NAME

idmap_ldap - Samba’s idmap_ldap Backend for Winbind

DESCRIPTION

The idmap_ldap plugin provides a means for Winbind to store and retrieve SID/uid/gid mapping tables in an LDAP directory service.

In contrast to read only backends like idmap_rid, it is an allocating backend: This means that it needs to allocate new user and group IDs in order to create new mappings.

IDMAP OPTIONS

ldap_base_dn = DN

Defines the directory base suffix to use for SID/uid/gid mapping entries. If not defined, idmap_ldap will default to using the "ldap idmap suffix" option from smb.conf.

ldap_user_dn = DN

Defines the user DN to be used for authentication. The secret for authenticating this user should be stored with net idmap secret (see **net**(8)). If absent, the ldap credentials from the ldap passdb configuration are used, and if these are also absent, an anonymous bind will be performed as last fallback.

ldap_url = ldap://server/

Specifies the LDAP server to use for SID/uid/gid map entries. If not defined, idmap_ldap will assume that ldap://localhost/ should be used.

range = low - high

Defines the available matching uid and gid range for which the backend is authoritative.

EXAMPLES

The following example shows how an ldap directory is used as the default idmap backend. It also configures the idmap range and base directory suffix. The secret for the ldap_user_dn has to be set with "net idmap secret ’*’ password".

```
[global]
idmap config * : backend      = ldap
idmap config * : range        = 1000000-1999999
idmap config * : ldap_url     = ldap://localhost/
idmap config * : ldap_base_dn = ou=idmap,dc=example,dc=com
idmap config * : ldap_user_dn = cn=idmap_admin,dc=example,dc=com
```

This example shows how ldap can be used as a readonly backend while tdb is the default backend used to store the mappings. It adds an explicit configuration for some domain DOM1, that uses the ldap idmap backend. Note that a range disjoint from the default range is used.

```
[global]
# "backend = tdb" is redundant here since it is the default
idmap config * : backend = tdb
idmap config * : range = 1000000-1999999

idmap config DOM1 : backend = ldap
idmap config DOM1 : range = 2000000-2999999
idmap config DOM1 : read only = yes
idmap config DOM1 : ldap_url = ldap://server/
idmap config DOM1 : ldap_base_dn = ou=idmap,dc=dom1,dc=example,dc=com
idmap config DOM1 : ldap_user_dn = cn=idmap_admin,dc=dom1,dc=example,dc=com
```

NOTE

In order to use authentication against ldap servers you may need to provide a DN and a password. To avoid exposing the password in plain text in the configuration file we store it into a security store. The "net idmap " command is used to store a secret for the DN specified in a specific idmap domain.

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.