OpenLDAP - Sécurité

Considérations de sécurité

Écoute sélective : Par défaut, slapd écoute sur toutes les adresses IPv4 et IPv6. Pour spécifier les ip sur lesquelles slapd écoute : **slapd -h ldap ://127.0.0.1**

Firewall IP : Les capacités de firewalling IP du système peuvent être utilisées pour restreindre l'accès. Généralement, slapd écoute sur le port 389/tcp pour ldap :// et le port 636/tcp pour ldaps ://. slapd peut être configuré pour écouter sur d'autres ports.

TCP Wrappers : TCP wrappers fournis un système de contrôle d'accès basé sur des règles pour contrôler les accès TCP/IP sur le serveur. Par exemple : **slapd : 10.0.0.0/255.0.0.0 127.0.0.1 : ALLOW**, **slapd ALL : DENY**

Protection de confidentialité et d'intégrité de données : TLS peut être utilisé pour fournir une protection de confidentialité et d'intégrité de données. OpenLDAP supporte la négociation de TLS (SSL) via StartTLS et ldaps ://. Des mécanismes SASL (Simple Authentication and Security Layer) comme DIGEST-MD5 et GSSAPI sont également disponible.

Facteurs de sécurité forte : Le serveur utilise SSF pour indiquer la force du mécanisme. Un SSF de 0 spécifie aucune protection, à 1 des protections d'intégrité sont en place. un SSF > 1 indiquent la longueur de clé de cryptage. par exemple : DES fait 56, 3DES fait 112, AES fait 128, 192 ou 256.

'security' contrôle les opérations de restriction quand les protections appropriées ne sont pas en place. Exemple :
security ssf=1 update_ssf=112
requière une protection d'intégrité pour toutes les opérations et une protection 3DES ou équivalent, pour les opérations de mise à jour (add, delete, modify, etc.)

Méthodes d'authentification

La méthode simple a 3 modes d'opération : anonyme, non-authentifié, authentifié par user/password.

L'accès anonyme est requis en ne fournissant pas de nom et de mot de passe pour une simple opération. l'accès non authentifié est requis en fournissant un nom, mais pas de mot de passe. L'accès authentifié requière un nom valide et un mot de passe.

le mécanisme anonyme est activé par défaut, il peut être désactivé par "**disallow bind_anon**".

note : désactiver le mécanisme anonyme n'empêche pas les accès anonymes à l'annuaire. Pour exiger une authentification pour accéder à l'annuaire, utiliser "**require authc**"

L'accès non-authentifié est désactivé par défaut et peut être activé par "**allow bind_anon_cred**"

L'accès authentifié est activé par défaut. Cependant les mots de passe sont stockés en clair, il est recommandé de l'utiliser uniquement avec des session chiffrées. Il est recommandé que toutes les authentifications non protégées soient désactivées en utilisant par ex : **security simple_bind=56** qui exige les simple_bind d'utiliser le cryptage DES ou meilleur.

Le mécanisme d'authentification user/password peut être complètement désactivé en utilisant "**disallow bind_simple**".

Stockage des mots de passe

Les mots de passe LDAP sont normalement stockés dans l'attribut **userPassword**. la RFC4519 spécifie que les mots de passe ne sont pas stockés sous forme chiffrée. Cela permet d'utiliser une grande quantité de mécanismes basés sur les mots de passe, comme DIGEST-MD5.

Cependant, il peut être préférable de stocker un hash des mots de passe. slapd supporte plusieurs schémas de stockage.

L'attribut **userPassword** peut avoir une ou plusieurs valeurs, et il est possible pour chaque valeur d'être stockées sous une forme différente. durant l'authentification, slapd va chercher un des mots de passe qui correspondrai. Le schéma de stockage est stocké comme préfixe dans la valeur, donc un hash utilisant SHA1 ressemblera à :

userPassword : {SSHA}DkMTwBl+a/3DQTxCYEApdUtNXGgdUac3

Schéma de stockage de mot de passe SSHA

ces valeurs sont représentée sous la forme :
userPassword : {SSHA}DkMTwBl+a/3DQTxCYEApdUtNXGgdUac3
schéma de stockage de mot de passe CRYPT
Ce schéma utilise la fonction système crypt(3). Il produit le hash traditionnel à 13 caractères, mais peut également générer le hash MD5 34 octets de glibc2.
userPassword : {CRYPT}aUihad99hmev6
userPassword : {CRYPT}1czBJdDqS$TmkzUAb836oMxg/BmIwN.1

Schéma de stockage de mot de passe MD5

Ce schéma prend simplement le hash md5 et le stocke sous la forme base64 :
userPassword : {MD5}Xr4ilOzQ4PCOq3aQ0qbuaQ==
schéma de stokage de mot de passe SMD5
Il améliore le schéma MD5
userPassword : {SMD5}4QWGWZpj9GCmfuqEvm8HtZhZS6E=
schéma de stockage de mot de passe SHA
SHA est plus sécurisé que MD5
userPassword : {SHA}5en6G6MezRroT3XKqkdPOmY/BfQ=

Schéma de stockage de mot de passe SASL

Ce n'est pas vraiment un schéma de stockage de mot de passe. Il utilise l'attribut **userPassword** pour déléguer la vérification à un autre processus.

Schéma de stockage de mot de passe Kerberos

Ce n'est pas un schéma de stockage de mot de passe, il utilise la valeur de l'attribut de **userPassword** pour déléguer la vérification à Kerberos

Authentification Externe

Depuis OpenLDAP 2.0 slapd a la capacité de déléguer la vérification de mot de passe à un processus séparé. Il utilise la fonction sasl_checkpass(3). Le choix est très large, comme l'option d'utiliser saslauth(8) qui utiliser les fichiers local, kerberos, un serveur IMAP, un autre serveur LDAP ou tout ce qui peut supporter le mécanisme PAM.

L'authentification externe fonctionne seulement avec les mots de passe en clair. ce système est sélectif, il utilise uniquement les

utilisateurs dont l'attribut userPassword est marqué avec "SASL".

exemple :
userPassword : {SASL}username@realm

Configurer slapd pour l'utilisation d'un fournisseur d'authentification

Quand une entrée a une valeur de mot de passe "**{SASL}**", OpenLDAP délègue tout le processus de validation à cyrus SASL. Tout la configuration est faite dans les fichiers de configuration de SASL.

Un fichier nommé /usr/lib/sasl2/slapd.conf gouverne l'utilisation de SASL quand il communique avec slapd.

Simple exemple pour un serveur qui utilise saslauth pour vérifier les mots de passe :
mech_list : plain
pwcheck_method : saslauthd
saslauthd_path : /var/run/sasl2/mux

Configurer saslauth

saslauthd est capable d'utiliser différents services d'authentification, vois saslauthd(8). Exemple de saslauthd.conf qui utilise M$ Active Directory :
ldap_servers : ldap ://dc1.example.com/ ldap ://dc2.example.com/
ldap_search_base : cn=Users,DC=ad,DC=example,DC=com
ldap_filter : (userPrincipalName=%u)
ldap_bind_dn : cn=saslauthd,cn=Users,DC=ad,DC=example,DC=com
ldap_password : secret
dans ce cas, saslauthd est lancé avec le mécanisme d'authentification ldap et est définis pour combiner SASL avec le login :
saslauthd -a ldap -r