Rocky Enterprise Linux 9.2 Manual Pages on command 'idmapd.conf.5'

$ man idmapd.conf.5

idmapd.conf(5)   File Formats Manual   idmapd.conf(5)

NAME

    idmapd.conf - configuration file for libnfsidmap

SYNOPSIS

    Configuration file for libnfsidmap. Used by idmapd and svcgssd to map NFSv4 name to and

    from ids.

DESCRIPTION

    The idmapd.conf configuration file consists of several sections, initiated by strings of

    the form [General] and [Mapping]. Each section may contain lines of the form

     variable = value

    The recognized sections and their recognized variables are as follows:

  [General] section variables

    Verbosity

        Verbosity level of debugging (Default: 0)

    Domain The local NFSv4 domain name. An NFSv4 domain is a namespace with a unique user?

        name<->UID and groupname<->GID mapping. (Default: Host's fully-qualified DNS do?

        main name)

    No-Strip

        In multi-domain environments, some NFS servers will append the identity management

        domain to the owner and owner_group in lieu of a true NFSv4 domain.   This option

        can facilitate lookups in such environments. If set to a value other than "none",

        the nsswitch plugin will first pass the name to the password/group lookup function

        without stripping the domain off. If that mapping fails then the plugin will try

again using the old method (comparing the domain in the string to the Domain value, stripping it if it matches, and passing the resulting short name to the lookup function). Valid values are "user", "group", "both", and "none". (Default: "none")

Reformat-Group

Winbind has a quirk whereby doing a group lookup in UPN format (e.g. staff@ameri‐cas.example.com) will cause the group to be displayed prefixed with the full domain in uppercase (e.g. AMERICAS.EXAMPLE.COM\staff) instead of in the familiar netbios name format (e.g. AMERICAS\staff). Setting this option to true causes the name to be reformatted before passing it to the group lookup function in order to work around this. This setting is ignored unless No-Strip is set to either "both" or "group". (Default: "false")

Local-Realms

A comma-separated list of Kerberos realm names that may be considered equivalent to the local realm name. For example, users juser@ORDER.EDU and juser@MAIL.ORDER.EDU may be considered to be the same user in the specified Domain. (Default: the host's default realm name)

Note: If a value is specified here, the default local realm must be included as well.

[Mapping] section variables

Nobody-User

Local user name to be used when a mapping cannot be completed.

Nobody-Group

Local group name to be used when a mapping cannot be completed.

[Translation] section variables

Method A comma-separated, ordered list of mapping methods (plug-ins) to use when mapping between NFSv4 names and local IDs. Each specified method is tried in order until a mapping is found, or there are no more methods to try. The methods included in the default distribution include "nsswitch", "umich_ldap", and "static". (Default: nsswitch)

GSS-Methods

An optional comma-separated, ordered list of mapping methods (plug-ins) to use when mapping between GSS Authenticated names and local IDs. (Default: the same list as

specified for Method)

[Static] section variables

   The "static" translation method uses a static list of GSS-Authenticated names to local

   user names. Entries in the list are of the form:

    principal@REALM = localusername

[REGEX] section variables

   In Ubuntu, the regex plugin is shipped in the libnfsidmap-regex package. If you want to

   use this plugin, please install that package and consult the libnfsidmap-regex(5) manpage.

[UMICH_SCHEMA] section variables

   If the "umich_ldap" translation method is specified, the following variables within the

   [UMICH_SCHEMA] section are used.

   LDAP_server

      LDAP server name or address (Required if using UMICH_LDAP)

   LDAP_base

      Absolute LDAP search base. (Required if using UMICH_LDAP)

   LDAP_people_base

      Absolute LDAP search base for people accounts. (Default: The LDAP_base value)

   LDAP_group_base

      Absolute LDAP search base for group accounts. (Default: The LDAP_base value)

   LDAP_canonicalize_name

      Whether or not to perform name canonicalization on the name given as LDAP_server

      (Default: "true")

   LDAP_follow_referrals

      Whether or not to follow ldap referrals. (Default: "true")

   LDAP_use_ssl

      Set to "true" to enable SSL communication with the LDAP server. (Default: "false")

   LDAP_ca_cert

      Location of a trusted CA certificate used when SSL is enabled (Required if

      LDAP_use_ssl is true and LDAP_tls_reqcert is not set to never)

   LDAP_tls_reqcert

      Controls the LDAP server certificate validation behavior. It can take the same

      values as ldap.conf(5)'s TLS_REQCERT tunable. (Default: "hard")

   LDAP_timeout_seconds

Number of seconds before timing out an LDAP request (Default: 4)

LDAP_sasl_mech

SASL mechanism to be used for sasl authentication. Required if SASL auth is to be

used (Default: None)

LDAP_realm

SASL realm to be used for sasl authentication. (Default: None)

LDAP_sasl_authcid

Authentication identity to be used for sasl authentication. (Default: None)

LDAP_sasl_authzid

Authorization identity to be used for sasl authentication. (Default: None)

LDAP_sasl_secprops

Cyrus SASL security properties. It can the same values as ldap.conf(5)'s

sasl_secprops.

LDAP_sasl_canonicalize

Specifies whether the LDAP server hostname should be canonicalised. If set to yes

LDAP lib with do a reverse hostname lookup. If this is not set the LDAP library's

default will be used. (Default: None)

LDAP_sasl_krb5_ccname

Path to kerberos credential cache. If it is not set then the value of environment

variable KRB5CCNAME will be used. If the environment variable is not set then the

default mechanism of kerberos library will be used.

NFSv4_person_objectclass

The object class name for people accounts in your local LDAP schema (Default:

NFSv4RemotePerson)

NFSv4_name_attr

Your local schema's attribute name to be used for NFSv4 user names (Default:

NFSv4Name)

NFSv4_uid_attr

Your local schema's attribute name to be used for uidNumber (Default: uidNumber)

GSS_principal_attr

Your local schema's attribute name for GSSAPI Principal names (Default: GSSAuth?

Name)

NFSv4_acctname_attr

Your local schema's attribute name to be used for account names (Default: uid)

NFSv4_group_objectclass

The object class name for group accounts in your local LDAP schema (Default: NFSv4RemoteGroup)

NFSv4_gid_attr

Your local schema's attribute name to be used for gidNumber (Default: gidNumber)

NFSv4_group_attr

Your local schema's attribute name to be used for NFSv4 group names (Default: NFSv4Name)

LDAP_use_memberof_for_groups

Some LDAP servers do a better job with indexing where searching through all the groups searching for the user in the memberuid list. Others like SunOne directory that search can takes minutes if there are thousands of groups. So setting LDAP_use_memberof_for_groups to true in the configuration file will use the mem? berof lists of the account and search through only those groups to obtain gids. (Default: false)

NFSv4_member_attr

If LDAP_use_memberof_for_groups is true, this is the attribute to be searched for. (Default: memberUid)

NFSv4_grouplist_filter

An optional search filter for determining group membership. (No Default)

EXAMPLES

An example /etc/idmapd.conf file:

[General]

Verbosity = 0

Domain = domain.org

Local-Realms = DOMAIN.ORG,MY.DOMAIN.ORG,YOUR.DOMAIN.ORG

[Mapping]

Nobody-User = nfsnobody

Nobody-Group = nfsnobody

[Translation]

Method = umich_ldap,nsswitch

GSS-Methods = umich_ldap,static

[Static]

johndoe@OTHER.DOMAIN.ORG = johnny

[UMICH_SCHEMA]

LDAP_server = ldap.domain.org

LDAP_base = dc=org,dc=domain

SEE ALSO

idmapd(8) svcgssd(8)

BUGS

Report bugs to <nfsv4@linux-nfs.org>

<div align="center">19 Nov 2008   idmapd.conf(5)</div>