slapo-nssow

Requêtes NSS et PAM via un socket unix

Il utilise le même protocole IPC que nss-pam-ldapd de Arthur de Jong. Utiliser un protocole IPC séparé pour les demandes NSS et PAM élimine les dépendance libldap dont souffrent les solutions pam_ldap/nss_ldap. Cet overlay s'exécute dans slapd, profitant d'un cache sophistiqué, sans les faiblesses de nscd. Une base LDAP distante peut être accédée en utilisant back-ldap avec un proxy-cache. Un autre bénéfice est que toutes les stratégies de sécurité sont administrées centralement via LDAP.

Configuration

nssov-ssd <service> <url> Configure un Service Search Descriptor (SSD) pour chaque service NSS qui sera utilisée.

ldap :/// [<basedn>] [? ? [<scope>] [?<filter>]] Le suffixe de la base, scope et filtre de recherche.

nssov-map <service> <orig> <new> Si la base locale est un proxy, certains mappages du schéma peuvent être nécessaire. Cette directive permet une substitution d'attribut simple.

nssov-pam <option> [...] Détermine le nombre de mode PAN. Les options valides sont :

- **userhost** Vérifie l'attribut host dans l'entrée pour l'autorisation
- **userservice** Vérifie l'attribut authorizedService dans l'entrée pour l'autorisation
- **usergroup** Vérifie que l'utilisateur est membre d'un groupe spécifique pour l'autorisation.
- **hostservice** Vérifie l'attribut authorizedService dans l'entrée pour l'autorisation
- **authz2dn** Utilise authz-regexp pour mapper l'uid à un DN ldap.
- **uid2dn** Utilise le SSD passwd NSS pour mapper un uid à un DN ldap.

nssov-pam-defhost <hostname> Spécifie un hostname par défaut pour vérifier si une entrée ipHost pour le nom d'hôte courant ne peut pas être trouvé

nssov-pam-group-ad <attribute> Spécifie de DN d'un groupe LDAP pour vérifier l'autorisation. L'utilisateur LDAP doit être membre de ce group pour être autorisé à s'authentifier. Il n'y a pas de valeurs par défaut.

nssov-pam-group-ad <attribute> Spécifie l'attribut à utiliser pour la vérification au groupe.

nssov-pam-min-uid <integer> Spécifie un uid minimum autorisé au login

nssov-pam-max-uid <integer> Spécifie un uid maximum autorisé au login

nssov-pam-template-ad <attribute> Spécifie un attribut à vérifier dans l'entrée utilisateur pour un template de nom de login.

nssov-pam-template <name> Spécifie un nom d'utilisateur pas défaut si aucun attribut template n'est trouvé dans l'entrée utilisateur.

nssov-pam-session <service> Spécifie un nom de service PAM dont les sessions seront enregistrés.

nssov-pam-password-prohibit-message <message> Désactive le service de changement de mot de passe et retourne le message spécifié aux utilisateurs

nssov-pam-pwdmgr-dn <dn> Spécifie le dn du responsable des mots de passe

nssov-pam-pwdmgr-pwd <pwd> Spécifie le mot de passe du responsable des mots de passe

loginStatus

Attribut opérationnel de l'entrée utilisateur. Les valeurs de l'attribut sont sous la forme **<generalizedTime> <host> <service> <tty> (<ruser@rhost>)**. À la déconnexion, la valeur correspondante est supprimée. Cela permet de vérifier si des utilisateur sont loggés sur tous les hôtes du réseau via un ldapsearch. Le rootdn de la base est utilisée pour effectuer les mises à jours de cet attribut, donc un rootdn doit toujours être configuré pour que cette fonctionnalité fonctionne.

Les fonctions PAM supportent LDAP password Policy également. Si l'overlay password policy est utilisé, les informations de stratégie peuvent être retournés au client PAM en résultat de l'authentification, gestion du compte, et demande de changement de mot de passe.

Exemple :

```
dn: olcOverlay={0}nssov,ocDatabase={1}hdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcNssOvConfig
olcOverlay: {0}nssov
olcNssSsd: passwd ldap:///ou=users,dc=example,dc=com??one
olcNssMap: passwd uid accountName
olcNssPam: hostservice uid2dn
olcNssPamDefHost: defaulthost
olcNssPamMinUid: 500
olcNssPamMaxUid: 32000
olcNssPamSession: login
olcNssPamSession: sshd
```