Bring Linux into Microsoft´s ADS

A lecture by Jens Kühnel

Jens Kühnel
Konsult und Training
Bad Vilbel Germany

About the speaker

- Jens Kühnel
  - computer freak since age 8
  - Linux user since 1995
  - freelancer since 1999
  - certified RedHat, SuSE and Microsoft trainer
  - RHCE, 4/5 RHCA, RHCX, SCLT, MCSE, MCT
  - book author:
    Samba 3.0 – “Wanderer zwischen den Welten“

Overview

- Samba
  - Security = server/Domain
  - Security = ADS
  - add user script
- Kerberos (pure)
- Winbindd
- Winbindd with LDAP-IDMAP
- SFU

What is Active Directory

- Domain-Model of Microsoft since Windows 2000
- Technical Parts:
  - LDAP-Server with strange schema and Multi master replication
  - Kerberos with „MS-enhancements“
  - DDNS (with Kerberos)

Samba and NT-Domains

- *security = server*
  - available since 1.x
  - uses any server (with user-security)
- *security = domain*
  - available since 1.x
  - uses an NT4 domain
  - Needs an machine account or admin password
- *security = ads*
  - Available since 3.x
  - Uses LDAP and Kerberos
  - Needs an machine account or admin password

User-ID Problem

- Every Samba-User needs a Unix-User-ID
- User can be created by *add user script*
- User-IDs are created in passwd/shadow on every machine

Winbindd

- Winbindd creates a Unix user accounts on the fly
- Winbindd connects to Windows NT4 or ADS-Domain
- Winbindd is a nsswitch- and PAM-Module
- Winbindd is a service shipped with Samba

Configure Winbindd

- Use *authconfig* with RedHat
- manual
  - Add winbind to */etc/nsswitch.conf* and */etc/pam.d/system-auth*
  - Join Domain (*net join -U Administrator*)
  - *smb.conf*
    - *Winbind seperator* = +
    - *Idmap uid = 10000 - 20000*
    - *Idmap gid = 10000 – 20000*
    - *Template homedir = /home/%D/%U*
    - *Template shell = /bin/bash*
  - Use *wbinfo* and *getent* to test

Advanced Winbindd

- *Winbind cache time = 300*
  - How long are the User-List cached on the client
- *Winbind enum user/Group = yes*
  - Should a list of all users be possible
  - Can be used by large installations
  - Problem with some programs
- *Winbind Nested Group = no*
  - Windows allow groups in groups
  - New feature, handle with care
- *Winbind use default domain = no*
  - Users without domainname are handled like they are in the default domain.

User-ID Problem 2

- When using NFSv3 or similar the Unix-User-IDs should be the same on all Systems (NFSv3, ...)
- Networked Systems should use
  - LDAP
  - NIS
  - Winbindd with IDMAP

Winbindd and IDMAP

- Winbindd can use a LDAP-Directory to Sync the User-IDs throughout the systems.
- Winbindd needs the Samba schema.
- *smb.conf*
  - *ldmap backend = ldap:ldap://ldap-server*
  - *ldmap backend = idmap_rid:DOMAINNAME:1000-100000*

LDAP and NIS

- OpenLDAP or Redhat-/Fedora-Directory-Server
- Samba can use LDAP to store all information in one place
- NIS and LDAP without TLS, please without password

Kerberos

- Windows uses Kerberos
  Linux can use Kerberos
- Windows needs an account for every non-Windows Kerberos-System and the command *keytab*
- Kerberos Trusts between Windows-KDC and Linux-KDCs are possible
  - For more Information see: Interoperatibily Whitepaper from Microsoft
    http://www.microsoft.com/windows2000/techinfo/planning/security/kerbsteps.asp

SFU

- Services for Unix is a free compatibility tool for integration Unix into Windows-Networks
- Parts are
  - NFS-Server/Client
  - NIS-Server/Client
  - Shells (bourne, korn)
  - Perl
- Posix-compatible Schema-Enhancement
  - Can be used by nss-ldap

NSS-LDAP and PAM-Kerberos

- *nss_ldap*
  - Use *nss_map_objectclass* to change SfU 3.5 to NSS-OpenLDAP in */etc/ldap.conf*
  - Look for Service for Unix 3.5 mapping

- PAM-Kerberos
  - Create Account like “account-name”
  - Map Account to a Kerberos Instance

    Ktpass –princ service-instance@REALM –mapuser account-name -pass password -out UNIXmachine.keytab
  - Add UNIXmachine.keytab to */etc/krb5.keytab*

Synopsis

- Linux and Windows can work together, ...

  but some work is necessary