NAME

idmap_ad - Samba’s idmap_ad Backend for Winbind

DESCRIPTION

The idmap_ad plugin provides a way for Winbind to read id mappings from an AD server that uses RFC2307/SFU schema extensions. This module implements only the "idmap" API, and is READONLY. Mappings must be provided in advance by the administrator by adding the uidNumber attributes for users and gidNumber attributes for groups in the AD. Winbind will only map users that have a uidNumber and whose primary group have a gidNumber attribute set. It is however recommended that all groups in use have gidNumber attributes assigned, otherwise they are not working.

Currently, the *ad* backend does not work as the default idmap backend, but one has to configure it separately for each domain for which one wants to use it, using disjoint ranges. One usually needs to configure a writeable default idmap range, using for example the *tdb* or *ldap* backend, in order to be able to map the BUILTIN sids and possibly other trusted domains. The writeable default config is also needed in order to be able to create group mappings. This catch-all default idmap configuration should have a range that is disjoint from any explicitly configured domain with idmap backend *ad*. See the example below.

IDMAP OPTIONS

range = low - high

Defines the available matching UID and GID range for which the backend is authoritative. Note that the range acts as a filter. If specified any UID or GID stored in AD that fall outside the range is ignored and the corresponding map is discarded. It is intended as a way to avoid accidental UID/GID overlaps between local and remotely defined IDs.

schema_mode = <rfc2307 | sfu | sfu20>

Defines the schema that idmap_ad should use when querying Active Directory regarding user and group information. This can be either the RFC2307 schema support included in Windows 2003 R2 or the Service for Unix (SFU) schema. For SFU 3.0 or 3.5 please choose "sfu", for SFU 2.0 please choose "sfu20". Please note that the behavior of primary group membership is controlled by the *unix_primary_group* option.

unix_primary_group = yes/no

Defines whether the user’s primary group is fetched from the SFU attributes or the AD primary group. If set to *yes* the primary group membership is fetched from the LDAP attributes (gidNumber). If set to *no* the primary group membership is calculated via the "primaryGroupID" LDAP attribute.

Default: no

unix_nss_info = yes/no

If set to *yes* winbind will retrieve the login shell and home directory from the LDAP attributes. If set to *no* or the AD LDAP entry lacks the SFU attributes the options *template shell* and *template homedir* are used.

Default: no

EXAMPLES

The following example shows how to retrieve idmappings from our principal and trusted AD domains. If trusted domains are present id conflicts must be resolved beforehand, there is no guarantee on the order conflicting mappings would be resolved at this point. This example also shows how to leave a small non conflicting range for local id allocation that may be used in internal backends like BUILTIN.

```
[global]
workgroup = CORP

idmap config * : backend = tdb
idmap config * : range = 1000000-1999999

idmap config CORP : backend  = ad
idmap config CORP : range = 1000-999999
```

AUTHOR

The original Samba software and related utilities were created by Andrew Tridgell. Samba is now developed by the Samba Team as an Open Source project similar to the way the Linux kernel is developed.