univention

linux for your business

Samba as a Backup Domain Controller

Samba XP 2007

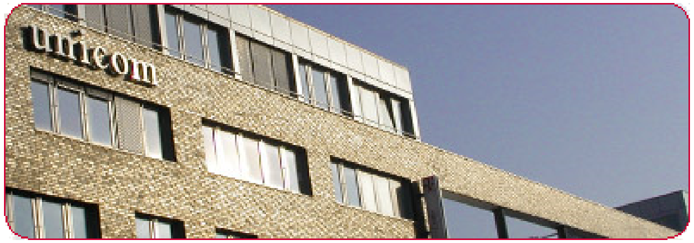
Agenda

1. speaker and company
2. motivation
3. basics
    1. existing code
    2. installation and configuration
4. additional challenges
5. real life behaviour
6. conclusion/discussion

speaker - company

- studied Applied Computer Science in the Natural Sciences
- experiences in Linux and Open Source since 1998 (user, administrator, developer, consultant)
- joined Univention GmbH in 2004 as developer and project manager

- Univention GmbH was founded 2001 in Bremen/Germany
- one of the leading Open Source solution providers in Germany
- developer of „Univention Corporate Server“ (UCS), a Linux Distribution focused on management of heterogeneous networks



motivation

- long-time (several month) migration of a Windows NT domain with > 2.500 users to Linux
- synchronisation of NT users and passwords to POSIX accounts
- OpenLDAP based storage of users and groups
- no more windows after migration (no long-term dependency on windows-services)
- implement new concepts of group-membership while user-passwords are synchronized from Windows NT

why don't use „net rpc vampire“, „pwdump“ or ... ?

- transfers always the complete userbase, not only changes
  - may cause high load
  - may take several minutes (every object needs to be compared)
- not event driven
  - needs a schedule (i.e. cron job)
  - a new sync must not start while an old one is running
  - time between change and synchronisation not predictable

technical basics: code and patches

- original patch against Samba 3.0.11, posted in March 2005 by Richard Renard (www.idealx.com)
- being an interim solution Samba 3.0.11 was sufficient for this project
- the patch did not need any changes in terms of functionality or bugfixes

technical basics: installation

- patch, compile and install Samba (precompiled packages are only available for UCS)
- configure Samba as BDC (which means: like a Samba-PDC, but with "domain master = no")
- join into the Windows NT domain („net rpc join“)
- start new daemon "samsyncd" once in "one shot mode" for initial replication
- add „samsyncd“ to init-scripts to synchronize further changes

technical basics: operation

- each change on NT increases a „modcount“
- at startup samsyncd connects to its PDC, gets the actual modcount and replicates all changes since its last stored modcount
- afterwards it runs daemonized and waits for changes:
  - the Windows NT PDC announces changes to nmbd
  - nmbd informs samsyncd
  - samsyncd asks the modcount and replicates the changes

technical basics: configuration

- synchronisation interval is controlled on the PDC in „HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ NetLogon \ Parameters“
  - Pulse: changes made within this time are send bundled to a BDC, if no change occured no pulse is send (default: 300 seconds)
  - PulseMaximum: time after which a pulse is always send, even if there are no changes made
- modcount.tdb stores the last replicated change-id (modcount) for samsyncd, if this file doesn't exist samsyncd will replicate all data
- everything else is configured like a Windows NT migration with „net rpc vampire“, in particular scripts like „add user script“ etc. should exist

project challenges: meet LDAP structure

- several add/del/modify scripts needed, in particular:
  - sync of machines, groups and group-membership needed to be disabled: deactivation of add group/machine script was sufficient
  - usernames which are upper-case in NT should be lower case in LDAP: implemented in add user script, samba-ldap-backend maps case-insensitive
  - rename of users in group-memberships: modifications like rename need to be done also in existing LDAP-groups (modify user script)
- one additional script-option was needed:
  - "post modify user script" to add kerberos-attributes based on the synced NT/LM-Password

project challenges: isolation

- Samba logon services must not be available:
  - group memberships are different
  - machine accounts don't exist
- Samba BDC must not be visible in the NT Domain because logon services are not available
- Configuration:
  - Samba is configured to only one interface
  - network activity is limited to communication with NT PDC (iptables): this means also TCP and UDP broadcasts, which need to be rewritten

project challenges: bidirectional synchronisation

- on Linux side password changes don't occur against the PDC
- password changes modify also NT/LM-hashes in LDAP
  - using PAM-modules if changed by an user
  - using scripts/tools if changed by an administrator
- by LDAP change notifications (part of UCS LDAP management system) new hashes are send to the NT PDC
- a daemon receives the new password hashes and announces them in NT with "pwdump"
  - users are disabled in NT if their password is set, further action is necessary (i.e. call cusrmgr.exe)

experiences in „real life“

- good experiences
  - easy integration in existing samba distribution
  - stable and reliable system for several month
  - found no bugs in the original patch
  - hanging syncs resulted always from wrong configuration or firewall-settings
- possible improvements
  - samsyncd uses stdout/stderr without timestamps, it should use logfiles

conclusion/discussion

contact:

Univention GmbH

www.univention.de

Bremen/Germany

Ingo Steuwer

steuwer@univention.de