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
- hierarchical structure (tree)
- data saved in objects
- objects with attributes
  - self defined attributes possible
- objects addressed by distinguished name
  - DNS: host.domain.tld
  - LDAP: dc=host,dc=domain,dc=tld
Notation

- **OU** Organisational 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 environment
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
• install slapd
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}nSOVMp0ESCgmeteCQxF9eoc
  - loglevel 256
  - include /etc/ldap/schema/samba.schema

- password generated with „slappasswd“
Config Changes slapd.conf

- configure access restrictions

access to

attrs=userPassword,shadowLastChange,sambaNTPassword,sambaLMPassword,sambaPwdMustChange,sambaPwdLastSet

by dn="cn=admin,cn=testdomain,dc=local" write
by anonymous auth
by self write
by * none
Access LDAP

- console with ldaputils: ldapsearch etc.
- GQ
- LDAP-Browser
- ldapvi
- ...

Source: http://gq-project.org/
Step 2

• install samba
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
Step 3

• local PAM authentication
PAM and LDAP on Server

• Plugable 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
• 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

Welcome and reboot :-)

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.

Member of

- Domain: testdomain.local
- Workgroup:

OK Cancel
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

- Samba / LDAP Server
- Windows Client
- Linux Client
- Samba daemon
- slapd
- PAM
- local authentication
- PAM
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
  – files server / storage
  – ...
Redundancy of slapd and samba

Diagram:
- Fileserver
- Samba PDC LDAP Master
- Samba BDC LDAP Slave2
- LDAP Slave1
- Windows Client
- Linux Client
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

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
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
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>189</td>
<td>2.931029</td>
<td>192.168.0.50</td>
<td>192.168.0.20</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>190</td>
<td>2.931847</td>
<td>192.168.0.50</td>
<td>192.168.0.20</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>191</td>
<td>2.933995</td>
<td>192.168.0.50</td>
<td>192.168.0.20</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>192</td>
<td>2.934282</td>
<td>192.168.0.50</td>
<td>192.168.0.20</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>194</td>
<td>2.936109</td>
<td>192.168.0.20</td>
<td>192.168.0.50</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>195</td>
<td>2.938728</td>
<td>192.168.0.50</td>
<td>192.168.0.20</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>196</td>
<td>2.939168</td>
<td>192.168.0.50</td>
<td>192.168.0.20</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>197</td>
<td>2.939921</td>
<td>192.168.0.20</td>
<td>192.168.0.50</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
<tr>
<td>198</td>
<td>2.942186</td>
<td>192.168.0.50</td>
<td>192.168.0.20</td>
<td>TLSv1</td>
<td>Application Data</td>
</tr>
</tbody>
</table>

Secured
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?