

Samba / LDAP Lessons learnt

LDAPConf 2007

Cologne

6./7. September 2007

Volker Lendecke

SerNet

Samba Team



Volker Lendecke

- Co-founder SerNet - Service Network GmbH
 - Free Software as a successful business model
 - Network Security for the industry and the public sector
 - Samba-Support/Development in Germany
- For 15 years concerned with Free Software
- First patches to Samba in 1994
- Consultant for industry in IT questions
- Co-founder emlix GmbH (Embedded Systems)



Overview

- Samba3 with LDAP
- A view on /etc/passwd and /etc/group
- Why the German Parliament migration failed 1st time
- Libldap
- Samba4 / LDAP



Samba3 with LDAP

- Samba needs more information about a user than Unix provides
 - Different password hash style
 - All information you can find in usrmgr.ex or mmc
- Modular so-called „passdb“ backends
 - Smbpasswd (plain text), tdbsam (local db), ldapsam
- Winbind can store its ID mappings in LDAP
- ADS-Membership needs LDAP connectivity



Samba3 with LDAP

- The samba Schema designed very closely to the internal Samba APIs
- Samba4 will have a schema close to AD, which is completely different
- Mapping between the two has been tried, but as Samba4 is not in production yet, the need is limited



/etc/passwd, /etc/group

- Most important question during login:
 - What are my ID's to base access right on?
 - Uid, primary gid and auxiliary groups
- /etc/group: dialout:x:16:vlendec,administrator,vl
- Enumerating the file /etc/group is necessary to find all auxiliary group memberships
- „id <user>“ on my box does exactly this, „su - <user>“ doesn't
 - Linux nss knows the „initgroups“ call



Typical Windows-Login

- SamLogon call for the real login, calculates groups
- Applications can issue GetGroupsForUser and GetAliasMembership calls
 - These application-level calls also calculate groups
- Some Windows autostart applications do this
- The German Parliament's logon session did this 3 times
 - 4 times calculate group memberships



Samba as a Unix daemon

- Samba has followed the philosophy to be a „good citizen“ in the Unix environment: Use libc APIs where available
- man getgrouplist in Linux:
 - The glibc 2.3.2 implementation of this function is broken: It overwrites memory when the actual number of groups is larger than *ngroups
- 4 enumerations of 5000 groups per windows login
- Very quickly slapd was very unhappy



Fixes

- The obvious fix here was to dump the „good citizen“ policy
- LDAP queries done directly, this time optimized
- (&(objectclass=sambaGroupMapping)
(|(memberUid=<username>)(gidNumber=<gid>)))
- This breaks the Unix compatibility
- Enabled with „ldapsam:trusted = yes“



Round-Trips are evil

- When Windows views an ACL, it has to display names
- query_securitydescriptor only sends SIDs
 - Sid2name translation happens in bulk
- Naive implementation via individual getgrgid calls
- ldapsam:trusted: One large query is sent with all SIDs, only asking for the names



Winbind in AD

- Winbind provides Windows domain users and groups as /etc/passwd and /etc/group entries
- Quite some Unix applications enumerate /etc/passwd and /etc/group
- Enumeration of anything is evil, there might be MANY entries coming in
- PSA in France implements Linux desktops using winbind: > 100.000 users in a single domain
- „winbind enum users/groups = no“



The „id“ command

- List current ID's numerically and by name
- getgroups() fetches numeric IDs
- Translation to the name via getgrgid()
- getgrgid for „Domain Users“ might take a while
 - In addition to the name, getgrgid also gives all members (remember PSA, >100.000)
- No way to cheat like with ldapsam:trusted
 - Applications issue this command
- Winbind has to cut „Domain Users“



libldap

- OpenLDAP's libldap contains async calls
- These calls are not as async as necessary
 - connect(2), write(2) calls to the network are synchronous
 - LDAP server down leads to hard blocks
- Libldap didn't allow access to the data stream (SASL)
- This is what led me to write the (now) S4 LDAP libs
- Later OpenLDAP libs do allow access to the data stream, we can do our own network calls now



Samba4 / LDAP

- Active Directory is basically LDAP, Kerberos, CIFS and DNS bundled
- (caveat: I'm not a Samba4 developer...)
- Samba4 contains its own LDAP server
- Internal to Samba4, ldb provides a simple local database with the basic LDAP data model
- OpenLDAP / Cyrus SASL source as of 3 years ago was quite a big piece to swallow
- „How hard can it be“



Samba4 / LDAP

- Well, it turns out to be harder than expected
- Full LDAP semantics are quite complex
- Andrew Bartlett works on Samba4 with Fedora DS as the backend database
- An alternative approach to doing it on our own might be a local slapd fully configured via ldapi
- If we had known the OpenLDAP developers personally and if OpenLDAP had been at the point where it is now 3 years ago, we might not have done it.



Questions/comments?

Volker Lendecke, VL@SerNet.DE

SerNet - Service Network GmbH
Bahnhofsallee 1b
37081 Göttingen

Tel: +49 551 370000 0

Fax: +49 551 370000 9

<http://www.SerNet.DE>

<http://Samba.SerNet.DE>

