Going in production – Winbind in large AD domains today

Günther Deschner
gd@samba.org

(Red Hat / Samba Team)

Agenda

- To go where no-one has gone before
- Winbind scalability
- Find Domain Controllers
- Active Directory Sites
- Domain Controller Fallback
- Cached Logins
- Extended PAM module
- Winbind and system krb5 libraries

To go where no-one has gone before

- Winbind is starting to play a critical role as the glue to Active Directory on Linux desktops
- On Linux desktops, winbind is responsible today for:
  - Authentication and account name translations
  - Authorization and group membership
  - Event-based Kerberos ticket refreshing
  - Disconnected workstation usability
  - Name resolution, service discovery, etc.
- At the same time, winbind is expected to work well in large environments (> 100k users)

To go where no-one has gone before

- Async interface doing very well in general
- Winbind had a difficult start in large AD domains
- Often heard by customers:
  - *“winbindd cannot start after join”*
  - *“winbindd logons are extremely slow”*
  - *“winbindd doesn't use the nearest DC”*
  - *“winbindd can't use cached logon”*

Winbind Scalability

- *“winbindd logons are extremely slow”*
- The horror, aka `nsswitch`
  - Turned off enumeration calls in 3.0.23
  - Workarounds for Windows 2000, where the default primary group (RID 512 - Domain Users) has member attributes in LDAP (!)
  - Currently trying to improve `initgroups()`/`getgroups()` to avoid massive LDAP lookups for large groups (by using extended_dn LDAP control, range retrieval and cache lookups where possible)
- Winbind context switches and `nscd`
  - `getpwuid` and `getgrgid` can dramatically slow down the system
  - `nscd` (as long as it can be controlled via `libnscd`) is imperative in large environments

Find Domain Controllers

- *“winbindd cannot start after join”*
- winbind often talked to the “wrong”, remote DCs / KDCs
- Example:
  - `net ads join` finds a DC and creates machine account
  - `winbindd` is started and talks to a different DC that the machine account has not yet replicated to, so it fails
  - DC mixup not only between samba binaries but also the system krb5 library (DNS round robin list of equally weighted DCs)
- Too many ways to find a valid DC in Samba
  - Need to be merged and mimic the behavior of Windows clients

Active Directory Sites

- Winbind needed to support AD sites to find “local” DCs / KDCs, added with Samba 3.0.25
- What is a site?
  - Concept of geographical / physical partitioning
  - Consists of Name, physical subnets
  - DCs, Group Policy, Replication settings are assigned to sites
- Where are sites defined ?
  - Sites and site-topology is defined in AD (in mmc)
  - All Domain Controllers share their site-knowledge and thereby can identify to which site a client belongs

Active Directory Sites

- Sites and Domain Controllers
  - AD automatic site coverage for sites without local DCs
  - “closest DC” flag in CLDAP indicates either client and server are on the same site or that remote DC is assigned to a site via site coverage
- How does a Windows client find it's site?
- “Windows AD Locator”:
  - DNS lookups for domain
  - Send CLDAP request to first DC
  - Retrieve client sitename (if any) from CLDAP reply
  - Look for site DCs
  - Use one that matches the required flags

Active Directory Sites

- A typical CLDAP reply structure:

```
Information for Domain Controller: 192.168.1.1
Response Type: SAMLOGON
GUID: 3728a73b-3722-27d1-1732-2cef03493ff9
Flags:
    Is a PDC:                                   yes
    Is a GC of the forest:                      yes
    Is an LDAP server:                          yes
    Supports DS:                                yes
    Is running a KDC:                           yes
    Is running time services:                   yes
    Is the closest DC:                          no
    Is writeable:                               yes
    Has a hardware clock:                       yes
    Is a non-domain NC serviced by LDAP server: no
Forest:                 example.com
Domain:                 example.com
Domain Controller:      mydc.example.com
Pre-Win2k Domain:       EXAMPLE
Pre-Win2k Hostname:     MYDC
Server Site Name :              berlin-pankow
Client Site Name :              berlin-adlershof
NT Version: 5
LMNT Token: ffff
LM20 Token: ffff
```

Domain Controller Fallback

- Winbind needs to handle all kinds of fallback scenarios:
  - What if my current Domain Controller is down?
  - What if all my site Domain Controllers are down?
  - What if all Domain Controllers are down?

Cached Logins

- “Popular” feature invented with Windows 2000/XP
  - MS changed the client to no longer report that it used a cached account with SPx
- Users take their laptop with them, work during travel, from home, etc.
- Works like a `smbpasswd` or `passdb.tdb` account
  - Credentials stored in `winbind_cache.tdb`
  - Account stored in `samlogon_cache.tdb`
- Cached Logins and Security Settings (Group Policy)
- External signaling of interface status (cable plug/un-plug)
  - Network Managing daemons (`ifplugd`, `NetworkManager`) call `smbcontrol` wrapper script to signal interface change, vendor specific implementations

Cached Logins

- Winbind detecting offline by itself is extremely difficult
  - *“winbindd can't use cached logon”*
  - Winbindd needs to wait for the interface to be “up”
  - Winbindd may not switch to offline mode too fast (when there is just a temporary network problem)
- Auth (PAM) and account (NSS)
  - New IDMAP interface (3.0.25) finishes offline capability
- Configuration options:
  - Winbindd daemon (`smb.conf`): “`winbind offline logon = yes`”
  - Calling application:
    `pam_winbind` “`cached_login=yes`”
    `ntlm_auth` “`--use-cached-creds`”

Extended PAM module

- Features driven by customer demand
- Kerberized since 3.0.24 (`krb5_auth=yes`)
  - KRB5 logon (tgt + service ticket)
  - register a krb5 credential cache refreshing event
  - NTLM fallback
- Offline logon ability
- Communicate policy information (security settings) via PAM conv.
- Interactive password change for expired accounts
- Grace Logons for accounts that expire while offline
- Enforcing security settings, Windows vs. Linux

Extended PAM module

- Needs to be more configurable
  - Registry ?
  - `/etc/security/pam_winbind.conf`
- Planned features:
  - UPN logon (logon as `gdeschner@EXAMPLE.COM` while being `EXAMPLE\gd`)
  - logon script download and execution

Winbindd and system krb5 libs

- Problem:
  all krb5 clients (firefox, konqueror, etc.) need to talk to the same KDC winbindd does, finding a new KDC (site-aware!) if there is none
- Overwriting `/etc/krb5.conf` ?
- Exporting custom `krb5.conf` via KRB5_CONFIG variable ?
- Locator plugin API in MIT (> 1.5) and Heimdal (> 0.8) kerberos libs
  - Allows to bypass DNS resolution of krb5 libs
  - Samba 3.0.25 ships with locator plugin prototype that works for all non-samba krb5 clients (kinit, firefox, etc.)
  - Currently only accesses the global Samba `gencache.tdb` and Samba internal name resolution routines
  - Will probably be replaced by another set of winbind calls

Winbindd future

- Fully support trusted domains
- SoC project Samba4 winbind

Thank you for your attention!