ldap.conf, .ldaprc

Fichier de configuration LDAP

ldap.conf est utilisé pour définir les paramètres LDAP par défaut pour les clients. les utilisateurs peuvent créer un fichier **ldaprc** ou **.ldaprc** dans leur répertoire personnel. D'autres fichiers de configuration peuvent être spécifiés en utilisant les variables d'environnement **LDAPCONF** et **LDAPRC**. Les options peuvent être également définies par des variables d'environnement en les préfixant par "**LDAP**" (ex : pour **BASE**, **LDAPBASE**). Certaines options sont user-only et sont ignorés s'ils sont trouvés dans ldap.conf.

Les fichiers et variables sont lus dans cet ordre :

variable $LDAPNOINIT , et si non définie :

system file /usr/local/etc/openldap/ldap.conf,

user files $HOME/ldaprc, $HOME/.ldaprc, ./ldaprc,

system file $LDAPCONF,

user files $HOME/$LDAPRC, $HOME/.$LDAPRC, ./$LDAPRC,

variables $LDAP<uppercase option name>.

OPTIONS

URI <ldap[si] ://[name[:port]] ...> Spécifie les URI des serveurs LDAP.

BASE <base> Spécifie le DN de base pour les opérations de recherche

BINDDN <dn> Spécifie le Bind DN à utiliser (user-only)

DEREF <when> Spécifie comment les alias sont déréférencés. peut être : **never** Jamais déréférencés **searching** les alias sont déréférencés en subordonnés de l'objet de base, mais pas en localisant l'objet de base de la recherche **finding** Les alias sont déréférencés en localisant l'objet de base de la recherche **always** Les alias sont toujours déréférencés.

NETWORK_TIMEOUT <integer> Spécifie le timeout en seconde pour les connections

REFERRALS <on/true/yes/off/false/no> Spécifie si le client devrait automatiquement suivre les référant retournés par le serveur. Noter que ldapsearch n'utilise pas cette option.

SIZELIMIT <integer> Spécifie le nombre d'entrées à utiliser pour les recherches.

TIMELIMIT <integer> Spécifie une limite de temps en seconde pour les recherches.

TIMEOUT <integer> Spécifie un timeout en secondes après lesquels les appels LDAP sont annulés si aucune réponse n'est reçue.

Options SASL

SASL_MECH <mechanism> Spécifie le mécanisme SASL à utiliser (user-only)

SASL_REALM <realm> Royaume SASL

SASL_AUTHCID <authcid> Spécifie l'identité d'authentification (user-only)

SASL_AUTHZID <authcid> Spécifie l'identité d'authorisation (user-only)

SASL_SECPROPS <properties> Spécfie les propriétés de sécurité SASL. peut être :

none seul, désactive ("noanonymous,noplain")

noplain Désactive les mécanismes sujets à attaques simple

noactive Désactive les mécanismes suet à attaques actives.

nodict Désactive les mécanismes sujets à attaque passive par dictionnaire

noanonymous Désactive les mécanismes qui supportent les logins anonymes

forwardsec Nécessite de renvoye un secret entre les sessions

passcred Nécessite des mécanismes qui passent les accréditations client.

minssf=<factor> Spécifie le facteur minimum à utiliser

maxssf=<factor> Spécifie le facteur maximum à utiliser

maxbufsize=<factor> Spécifie la taille de tampon maximum. (0 désactive)

Options GSSAPI

GSSAPI_SIGN <on/true/yes/OFF/false/no> Spécifie si GSS_C_INTEG_FLAG devrait être utilisé

GSSAPI_ALLOW_REMOTE_PRINCIPAL <on/true/yes/OFF/false/no> Spécifie si l'authentification devrait tenter de former le principal de l'attribut ldapServiceName ou dnsHostName des entrées RootDSE cibles.

Options TLS

TLS_CACERT <filename> Spécifie le fichier contenant les certficats des autorités reconnus par le client

TLS_CACERTDIR <path> Spécifie le répertoire contenant les certficats des autorités reconnus par le client

TLS_CERT <filename> Fichier contenant le certificat du client (user-only)

TLS_KEY <filename> Spécifie le fichier contenant la clé privée (user-only)

TLS_CIPHER_SUITE <cipher-suite-spec> Spécifie les suites de chiffrement accèptables, par ordre de préférence

TLS_PROTOCOL_MIN <major>[.<minor>] Spécifie la version de protocol SSL/TLS minimum. (pour TLS v1.1 mettre 3.2)

TLS_RANDFILE <filename> Spécifie le fichier contenant des données aléatoires quand /dev/urandom n'est pas disponible.

TLS_REQCERT <level> Spécifie quels vérifications effectuer sur les certificats serveur dans une session TLS :

never Ne vérifie rien

allow Le certification serveur est requis. S'il n'est pas fournis, ou s'il n'est pas valide, la session procède normalement

try Le certificat serveur est requis. si le certificat n'est pas fournis, la session continue normalement. Si le certificat n'est pas valide, termine la session.

demand|hard Le certificat serveur est obligatoire et doit être valide.

TLS_CRLCHECK <level> Spécfie si la CRL doit être vérifiée : none

Pas de vérification peer

Vérifie la CRL du certificat du partie all

Vérifie la CRL pour toute la chaîne de certificat

TLS_CRLFILE <filename> Spécifie le fichier contenant la CRL.

Variables d'environnement

LDAPNOINIT Désactive tous les paramètres par défaut

LDAPCONF Chemin du fichier de configuration

LDAPRC Fichier de configuration dans $HOME ou $CWD

LDAP<option-name> Options comme dans ldap.conf