**Migración a OpenLDAP**

( Tiempo estimado por sucursal 15 minutos aprox. )

1 – Montar por nfs slnxapp3:/export y moverse al directorio MigracionOpenLDAP y copiar los archivos que se muestran a continuación a los directorios indicados:

[root@slnxapp3 MigracionOpenLDAP]#

/export/MigracionOpenLDAP

cert.pem - > /etc/openldap/cacerts

ldap.conf -> /etc/

nscd.conf -> /etc

pam\_ldap.conf -> /etc

sshd -> /etc/pam.d

system-auth -> /etc/pam.d

2 - Habilitar el servicio de cacheo de claves e iniciarlo:

**chkconfig nscd on**

**service nscd start**

3 - Editar /etc/nsswitch.conf y modificar el orden de búsqueda de usuarios y grupos de la siguiente manera:

**passwd: files ldap**

**shadow: files ldap**

**group: files ldap**

4 - Si todo está correcto en este punto ya deberíamos ver los usuarios que están el OpenLDAP, podemos probar consultando por el usuario cotoldap:

**suc02:/root>id cotoldap**

uid=1000(cotoldap) gid=3(sys) groups=3(sys)

5 – Como en algunas sucursales no están todos los ID de los usuarios iguales, por ejemplo en le suc02 el id del usuario pmorales es 786 y en la sucursal 121 es 728 debemos verificar por las dudas que los permisos y ownership en el directorio /home de cada usuario son los correctos para cada usuario, con un ls podemos ver si están bien o no, de lo contrario hay que cambiarlo con el comando **chown usuario home\_de\_usuario/**

6 – Todos los usuarios están dados de alta en OpenLDAP, así que podemos probar conectarnos a la sucursal, el portal para la administración de los usuarios es <https://slnxldap1.redcoto.com.ar/phpldapadmin> el usuario y clave están en keepass, para la administración de los mismos referirse a este documento, <http://intranet/SiteDirectory/gerenciadesistemas/unix/Documentos%20compartidos/Linux/Autenticacion%20Centralizada%20con%20OpenLDAP.docx>.

7 – En este punto ya deberíamos ver el servicio nscd conectado a slnxldap1 al puerto 636.

**suc02:/etc>lsof -i -a -n -P|grep nscd**

**nscd 28325 root 11u IPv4 18734861 TCP 129.2.255.253:30095-128.2.1.42:636 (ESTABLISHED)**

8 – La consulta de grupos nos debe traer los grupos de ldap también:

**suc02:/etc>getent group**

---- SNIP ----

seginf:x:904:

seginf:x:903:opsi2 opsi1

dba:x:501:jmachado fgauna rcastill panuccio oracle

sfsw:x:90:jchariano sortiz mescalante dsama cvillalba sfctrl opma1 opma2 opma3 opma4 opma5 opma6 opma7 opma8 opma9 opma10 opma11 opma12

sys:x:3:pmorales galonso cerizola clarrosa

users:x:100:

vtareser:x:506:

oinstall:x:900:jmachado fgauna rcastill panuccio oracle

java:x:500:

oper:x:300:ope1 ope2 ope3 ope4 ope5 ope6 opma1 opma2 opma3 opma4 opma5 opma6 opma7 opma8 opma9 opma10 opma11 opma12

ftp:x:50:ftpcam

9 – Desde slnxldap1 podemos ver las consultas, el log está en /var/log/slapd.log:

**adm01/home/pmorales>ssh suc02**

pmorales@suc02's password:

Last login: Thu Dec 26 15:33:32 2013 from 172.16.7.39

[pmorales@suc02 ~]$

**root@slnxldap1 log]# tail -f slapd.log**

Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 fd=20 ACCEPT from

**IP de la Sucursal al Puerto seguro 636.**

**IP=129.2.255.253:25680 (IP=0.0.0.0:636)**

**TLS, ssf=256 indica que está usando un canal encriptado con certificado.**

**Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 fd=20 TLS established tls\_ssf=256 ssf=256**

Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 op=0 BIND dn="" method=128

Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 op=0 RESULT tag=97 err=0 text=

Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 op=1 SRCH

**Donde está buscando los Usuario:**

**base="ou=Usuarios,dc=coto,dc=com,dc=ar" scope=1 deref=0 filter="(&(objectClass=posixAccount)(uid=pmorales))"**

Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 op=1 SEARCH RESULT tag=101 err=0 nentries=1 text=

Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 op=2 BIND dn="cn=Pablo Morales,ou=Usuarios,dc=coto,dc=com,dc=ar" method=128

**Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 op=2 BIND dn="cn=Pablo Morales,ou=Usuarios,dc=coto,dc=com,dc=ar" mech=SIMPLE ssf=0**

Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 op=2 RESULT tag=97 err=0 text=

Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 op=3 BIND anonymous mech=implicit ssf=0

Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 op=3 BIND dn="" method=128

Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 op=3 RESULT tag=97 err=0 text=

Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 op=4 UNBIND

Dec 27 14:08:15 slnxldap1 slapd[1053]: conn=7100 fd=20 closed

MIGRACION DE LAS CLAVES

Debemos migrar el uso de las nuevas claves antes de deshabilitar el usuario local porque no podemos tener usuarios duplicados, cuando los usuarios hayan cambiado su clave en LDAP y estén migradas las sucursales ( su configuración ) en ese momento bloqueamos el usuario local, los usuarios por defecto ya tienen la clave 123456 y están configurados para que cambien la clave al primer intento de conexión ( revisar antes por las dudas ver más abajo ), el procedimiento de cómo hacerlo está mas detallado también en:

<http://intranet/SiteDirectory/gerenciadesistemas/unix/Documentos%20compartidos/Linux/Autenticacion%20Centralizada%20con%20OpenLDAP.docx>

Recordemos que los únicos usuarios que no expiran son los opmaX y están en la política no expire, el resto de los usuario están dentro de la política default que tiene las directivas solicitadas por seguridad de la informacion las cuales están documentadas en el documento de PCI-DSS pueden hacer referencia a él en este link:

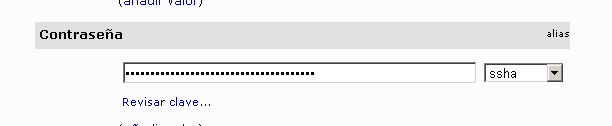
<http://intranet/SiteDirectory/gerenciadesistemas/unix/Documentos%20compartidos/PCI-DSS/Hardening%20de%20accesos%20-%20PCI_LIN_02.docx>



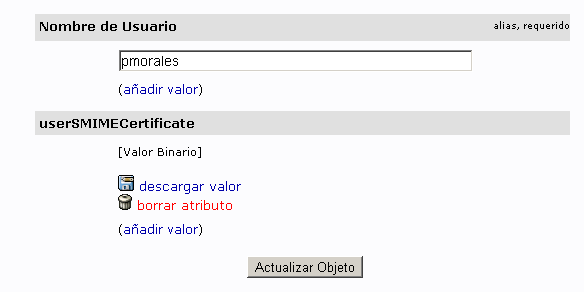
Repasando lo que está en el documento original, vamos a cambiar la clave de un usuario a 123456 y forzarle a que la cambie cuando ingrese, probamos con el usuario pmorales:



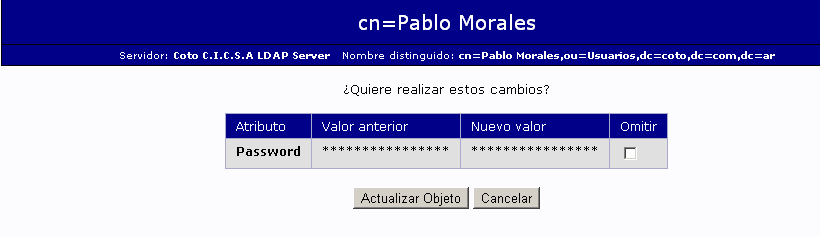
Le ponemos 123456



Grabamos los cambios en actualizar objeto:



Hacemos click en Actualizar Objeto nuevamente:



Ahora tenemos que forzar a que el usuario cambie su clave al ingresar, los scripts ( los de extensión .ldif ) están en:

**[root@slnxldap1 ldap]# pwd**

**/root/temp/ldap**

agrega-usuario-a-grupo.ldif

borro-usuario.ldif

cambio-password.ldif

crea-grupo.ldif

desbloqueo-usuario.ldif

**fuerza-cambio-passowrd.ldif**

host-attribute.ldif

operadores.ldif

pmorales.ldif

usuario-nuevo.ldif

Editamos el que dice **fuerza-cambio-passowrd.ldif**, el atributo **pwdReset** tiene que estar en **TRUE.**

dn: cn=Pablo Morales,ou=Usuarios,dc=coto,dc=com,dc=ar

changetype: modify

add: pwdReset

#delete: pwdReset

pwdReset: TRUE

Ejecutamos el siguiente comando, la clave es la misma que se utiliza para conectarse a la consola web:

**[root@slnxldap1 ldap]# ldapmodify -Wx -D "cn=Manager,dc=coto,dc=com,dc=ar" -f fuerza-cambio-passowrd.ldif**

Enter LDAP Password:

modifying entry "cn=Pablo Morales,ou=Usuarios,dc=coto,dc=com,dc=ar"

Verificamos que el usuario tenga el atributo pwdReset en TRUE:

**[root@slnxldap1 ldap]# ldapsearch -x "(uid=pmorales)" pwdReset**

# extended LDIF

#

# LDAPv3

# base <dc=coto,dc=com,dc=ar> (default) with scope subtree

# filter: (uid=pmorales)

# requesting: pwdReset

#

# Pablo Morales, Usuarios, coto.com.ar

dn: cn=Pablo Morales,ou=Usuarios,dc=coto,dc=com,dc=ar

**pwdReset: TRUE**

Nos conectamos a la sucursal:

**adm01/home/pmorales>ssh suc02**

pmorales@suc02's password:

You are required to change your LDAP password immediately.

Last login: Fri Dec 27 16:42:24 2013 from 172.16.7.39

WARNING: Your password has expired.

You must change your password now and login again!

Changing password for user pmorales.

Changing password for pmorales

**(current) UNIX password: 123456**

**Enter login(LDAP) password: 123456**

**New UNIX password: pepe123**

**BAD PASSWORD: is too simple**

New UNIX password:

Retype new UNIX password:

LDAP password information changed for pmorales

passwd: all authentication tokens updated successfully.

Connection to suc02 closed.

**adm01/home/pmorales>ssh suc02**

pmorales@suc02's password:

Last login: Fri Dec 27 16:42:42 2013 from 172.16.7.39

[pmorales@suc02 ~]$

El atributo **pwdReset** se borra automáticamente al actualizar la clave:

**[root@slnxldap1 ldap]# ldapsearch -x "(uid=pmorales)" pwdReset**

# extended LDIF

# LDAPv3

# base <dc=coto,dc=com,dc=ar> (default) with scope subtree

# filter: (uid=pmorales)

# requesting: pwdReset

#

# Pablo Morales, Usuarios, coto.com.ar

dn: cn=Pablo Morales,ou=Usuarios,dc=coto,dc=com,dc=ar

Si intentamos cambiar la clave se va a aplicar la política de seguridad ( **cn=default,ou=Policies,dc=coto,dc=com,dc=ar** ) la cual impide que se cambie tan pronto, debemos esperar 7 días o el equivalente en segundo 604800 el atributo en LDAP que define esto es **pwdMinAge** como referencia podemos consultar el siguiente link para el resto de los valores <http://www.zytrax.com/books/ldap/ch6/ppolicy.html>

Podemos ver a qué política de seguridad el usuario está asociado de la siguiente manera:

**[root@slnxldap1 ldap]# ldapsearch -x uid=pmorales pwdPolicySubentry**

# extended LDIF

#

# LDAPv3

# base <dc=coto,dc=com,dc=ar> (default) with scope subtree

# filter: uid=pmorales

# requesting: pwdPolicySubentry

# Pablo Morales, Usuarios, coto.com.ar

dn: cn=Pablo Morales,ou=Usuarios,dc=coto,dc=com,dc=ar

**pwdPolicySubentry: cn=default,ou=Policies,dc=coto,dc=com,dc=ar**

Intentemos cambiar la clave a ver si aplica la política asociada:

pmorales@suc02 ~]$ passwd

Changing password for user pmorales.

Changing password for pmorales

(current) UNIX password:

Enter login(LDAP) password:

New UNIX password:

Retype new UNIX password:

LDAP password information update failed: Can't contact LDAP server

**Password is too young to change**

passwd: Permission denied