nslcd.conf

Fichier de configuration de nslcd

options runtimes

threads NUM Spécifie le nombre de threads. Défaut : 5

uid UID user id du service

gid GID Groupe du service

log SCHEME [LEVEL] Contrôle les logs. SCHEME peut être none ou syslog. (défaut : syslog info)

options de connexion

uri URI URI du serveur LDAP. La valeur alternative DNS peut être utilisée pour rechercher les DNS SRV avec la syntaxe DNS :DOMAIN.

ldap_version VERSION Spécifie la version du protocole LDAP à utiliser

binddn DN DN à utiliser pour le bind.

bindpw PASSWORD Mot de passe du binddn

rootpwmoddn DN Spécifie le DN à utiliser quand root tente de modifier le mot de passe d'un utilisateur en utilisant le module PAM.

rootpwmodpw PASSWORD Mot de passe de rootpwmoddn

options SASL

sasl_mech MECHANISM Spécifie le mécanisme SASL à utiliser pour l'authentification SASL

sasl_realm REALM Domaine SASL

sasl_authcid AUTHCID Identité d'authentification

sasl_authzid AUTHZID Identité d'authorisation (doit être spécifié au format dn :<dn> ou u :<username>)

sasl_secprops PROPERTIES Spécifie les propriétés de sécurité SASL de Cyrus. les valeurs permise sont décrites dans ldap.conf

sasl_canonicalize yes|no Détermine si le nom d'hôte du serveur LDAP devrait être canonisé ou non. À yes, effectue un reverse lookup.

options Kerberos

krb5_ccname NAME Nom pour le cache d'accréditations Kerberos

options de recherche et mappage

base [MAP] DN Base de recherche. Peut être spécifié plusieurs fois. Une base de recherche globale peut être spécifiée ou un map spécifique.

scope [MAP] sub[tree]|one[level]|base|children Spécifie le scope de recherche.

deref never|searching|finding|always Définis la stratégie de dé-référencement des alias.

referrals yes|no Spécifie si les référant doivent être suivis ou non.

filter MAP FILTER Filtre de recherche à utiliser pour un map spécifique.

map MAP ATTRIBUTE NEWATTRIBUTE Permet de définir d'autres attributs que ceux de la rfc2307.

options de timing et reconnexion

bind_timelimit SECONDS limite de temps pour la connexion au serveur. Défaut : 10 secondes

timelimit SECONDS Spécifie la limite de temps pour une réponse du serveur. 0 pour une attente infinie.

idle_timelimit SECONDS Période d'inactivité avant de fermer la connexion au serveur. Défaut : pas de limite

reconnect_sleeptime SECONDS Temps au delà duquel un serveur ldap est considéré indisponible. Une fois ce temps atteins, les tentatives seront faites une fois par cette tranche de temps. défaut : 10 secondes.

options SSL/TLS

ssl on|off|start_tls Spécifie le mode à utiliser

tls_reqcert never|allow|try|demand|hard Spécifie quelles vérifications effectuer sur le certificat du serveur. Les valeurs sont décrites dans ldap.conf.

tls_cacertdir PATH Répertoire contenant les certificats X.509 pour l'authentification du paire. Ignoré avec GnuTLS.

tls_cacertfile PATH Spécifie le chemin du certificat X.509 pour l'authentification du paire.

tls_randfile PATH Chemin de la source d'entropie. Ignoré avec GnuTLS

tls_ciphers CIPHERS Chiffrement à utiliser pour TLS.

tls_cert PATH Chemin du certificat du client

tls_key PATH Chemin du fichier contenant la clé privé du client.

autres options

pagesize NUMBER > 0, définis le nombre de résultat pour une recherche paginés. Défaut : 0.

nss_initgroups_ignoreusers user1,user2,... Empêche la recherche du groupe membership dans ldap pour les utilisateurs spécifiés. Peut être spécifié plusieurs fois.

nss_min_uid UID uid minimum pour les recherches dans ldap

nss_nested_groups yes|no Si l'attribut member pointe vers un autre groupe, les membres imbriqués sont retournés. Défaut : no.

validnames REGEX pattern pour déterminer les noms d'utilisateurs et de groupes valides.

ignorecase yes|no Prend en compte ou non la casse. yes peut exposer le système à des vulnérabilités.

pam_authz_search FILTER Permet de paramétrer la vérification d'authorisation. Le filtre spécifié est exécuté et si une entrée matche, l'accès est donné. Le filtre peut contenir les variables suivantes : **$username, $service, $ruser, $rhost, $tty, $hostname, $fqdn, $dn, $uid**. Peut être spécifié plusieurs fois.

pam_password_prohibit_message "MESSAGE" Refuse la modification de mot de passe avec pam_ldap et affiche le message spécifié. Peut être utilisé pour rediriger l'utilisateur vers un autre moyen de changer son mot de passe.

reconnect_invalidate DB,DB,... Si définis, vide les caches spécifiés au démarrage et lors des reconnexions au serveur. db est une des maps nsswitch.

cache CACHE TIME [TIME] Durée de rétentions des entrées dans le cache interne.

Expressions de mappage d'attributs

Pour certains attributs, une expression de mappage peut être utilisé pour construire la valeur résultante. C'est actuellement seulement possible pour les attributs qui n'ont pas besoin d'être utilisés dans les filtres de recherche. Les expressions sont un sous-jeu d'expressions shell. Au lieu de substitution de variable, la recherche d'attribut est faite sur l'entrée courante et la valeur d'attribut est substituée. Les expressions suivantes sont supportés :

${attr}, $attr Substitue la valeur de l'attribut

${attr :-word} Substitue la valeur de l'attribut ou, si l'attribut n'est pas définis ou vide, substitue le mot.

${attr :+word} Substitue le mot si l'attribut si l'attribut est mis, sinon substitue une chaîne vide.

${attr#word} Supprime le match le plus court possible de la gauche de la valeur de l'attribut

${attr##word} Supprime le match le plus long possible de la gauche de la valeur de l'attribut

${attr%word} Supprime le match le plus long possible de la droite de la valeur de l'attribut

${attr%%word} Supprime le match le plus court possible de la droite de la valeur de l'attribut

Seul la version '#' est supportée par nslcd, les autres sont supportés par pynslcd. Également, le seul wilcard supporté par nslcd est ?. Les caractères **"**, **$** et **** doivent être échappés.

Exemples

Utilise l'attribut shadowFlag, avec la valeur 0 par défaut :
"${shadowFlag :-0}"
Utilise uid pour construire homeDirectory si cette attribut est manquant :
"${homeDirectory :-/home/$uid}"
Si isDisabled est mis, retourne 100 :
"${isDisabled :+100}"
Enlève le préfixe {crypt} de userPassword :
"${userPassword#{crypt\}}"