Groupe de travail Réseau
Request for Comments : 3062
Catégorie : En cours de normalisation

K. Zeilenga, OpenLDAP Foundation
février 2001
Traduction Claude Brière de L'Isle

Opération étendue de modification de mot de passe LDAP

Résumé
L'intégration du protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*) et des services externes d'authentification a introduit des identités d'authentification qui ne sont pas des noms distinctifs et a permis une mémorisation des mots de passe en dehors de répertoires. À ce titre, les mécanismes qui mettent à jour le répertoire (par exemple, Modify) ne peuvent pas être utilisés pour changer un mot de passe d'utilisateur. Le présent document décrit une opération LDAP étendue pour permettre la modification des mots de passe d'utilisateur qui ne dépend pas de la forme de l'identité d'authentification ni du mécanisme de mémorisation du mot de passe utilisé.

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

1. Fondements et destination

Le protocole léger d'accès à un répertoire (LDAP) [RFC2251] est conçu pour prendre en charge un certain nombre de mécanismes d'authentification incluant de simples paires de nom d'utilisateur/mot de passe. Traditionnellement, les utilisateurs LDAP étaient identifiés par le nom distinctif (DN, *Distinguished Name*) [RFC2253] d'une entrée de répertoire et cette entrée contenait un attribut Mot de passe d'utilisateur [RFC2256] contenant un ou plusieurs mots de passe.

Le protocole ne rend pas obligatoire que les mots de passe associés à un utilisateur soient mémorisés dans le serveur de répertoire. Le serveur peut utiliser tout attribut convenable pour la mémorisation du mot de passe (par exemple, userPassword) ou utiliser une mémorisation en dehors du répertoire.

L'intégration [RFC2829] de services SASL [RFC2222] neutres à l'égard de l'application qui prennent en charge des mécanismes simples de nom d'utilisateur/mot de passe (comme DIGEST-MD5) a introduit des formes d'identité d'authentification de nom distinctif non LDAP et a rendu la mémorisation des mots de passe de la responsabilité du fournisseur de service SASL.

Les opérations de mise à jour LDAP sont conçues pour agir sur les attributs d'une entrée dans le répertoire. Les opérations de mise à jour LDAP ne peuvent pas être utilisées pour modifier un mot de passe d'utilisateur lorsque l'utilisateur n'est pas représenté par un DN, n'a pas d'entrée, ou lorsque le mot de passe utilisé par le serveur n'est pas mémorisé comme un attribut d'une entrée. Un mécanisme de remplacement est nécessaire.

Le présent document décrit une opération d'extension de LDAP destinée à permettre aux client de répertoire de mettre à jour les mots de passe d'utilisateur. L'utilisateur peut être associé ou non à une entrée de répertoire. L'utilisateur peut être représenté ou non comme un nom distinctif LDAP. Le mot de passe de l'utilisateur peut être mémorisé ou non dans le répertoire.

L'opération NE DEVRAIT PAS être utilisée sans une protection de sécurité adéquate car l'opération n'assure aucune protection de sa confidentialité ou de son intégrité. Cette opération NE DEVRA PAS être utilisée de façon anonyme.

2. Demande et réponse de modification de mot de passe

L'opération Password Modify est une opération de LDAPv3 étendu du paragraphe 4.12 de la [RFC2251] et est identifiée par l'identifiant d'objet passwdModifyOID. La présente section précise la syntaxe de la demande et la réponse du protocole.

IDENTIFIANT D'OBJET passwdModifyOID ::= 1.3.6.1.4.1.4203.1.11.1

```
PasswdModifyRequestValue ::= SEQUENCE {
  userIdentity      [0]  CHAINE D'OCTETS FACULTATIF
  oldPasswd         [1]  CHAINE D'OCTETS FACULTATIF
  newPasswd         [2]  CHAINE D'OCTETS FACULTATIF }

PasswdModifyResponseValue ::= SEQUENCE {
  genPasswd         [0]   CHAINE D'OCTETS FACULTATIF }
```

2.1 Demande de modification de mot de passe

Une demande de modification de mot de passe est une ExtendedRequest *(demande étendue)* avec le champ requestName *(nom de demande)* qui contient l'OID passwdModifyOID et fournit facultativement un champ requestValue *(valeur de demande)*. Si le champ requestValue est fourni, il DEVRA contenir une PasswdModifyRequestValue *(valeur de demande de modification de mot de passe)* avec un ou plusieurs champs présents.

Le champ userIdentity *(identité de l'utilisateur)*, si il est présent, DEVRA contenir une représentation de chaîne d'octet de l'usager associé à la demande. Cette chaîne peut être ou non un nom distinctif LDAP (LDAPDN) [RFC2253]. Si aucun champ userIdentity n'est présent, la demande agit sur le mot de passe de l'usager actuellement associé à la session LDAP.

Le champ oldPasswd *(vieux mot de passe)*, si il est présent, DEVRA contenir le mot de passe actuel de l'usager.

Le champ newPasswd *(nouveau mot de passe)*, si il est présent, DEVRA contenir le mot de passe désiré de cet usager.

2.2 Réponse de modification de mot de passe

Une réponse de modification de mot de passe est une ExtendedResponse où le champ responseName est absent et où le champ response est facultatif. Le champ response, si il est présent, DEVRA contenir une PasswdModifyResponseValue *(valeur de réponse de modification de mot de passe)* avec un champ genPasswd *(mot de passe généré)* présent.

Le champ genPasswd, si il est présent, DEVRA contenir un mot de passe généré pour l'usager.

Si un code de résultat (resultCode) autre que succès (0) est indiqué dans la réponse, le champ response DOIT être absent.

3. Exigences du fonctionnement

Les clients NE DEVRAIENT PAS soumettre une demande de modification de mot de passe sans s'assurer que des sauvegardes de sécurité adéquates sont en place. Les serveurs DEVRAIENT retourner un code de résultat de non succès si une protection de la sécurité suffisante n'est pas établie.

Les serveurs DEVRAIENT indiquer leur prise en charge de cette opération d'extension en fournissant un PasswdModifyOID comme valeur du type d'attribut supportedExtension *(extension prise en charge)* dans leur DSE racine. Un serveur PEUT choisir de n'annoncer cette extension que lorsque le client est autorisé et/ou a établi les protections de sécurité nécessaires pour utiliser cette opération. Les clients DEVRAIENT vérifier que le serveur met en œuvre cette opération d'extension avant de tenter l'opération en affirmant que l'attribut supportedExtension contient une valeur de PasswdModifyOID.

Le serveur DEVRA ne retourner un succès que si il réussit à changer le mot de passe de l'usager. Autrement, le serveur DEVRA laisser le mot de passe inchangé et retourner un code de résultat de non succès.
Si le serveur ne reconnaît pas les champs fournis ou ne prend pas en charge la combinaison des champs fournis, il NE DEVRA PAS changer le mot de passe de l'usager.

Si oldPasswd est présent et si la valeur fournie ne peut pas être vérifiée ou est incorrecte, le serveur NE DEVRA PAS changer le mot de passe de l'usager. Si oldPasswd n'est pas présent, le serveur PEUT utiliser d'autres politiques pour déterminer si il change ou non le mot de passe.

Le serveur NE DEVRA PAS générer un mot de passe au nom du client si le client a fourni un nouveau mot de passe. En l'absence d'un nouveau mot de passe fourni par le client, le serveur DEVRA soit générer un mot de passe au nom du client, soit retourner un code de résultat de non succès. Le serveur DOIT fournir le mot de passe généré en cas de succès comme valeur du champ genPasswd.

Le serveur PEUT retourner le code de résultat adminLimitExceeded *(limite administrative dépassée)*, busy *(occupé)* , confidentialityRequired *(confidentialité exigée)*, operationsError *(erreur de fonctionnement)*, unavailable *(indisponible)*, unwillingToPerform *(refus d'exécution)*, ou d'autres codes de non succès, comme approprié pour indiquer qu'il n'a pas été capable de réussir à mener à bien l'opération.

Les serveurs PEUVENT mettre en œuvre des politiques administratives qui interdisent cette opération.

4. Considérations pour la sécurité

Cette opération est utilisée pour modifier les mots de passe d'utilisateurs. L'opération ne fournit par elle-même aucune protection pour assurer la protection de l'intégrité et/ou de la confidentialité des informations. L'utilisation de cette opération est fortement déconseillée lorsque des protections de la confidentialité ne sont pas en place pour garantir la confidentialité et elle peut résulter en la divulgation du mot de passe à des tiers non autorisés. Cette extension DOIT être utilisée avec une protection de la confidentialité, telle que Start TLS [RFC2830]. La suite de chiffrement NUL NE DOIT PAS être utilisée.

5. Références

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2222] J. Myers, "Authentification simple et couche de sécurité (SASL)", octobre 1997. (*Obsolète, voir* RFC4422, RFC4752) (*MàJ par* RFC2444) *(P.S.)*

[RFC2251] M. Wahl, T. Howes et S. Kille, "Protocole léger d'accès à un répertoire (v3)", décembre 1997.

[RFC2252] M. Wahl, A. Coulbeck, T. Howes, S. Kille, "Protocole léger d'accès à un répertoire (v3) : Définitions de syntaxe d'attribut", décembre 1997. (*Obsolète, voir* RFC4510, RFC4517, RFC4523, RFC4512) *(P.S.)*

[RFC2253] M. Wahl, S. Kille et T. Howes, "Protocole léger d'accès à un répertoire (LDAPv3) : Représentation de chaîne UTF-8 des noms distinctifs", décembre 1997.

[RFC2256] M. Wahl, "Résumé du schéma d'utilisateur X.500(96) à utiliser avec LDAPv3", décembre 1997. (*Obsolète, voir* RFC4517, RFC4519, RFC4523, RFC4512, RFC4510) *(P.S.)*

[RFC2829] M. Wahl et autres, "Méthodes d'authentification pour LDAP", mai 2000. (*Obsolète, voir* RFC4513, RFC4510) *(P.S.)*

[RFC2830] J. Hodges, R. Morgan, M. Wahl, "Protocole léger d'accès à un répertoire (v3) : extension pour la sécurité de la couche transport", mai 2000. (*Obsolète, voir* RFC4511, RFC4513, RFC4510) *(P.S.)*

6. Remerciements

Le présent document fait des emprunts à un certain nombre de documents de l'IETF et se fonde sur les travaux du groupe de travail LDAPext de l'IETF.

7. Adresse de l’auteur

Kurt D. Zeilenga
OpenLDAP Foundation
mél : Kurt@OpenLDAP.org

8. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d’éditeur des RFC est actuellement fourni par la Internet Society.