SerNet

Samba 3 update

SambaXP 2006

Göttingen

24.-26. April 2006

Volker Lendecke

SerNet - Service Network GmbH

Network Service in a Service Network

SerNet

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)

Network Service in a Service Network

Samba 3 and beyond

- Completely, non-scientific change rates:
  - 3.0.3 -> 3.0.14: 102773 lines
  - 3.0.14 -> 3.0.20 119458
  - 3.0.20 -> 3.0.21 108087
  - 3.0.21 -> 3.0.22 14316 (security release)
  - 3.0.22 -> 3.0.23 116090
- So, something has happened after 3.0.14
- Samba 3 is back to speed again – what has changed for 3.0.23?

Samba 3.0.23pre1

- New offline mode in winbindd
- New kerberos support for pam_winbind.so
- New non-root share management tools
- New handling of unmapped users and groups
- net sam utility
- Improved support for local and BUILTIN groups

winbind offline mode

- Windows workstations are normal domain members
- Authentication is online against the DC
- „The Laptop taken home“
  - Windows users can log in using cached credentials
- For the NLD (SLD? SLED? ;-)) Günther Deschner added cached credentials to winbind
  - Users taking laptops home can still log in
  - But how do I get /home then...? (Someone needs to revitalize coda)

Kerberos support for pam_winbind

- With pam_krb5 you can get Kerberos tickets
- Windows typically issues renewable tickets
  - The ticket issued is valid for, say, 10 hours
  - Using the ticket issued you can get new tickets for maybe a week
- With winbind taking care of the user's credential cache, it takes care of re-newing tickets

New non-root share definitions

- Using Windows XP, non-Admin users can be given the privilege to maintain their own shares
- Jeremy Allison added the „usershare“ parameters
- Administrators can give users the ability to define shares
- See Jeremy's talk tomorrow

Handling user and group IDs I

- Unix uses uid/gid's (32-bit numbers) to identify users and groups
- Windows does the same with SIDs, essentially 128-Bit ID's with some additions
- Samba needs to map between both in various places
- Until 3.0.22 this is messy at best
- Ad-Hoc ID mapping could lead to conflicting maps

Handling user and group IDs II

- Mapping SIDs to Unix IDs
  - Unix IDs are allocated by winbind from the idmap range
- Mapping Unix IDs to SIDs
  - Users are mapped from passdb backend (tdb/ldap)
  - Groups are mapped from group mapping (net groupmap)
- Fall back to algorithmic mapping (RID=uid*2+1000)
- Collisions are easy to generate

Handling user and group IDs III

- Samba 3.0.23: No fallback to algorithmic mapping
- Unmapped users and groups are assigned SIDs:
  - S-1-22-1-<uid> and S-1-22-2-<gid>
- Unmapped groups can not be part of the Token shipped to a domain member at logon time
- 3.0.23 contains a RID allocator in the user database

net sam utility

- net groupmap and pdbedit: Interfaces only the developer could love
- net sam mapunixgroup: Allocate a new RID and map a unix group to the corresponding SID
- net sam create[builtin|local]group: Add a mapping representing a local group, needs winbind to allocate a gid
- net sam set: Edit user accounts

Improved local group handling

- Release notes of 3.0.3: „Support for local nested groups via winbind“
  - Late last year a customer of mine actually wanted to use this in a large installation, so I had to fix it...
  - This is what started the user/group id changes I described
- valid users = @BUILTIN\users

SerNet

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

Network Service in a Service Network