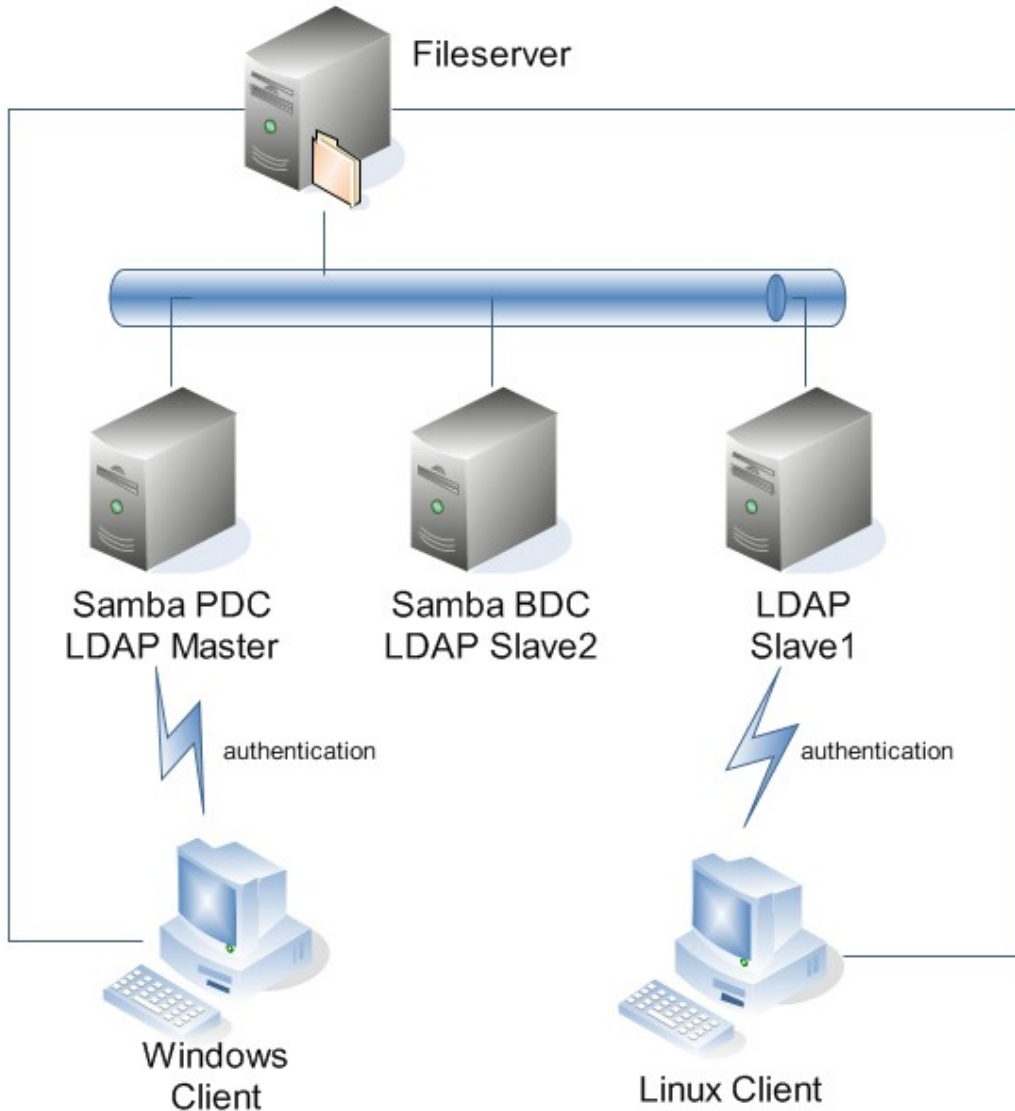


Hannes Kasparick

Samba as PDC / BDC with OpenLDAP



Overview



- authentication for Linux and Windows
- one password
- redundant authentication servers

What about LDAP?

- directory service
- database
- hierachical structure (tree)
- data saved in objects
- objects with attributes
 - self defined attributes possible
- objects adressed by distinguished name
 - DNS: host.domain.tld
 - LDAP: dc=host,dc=domain,dc=tld

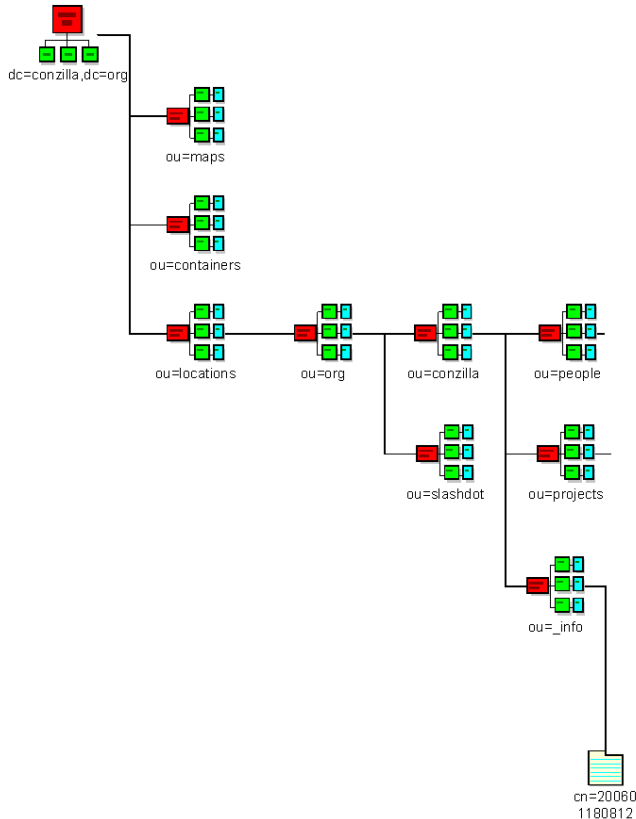
Notation

- OU Organizational Unit
- DC Domain Component
- CN Common Name

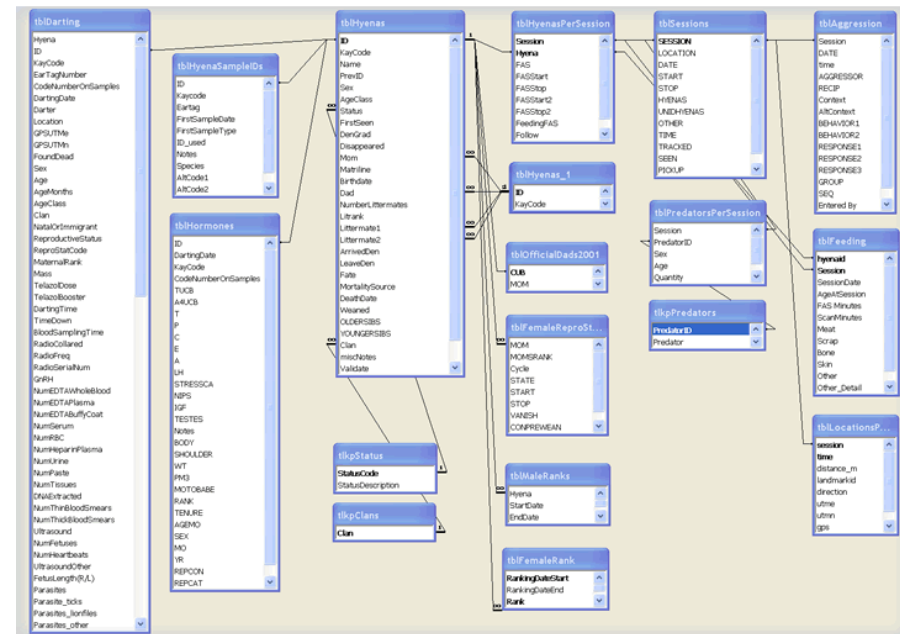
LDAP vs. Relational Database

- LDAP tree

- Relational DB



Source: <http://kmr.nada.kth.se>



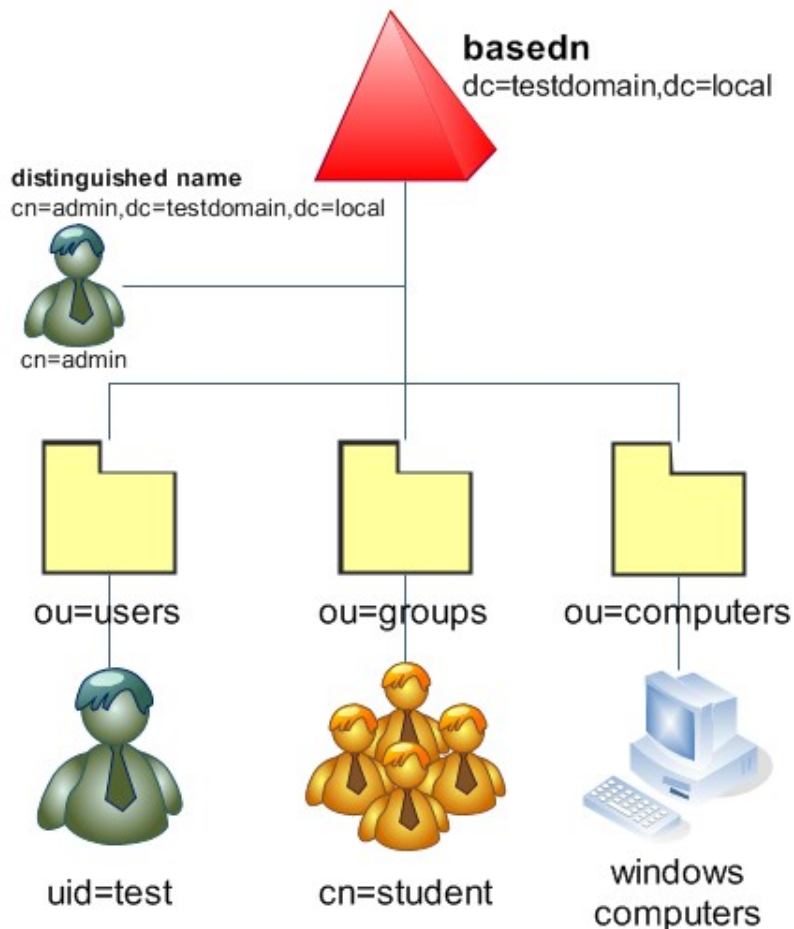
Source: <http://hyenas.zoology.msu.edu>



Approach

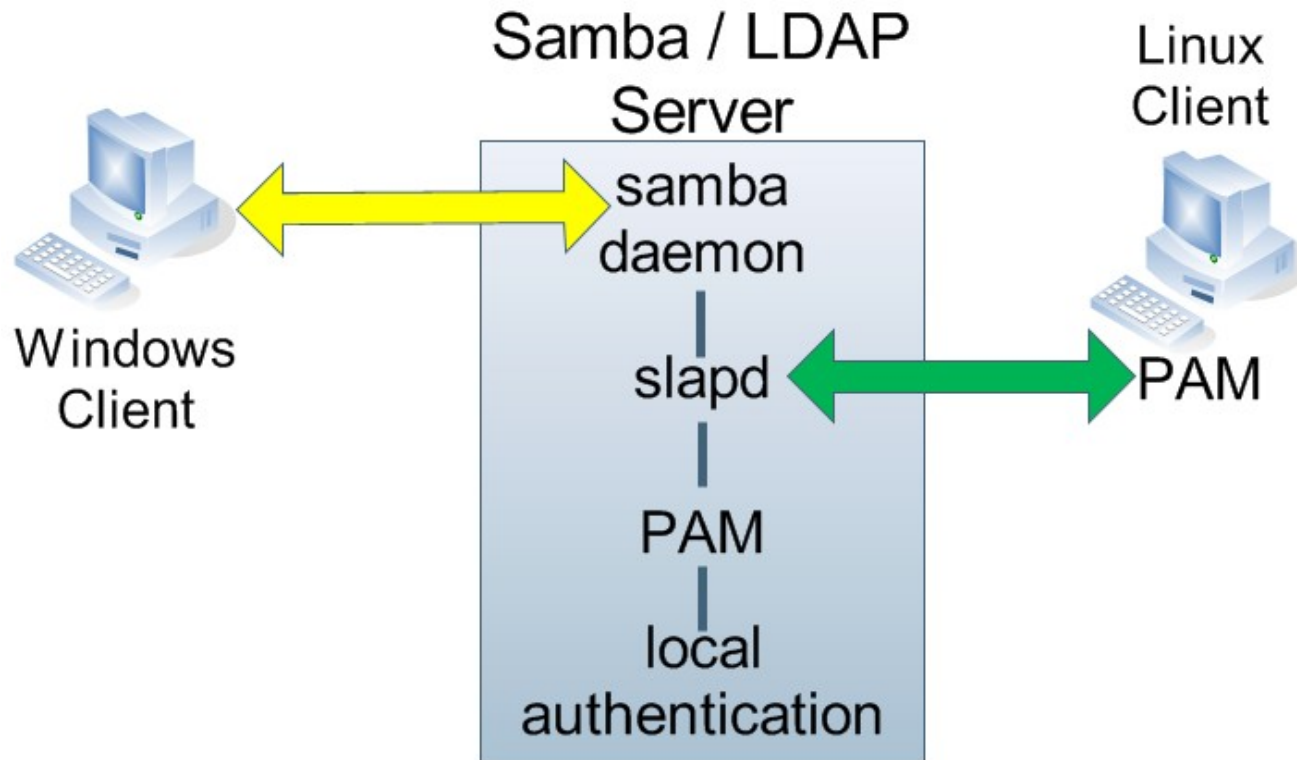
- 1) design LDAP structure of enviroment
- 2) set up OpenLDAP for Linux auth.
- 3) set up Samba PDC with LDAP auth.
- 4) set up OpenLDAP Slave
- 5) set up Samba BDC
- 6) if required: enable encryption

LDAP Structure



- keep it simple
- basedn is local domain name
- basedn can be different to samba domain name

Overview



Samba + OpenLDAP + Windows in 4 steps

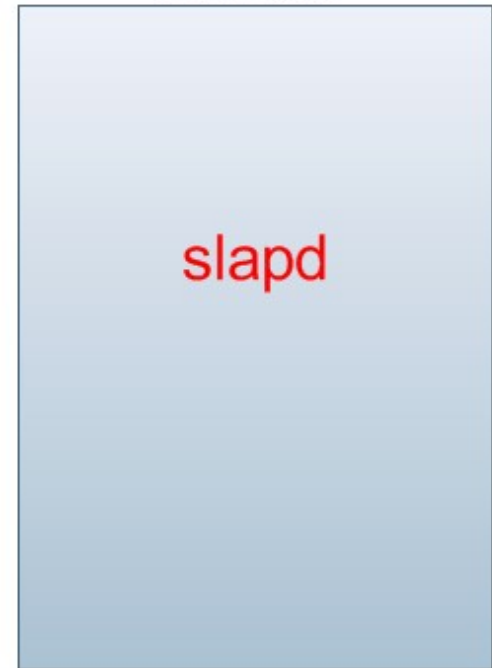
Step 1

- install slapd



Windows
Client

Samba / LDAP
Server



OpenLDAP Server



- slapd
- download at www.openldap.org
- use package of your distribution if possible

Installation

- Debian packages: slapd and ldap-utils
 - can differ in other distributions
- use LDAPv3 protocol
- set suffix (domainname)
- configure loglevel
 - see manpage for details
- add samba.schema

Config Changes slapd.conf

- general settings

suffix "dc=testdomain,dc=local"

rootdn "cn=admin,dc=testdomain,dc=local"

rootpw {SSHA}nSOVMp0ESCGmteCQxF9eoc

loglevel 256

include /etc/ldap/schema/samba.schema

– password generated with „slappasswd“

Config Changes slapd.conf

- configure access restrictions

access to

```
attrs=userPassword,shadowLastChange,sambaNT  
Password,sambaLMPassword,sambaPwdsMustC  
hange,sambaPwdsLastSet
```

by dn="cn=admin,cn=testdomain,dc=local" write

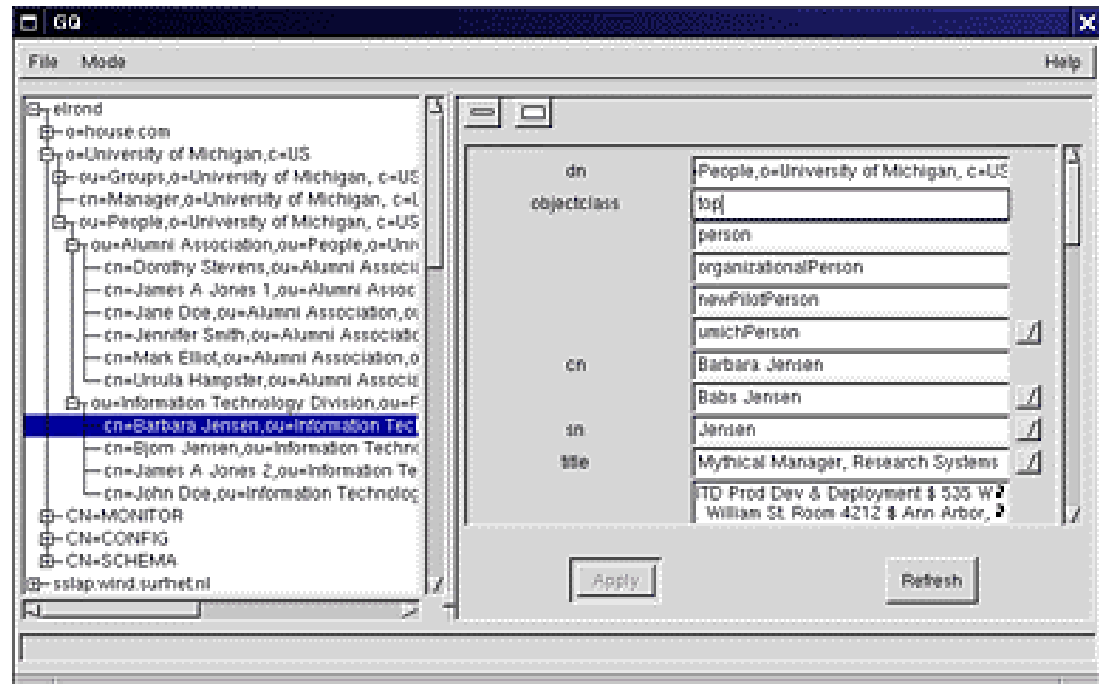
by anonymous auth

by self write

by * none

Access LDAP

- console with Idaputils: Idapsearch etc.
- GQ
- LDAP-Browser
- Idapvi
- ...



Source: <http://gq-project.org/>

Step 2

- install samba



Windows
Client

Samba / LDAP
Server



Samba as Domain Controller

- Samba 3.x acts as NT4 compatible DC
 - Primary and Backup Domain Controllers
 - can be used as BDC with NT4 together
 - no group policies per default (commercial products exist)
- Samba 4 with Active Directory
 - see talk of Kai Blin at 3:15pm here

show smb.conf



smbldap-tools

- powerful console management tools
- ~#: smbldap-populate
 - creates basic settings / users / groups
- no „adduser“ or „passwd“ any more!
- only smbldaptools or compatible tool
 - ~#: smbldap-useradd -a -m <username>
 - ~#: smbldap-passwd <username>
 - ~#: smbldap-usermod --shadowExpire 2008-04-18 hkaspari

Result

The screenshot shows the LDAP Browser Editor v2.8.2 interface. The left pane displays a tree structure with the entry 'uid=dom1' selected under 'ou=Users'. The main pane shows the following LDAP entry details:

Attribute	Value
sambaLMPassword	4EFC971E2C6A11F0C08DF1A38F3BA9D5
sambaPrimaryGroupSID	S-1-5-21-1517061898-121938522-113803174
displayName	System User
sambaLogonScript	dom1.cmd
objectClass	top
objectClass	inetOrgPerson
objectClass	posixAccount
objectClass	shadowAccount
objectClass	sambaSamAccount
userPassword	BINARY (34b)
sambaHomeDrive	H:
sambaLogonTime	0
uid	dom1
uidNumber	1000
cn	dom1
sambaLogoffTime	2147483647
sambaPwdLastSet	1172046615
sambaAcctFlags	[U]
loginShell	/bin/bash
sambaProfilePath	\\hkvm1\dom1\profile
gidNumber	513
sambaPwdMustChange	2147483647
sambaNTPassword	CAF90659636EA42A1C6946B045BCB6F5
sambaPwdCanChange	1172046615
gecos	System User
sambaSID	S-1-5-21-1517061898-121938522-113803174
description	System User
homeDirectory	/home/dom1
sambaKickoffTime	2147483647
sn	dom1
sambaHomePath	\\hkvm1\dom1
sambaPasswordHistory	00000000000000000000000000000000

The status bar at the bottom of the window shows 'Ready.' on the left and 'U' on the right.



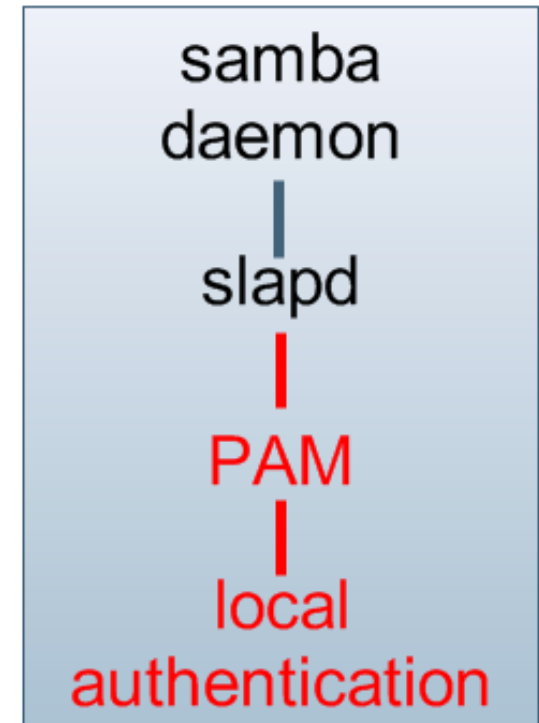
Step 3

- local PAM authentication



Windows
Client

Samba / LDAP
Server

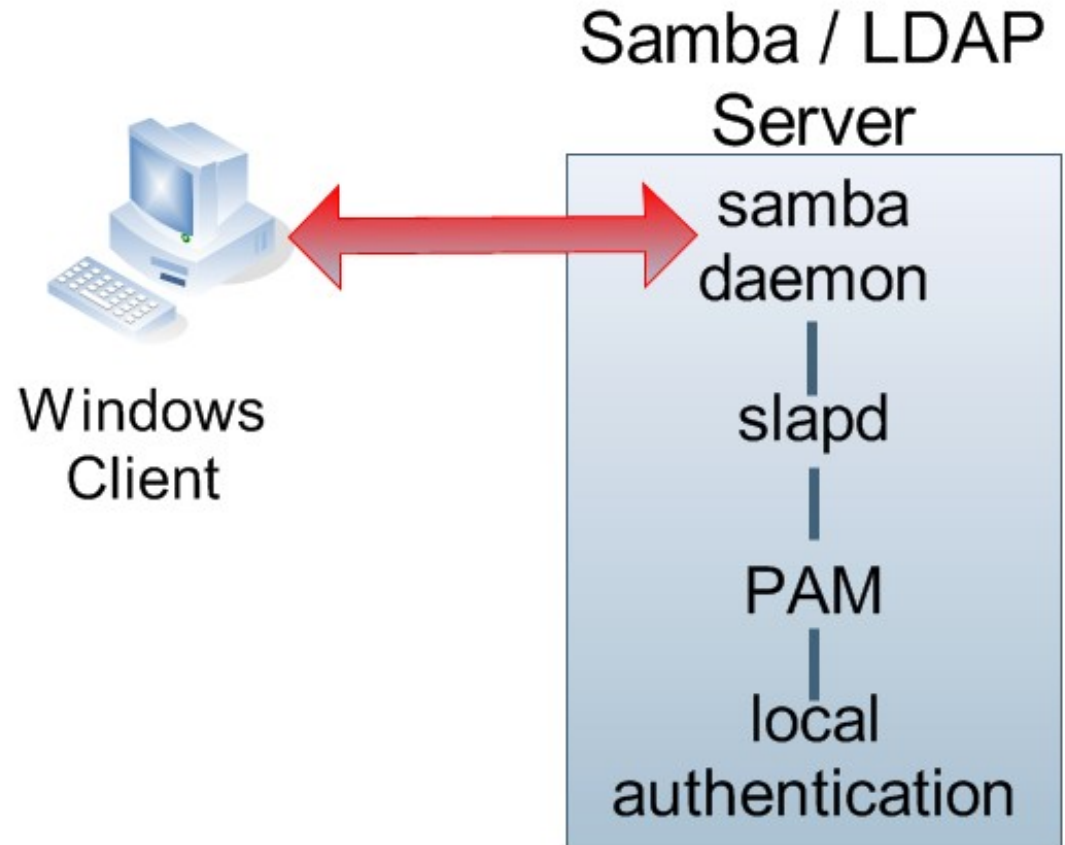


PAM and LDAP on Server

- Pluggable Authentication Modules
- libnss-ldap & libpam-ldap packages
- configure /etc/pam.d/*
- /etc/nsswitch.conf
 - passwd: files ldap
 - group: files ldap
 - shadow: files ldap
- ~#: getent passwd

Step 4

- integrate Windows



Adding Windows Clients

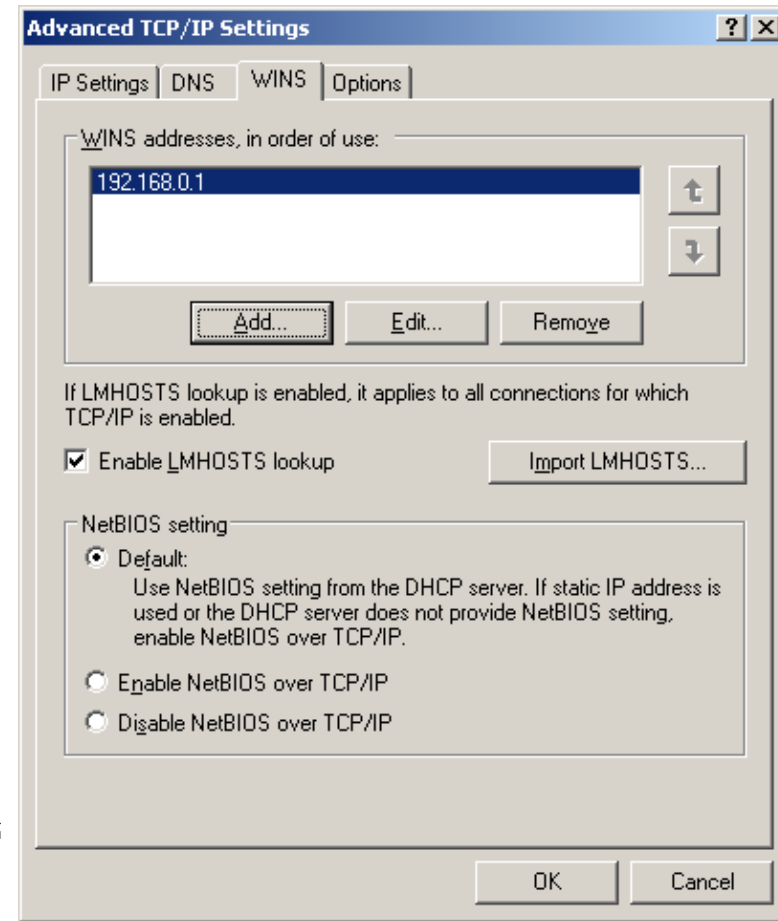
- Client needs to know the WINS server
 - DHCP or manually
- LDAP-root account
or

„~#: net rpc rights grant

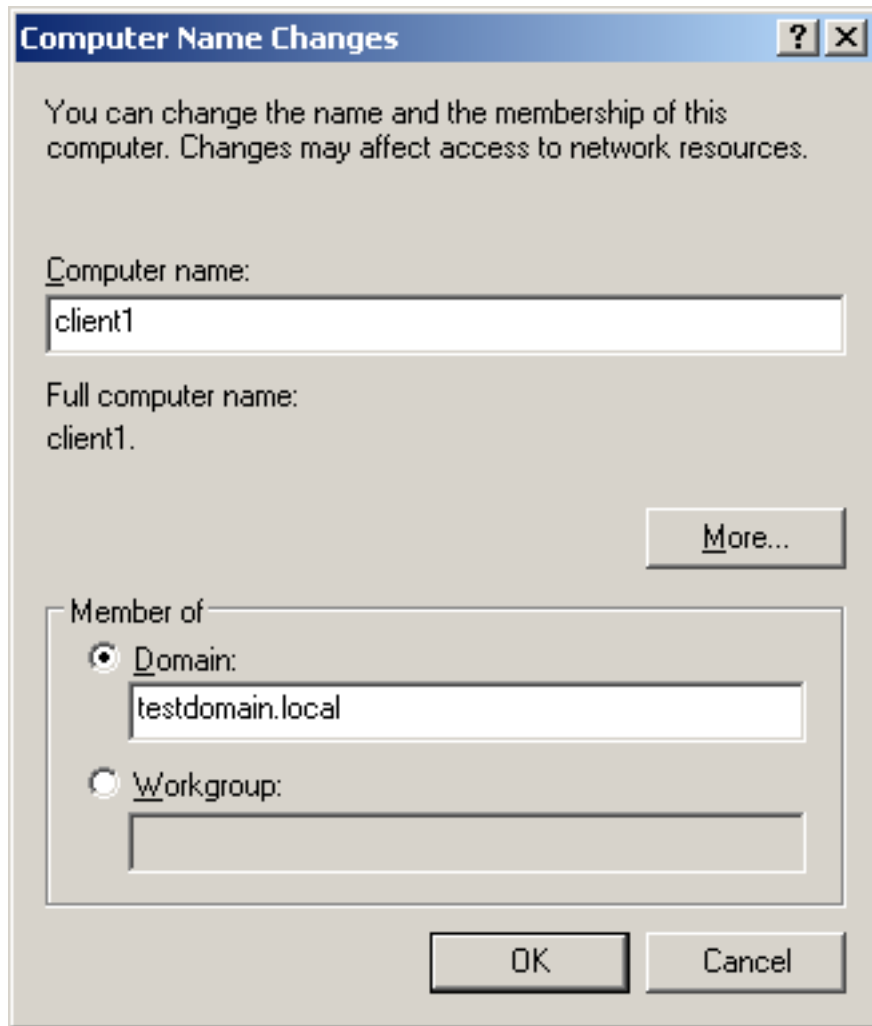
<username>

SeMachineAccountPrivilege“

„Successfully granted rights.“



Welcome to domain testdomain



Computer Name Changes [?] [X]

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name:
client1

Full computer name:
client1.

More...

Member of

Domain:
testdomain.local

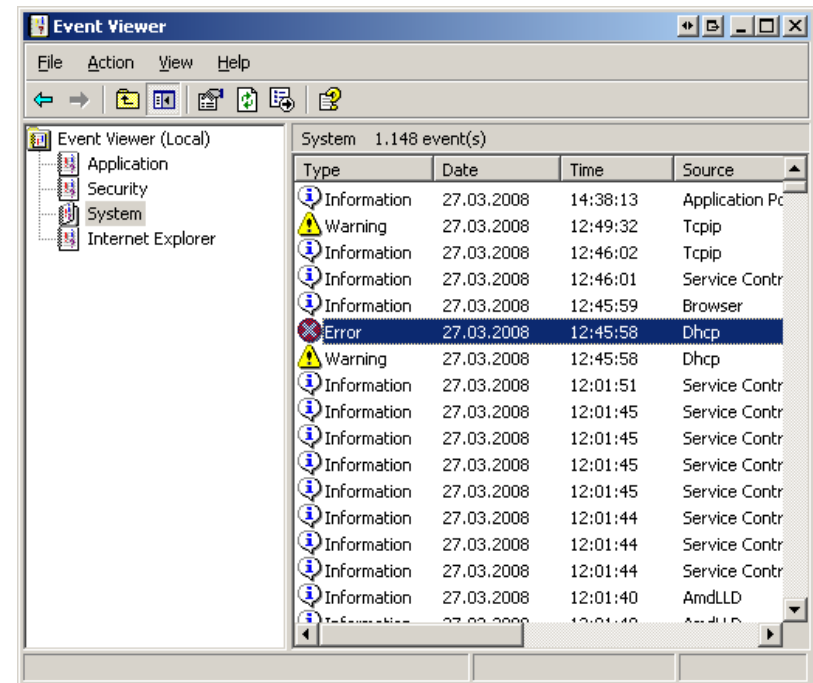
Workgroup:

OK Cancel

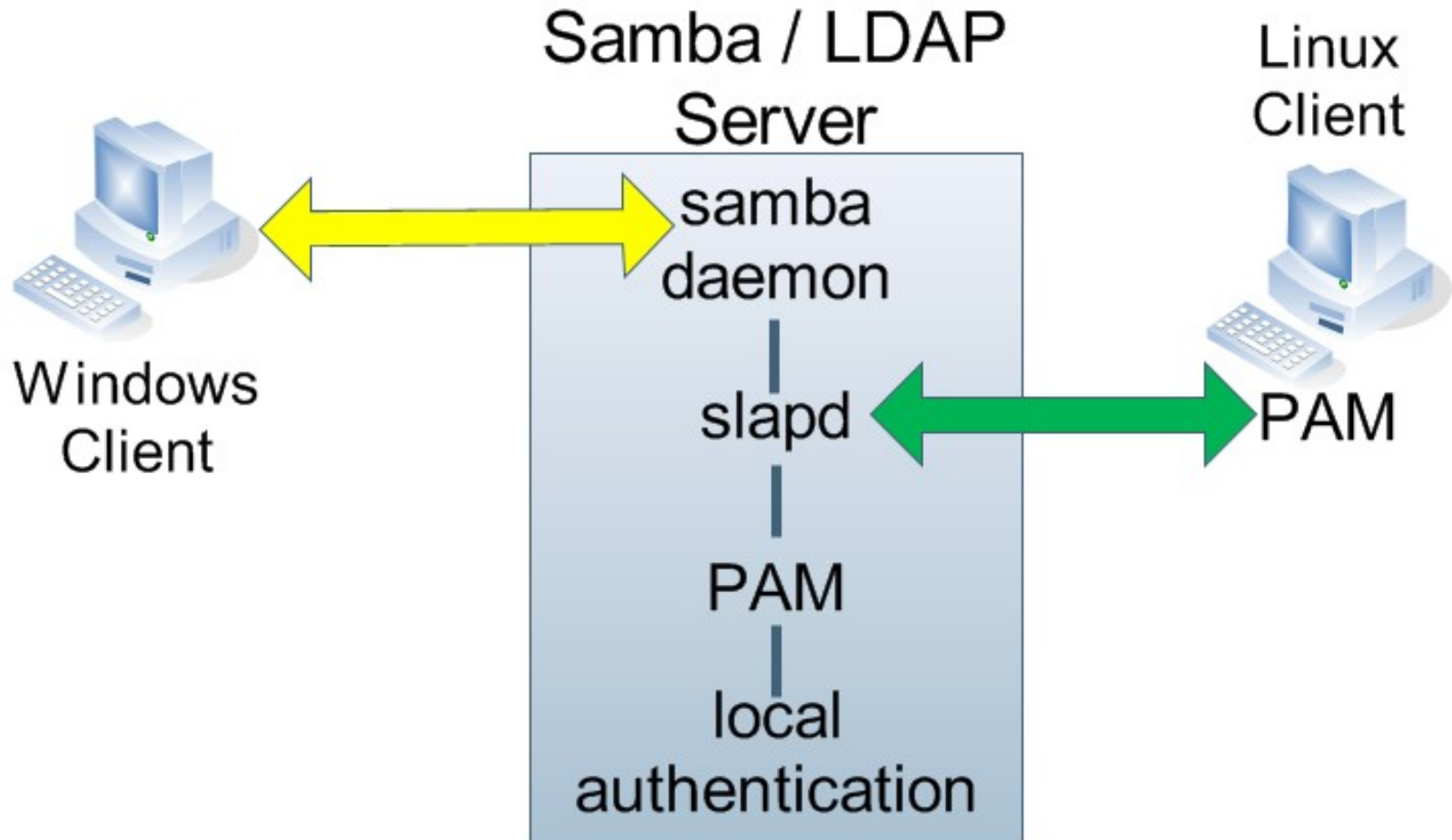
Welcome and
reboot :-)

Troubleshooting

- Look at Windows „eventlog“
 - Enable auditing: Control Panel | Administrative Tools | Local Security Policy | Local Policy | Audit Policy
- log.smbd
- slapd.log



What we have now



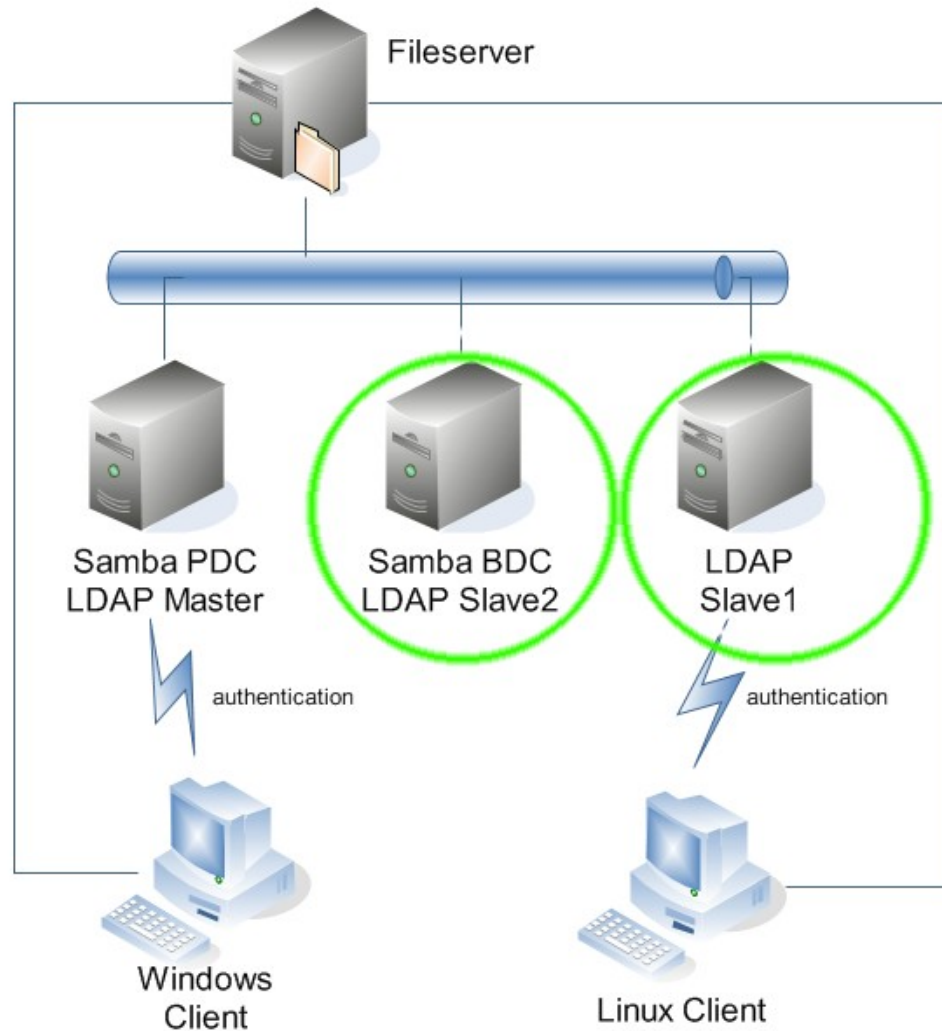
too bad...



High Availability

- domain controller down!?
 - Windows 2000 and newer caches logins
 - nscd daemon for caching in Unix
- more than redundant domain controller
 - switches, routing protocols
 - fileserver / storage
 - ...

Redundancy of slapd and samba



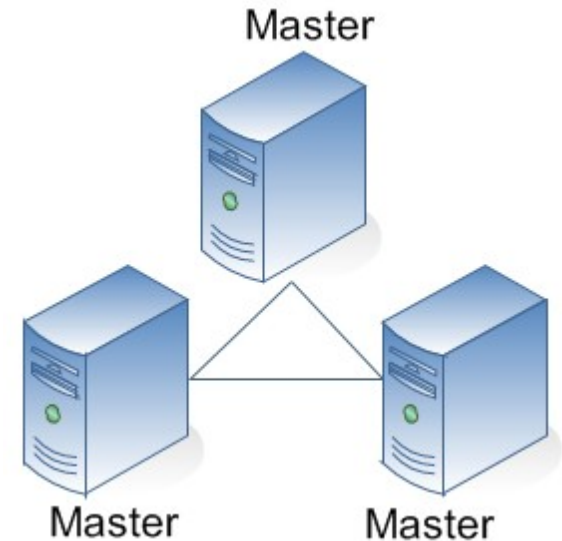
slapd-HA

- traditional: slurpd – Master / Slave
 - removed in version 2.4
- new since 2.2: syncrepl – Master / Slave
 - in 2.2 not for productive use
- current Version 2.4 (Oct. 2007)
 - N-Way Multi-Master replication
 - MirrorMode replication
 - Push mode / pull mode
 - delta-syncrepl

Multi Master Replication

- pro

- no single point of failure
- automatic failover
- can be in different locations

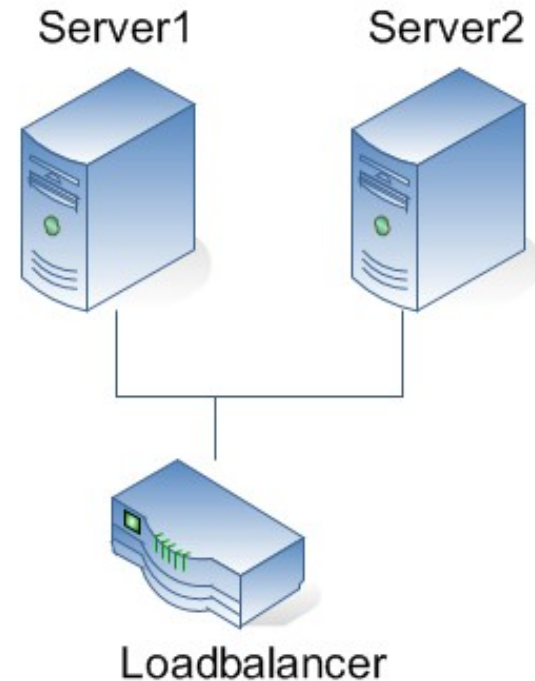


- contra

- network failures could lead to inconsistencies
- all writes must be propagated to all servers – might be much network traffic
- exact time needed (VMware time problems!?)

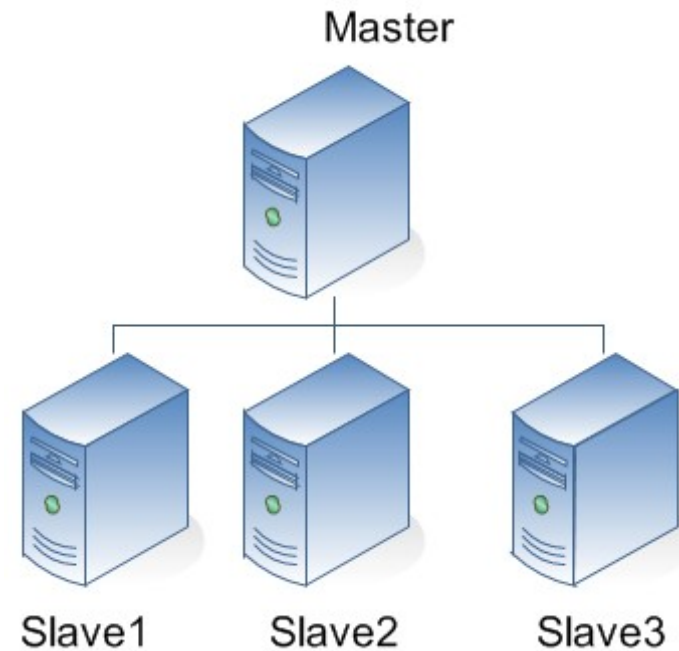
Mirror-Mode

- consistency guarantees of single-master replication, while providing HA
- external frontend directs access to servers
 - Active-Active Hot-Standby
- secondary master will only be used when first master crashed
- syncrepl / delta-syncrepl can be used



Master Slave Replication

- easy to manage
 - one master, many slaves
- all slaves copy data from master server
- when master down, only read access to slaves
- manual recovery: make one of the slaves a master



slapd.conf Master – Slave

- master

- moduleload syncprov

- slaves

- syncrepl rid=001

- provider=ldap://master.testdomain.local

- type=refreshOnly

- interval=00:00:00:10

- searchbase="dc=testdomain,dc=local"

- binddn="cn=admin,dc=testdomain,dc=local"

- credentials=password

HA - keep it simple

- you only have few changes and you do not need HA?
 - use one virtual machine with all services, make daily full backup
- pro
 - easy to configure
 - easy to manage
- contra
 - restore time probably longer
 - downtime while backup

Samba BDC

- backup Domain Controller like in NT4
 - since Windows 2000 there is no BDC
- almost identical configuration like PDC
- differences in smb.conf

netbios name = Samba-BDC

local master = no

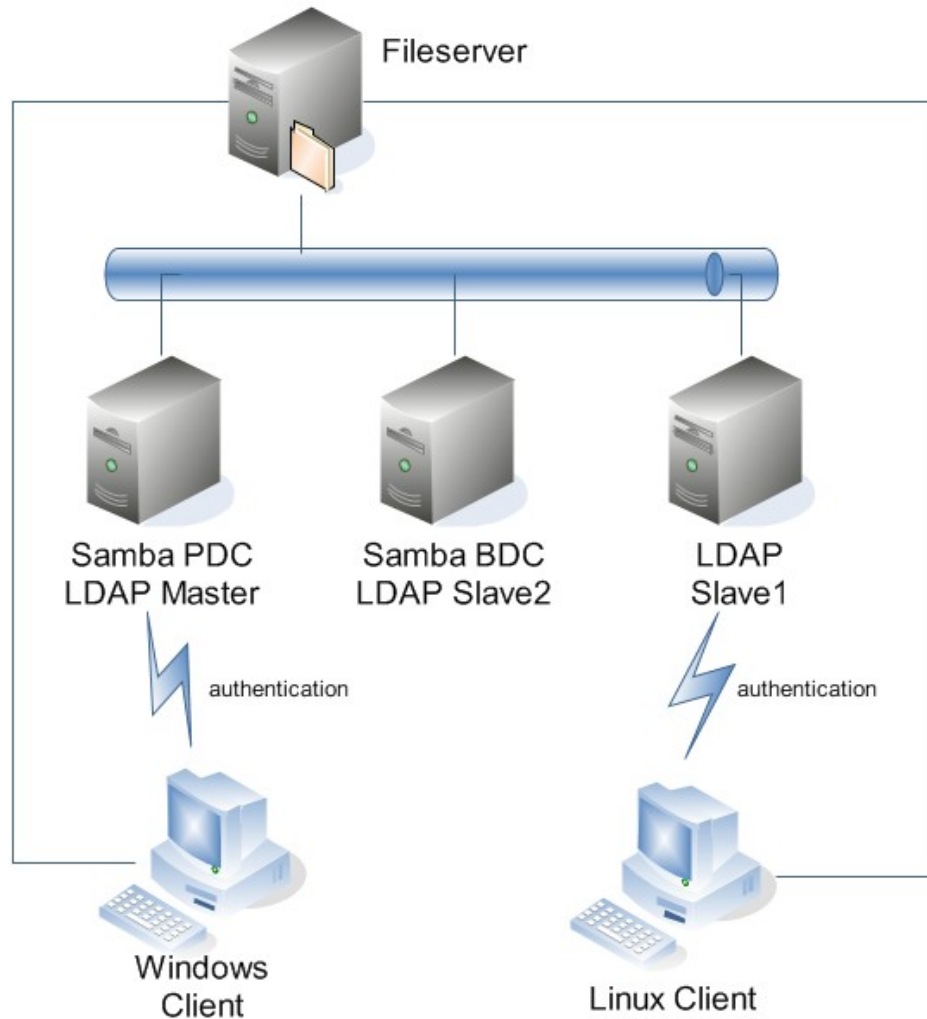
os level = 60

domain master = no

preferred master = no

passdb backend = ldapsam:"ldap://master ldap://slave/"

Done – everything reliable



Migration

- Windows NT to Samba
 - 1) Windows as PDC, Samba as BDC
 - 2) Upgrade Samba BDC to Samba PDC
 - 3) Add new Samba BDC
- NIS to Samba
 - Migration Tools [1] + scripting

[1] <http://www.padl.com/OSS/MigrationTools.html>

Migration Tools

- useful perlscript collection
- install them on PC in NIS-Domain
- change variables in migrate_common.ph
- export data from NIS
 - migrate_all_nis_offline.sh > nis.ldif
- split into relevant parts & scrub
- import data into LDAP

LDAP Security

Per default
unencrypted
but passwords
are hashed

Picture: client
server traffic
while ssh login

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

No.	Time	Source	Destination	Protocol	Info
22	2.077624	192.168.0.50	192.168.0.20	LDAP	searchResEntry(2) "uid=hkaspari
21	2.075406	192.168.0.20	192.168.0.50	LDAP	searchRequest(2) "dc=testdomain
19	2.074801	192.168.0.50	192.168.0.20	LDAP	bindResponse(1) success
17	2.072507	192.168.0.20	192.168.0.50	LDAP	bindRequest(1) "<ROOT>" simple
4	0.003138	192.168.0.50	192.168.0.20	LDAP	searchResDone(3) success [1 re
3	0.002988	192.168.0.50	192.168.0.20	LDAP	searchResEntry(3) "uid=hkaspari
2	0.000757	192.168.0.20	192.168.0.50	LDAP	searchRequest(3) "dc=testdomain

```

0000 08 00 46 67 a7 b9 00 0c 29 ce c7 96 08 00 45 00 ..Fg... )....E.
0010 01 c0 82 f3 40 00 40 06 34 ae c0 a8 00 32 c0 a8 ....@.@. 4....2..
0020 00 14 01 85 b5 93 f3 30 9f af 5d bc b6 12 80 18 .....0 ..].....
0030 00 f8 6c 88 00 00 01 01 08 0a 00 24 26 ae 00 08 ..l..... ..$&...
0040 3e e3 30 82 01 88 02 01 03 64 82 01 81 04 2c 75 >.0..... .d....,u
0050 69 64 3d 68 6b 61 73 70 61 72 69 2c 6f 75 3d 55 id=hkasp ari,ou=U
0060 73 65 72 73 2c 64 63 3d 74 65 73 74 64 6f 6d 61 sers,dc= testdoma
0070 69 6e 2c 64 63 3d 6c 6f 63 61 6c 30 82 01 4f 30 in,dc=lo cal0..00
0080 6f 04 0b 6f 62 6a 65 63 74 43 6c 61 73 73 31 60 o..objec tClass1`
0090 04 03 74 6f 70 04 06 70 65 72 73 6f 6e 04 14 6f ..top..p erson..o
00a0 72 67 61 6e 69 7a 61 74 69 6f 6e 61 6c 50 65 72 rganizat ionalPer
00b0 73 6f 6e 04 0d 69 6e 65 74 4f 72 67 50 65 72 73 son..ine tOrgPers
00c0 6f 6e 04 0c 70 6f 73 69 78 41 63 63 6f 75 6e 74 on..posi xAccount
00d0 04 0d 73 68 61 64 6f 77 41 63 63 6f 75 6e 74 04 ..shadow Account.
00e0 0f 73 61 6d 62 61 53 61 6d 41 63 63 6f 75 6e 74 .sambaSa mAccount
00f0 30 10 04 02 63 6e 31 0a 04 08 68 6b 61 73 70 61 0...cn1. ..hkaspa
0100 72 69 30 11 04 03 75 69 64 31 0a 04 08 68 6b 61 ri0...ui d1...hka
0110 73 70 61 72 69 30 13 04 09 75 69 64 4e 75 6d 62 spari0.. .uidNumb
0120 65 72 31 06 04 04 31 30 30 31 30 12 04 09 67 69 er1...10 010...gi
0130 64 4e 75 6d 62 65 72 31 05 04 03 35 31 33 30 21 dNumber1 ..5130!
0140 04 0d 68 6f 6d 65 44 69 72 65 63 74 6f 72 79 31 ..homeDi rectory1
0150 10 04 0e 2f 68 6f 6d 65 2f 68 6b 61 73 70 61 72 .../home /hkaspas
0160 69 30 19 04 0a 6c 6f 67 69 6e 53 68 65 6c 6c 31 i0...log inShell1
0170 0b 04 09 2f 62 69 6e 2f 62 61 73 68 30 16 04 05 .../bin/ bash0...
0180 67 65 63 6f 73 31 0d 04 0b 53 79 73 74 65 6d 20 gecoc1.. .System
0190 55 73 65 72 30 38 04 0c 75 73 65 72 50 61 73 73 User08.. userPass
01a0 77 6f 72 64 31 28 04 26 7b 53 53 48 41 7d 49 6e word1(.& {SSHA}In
01b0 67 6d 74 5a 4b 56 68 4c 34 30 64 59 58 65 62 62 gmtZkVhL 40dyxebb
01c0 5a 38 71 30 77 51 2f 4b 56 6d 4e 6d 6c 77 z8q0wQ/K vMnMlw

```


How to secure?

- StartTLS or LDAPS possible
 - StartTLS is standard method today
 - LDAPS listed as deprecated
- both methods can be used on same server
- note: it is tricky to configure!

considerations

- use stable distribution
- if it works – avoid updates
- maybe problems with gnutls versions
- debug TLS

```
ldapsearch -x -D cn=admin,dc=testdomain,dc=local  
-W -H ldap://master -ZZ -d 8
```

procedure

- create Certificate Authority and certificates
 - OpenSSL package includes scripts
 - no passwords for server certificates
- configure slapd with TLS
 - beware of AppArmor in new Ubuntu
- propagate CA-certificate to Clients
- configure clients to use TLS

Secured

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

No.	Time	Source	Destination	Protocol	Info
189	2.931029	192.168.0.50	192.168.0.20	TLSv1	Application Data
190	2.931847	192.168.0.20	192.168.0.50	TLSv1	Application Data
191	2.933995	192.168.0.50	192.168.0.20	TLSv1	Application Data
192	2.934282	192.168.0.50	192.168.0.20	TLSv1	Application Data
194	2.936109	192.168.0.20	192.168.0.50	TLSv1	Application Data
195	2.938728	192.168.0.50	192.168.0.20	TLSv1	Application Data
196	2.939168	192.168.0.50	192.168.0.20	TLSv1	Application Data
197	2.939921	192.168.0.20	192.168.0.50	TLSv1	Application Data
198	2.942186	192.168.0.50	192.168.0.20	TLSv1	Application Data
202	2.944779	192.168.0.20	192.168.0.50	TLSv1	Application Data
204	2.947785	192.168.0.50	192.168.0.20	TLSv1	Application Data
205	2.948074	192.168.0.50	192.168.0.20	TLSv1	Application Data
232	2.995477	192.168.0.50	192.168.0.20	TLSv1	Server Hello
233	2.995645	192.168.0.50	192.168.0.20	TLSv1	Certificate

0000 08 00 46 67 a7 b9 00 0c 29 ce c7 96 08 00 45 00 ..Fg....).....E.
0010 01 09 90 22 40 00 40 06 28 36 c0 a8 00 32 c0 a8 ..."@.@.(6...2..
0020 00 14 01 85 d5 20 4b cc 1e 7e 17 a4 ee 6f 80 18K.~...o..
0030 01 3b 50 8c 00 00 01 01 08 0a 00 39 84 86 00 14 .;P.....9....
0040 1d 6a 17 03 01 00 d0 77 6c 80 bb 8d 12 53 d0 65 .j.....w}....S.e
0050 51 2f 64 5f dd 2d 67 08 5c 7b 34 61 c8 b2 7e 30 Q/d_-g. \{4a..~0
0060 2f a7 3e 6e ab eb 9f 9d 2d 8a 8b aa 6a 63 49 7f /.>n....-...jCI.
0070 08 8d ed 4c d8 0f ad 94 7d e9 91 4c 62 0e c4 f6 ...L.....}..Lb...
0080 91 21 a0 d9 ef 96 77 af ba 45 3e c3 f5 50 b2 2e .!.....w. .E>..P..
0090 14 95 9a 59 c1 1d 2f d9 65 41 09 ba 30 65 3f df ...Y.../. eA..0e?.
00a0 af 8d a5 30 79 ef fa 45 6b 76 ab ca e6 e2 61 d2 ...0y..E kv....a.
00b0 05 62 c0 e9 a5 8e 3a ee 62 4c d5 37 18 9f 20 35 .b.....: bL.7.. 5

More Information?

- Matt Butcher - Mastering OpenLDAP
Packt Publishing (2007)
- <http://wiki.samba.org>
- <http://de5.samba.org/samba/docs/man/Samba-HOWTO-Collection/>
- <http://samba-ldap.de/> - German howto

Questions?

