OpenLDAP, ppolicy und passwd - Oder wie man den Passwortwechsel auf der Shell erzwingen kann

Dies ist kein Vollständiges Howto. Es ist nur ein ein kleiner Teil eines größeren Linux LDAP und Fileserver Projektes basierend auf Debian 5 Lenny, OpenLDAP, Samba und diversen Weiteren Linux Komponenten. Es ist ein TEIL des Linux Login-Scriptes welches über /etc/profile aufgerufen wird. Es überprüft ob das Linux-Passwort des Users abgelaufen ist und warnt bzw zwingt den Benutzer dazu sein Linux Passwort ggf zu ändern.

Diese Seite soll nur für Anregungen dienen und zeigen wie ich das eine oder andere Problem dabei gelöst habe.

Dabei ist zu bemerken dass ich hier nicht die in linux sonst so übliche Shadow-Passwords Technologie verwende, sondern primär auf OpenLDAP als Benutzerdatenbank im zusammenspiel mit dem OpenLDAP Overlay ppolicy setze.

check-for-pw-reset4.sh

check-for-pw-reset4.sh

```
#!/bin/sh
#
################################################
# /usr/local/bin/check-for-pw-reset4.sh         by Axel Werner
(mail@awerner.myhome-server.de)
#
#   FREE for Use/modify/copy as long you include my Name and eMail
Adress as original Source.
#   SELLING of this Script or even Parts of this Script is not allowed!
#
# This Script is to be sourced by /etc/profile or similar login script
to
# check a users homedir for a "Flare"-File dropped by the Administrator
after
# he reset the Users password. If that Flare-File is found the user is
been
# forced to change his password for security reasons.
#
################################################
#
# Version:    2009-07-20
#
#
# Version History:
#
```

```
# 2008-01-22  first Release by Axel Werner
# 2009-02-26  change: removed that "flare file" check. only check if
pwdReset flag is set in LDAP.
#         Else dont force user to reset pw as its been already set by
samba or something else.
# 2009-03-05  add:    since debian 5.0 the "grace login" feature of
openldaps ppolicy overlay got fixed.
#         therefor its nesesary to handly with it so users with expired
passwords are not
#         getting locked out permanently. i added a check for grace
logins so the user gets
#         a warning and an information about how many grace logins he
got left.
# 2009-03-16  add:    notice added that the user needs to change samba
pw separatly
#     change:    re-added the "flare file" check. because there are
problems with the pwdreset attribut
#         which locks out the user for some reason.
# 2009-07-20  change:    Enabled TLS by adding -ZZ to any LDAP Command
#
#
################################################
#
#
#set -x

# set the default ppolicy for normal users here so i can lookup their
grace logins
ppolicydn='cn=default,ou=policies,dc=someou,dc=higherou,dc=de'
flare='.password-reset-required'


flag=false

# check for ldap attribut 'pwdReset' if users pw has been reseted by
admin
flag=`ldapsearch -ZZ -x -LLL '(uid='"${USER}"')' 'pwdReset' | grep
pwdReset | cut -s -f2 -d':'`

# check for flare-file if users pw has been reseted by admin
if test -f ~/${flare}; then {
    #echo "Flare-File found in Homedirectory..."
    flag=' TRUE'
}
fi


if [ "${flag}" = ' TRUE' ] ; then
    cat <<EOF

ATTENTION:  Your Password has been reseted by your Administrator.
```

```
        For security reason you will NOW have to change your password
        to something ONLY YOU know about.

NOTE:       MAKE SURE your new password contains at least one
UPPERCASE,
        a NUMBER and one SPECIAL character. Else your will not be able
to
        change your password and so you cannot log in properly.

        NOW Please Enter Your OLD PASSWORD FIRST! (Those given by your
Admin)

EOF
    while ! passwd; do
    cat <<EOF

FAILURE: Changing your password failed. Maybe you used one of your
older passwords or
         your new password does not meet the password-requirements.
Please Retry!

AGAIN: Start entering your OLD Passwort first, then enter new Password
and confirm
       new password again.

EOF
    done
    rm ~/${flare} > /dev/null 2>&1
    cat <<EOF

Your Linux Console-Password has been Changed successfully! Thank You!
NOTICE: Dont forget to change/update your Samba Password too using your
Windows PC.

EOF
fi


################## GRACE LOGIN CHECK
################################################
#
#
#
#
GraceLoginsUses=false
GraceLoginsUses=`ldapsearch -ZZ -x -LLL '(uid='"${USER}"')'
pwdGraceUseTime | grep ^pwdGraceUseTime | wc -l`
if [ "${GraceLoginsUses}" != '0' ] ; then

    pwdGraceAuthNLimit=false
    loginsleft=false
```

```
    pwdGraceAuthNLimit=`ldapsearch -ZZ -x -LLL -b "${ppolicydn}"
pwdGraceAuthNLimit | grep ^pwdGraceAuthNLimit | cut -s -f2 -d':'`

    # trim leading and trailing whitespace from a variable
    pwdGraceAuthNLimit=${pwdGraceAuthNLimit##+([[:space:]])}
    pwdGraceAuthNLimit=${pwdGraceAuthNLimit%%+([[:space:]])}

    let loginsleft="${pwdGraceAuthNLimit}-${GraceLoginsUses}-1"

    if [ "${loginsleft}" -lt "1" ] ; then

        cat <<EOF

ATTENTION:  Your Password has expired!
        THIS IS YOUR LAST CHANCE TO CHANGE YOUR PASSWORD!
        If you dont change your password NOW your Account will
        become permanently locked.

NOTE:       MAKE SURE your new password contains at least one
UPPERCASE,
        a NUMBER and a SPECIAL character. Else your will not be able to
        change your password and so you cannot log in properly.

        NOW Please Enter Your OLD PASSWORD FIRST!

EOF
        while ! passwd; do
            cat <<EOF

FAILURE: Changing your password failed. Maybe you used one of your
older passwords or
         your new password does not meet the password-requirements.
Please Retry!

AGAIN: Start entering your OLD Passwort first, then enter new Password
and confirm
       new password again.

EOF
        done
        cat <<EOF

Your Linux Console-Password has been Changed successfully! Thank You!
NOTICE: Dont forget to change/update your Samba Password too using your
Windows PC.

EOF

    else
        cat <<EOF
```

```
#########
WARNING!
#########
It seems your Password has expired and THIS is a GRACE LOGIN.
You MUST change your Password within your remaining grace logins,
else your account will become LOCKED.

EOF
        echo "You have ${loginsleft} grace logins left!"
        echo
        echo "Press ENTER to confirm..."
        read

fi

fi

set +x
```

— *Axel Werner* *2010-12-30 19:26*

linux, openldap, ldap, ppolicy, samba, passwd, passwort, wechsel, erzwingen, articles, artikel, scripting, shell, bash