDS
- IdealX tools needed but unsupported by standard IBM agreements
- No print quota support
  - Not provided by CUPS either
- Samba supported, but not always the latest
  - Samba 3.0 DC improvements not yet available on RedHat EL 3.0
PyKota

- http://www.librelogiciel.com
- Python-based print quota system for CUPS
- User print quota
- Allows for auditing/reporting
- Storage in LDAP
- Printer info via SNMP
PyKota Issues

- Unsupported by standard IBM agreements
  - Same issue with prerequisite software
- Schema incompatibilities (caseIgnoreIA5SubstringsMatch) and reformatting for ITDS
- Logs everything in LDAP
- Will not allow printing if LDAP is unreachable
- However, PyKota team was very responsive to requests
High Availability

- Each school has 2 servers, data replicated via drbd
  - Samba shares
  - Samba config
  - Samba tdbss
  - Squid config
  - CUPS config

- LDAP replication handled by ITDS
  - Samba domain objects
  - PyKota config and data

- WebSense replication handled by WebSense Enterprise software
Squid

- Web caching
- Cache preloads
- Usernames from Identd on clients
SquidGuard

- Web content filtering
- **Filter based on sources:**
  - Username
  - Address
  - Domain
- **Filter based on destinations:**
  - URL
  - Addresses
- Public blacklists
- Selective Logging
- Enterprise management and reporting tools lacking
WebSense Enterprise

- **Web content filtering**
- **Enterprise management**
  - Centralised policy management
  - Flexible reporting
- **Issue: local policy additions/customizations**
  - Current fixed by external merging of xml files at each site
  - Will be supported by upcoming version of WebSense
Management

- Local school admins and teachers need to perform minor tasks on multiple applications
- WebMin-based custom GUI for tasks such as:
  - Proxy cache management (restart, load, purge)
  - User password reset
  - Share creation
  - Print job management
  - Quota manipulation
  - Usage reporting
  - Application status
- DataCenter administration requires more training
Current State

- 3-school pilot with 2000 users in process
- Pilot is proceeding well
- Education and tweaking currently
- ITDS Scaling questions
  - We know it scales to 300K users at the Data Center
  - We know it scales to 1600 users locally
  - Replication is the question
    - Can the WAN handle it?
    - Do the updates stack up and flood the server and WAN?