SambaXP Tutorial 2009:

Samba 3 and Directory Services

Günther Deschner
gd@samba.org

(Red Hat / Samba Team)

Agenda:

Generalities

- Samba version used in examples: Samba 3.3.3
- Tutorial assumes participants are familiar with
  - basic Windows security concepts
  - installation, setup and configuration of Samba

Part 1: Samba and Active Directory

- Domain membership with winbind
- Winbind features
- Winbind configuration
- Winbind components
  - NSS module (Name Service Switch)
  - PAM module (Pluggable Authentication Modules)
  - Kerberos5 locator plugin
- Active Directory Schema extensions:
  - Windows Services for Unix
  - RFC2307

Part 1: Samba and Active Directory

- idmap subsystem
- idmap plugins
- nssinfo subsystem
- nssinfo plugins

Part 2: Samba and Directory Servers

- Samba LDAP backend
  - Configuration
  - Backend scripts
  - Provisioning
  - Administration
- Samba and OpenLDAP
- Samba and FDS (Fedora Directory Server)
- Samba and FreeIPA
  - A kerberized DS based infrastructure out of the box

Part 1:

Samba and Active Directory

Domain Member in Active Directory

- Real Active Directory integration requires Domain Membership
- Samba 3 can be a full member in Active Directory
- More then one option for Domain Join:
  - “net” binary
  - libnetapi shared library and frontends (gui)
    (NEW! since 3.2.0)
  - 3rd party

Domain Join - revisited

- Registry based configuration backend allows programmatic modification of Samba configuration
- Internal libnetjoin interface
  - supports registry based configuration
  - supports joining with administrator as well as with other privileged users
  - supports joining Samba3, NT4 and Active Directory (incl. Windows 2008)
  - used by smbd to allow remote-join
- Using net
  - net ads join vs. net rpc join

Domain Join with “net rpc join”

- net rpc join -U $USERNAME
  - Configuration in smb.conf must be appropriate prior joining
  - no support for join from scratch using “config backend = registry” yet
  - Optional: -S defines Domain Controller to join to
  - NetBIOS name lookup for #1b

Domain Join with “net ads join”

- net ads join -U $USERNAME {$DOMAIN}
  - Support for “config backend = registry”
  - Support for joining from scratch when $DOMAIN is given
  - Supports joining with long (DNS) or short (NetBIOS) domain name
  - Using internal DsGetDcName() interface:
  - Does MAILSLOT query for Domain Controller
  - Does detect DNS name when joining with just NetBIOS name

Domain Join with libnetapi.so

- New shared library, started with Samba 3.2 (22 calls), greatly extended in Samba 3.3 (59 calls)
- Supports:
  - Domain Controller queries
  - Local and remote join
  - User and group management
  - Share management
- Header: /usr/include/netapi.h
- Library: /usr/lib/libnetapi.so
- Some Linux distributions ship separate libnetapi package

Domain Join with libnetapi.so

- NetJoinDomain() call in libnetapi.so
- Syntax is almost identical to NetJoinDomain() call in netapi32.dll
- Samba comes with command line and gtk frontend in lib/netapi/example directory
- Some distros ship with a samba-domainjoin-gui.rpm

NetDomainJoin call header

- **NetJoinDomain on Windows (LMJoin.h):**

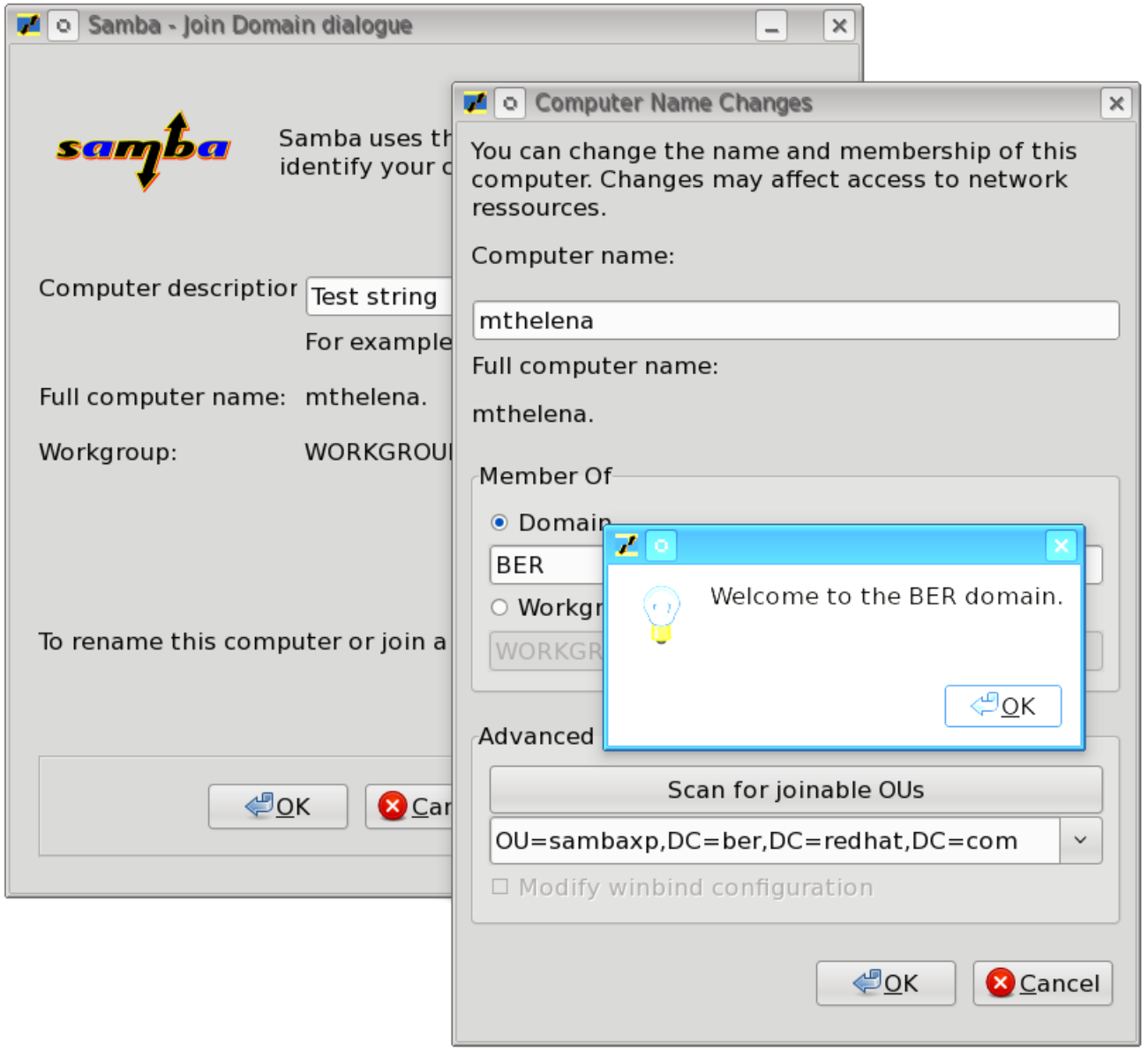
```
NET_API_STATUS NetJoinDomain(__in  LPCWSTR lpServer,
                             __in  LPCWSTR lpDomain,
                             __in  LPCWSTR lpAccountOU,
                             __in  LPCWSTR lpAccount,
                             __in  LPCWSTR lpPassword,
                             __in  DWORD fJoinOptions);
```

- **NetJoinDomain on Unix/Linux (netapi.h):**

```
NET_API_STATUS NetJoinDomain(const char * server /* [in] */,
                             const char * domain /* [in] [ref] */,
                             const char * account_ou /* [in] */,
                             const char * account /* [in] */,
                             const char * password /* [in] */,
                             uint32_t join_flags /* [in] */);
```

Live Demo:

Joining Active Directory using Samba GUI


Samba - Join Domain dialogue
Samba uses th
identify your c
Computer description
Test string
For example
Full computer name: mthelena.
Workgroup: WORKGROU
To rename this computer or join a
OK
Car
Computer Name Changes
You can change the name and membership of this computer. Changes may affect access to network ressources.
Computer name:
mthelena
Full computer name:
mthelena.
Member Of
Domain
BER
Workgr
WORKGR
Welcome to the BER domain.
OK
Advanced
Scan for joinable OUs
OU=sambaxp,DC=ber,DC=redhat,DC=com
Modify winbind configuration
OK
Cancel

Domain Join Overview

Type	Short domainname	DNS domainname	UI / cli	Can modify smb.conf	Remote Join
net rpc join	yes	no	cli	no	no
net ads join	yes	yes	cli	yes	no
NetJoinDomain() libnetapi.so	yes	yes	UI / cli	yes	yes

Winbind and Active Directory

- Full Active Directory client integration requires winbind
- Winbind is the central OS daemon that talks to Active Directory
- Many subsystems and tools will talk to Winbind
- Winbind maintains the Domain Membership
- Winbind maintains mapping of Active Directory user and groups to Linux equivalents
- Can be seen as our local LSASS daemon

Winbind features

- Identity mapping of Active Directory / NT4 accounts and groups
- Site-aware DNS Domain Controller Lookup
- Local Nested Groups
- Full Offline Capabilities
- Interdomain Trust support
  - One way trusts
  - Two way trusts
  - Forest Trusts
- Automatic update of machine account password

Winbind features

- **Local User Logon (PAM):**
  - **Cached (offline) Login**
  - **Kerberized Login**
  - **Login with userPrincipalName**
  - **Password change with password policy reporting**
  - **Automatic homedirectory creation**

Winbind configuration

- winbind separator
  - Defaults to '\', do not use '@' when logging in with user principal name
- winbind cache time
  - Amount of seconds until entries in winbindd_cache.tdb expire
- winbind enum users, winbind enum groups
  - Controls whether winbindd will reply on NSS enumeration calls for users and groups. Can be massive performance killer so disabled by default
- winbind use default domain
  - Omits Domain name prefix in user- and groupnames returned by NSS calls
- winbind trusted domains only
  - Winbind will only try to allocate uids and gids for remote trusted domains

Winbind configuration

- winbind rpc only
  - Sometimes winbind uses LDAP mechanisms although running in security=rpc, this parameter can be used to enfored only MSRPC methods
- winbind nested groups
  - Winbind handles unrolling of nested groups for Name Service Switch
  - Defaults to yes
  - Nested Groups are managed through “usrmgr”, “net rpc” or “net sam”
- winbind expand groups
  - Defines depth of flattening domain groups, defaults to 1
  - Setting to a high value can impact performance of winbind

Winbind configuration

- winbind nss info
  - Controls nss info API mapping
- winbind refresh tickets
  - Enable winbind to control kerberos credential cashes of users that logged on using pam_winbind's kerberized features
- winbind offline logon
  - Enables offline accessibility of mapping and authentication
- winbind reconnect delay
  - Amount of seconds to wait until winbind retries to contact an offline Domain Controller
- winbind normalize names

Winbind offline support

- Winbind can cache mapping and authentication data from Active Directory for offline use (disconnected laptops, broken network, etc.)
- Kerberos PAC is cached in samlogoncache.tdb
- Account mapping data is stored in winbindd_cache.tdb
- Configuration: “winbind offline logon = yes
  - Note: when pam_winbind is used, passwords are then cached as a salted hash in winbindd_cache.tdb

Winbind offline support

- How to change online state?
- Un-plug, plug cable or use smbcontrol tool
- smbcontrol winbind online
  - Winbind will try to set handling of remote domains online
- smbcontrol winbind offline
  - Winbind will try to set handling of remote domains offline
- smbcontrol winbind onlinestatus
  - Winbind reports back online-state of individual domains
- Winbind tries to rediscover a valid DC on a regular basis
- “winbind reconnect delay” can limit this behaviour

libwbclient.so

- Shared library libwbclient (NEW! Since 3.2.0)
- Header-File: /usr/include/wbclient.h
- Initially designed to decouple smbd and winbindd
- Hides complexity of winbind pipe struct from callers
- Comprehensive API
- Doxygen Documentation available
- Used by smbd, wbinfo, pam_winbind and locator plugin

libwbclient.so – simple examples

- How to authenticate a user:
  - wbcErr wbcAuthenticateUser(const char *username,
    const char *password);
- How to lookup a user:
  - wbcErr wbcLookupName(const char *dom_name,
    const char *name,
    struct wbcDomainSid *sid,
    enum wbcSidType *name_type);
- How to change a password:
  - wbcErr wbcChangeUserPassword(const char *username,
    const char *old_password,
    const char *new_password);

pam_winbind.so

- Separate configuration:
  - Globally: /etc/security/pam_winbind.conf
  - Globally: /etc/pam.d/$SERVICE
- Support for all 4 PAM facilities: auth, account, password and session block
- Manpage: pam_winbind.7
- Internationalized error messages (currently: EN, DE)

/etc/pam.d/system-auth (Fedora 10)

```
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        sufficient    pam_winbind.so try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     sufficient    pam_winbind.so
account     required      pam_permit.so

password    sufficient    pam_winbind.so
password    requisite     pam_cracklib.so try_first_pass retry=3
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so  service in crond quiet use_uid
session     sufficient    pam_winbind.so
session     required      pam_unix.so
```

pam_winbind.so – offline authentication

- Required for laptop users, detached networks, etc.
- Documentation:
  - http://wiki.samba.org/index.php/PAM_Offline_Authentication
  - man pam_winbind.7, smb.conf.5
- Configuration:
  - “winbind offline logon = yes” in /etc/samba/smb.conf
  - “cached_login = yes” in /etc/security/pam_winbind.conf
- Users need to logon successfully at least once before offline logons can succeed
- Users receive a warning that network resources may be unavailable

pam_winbind.so – kerberized login

- Enhance pam_winbind login for accessing kerberized services
- Documentation:
  - http://wiki.samba.org/index.php/PAM_Kerberos_Authentication
  - man pam_winbind.7, smb.conf.5
- Configuration:
  - “krb5_auth = yes” in /etc/security/pam_winbind.conf
  - “krb5_ccache_type = FILE” in /etc/security/pam_winbind.conf
- Automatic Kerberos ticket refresh and renew
  - Winbind can control the krb5 ticket caches that were created with pam_winbind
  - “winbind refresh tickets = yes” in /etc/samba/smb.conf

pam_winbind.so – homedirectory creation

- Automatically generate a home for a user
- Documentation:
  - man pam_winbind.7
- Configuration:
  - “mkhomedir = yes” in /etc/security/pam_winbind.conf
- Creates homedirectory as returned by Name Service Switch
- Does not (yet) copy skeleton into the new homedirectory
- Note that pam_mkhomedir is not available on all platforms

nss_winbind.so

- Offline name resolution
  - “winbind offline logon = yes” in /etc/samba/smb.conf
- Configuration in /etc/nsswitch.conf (Linux)

```
passwd:  files winbind
group:   files winbind
```

Live Demo:

Offline and Kerberos Logon using pam_winbind

Picking the closest Domain Controller

- In complex networks (many geographical locations, many Active Directory sites, many Domain Controllers) it is required to pick a close Domain Controller
- Critical: Domain Controller chosen by Samba needs to be used by entire OS, in particular by Kerberos Library
- Even with enabling DNS SRV lookups in /etc/krb5.conf this can not be achieved, as all known Kerberos libraries are unaware of sites and the concept of closest Domain Controllers
- Modern Kerberos Libraray support locator plugin API (since MIT 1.5, Heimdal 1.0)
- Samba provides a Kerberos5 locator plugin (NEW! Since 3.2.0)

winbind_krb5_locator.so

- Plugin is built automatically when local krb5 library supports locator plugin API
- Plugin has not been seen to be packaged separately so it needs to be manually copied into the local krb5 lib plugin path
  - /usr/{lib,lib64}/krb5/plugins/libkrb5/ on Fedora 10

winbind_krb5_locator.so

- No modification in /etc/krb5.conf required
- Requires winbindd to run
- Intercepts all name lookups for KDC and KPASSWD services from the kerberos library and delegates them to the samba name lookup and caching routines
- Discovers Active Directory site infrastructure and does appropriate site-aware DNS SRV lookups like:
  - _kerberos._tcp.MYSITE._sites.dc.msdcs.BER.REDHAT.COM
- Documentation:
  - Manpage: winbind_krb5_locator.7
  - http://wiki.samba.org/index.php/Winbind_Kerberos_Locator

Active Directory LDAP Sign & Seal

- Active Directory policies might require to sign and encrypt LDAP connection
- Configuration:
  - client ldap sasl wrapping = [plain|sign|seal]
- client ldap sasl wrapping = plain
  - LDAP connections are not altered
- client ldap sasl wrapping = sign
  - LDAP connections are signed
- client ldap sasl wrapping = seal
  - LDAP connections are signed and encrypted

Active Directory LDAP Sign & Seal

- **Windows registry key:**
  - **HKLM\System\CurrentControlSet\Services\NTDS\Parameters\ LDAPServerIntegrity**
- **Depending on underlying Kerberos library**
- **Alternative: use ldap ssl / ldap with Start TLS**
  - **ldap ssl ads = true**

Live Demo:

Active Directory LDAP Sign & Seal and winbind

Active Directory Schema Extensions

- "Windows Services for Unix" LDAP schema
  - Available since Windows 2000
  - NIS and NFS server implementations
  - Assign dedicated UID and GID to users
  - LDAP attribute names vary from version to version
  - Current version 3.5
- RFC2307 LDAP schema
  - Available since Windows 2003 R2
  - Assign dedicated UID and GID to users
  - Standard RFC2307 LDAP attribute names

idmap and nss_info

- Active Directory can provide the central store for Name Service Switch information
  - Username
  - Gecos
  - UID, GID
  - Homedirectory
  - Shell
- Samba has two APIs to access this information:
  - idmap: UID and GID
  - nss_info: Gecos, Homedirectory, Shell

idmap API

- idmap subsystem has gone various re-writes (separate talk from Michael Adam on this)
- “classic” idmap configuration still supported
- idmap supports modules via idmap backend
- modules are stored in $LIBDIR/idmap directory
- e.g. on Fedora 10: /usr/{lib/lib64}/samba/idmap:

```
-rwxr-xr-x 1 root root 140763 2009-04-01 14:58 adex.so*
-rwxr-xr-x 1 root root  67889 2009-04-01 14:58 ad.so*
-rwxr-xr-x 1 root root  32971 2009-04-01 14:58 hash.so*
-rwxr-xr-x 1 root root  37255 2009-04-01 14:58 rid.so*
```

idmap configuration

- idmap uid, idmap gid
  - Set main ranges of valid UIDs and GIDs inside idmap
  - Omitting these ranges cause winbind not to provide any information in NSS calls and is only useful in netlogon proxy case (idmap backend = NULL)
- idmap backend
  - Should define a writeable default backend (e.g. tdb)
- idmap cache time
  - Amount of seconds winbind will positively cache idmappings, defaults to one week
- idmap negative cache time
  - Amout of seconds winbind will negatively cache idmappings, defaults to 2 minutes

idmap configuration

- idmap config DOMAIN
  - Defines IDMAP configuration per domain
  - By default always two options are supported:
  - “idmap config DOMAIN backend = backend”
  - “idmap config DOMAIN range = low-high”
  - Note that all ranges need to fit into the global range defined with idmap uid and idmap gid
- idmap alloc backend
- idmap alloc config DOMAIN

idmap: tdb (default)

- Locally allocated UID and GID
- Configuration

```
idmap uid = 10000-50000
idmap gid = 10000-50000
```

- man idmap_tdb.8

idmap: tdb2

- Locally allocated UID and GID but using a shared tdb
- idmap_tdb2 is required on clustered setups
- Support for calling out a script
- Configuration:

```
idmap uid = 10000-50000
idmap gid = 10000-50000
idmap backend = tdb2
idmap:script = /path/to/script
```

- man idmap_tdb2.8
- ./configure --enable_shared_modules=..,idmap_tdb2,..

idmap: ldap

- Centrally stores centrally allocated UID and GID
- Requires an LDAP server as central repository
- Configuration:
  - idmap backend = ldap:ldap://localhost/
    idmap uid = 1000000-1999999
    idmap gid = 1000000-1999999
    idmap alloc backend = ldap
    idmap alloc config : ldap_url = ldap://id-master/
    idmap alloc config : ldap_base_dn = ou=idmap,dc=example,dc=com
- man idmap_ldap.8
- automatically built as long as there is LDAP support

idmap: rid

- Algorithmically calculated UID and GID
- Calculates the UID and GID off the account RID
  Configuration:
  - idmap backend = tdb
    idmap uid = 10000-50000
    idmap gid = 10000-50000
    idmap config TRUSTED : backend = rid
    idmap config TRUSTED : range = 50000 – 99999
- SID: S-1-5-21-2358920910-546136054-1568632707-500
  RID: 500
  UID: 50500
- man idmap_rid.8
- ./configure --enable_shared_modules=..,idmap_rid,..

idmap: ad

- Receives UID and GID directly from Active Directory
- Configuration:
  - idmap backend = tdb
    idmap uid = 10000-50000
    idmap gid = 10000-50000
    idmap config DOMAIN : backend = ad
    idmap config DOMAIN : range = 20000-30000
- man idmap_ad.8
- ./configure –enable_shared_modules=..,idmap_ad,..
- Read only backend: All UID/GID mappings need to be created in advance in Active Directory
- Supports trusted Active Directory domains

idmap: adex

- Receives UID and GID directly from Active Directory
- Configuration:
  - idmap backend = tdb
    idmap uid = 10000-50000
    idmap gid = 10000-50000
    idmap config DOMAIN : backend = adex
    idmap config DOMAIN : range = 20000-30000
- man idmap_adex.8
- ./configure –enable_shared_modules=..,idmap_adex,..
- Read only backend: All UID/GID mappings need to be created in advance in Active Directory
- Supports trusted domains (incl. two-way cross-forest trusts)

idmap: hash

- Algorithmically calculated UID and GID
- UID and GID are calculated from a SID using a hashing algorithm
- Configuration:

```
idmap backend = hash
idmap uid = 1000-4000000000
idmap gid = 1000-4000000000
winbind nss info = hash
winbind normalize names = yes
idmap_hash:name_map = /etc/samba/name_map.cfg
```

- man idmap_hash.8
- ./configure –enable_shared_modules=..,idmap_hash,..

idmap: passdb

- Statically compiled in
- undocumented

idmap: nss

- **Statically compiled in**
- **Primary purpose: replace “winbind trusted domains only”**
- **With this module, idmap will rely for simple NSS calls for the own domain while still supporting allocation of IDs for trusted domains**
- **Configuration:**

```
idmap backend = tdb
idmap uid = 1000000-1999999
idmap gid = 1000000-1999999
idmap config SAMBA : backend  = nss
idmap config SAMBA : range = 1000-999999
```

man idmap_nss.8

idmap plugin overview

name	allocation	readonly / readwrite	ID unique	shared mapping
idmap_tdb{2}	local	rw	no	no
idmap_ldap	central (LDAP server)	rw	yes	yes
idmap_rid	algorithmic	-	yes	yes
idmap_ad	central (AD LDAP)	ro	yes	yes
idmap_adex	central (AD LDAP)	ro	yes	yes
idmap_hash	algorithmic	-	yes and no (collisions)	yes
idmap_passdb				
idmap_nss				

nss_info API

- **nss_info API has been vastly reworked with 3.0.25**
- **nss_info configuration:**
  - winbind nss info = backend=DOMAINA,DOMAINB backend=DOMAINC,etc.
- **Currently re-written by Michael Adam**
- **modules are just symbolic links stored in $LIBDIR/nss_info directory that point to idmap modules in $LIBDIR/idmap**
- **e.g. on Fedora: /usr/{lib/lib64}/samba/nss_info**
- **lrwxrwxrwx 1 root root 16 2009-04-01 16:07 adex.so -> ../idmap/adex.so***
  lrwxrwxrwx 1 root root 16 2009-04-01 16:07 hash.so -> ../idmap/hash.so*
  lrwxrwxrwx 1 root root 14 2009-04-01 16:07 rfc2307.so -> ../idmap/ad.so*
  lrwxrwxrwx 1 root root 14 2009-04-01 16:07 sfu20.so -> ../idmap/ad.so*
  lrwxrwxrwx 1 root root 14 2009-04-01 16:07 sfu.so -> ../idmap/ad.so*

nss_info: template (default)

- statically linked in by default
- “template homedir” in smb.conf
  - defaults to /home/%D/%U
- “template shell” in smb.conf
  - defaults to /bin/false

nss_info: sfu

- Supports “Windows Services for Unix 3.0/3.5” LDAP schema
- Autodetects which LDAP schema is installed in Active Directory
- Only works in “security = ads”
- Fills in:
  - Homedirectory
  - Shell
  - Gecos
- Supports trusted Active Directory domains

nss_info: sfu20

- Supports “Windows Services for Unix 2.0” LDAP schema
- Only works in “security = ads”
- Fills in:
  - Homedirectory
  - Shell
  - Gecos
- Supports trusted Active Directory domains

nss_info: rfc2307

- Supports standard RFC2307 posixAccount LDAP schema
- Only works in “security = ads”
- Fills in:
  - Homedirectory (unixHomeDirectory)
  - Shell (loginShell)
  - Gecos (gecos)
- Supports trusted Active Directory domains

nss_info: adex

- Supports standard RFC2307 posixAccount LDAP schema
- Only works in “security = ads”
- Fills in:
  - Homedirectory (unixHomeDirectory)
  - Shell (loginShell)
  - Gecos (gecos)
- Supports only RFC2307 LDAP schema
- Supports domain trusts (incl. two-way cross-forest trusts)

nss_info: hash

- Supports standard RFC2307 posixAccount objectclass ?
- Only works in “security = ads”
- Fills in:
  - Homedirectory (unixHomeDirectory)
  - Shell (loginShell)
  - Gecos (gecos)

nss_info plugins overview

name	Active Directory domain	LDAP schema	note
template	-	-	
sfu	Primary & trusts	SFU 3.0,3.5	
sfu20	Primary & trusts	SFU 2.0	
rfc2307	Primary & trusts	RFC2307	
adex	trusts	RFC2307	Supports 3rd party AD extensions
hash	-	-	Supports external name map

Live Demo:

Service for Unix 3.5 installation & configuration

nss_winbind with SFU 3.5

Part 2:

Samba and other Directory Services

Samba3 ldapsam backend

- What ldapsam is:
  - Backend for the local (standalone, member) or shared (PDC/BDC) SAM
- What ldapsam is not:
  - Active Directory
  - Directory Service exposed to the Windows client
- Support for all LDAPv3 compliant LDAP servers including:
  - OpenLDAP
  - Fedora Directory Server
  - eDirectory / NDS
  - Mandriva Directory Server
  - Apple Directory Server

Samba3 ldapsam backend

- What is stored in LDAP:
  - Domain Object
  - User Accounts/Machine Accounts
  - Group Accounts
  - IDMAP Objects (optional)

ldapsam configuration

- passdb backend = ldapsam
  - Takes an LDAP URI
  - Defaults to “ldapsam:ldap://localhost”
- Supports multiple (replicated) LDAP servers:
  - passdb backend = ldapsam:”server1 server”
  - Failover is done by underlying (Open)-LDAP library
  - Account replication is done by LDAP server, not by Samba itself
- Supports ldap uri such as:
  - ldap://remote.somewhere.com
  - ldaps://here.somewhere.com
  - ldapi://%2fvar%2frun%2fldapi_sock/

ldapsam configuration

- ldap admin dn
  - Defines Admin DN that is used by Samba to access LDAP
  - Use “smbpasswd -w secret” to store password for admin dn
- ldap delete dn
  - Deletes LDAP dn when samba account is deleted
- ldap suffix
  - Main LDAP search suffix, e.g. dc=ber,dc=redhat,dc=com
- ldap {user,machine,group,idmap} suffix
  - Optional: defines sub-dn to “ldap suffix”, not full dn
  - e.g. ldap machine suffix = ou=users
    (when you mean ou=users,dc=ber,dc=redhat,dc=com)

ldapsam configuration

- ldap passwd sync
  - Bool option to enable LDAP Password Change extended operation
- ldap replication sleep
  - Time to wait before re-reading after a LDAP write operation
- ldap timeout
  - Number of seconds to wait until an LDAP server is considered unreachable
- ldap connection timeout
  - Number of seconds until an established LDAP session is closed
- ldap ssl = {no|start_tls}
  - Optionally enables LDAPv3 StartTLS extended operation (RFC2830)

ldapsam configuration

- ldap page size
  - Defines pagesize for LDAP paged results mechanism, defaults to 1024
- ldap debug level
  - OpenLDAP specific logging bitmask as defined in man slapd.conf
- ldap debug threshold
  - Defines debuglevel at which ldap debug information should be written to Samba debugsystem

ldapsam:trusted = yes

- Optimization for larger LDAP setups
- Saves roundtrips between nss lookups and LDAP queries
- Assumes that posix and samba attributes are stored in the same LDAP object
- Assumes that Server is running nss_ldap
- Can boost Samba/LDAP performance significantly
  - Group membership enumeration
  - SID to name translation
  - SID to uid / SID to gid translation

ldapsam:editposix = yes

- Added to provide an easier way of modifiying LDAP objects controlled by Samba
- Requires winbind
- Requires ldapsam:trusted = yes
- Creates RFC2307 structural objectclass objects in LDAP while adding samba Users

ldapsam backend scripts

- Samba can call script for specific user- group management actions:
  - add user script =
  - add machine script =
  - rename user script =
  - delete user script =
  - add user to group script =
  - delete user from group script =
  - set primary group script =
- Existing toolsets: “smbldap-tools” and “ldapsmb”
- Both poorly maintained and not contained in Samba

ldapsam provisioning

- Let samba take full control over users
- “net sam provision”
- Requires:
  - Configured samba and ldap server
  - ldapsam:editposix = yes
  - ldapsam:trusted = yes
  - Winbind needs to run
- Creates User Accounts:
  - Administrator and Guest
- Creates Domain Groups:
  - Domain Users, Domain Admins, Domain Guests

ldapsam LDAP schema

- Objectclasses
  - sambaDomain (structural)
  - sambaSamAccount (auxiliary)
  - sambaGroupMapping (auxiliary)
  - sambaTrustPassword (unused yet)
  - sambaTrustedDomainPassword (structural)
- Objectclasses used by idmap_ldap:
  - sambaUnixIdPool (auxiliary)
  - sambaIdmapEntry (auxiliary)
  - sambaSidEntry (structural)

ldapsam LDAP objects

- **Objectclass sambaDomain**
  - **Main entry to store domain name and sid**
  - **Generated at toplevel “ldap suffix” DN**
  - **Stores domain wide policies (min. password length, max. password age, etc.)**
  - **Generated for all “passdb backend = ldapsam” setups, not only on Domain Controllers but also for standalone and member servers**
  - **RDN is always NetBIOS domain name**

ldapsam LDAP objects

- **Objectclass sambaDomain example**

```
dn: sambaDomainName=SAMBA,dc=ber,dc=redhat,dc=com
sambaDomainName: SAMBA
sambaSID: S-1-5-21-2358920910-546136054-1568632707
sambaAlgorithmicRidBase: 1000
objectClass: sambaDomain
sambaNextUserRid: 1000
sambaMinPwdLength: 5
sambaPwdHistoryLength: 0
sambaLogonToChgPwd: 0
sambaMaxPwdAge: -1
sambaMinPwdAge: 0
sambaLockoutDuration: 30
sambaLockoutObservationWindow: 30
sambaLockoutThreshold: 0
sambaForceLogoff: -1
sambaRefuseMachinePwdChange: 0
sambaNextRid: 1005
```

ldapsam LDAP objects

- Objectclass sambaSamAccount
  - Generated at either “ldap user suffix” or “ldap suffix” for users
  - Generated at either “ldap machine suffix” or “ldap suffix” for machines
  - RDN is always UID

ldapsam LDAP objects

- **Objectclass sambaSamAccount example**

```
dn: uid=Administrator,dc=ber,dc=redhat,dc=com
objectClass: account
objectClass: posixAccount
objectClass: sambaSamAccount
objectClass: top
uid: Administrator
cn: Administrator
displayName: Administrator
uidNumber: 100000
gidNumber: 100010
homeDirectory: /home/SAMBA/Administrator
loginShell: /bin/false
sambaSID: S-1-5-21-2358920910-546136054-1568632707-500
sambaNTPassword: 878D8014606CDA29677A44EFA1353FC7
sambaPasswordHistory:
0000000000000000000000000000000000000000000000000000000000000000
sambaPwdLastSet: 1239727531
sambaAcctFlags: [U          ]
```

ldapsam LDAP objects

- Objectclass sambaGroupMapping
  - Generated at either “ldap group suffix” or “ldap suffix”
  - RDN is always sambaSID
- Objectclass sambaGroupMapping example

```
dn: sambaSid=S-1-5-32-544,dc=ber,dc=redhat,dc=com
objectClass: sambaSidEntry
objectClass: sambaGroupMapping
sambaSID: S-1-5-32-544
sambaGroupType: 4
displayName: Administrators
gidNumber: 100017
sambaSIDList: S-1-5-21-2358920910-546136054-1568632707-500
```

ldapsam LDAP objects

- Objectclass sambaTrustedDomainPassword
  - Generated at toplevel ldap suffix
  - Holds passwords for interdomain trust accounts

ldapsam administration

- Windows DCE-RPC based tools:
  - usrmgr.exe, lusrmgr.msc
  - hyena
  - net
- Unix DCE-RPC and LDAP based tools:
  - net, smbpasswd, libnetapi (gtk usrmgr in construction)
  - pdbedit (also allows import/export from/to other backends)
- Unix LDAP based tools:
  - gq
  - ldapadmin
  - kuser

Samba and OpenLDAP

- passdb backend = ldapsam
- Multimaster replication in newer versions
- Most common Samba/LDAP combination
- Known to work with very high performance
  (used in Samba-PDC setup at German Parliament)
- Rich support for LDAP features, such as:
  - paged results
  - extended password change operation
  - cn=config
  - SLAPI pugins, OL overlays

Samba and OpenLDAP

- Vital for good performance:
  - Proper Indexing
  - Appropriate settings in Berkeley DB DB_CONFIG file
- Support for re-using the stored sequence number as a sequence number for the Samba SAMR server when using OpenLDAP syncrepl replication
  - ldapsam:syncrepl_seqnum=true
  - ldapsam:syncrepl_rid=integer

Samba and OpenLDAP

- Simple Configuration File /etc/slapd.conf
- Add “include /etc/openldap/schema/samba.schema” to list of included schema
- database bdb
  suffix = dc=ber,dc=redhat,dc=com
  rootdn cn=admin,dc=ber,dc=redhat,dc=com
  rootpw {SSHA}/ZmwLAkB+tMLpBQtfseCytGkZxYPm8nd
- index sambaSid,sambaSidList
- Protect sensitive attributes:
  - sambaNTpassword, sambaLMpassword, sambaPasswordHistory
  - sambaClearTextPassword, sambaPreviousClearTextPassword

Live Demo:

Samba PDC with OpenLDAP

Samba and Fedora DS

- **Configuration:**
  - **passdb backend = ldapsam**
- **Multimaster Replication**
- **Installation: (Example on Fedora 10)**
  - `yum install fedora-ds-base`
  - `setup-ds.pl`
  - `cp /usr/share/doc/samba-3.3.3/LDAP/samba-schema-FDS.ldif \ /etc/dirserv/slapd-`hostname -s`/schema/98samba-schema-FDS.ldif`
  - `service dirsrv start`

Live Demo:

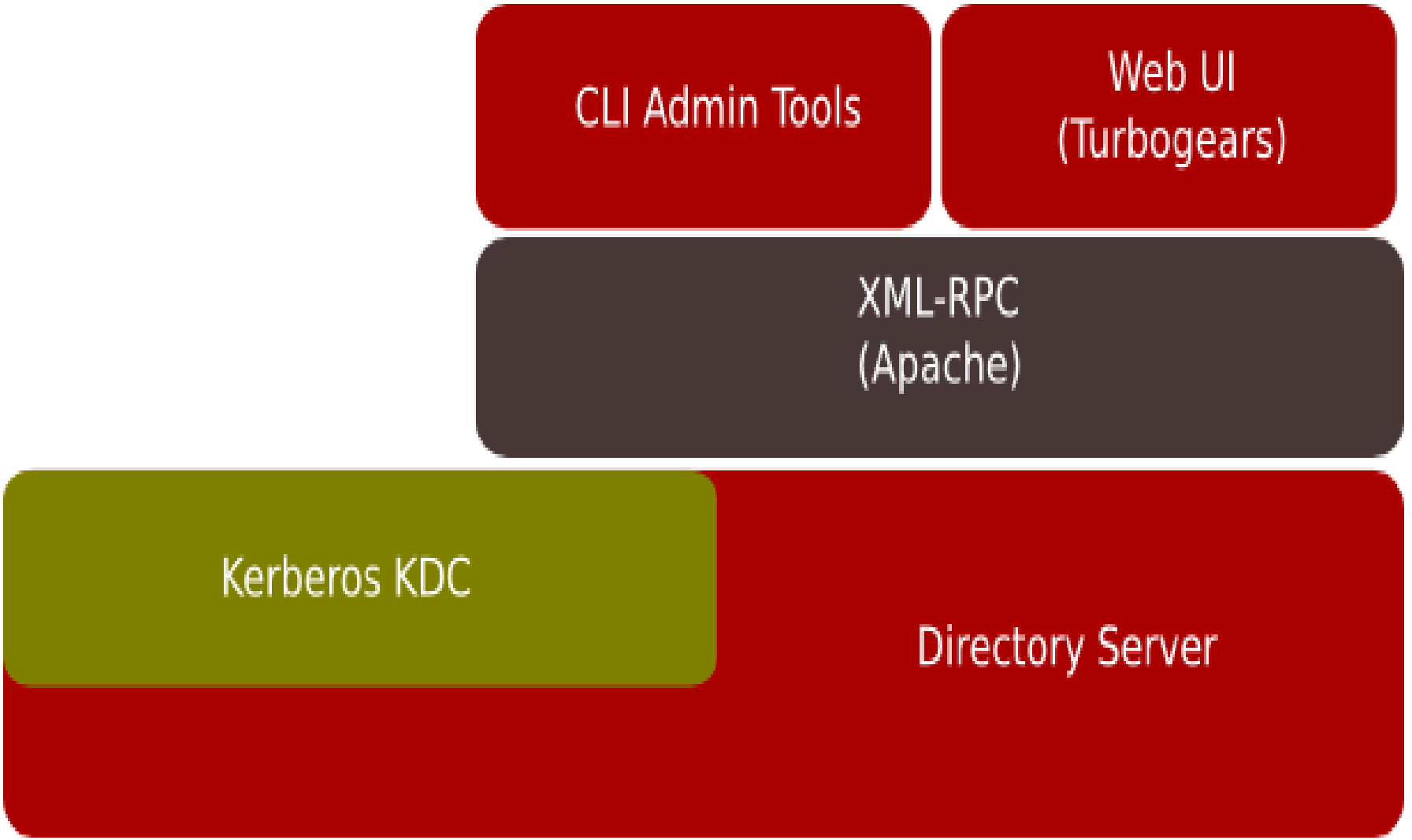
Samba PDC with Fedora DS

Samba and FreeIPA

freeIPA
identity | policy | audit

- What is FreeIPA ?
- IPA architecture:
  - Fedora DS,
  - MIT Kerberos
  - Apache + XML-RPC
  - DNS, NTP
  - Admin tools
- Single Sign On for Linux made easy
- DNS and replica provisioning
- FreeIPA comes with Samba and Kerberos LDAP schema installed

FreeIPA


CLI Admin Tools
Web UI
(Turbogears)
XML-RPC
(Apache)
Kerberos KDC
Directory Server

Samba and FreeIPA

freeIPA
identity | policy | audit

- Only Keytab required
- Samba and FreeIPA provide kerberized single-sign on for CIFS
- KDC does not provide Kerberos PAC yet
- Example Configuration:
  - [global]
    workgroup = IPA
    use kerberos keytab = yes
    realm = EXAMPLE.COM

Samba and FreeIPA

freeIPA
identity | policy | audit

- **Installation Server:**
  - **yum install fedora-ds ipa-server samba**
  - **Ipa-server-install –setup-bind**
- **Installation Client:**
  - **yum install ipa-client samba-client**
  - **Ipa-install-client**
  - **ipa-getkeytab –principal cifs/samba.example.com –keytab /etc/krb5.keytab**

Live Demo:

Kerberized CIFS infrastructure with FreeIPA and Samba

Outlook: Samba4 and Directory Servers

- Samba4 comes with an own LDAP Server
- OpenLDAP backend
- FDS backend

Further reading:

- www.samba.org
- www.openldap.org
- directory.fedoraproject.org
- www.freeipa.org

Thank you for your attention!

And a final word:

Samba needs YOU!
We are are constantly seeking for people helping out coding, website, documentation, testing