ZEROPIU
Difference as value

Samba in a distributed environment

manfred@zeropiu.it

Agenda

- Starting Situation
- Goals
- Solution
  - Client Side
  - Server Side
  - Directory Server
- Infrastructure
  - Network Design
  - Software
  - Directory Design
  - Configuration
- Migration
  - Requirements
  - Procedure
- Trouble
- Result
- Next Step

Overview

Italsempione

is nowadays the biggest Italian fully indipendent forwarding company covering any service related to transports and logistics with a worldwide agency network.

Company:

- Head Quarter in Italy
- 16 Branch Office in Italy
- 7 branch outside Italy
- 400 PC , Windows XX
- 150 PC , Linux
- 8 Windows NT Domain
- OpenVMS cluster
- Microsoft Exchange
- Wide Area Network
- No IT stuff on the branch office

Project Goals

- Cost Reduction
  - License
  - Hardware

- Simplified management
  - Centralized User Profile
  - Centralized Management
  - Server Consolidation

Distributed environment

In Distributed environment you need :

- Ability to replicate information widely to increase
  - availability
  - reliability
- Reducing response time.

Perfect Solution are Directories Server:

- Directories can manage all-size organizations, from small, focused user departments to global enterprises with millions of users.
- Directories can store information about devices, applications, people and other aspects of a computer network.
- Directories are based on a open standard technology (LDAP) for easy integration
- Directory entries are arranged in a hierarchical tree-like structure. Traditionally, this structure reflected the geographic and/or organizational boundaries.
- Directories are tuned to give quick response to high-volume lookup or search operations

Don’t Use Directory when:

- Your records change many times a day
- Your records is plain to store in a relational database

Client Side Solution

- Software OpenSource
  - PXES, remote Desktop for Windows Terminal Server
  - Linux Desktop

- Hardware Thin Client
  - Low Price
  - Low power consumption
  - Low noise and heat

Server Side Solution

- Software OpenSource
  - Linux
  - Linux Terminal Server Project (LTSP)
  - Samba Domain Controller
  - Network Service (DNS, DHCP, MAIL, ect)

- Hardware
  - -

Simplified management

Centrally administration “means” time and resource savings.

- Centralized User Profile
  - Identity life cycle management
  - Secure password management
  - Role-based administration capability/Delegation
  - User Self Provisioning
- Maintenance
  - Remote control (ex. ILo)
  - Automatic package distribution
  - Monitoring (ex. Centrilized log)
- Server consolidation
  - Reduction number of system
  - Reduction rack space
  - Simplified backup and monitoring operations
  - Simplified update operation

Cost Comparison for a Basic, 100 Node Network Business Computing System HW

Microsoft® Windows® Based PC Workstation/Server System				Linux /Samba/LTSP Based System	
Item	**Quantity**	**Price**	**Totals**	**Price**	**Totals**
Hardware					
PC Workstations	100	$600	$60,000	$400	$40,000
File, Print Server	2	$4,000	$8,000	$4,000	$8,000
Email Server	2	$4,000	$8,000	$4,000	$8,000
Terminal Server	2			$5,000	$10,000
Subtotal			**$76,000**		**$66,000**

Cost Comparison for a Basic, 100 Node Network Business Computing System SW

Microsoft® Windows® Based PC Workstation/Server System				Linux Samba/LTSP	
Item	**Quantity**	**Price**	**Totals**	**Price**	**Totals**
Software					
Microsoft® Office Suite	100	$400	$40,000	$0	
Microsoft® Server 2000 (with 5 CAL)	4	$1,000	$4,000	$370	$1,480
Microsoft® Exchange®	1	$700	$700	$0	$0
Microsoft® CALs (5)	19	$200	$3,800	$0	$0
Microsoft Windows XP (OEM)	100	$150	$15,000	$0	$0
Exchange® CALs	100	$67	$6,700	$0	$0
Subtotal			**$70,200**		**$1,480**

Use the Best Solution..

- Replace Domain Controller with Linux/Samba Server
  - Office with more 5 User Domain
  - Office where the number of Linux Desktop > Windows Desktop

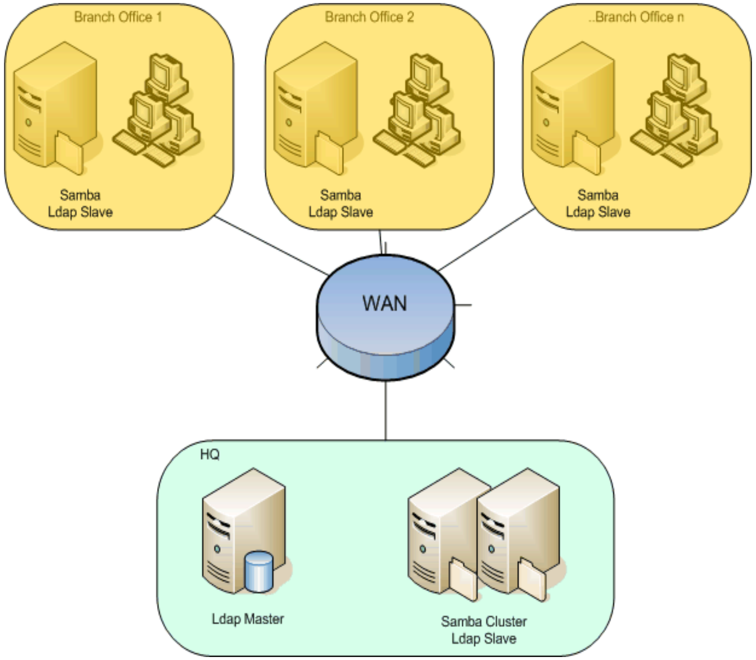
- Replace Windows Client with Linux Desktop (LTSP)
  - Employ with a executive job
  - Employ with light level of usage of Microsoft Office

- Replace Windows Client with Windows Terminal Server
  - Employ with usage of custom windows application
  - Employ with heavy level of usage of Microsoft Office

- Enterprise Directory
  - Centralize user profile

Design

- Headquarter
  - One Directory Master in HQ
  - One Samba Domain Controller
  - 2 Samba File Server based on cluster
  - One "Master" NTP Server
- Brach Office
  - One Directory slave in each branch office
  - One Samba Domain Controller in each branch office
  - One "Slave" NTP server
- Enterprise Directory
  - Unix user same as Windows user



Software

- Linux
  - Red Hat (kimberlite) Cluster for HQ office
  - Filesystem ext3 on LVM
  - Pam Ldap , NSS Ldap
  - Linux Terminal Server
  - PXES
- Enterprise Directory
  - OpenLDAP 2.2.x
  - Gosa Interface
- Samba 3.x
  - Ldap backend , ACL, CUPS, Quota
  - Monitor VFS module
  - External lib for password enforce (cracklib)
- Mailserver
  - Postfix Mail Transfer Agent
  - Cyrus , mailbox delivery and IMAP/POP Services
- Monitoring
  - Zabbix
- Backup
  - Amanda

Enterprise Directory

Ldap Design

- User

  User Profile, Unix Account, User Windows Account, User Email Account, User Proxy Account,..

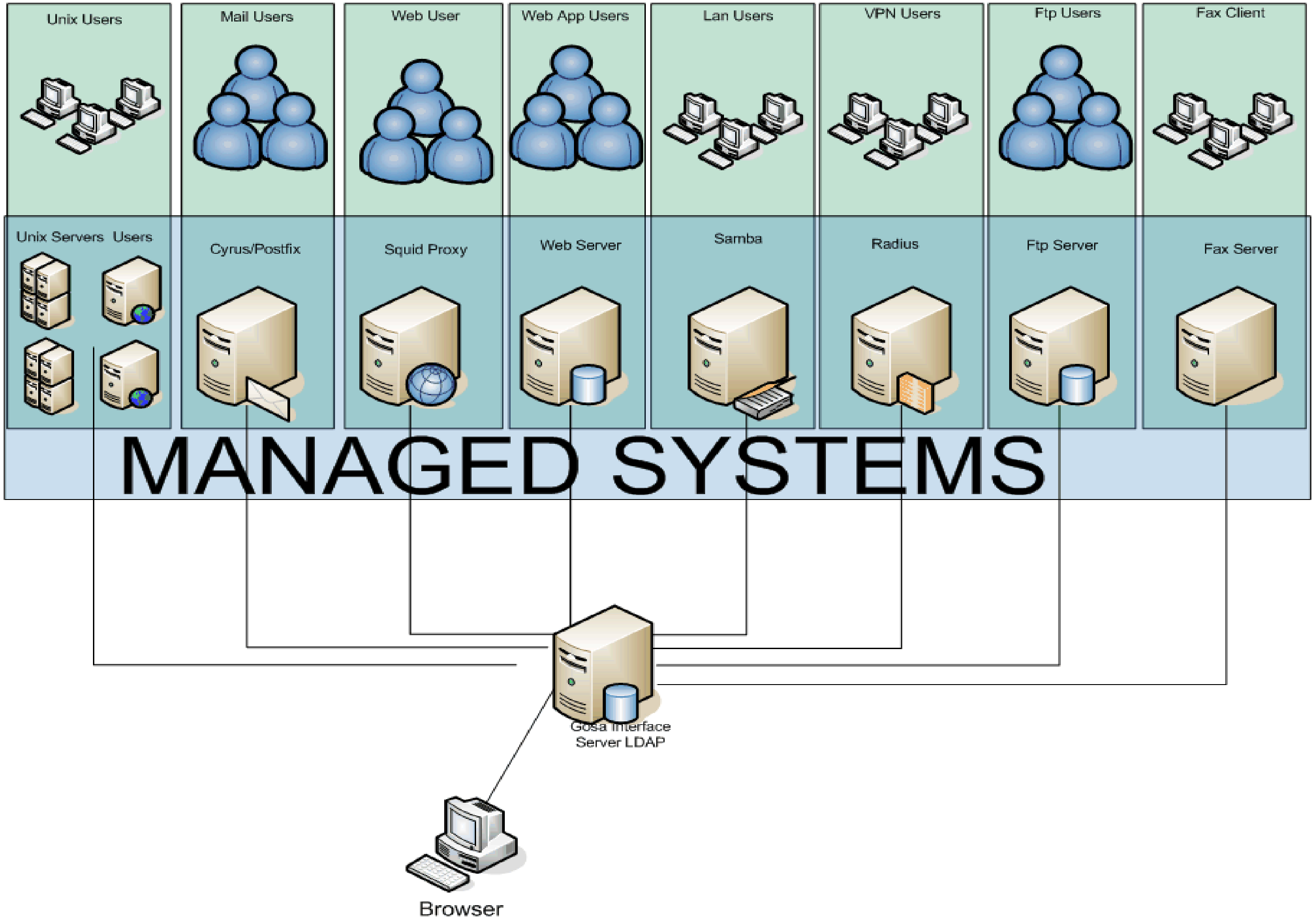
- Group

  Group Profile, Unix account, Windows Account, Email Shared Folder

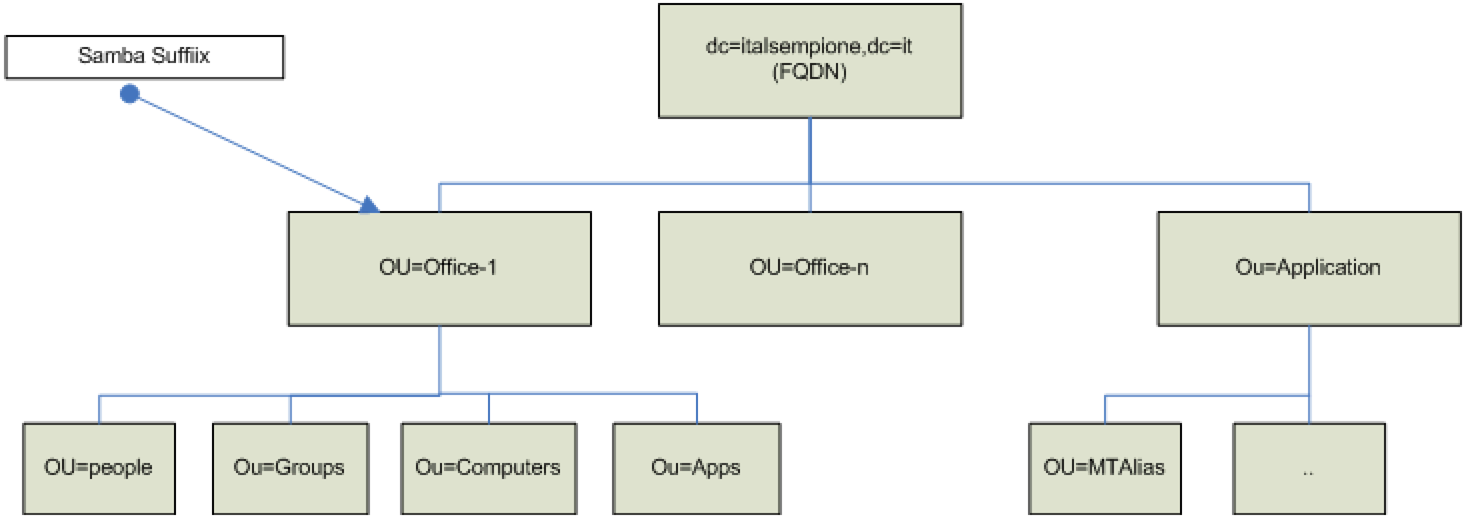
- Machine Account
  - Windows Machine Account

- Branch Office
  - Domain Information
  - Office Information

- Application
  - Administrative User
  - Application Attribute
  - User Role specific application


Unix Users
Mail Users
Web User
Web App Users
Lan Users
VPN Users
Ftp Users
Fax Client
Unix Servers Users
Cyrus/Postfix
Squid Proxy
Web Server
Samba
Radius
Ftp Server
Fax Server
MANAGED SYSTEMS
Gosa Interface
Server LDAP
Browser

Directory Information Tree (DIT)



Sample User Profile

Unix

- description: System User
- displayName: Manfred Furuholem
- sn: Soncin
- givenName: Manfred
- o: Italsempione S.p.A.
- ou: Edp
- l: Vittuone
- st: Italy
- telephoneNumber:xxxxxxxxxxx
- cn: Manfred Furuholmen
- postalAddress: via Restelli,5
- homeDirectory: /afs/italsempione.it/home/manfred
- loginShell: /bin/bash
- uid:manfred
- uidNumber: 201203
- gidNumber: 545
- gecos: Manfred Furuholmen
- shadowMin: 0
- shadowMax: 0
- shadowWarning: 0
- shadowInactive: 0
- shadowLastChange: 13238
- Userpassword: xxxxxxxxx

Mail

- mail: manfred@italsempione.it
- gosaMailServer: imap://imap.italsempione.it
- gosaMailQuota: 500000
- gosaMailDeliveryMode: [LV]
- gosaSpamSortLevel: 0
- gosaSpamMailbox: INBOX
- gosaVacationMessage: gosaMailAlternateAddress: manfred@is0404it20.italsempione.it
- gosaMailAlternateAddress: manfred.furuholmen@italsempione.it

Samba

- sambaSID: S-1-5-21-963014146-839875343-911163043-1229
- sambaLogonTime: 1037577600
- sambaLogoffTime: 1026432000
- sambaAcctFlags: [UX]
- sambaHomeDrive: U:
- sambaLogonScript: login.bat
- sambaPrimaryGroupSID: S-1-5-21-963014146-839875343-911163043-3009
- sambaDomainName: IS01DIT20
- sambaHomeDrive: U:
- sambaLogonScript: login.bat
- sambaPrimaryGroupSID: S-1-5-21-963014146-839875343-911163043-3009

Openldap Configuration

- Syncronization
  - LDAP Sync Replication vs Slapd
  - *refreshOnly* vs *refreshAndPersist*
  - All data vs single Branch

- Ldap Security
  - TLS/SASL
  - LDAP ACI/ACL
    - Grant users the ability to change their data
    - Grant application user to change their data
    - Deny read access to anyone attempting to query

- *Tuning*
  - Attribute Index
    - sambaSID
    - sambaPrimaryGroupSID
    - sambaDomainName
    - sambaSIDList
    - Watch log
  - *Berkeley Database backend* tuning
    - Cache size (slapd.conf)
    - Transaction log (DB_CONFIG)
    - db_stat
  - Thread size
  - Concurrency

Samba Configuration

- Ldap Backend
  - Branch Office is a organizational Unit (ou) used as suffix
  - Ldap Slave is the first server, Ldap master is configured as fall back (passdb backend = ldapsam:"ldap://127.0.0.1 ldap://10.1.21.247 ")
  - Write operation use referral to reach master server
  - Tuning search with suffix (ldap user suffix ,ldap machine suffix, ldap group suffix)
  - Disable delete DN (ldap delete dn = no)
  - Ldap passwd sync

- Custom Script (add machine, add group, add user to group, delete user from group , set primary group)
  - Add Gosa Schema
  - Add Italsempione Schema (Mail and application)
  - Delay for Ldap Replication

- Password Enforcement
  - CrackLib checking password
  - Costum script for password validation (check password script)

Linux Configuration

- LDAP support
  - System Databases and Name Service Switch (nss_switch.conf)
  - Pluggable Authentication Modules (PAM)
  - ldap.conf Configuration

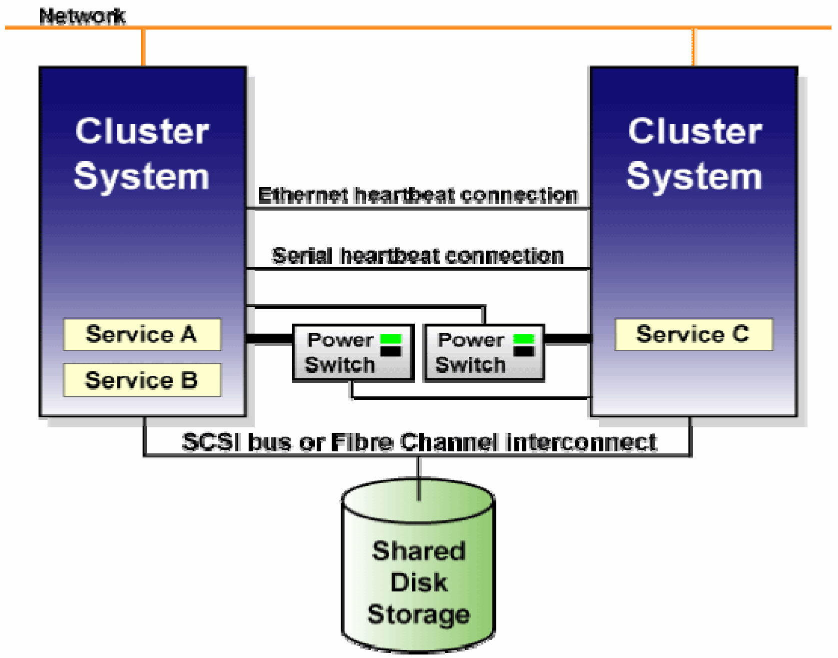
- Name services cache daemon nscd (nscd)
  - Cache TTL
    - positive-time-to-live, positive entries (successful queries)
    - negative-time-to-live, negative entries (unsuccessful queries)
  - Cache Size
  - Disable File check

- Ext3
  - Access Control List (ACL) support
  - Quota support

- Tuning
  - Elvtune

Samba Cluster

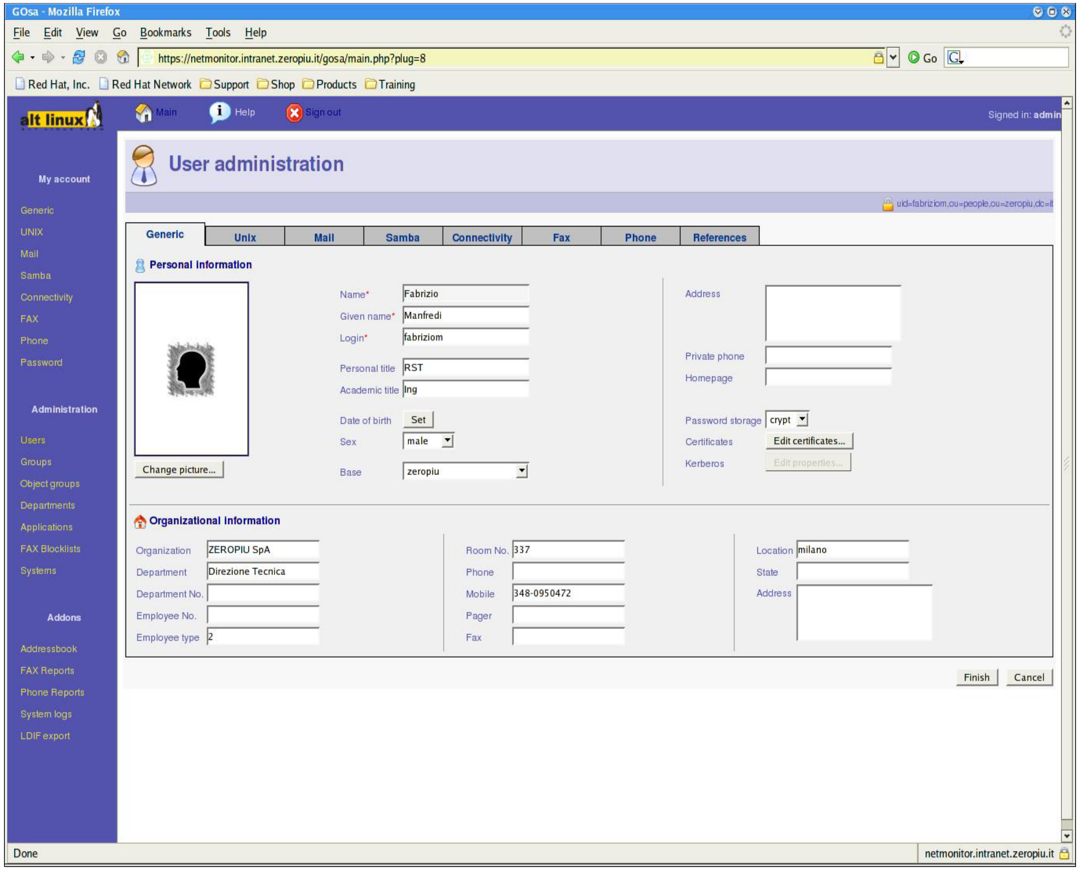
- Cluster
  - 2 node Active-Active
  - Disk shared
  - Kimberlite
  - Network HA (bond)
- Samba
  - Individual per-service samba configuration file, /etc/samba/smb.conf.sharename
  - Dedicated IP per-share



Provisioning Tool

Gosa automatically creates, modifies and deletes user accounts on multiple, heterogeneous systems or applications.

- Advanced graphical user interface
- Wide spectrum of platform coverage
- Password management
- Ldap back end
- Extensible



User administration

uid=fabriziom,ou=people,ou=zeropiu,dc=it

Personal information

Name* Fabrizio
Given name* Manfredi
Login* fabriziom
Personal title RST
Academic title Ing
Date of birth
Sex male
Base zeropiu

Address
Private phone
Homepage
Password storage crypt
Certificates
Kerberos

Organizational information

Organization ZEROPIU SpA
Department Direzione Tecnica
Department No.
Employee No.
Employee type 2

Room No. 337
Phone
Mobile 348-0950472
Pager
Fax

Location milano
State
Address

Migration Requirements

- Seamless Migration
  - Without rejoin machine
  - User access with same password
  - Share access with same names
- Maintain File Permission and ACL on share
- Access log on special share
- Introduce Password enforcement

Migration Procedure

- Catalogize Shares and Printers
- Pwdump2 vs Vampire
- Build LDIF from SAM information
  - User acconut SID and Password
  - Computer account SID and Password
  - Group account
  - User and Group mapping
- Install ldap infrastructure
- Populate ldap
- Install Samba Domain controller
- Share Migration
- Switch Domain Controller
- Test user Login, login script and share acccess
- Set Password Policy

Troubles

- Ldap
  - Slave sometime disconnects to master (ldapsync) and loses synchronization
  - Berckley db corruption, sometime we need to rebuild the database by hand
  - When TLS is in use the cost of connection setup and binding is likely to far outweigh the search load.
  - A large pool of clients will also result in many hundreds of connections being held open, with a big usage of file descriptors.

- PAM module
  - CHAGE command didn't read shadow parameter from Ldap, replace with pwdutils

- Samba
  - Failure to join new computer to domain in Branch Office, latency in Directory replication
  - Locking file (old samba Version)

- Backup Filesystems ACL
  - ACLs are not handled from amanda backup system you need a separate script for dump to text file.

Current Status

- Implementation
  - 7 Samba Domain Controller
  - 350 Linux Desktop (LTSP) on 11 Server
  - 70 Windows Terminal Client on 3 Server
  - 130 Windows client

- Reduction Cost
  - Direct impact on help desk costs, achieving 60% time reduction
  - License Reduction 50%

- Benefit
  - Increase performance (Server and Desktop)
  - Increase security
  - Single sign-on
  - Reduced down time

Next Step

- Fedora Ldap Server
  - Multimaster
  - Better performance
  - Robust
- Samba 3.0.23
  - Printer Configuration
- LTSP 4.2
  - Faster, 22 sec boot time
  - LTSPFS, local device
- Multicast Boot, for pxes image
- Bacula Backup system

Next Step (Under Testing)

- Fileserver with Distributed Filesystem
  - AFS vs GFS
  - AFS single file system cross network
  - GFS high performance in local network
- Samba with AFS module
- Kerberos V
  - Heimdal with ldap bckend
  - AFS with 2b ticket support
  - Kerberos Password for Unix System
- Load Balancing / HA
  - LVS
  - OpenSSI
  - Xen

The End

For Further Questions:

Fabrizio Manfredi
Zeropiu
Via Fra Luca Pacioli n.3
20144 Milano (Italy)
manfred@zeropiu.it
http://www.zeropiu.com