IdMap and Nss Info Interface Changes in Samba 3.0.25

Gerald Carter
jerry@samba.org
http://www.samba.org/
http://www.centeris.com/

Outline

- **What is IdMap and what was wrong in 3.0.24?**
  - idmap backend
- **IdMap V4 Design**
  - idmap domains, idmap alloc backend
- **Nss Info V1 Design**
  - winbind nss info
- **Pending Patch Queue**
  - login names and aliases

IdMap History

- **Version 1**
  - Samba 2.2.3 – 2.2.12
- **Version 2**
  - Samba 3.0.0 – 3.0.24
- **Version 3**
  - Never released
- **Version 4**
  - Samba 3.0.25

What is IdMap?

- **Interface to translate SIDs/uids/gids**
  - Example: getent passwd “BLUE\gcarter”
  - “BLUE\gcarter” -> S-1-5-21-...-1234 -> 10023
- **In Samba < 3.0.25, the SID/uid/gid resolution module defined by “idmap backend”**
  - One backend for all domains
  - BUILTIN, MACHINE, Primary Domain, Trusted Domains
- **Available idmap backends in 3.0.24**
  - *tdb* (default), *ldap*, *rid*, & *ad*

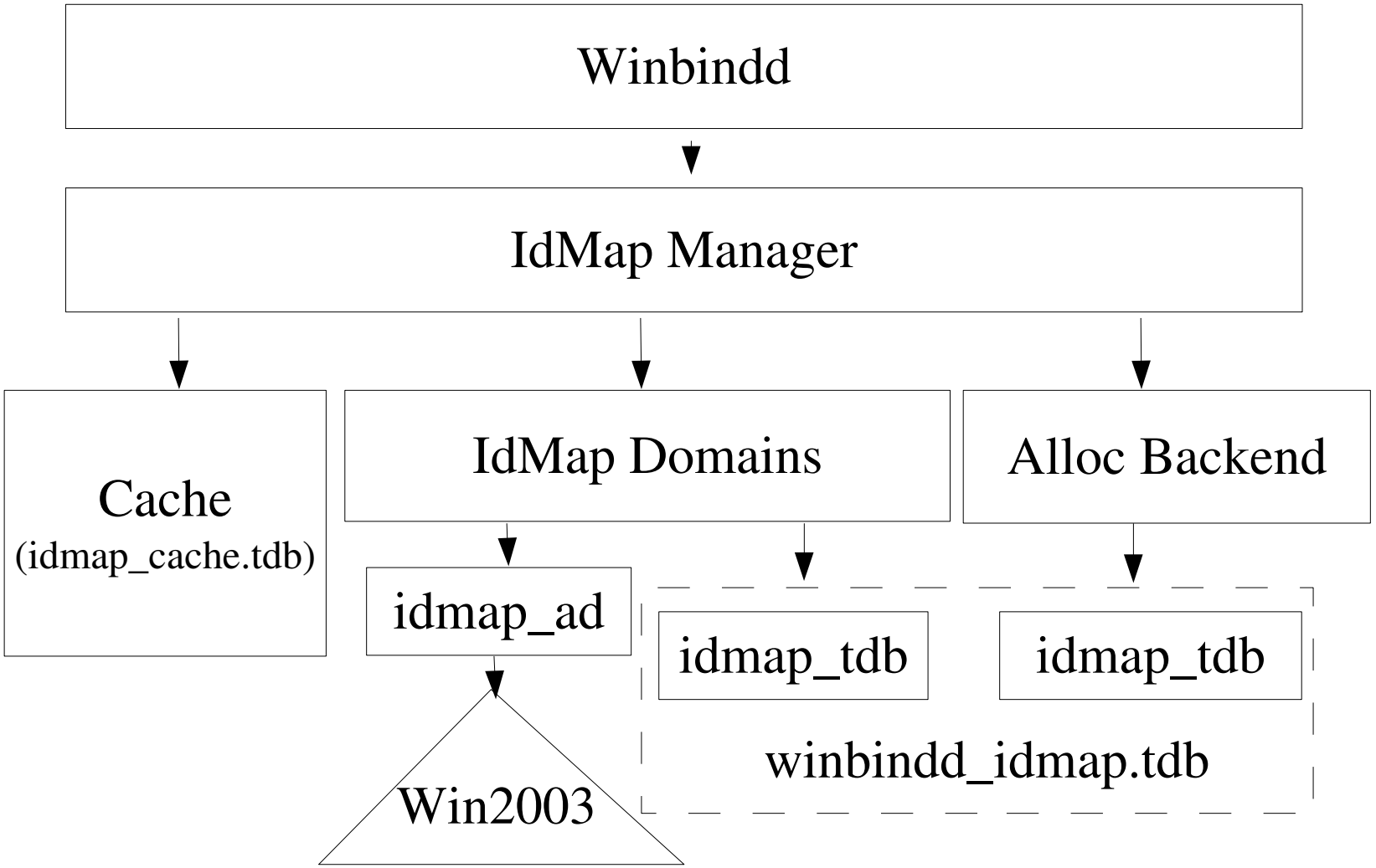
Problem Statement

- **The *rid* & *ad* backends are read-only**
  - Unable allocate gids for BUILTIN or Local groups
  - No *winbind nested groups* support
- **Domains may possess different IdMap needs**
  - BUILTIN – Use local gids (*tdb*)
  - Windows 2003 R2 – RFC 2307 (*ad*)
  - Trusted domains – LDAP Directory (*ldap*)
- **Non-expiring local cache of SID/uid/gid tables**
- **No bulk SID/uid/gid translation**

IdMap Version 4

- **Separate Query and Allocation interfaces**
  - Refer to idmap_*<name>*(8) for details
- **Query Backends (multiple)**
  - Defined using the “idmap domains” option
  - Associated with either a specific domain or marked as the default backend for all unlisted domains
  - Examples: *tdb* (default), *ldap*, *rid*, & *ad*
- **Allocation Backend (single)**
  - Defined using the “idmap alloc backend” option
  - Examples: *tdb*, *ldap*

IdMap Version 4 Architecture



Example Configuration

```
idmap domains = default BLUE

idmap config BLUE:backend      = ad
idmap config BLUE:schema_mode = rfc2307
idmap config BLUE:readonly     = yes
idmap config BLUE:range        = 100000 – 199999

idmap config default:backend = tdb
idmap config default:range   = 80000 – 99999
idmap config default:default = yes

idmap alloc backend       = tdb
idmap alloc config:range = 80000 – 99999
```

New IdMap plugins

- **idmap_nss**
  - Replacement for “winbind trusted domains only”
- **idmap_passdb**
  - Added implicitly to handle the server's passdb and local group mapping tables

Nss Info Version 1

- ***winbind nss info***
  - Provides a means of filling in the home directory and shell information in the getpwnam() return
  - Prior to 3.0.25, the support was static and integrated into the core winbindd code
- **Nss Info Plugin Interface**
  - Allows a run-time loadable interface for filling in the the home directory, login shell and primary group gid
- **Available modules**
  - *template* (default), *rfc2307*, & *sfu* (provided by idmap_ad)

Pending Patch Queue

- ***winbind normalize names***
  - Introduced in 3.0.25
  - Replace white space in account names with “_”
  - DOMAIN\Space Kadet -> DOMAIN\space_kadet
- **Provide *username map* in winbindd for queries via libnss_winbind.so**
  - Why ? NIS migration, usernames referenced in scripts, etc....
  - Add two calls to the nss_info interface
  - map_to_alias() and map_from_alias()
  - DOMAIN\gcarter -> jerry

IdMap Proxy Plugins

- **Deployments require flexibility of new IdMap interface**
- **Customers require vendor provided version of Samba**
  - Example: RHEL 4 ships Samba 3.0.10
- **Samba is tightly coupled to winbindd via static linking**
  - Should be replaced by linking with libwbclient.so

centeris™

IdMap and Nss Info Interface Changes in Samba 3.0.25

Gerald Carter
jerry@samba.org
http://www.samba.org/
http://www.centeris.com/