slapo-ppolicy

Overlay ppolicy

Overlay de stratégie de mot de passe. Il intercepte et applique des contrôles de mot de passe.

OPTIONS

ppolicy_default <policyDN> DN de l'objet pwdPolicy à utiliser quand aucune stratégie n'est définie dans l'entrée de l'utilisateur.

ppolicy_forward_updates Spécifie que les changements d'état de stratégie qui résultent des opérations bind devraient être forwardés à un master au lieu d'être écrit directement dans la base local.

ppolicy_hash_cleartext Spécifie que les mots de passe en clair devraient être hashés. celà viole le modèle d'information X500 mais peut être utile pour les clients qui n'utilisent pas l'opération étendue Password Modify.

ppolicy_use_lockout Un client reçoit toujours une réponse InvalidCredentials lors d'un bind avec un compte bloqué. Cette option change le code de réponse pour inclure AccountLocked. Noter que ce code fournis des informations à un attaquant.

Schéma

pwdPolicy utilisé par l'overlay

pwdPolicyChecker Utilisé pour vérifier la qualité des mots de passe.

pwdAttribute Contient le nom de l'attribut où la stratégie de mot de passe s'applique. (accèpte uniquement userPassword)

pwdMinAge Secondes minimum entre chaque modifications permises

pwdMaxAge Secondes maximum entre chaque modifications permises

pwdInHistory Nombre d'historique de mots de passe à conserver.

pwdCheckQuality Indique si et comment la syntaxe de mot de passe sera vérifiée. 0 pas de vérification, 2, vérifie la syntaxe et si le serveur ne peut pas le vérifier, dû à un mot de passe hashé, il sera accepté. 2 le serveur doit pouvoir vérifier la syntaxe.

pwdMinLength Nombre minimum de caractère du mot de passe

pwdExpireWarning secondes avant expiration où le serveur envoie un message d'avertissement

pwdGraceAuthnLimit Nombre de fois q'un mot de passe expiré peut être utilisé pour authentifier un utilisateur

pwdLockout Action à prendre quand un utilisateur a échoue l'authentification pwdMaxFailure fois. a TRUE, l'utilisateur ne pourra plus s'authentifier.

pwdLockoutDuration Durée en seconde pendant laquelle l'utilisateur ne peut pas s'authentifier après pwdMaxFailure échecs d'authentification.

pwdMaxFailure Nombre d'authentifications consécutives échouées.

pwdFailureCountInterval Secondes avant que le comptes d'échec d'authentification soit purgé.

pwdMustChange A TRUE, spécifie que l'utilisateur doit changer son mot de passe une fois authentifié.

pwdAllowUserChange Spécifie si l'utilisateur peut changer son mot de passe ou non. (les ACL devraient être utilisés à la place de cet attribut)

pwdSafeModify a TRUE, le mot de passe et le nouveau mot de passe doivent être envoyés en même temps.

pwdCheckModule Nomme un module qui doit instancier la fonction check_password().

userPassword (opérationnel) Contient le mot de passe de l'utilisateur

pwdPolicySubentry (opérationnel) réfère directement à pwdPolicy

pwdChangedTime (opérationnel) Date de dernier changement de mot de passe

pwdAccountLockedTime (opérationnel) date à laquelle le compte a été bloqué. (000001010000Z indique que le compte est bloqué de manière permanente).

pwdFailureTime (opérationnel) Date de chaque échec d'authentification.

pwdHistory (opérationnel) Contient l'hitorique des derniers mots de passe utilisés.

pwdGraceUseTime (opérationnel) Date des logins effectués après que le mot de passe ait expiré.

pwdReset (opérationnel) Indique que le mot de passe a été réinitialisé par un administateur (il doit être changé à la prochaine authentification)

```
( 1.3.6.1.4.1.42.2.27.8.2.1 NAME 'pwdPolicy' AUXILIARY SUP top MUST ( pwdAttribute ) MAY ( pwdMinAge $
pwdMaxAge $ pwdInHistory $ pwdCheckQuality $ pwdMinLength $ pwdExpireWarning $ pwdGraceAuthnLimit $
pwdLockout $ pwdLockoutDuration $ pwdMaxFailure $ pwdFailureCountInterval $ pwdMustChange $
pwdAllowUserChange $ pwdSafeModify ) )

( 1.3.6.1.4.1.4754.2.99.1 NAME 'pwdPolicyChecker' AUXILIARY SUP top MAY ( pwdCheckModule ) )

( 1.3.6.1.4.1.42.2.27.8.1.1 NAME 'pwdAttribute' EQUALITY objectIdentifierMatch SYNTAX
1.3.6.1.4.1.1466.115.121.1.38 )

( 1.3.6.1.4.1.42.2.27.8.1.2 NAME 'pwdMinAge' EQUALITY integerMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.8.1.3 NAME 'pwdMaxAge' EQUALITY integerMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.8.1.4 NAME 'pwdInHistory' EQUALITY integerMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.8.1.5 NAME 'pwdCheckQuality' EQUALITY integerMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.8.1.6 NAME 'pwdMinLength' EQUALITY integerMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.8.1.7 NAME 'pwdExpireWarning' EQUALITY integerMatch SYNTAX
1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.8.1.8 NAME 'pwdGraceAuthnLimit' EQUALITY integerMatch SYNTAX
1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.8.1.9 NAME 'pwdLockout' EQUALITY booleanMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.8.1.10 NAME 'pwdLockoutDuration' EQUALITY integerMatch SYNTAX
1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.8.1.11 NAME 'pwdMaxFailure' EQUALITY integerMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.8.1.12 NAME 'pwdFailureCountInterval' EQUALITY integerMatch SYNTAX
1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.8.1.13 NAME 'pwdMustChange' EQUALITY booleanMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
SINGLE-VALUE )

( 1.3.6.1.4.1.42.2.27.8.1.14 NAME 'pwdAllowUserChange' EQUALITY booleanMatch SYNTAX
1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )
```

(1.3.6.1.4.1.42.2.27.8.1.15 NAME 'pwdSafeModify' EQUALITY booleanMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE)

(1.3.6.1.4.1.4754.1.99.1 NAME 'pwdCheckModule' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE)

(1.3.6.1.4.1.42.2.27.8.1.23 NAME 'pwdPolicySubentry' DESC 'The pwdPolicy subentry in effect for this object' EQUALITY distinguishedNameMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 SINGLE-VALUE NO-USER-MODIFICATION USAGE directoryOperation)

(1.3.6.1.4.1.42.2.27.8.1.16 NAME 'pwdChangedTime' DESC 'The time the password was last changed' SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 EQUALITY generalizedTimeMatch ORDERING generalizedTimeOrderingMatch SINGLE-VALUE NO-USER-MODIFICATION USAGE directoryOperation)

(1.3.6.1.4.1.42.2.27.8.1.17 NAME 'pwdAccountLockedTime' DESC 'The time an user account was locked' SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 EQUALITY generalizedTimeMatch ORDERING generalizedTimeOrderingMatch SINGLE-VALUE NO-USER-MODIFICATION USAGE directoryOperation)

(1.3.6.1.4.1.42.2.27.8.1.19 NAME 'pwdFailureTime' DESC 'The timestamps of the last consecutive authentication failures' SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 EQUALITY generalizedTimeMatch ORDERING generalizedTimeOrderingMatch NO-USER-MODIFICATION USAGE directoryOperation)

(1.3.6.1.4.1.42.2.27.8.1.20 NAME 'pwdHistory' DESC 'The history of user passwords' SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 EQUALITY octetStringMatch NO-USER-MODIFICATION USAGE directoryOperation)

(1.3.6.1.4.1.42.2.27.8.1.21 NAME 'pwdGraceUseTime' DESC 'The timestamps of the grace login once the passwordhas expired' SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 EQUALITY generalizedTimeMatch NO-USER-MODIFICATION USAGE directoryOperation)

(1.3.6.1.4.1.42.2.27.8.1.22 NAME 'pwdReset' DESC 'The indication that the password has been reset' EQUALITY booleanMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE USAGE directoryOperation)