rfc3062

Opération Password Modify

L'intégration de LDAP et des services d'authentification externes a introduit des identités d'authentification non-DN et permis la décentralisation du stockage des mots de passe. Ainsi, les mécanismes de mise à jours de l'annuaire ne peuvent pas être utilisés pour changer les mots de passe.

Requête et réponse

L'opération étendue Password Modify est identifiée par l'OID passwdModifyOID :

```
passwdModifyOID OBJECT IDENTIFIER ::= 1.3.6.1.4.1.4203.1.11.1
PasswdModifyRequestValue ::= SEQUENCE {
 userIdentity [0] OCTET STRING OPTIONAL
 oldPasswd [1] OCTET STRING OPTIONAL
 newPasswd [2] OCTET STRING OPTIONAL }
PasswdModifyResponseValue ::= SEQUENCE {
 genPasswd [0] OCTET STRING OPTIONAL }
```

Une requête est une **ExtendedRequest** avec le champ **requestName** contenant le **passwdModifyOID** et fournis optionnellement un champs **requestValue**, qui devrait contenir un **PasswdModifyRequestValue** avec un ou plusieurs champs présents.

Le champ **userIdentity**, si présent, devrait contenir une chaîne représentant l'utilisateur associé avec la requête. Si ce champs n'est pas présent, la requête agis sur le mot de passe de l'utilisateur associé avec la session LDAP.

Le champ **oldPasswd**, si présent, devrait contenir le mot de passe courant de l'utilisateur

Le champ **newPasswd**, si présent, devrait contenir le nouveau mot de passe de l'utilisateur

Prérequis

Les clients ne devraient pas envoyer de requête sans s'assurer d'une sécurité adéquate. Les serveurs devraient retourner une erreur si la protection n'est pas suffisante.

Les serveurs devraient indiquer leur support pour cette opération étendu en fournissant **PasswdModifyOID** dans **supportedExtension**.

Si le serveur ne reconnaît pas les champs ou ne supporte pas la combinaison des champs fournis, il ne devrait pas changer le mot de passe.

Si **oldPasswd** est présent et que sa valeur ne peut être vérifiée ou est incorrect, le serveur ne devrait pas changer le mot de passe de l'utilisateur.

Le serveur ne devrait pas générer un mot de passe si le client a fournis un nouveau mot de passe. Si un client ne fournis pas de nouveau mot de passe, le serveur devrait soit générer un mot de passe, ou retourner une erreur.

Le serveur peut retourner **adminLimitExceeded, busy, confidentialityRequirement, operationError, unavailable, unwillingToPerform**, ou un autre resultCode s'il n'est pas en mesure de compléter l'opération.

Les serveurs peuvent implémenter des stratégies administratives pour restreindre cette opération.