POLÍTICAS DE SEGURIDAD - LDAP

Empresa:	Colsanitas S.A.
Objetivo del documento:	Resultado investigación de la implementación de las políticas de seguridad en OpenLDAP.

Control de versiones:

Versión	Fecha	Revisado por	Descripción del cambio
1.0	28-Nov-2011	Alex Márquez	Primera versión

1. Tabla de contenidos

Tabla de contenidos

2. Objetivos

Mostrar los mecanismos de seguridad que ofrece el servidor OpenLDAP y la forma como se se deben configurar sin entrar en el detalle del manejo de las ramas en LDAP.

3. Políticas de Seguridad.

A nivel de servidor OpenLDAP existen diversas políticas de seguridad que se implementaron en conjunto con la aplicación LoginAdmin que se detallan a continuación:

3.1. Control de Accesos

Permite el control de acceso a la información que se encuentra dentro del repositorio LDAP, esto se hace mediante Access Control Lists (ACLs). Cuando un cliente hace una petición al servidor, este evalúa si el cliente tiene los permisos suficientes para acceder a la información solicitada utilizando las listas en los archivos de configuración.

El control de accesos se debe configurar en el archivo sladp.conf y para esta implementación se configuró una regla simple agregando lo siguiente:

```
access to attrs=userPassword
        by anonymous auth
        by self write
        by * none
access to *
        by self write
        by * none
```

La intención de esta entrada es proteger el atributo userPassword, lo que quiere decir, que el atributo userPassword puede utilizarse por un usuario anónimo del sistema para realizar la comparación en el proceso de authenticación. Además, implica que un usuario puede escribir sobre su propio password y que un usuario cualquiera no puede ejecutar ninguna operación sobre el campo de otro usuario. Por otro lado, también se define quien puede escribir en la información de un usuario en este caso sólo él mismo.

Cabe aclarar que estas restricciones no aplican al administrador del sistema, y por ende, este puede disponer de la información cuando sea conveniente, pero se debe usar con mucha precaución.

Existen restricciones mucho más complejas que van desde el uso de expresiones regulares hasta la ip de la máquina cliente para determinar la información a la que puede acceder.

3.2. Uso de Base de Datos

Se utiliza la base de datos HDB que es la nueva generación de mecanismos de almacenamiento para OpenLDAP. Tal como su predecesor (BDB), HDB usa las base de datos Oracle Berkeley DB para el almacenamiento, pero almacena la información jerárquicamente que se ajusta perfectamente a la estructura de árbol de LDAP.

El control de accesos se debe configurar en el archivo sladp.conf y para esta implementación se configuró el uso de HBD agregando lo siguiente:

moduleload back_hdb.so
database hdb

3.3. Políticas de Password

La extensión Password Policy tiene muchas características, todas bien documentadas tal como el borrador de estándar de IETF. La categoría de este módulo es experimental, clasificación que no se refleja en la estabilidad de su implementación con calidad tipo producción.
Esta extensión provee funcionalidades como: envejecimiento de cuentas, expiración de claves, validación de fortaleza de claves, logins de gracia, y una variedad de otros servicios de mantenimiento de claves.

El control de accesos se debe configurar en el archivo sladp.conf y para esta implementación se configuró el uso de dichas políticas agregando lo siguiente:

include /etc/ldap/schema/ppolicy.schema
moduleload ppolicy.so

overlay ppolicy

ppolicy_default "cn=Default,ou=Policies,dc=colsanitas,dc=com"

ppolicy_hash_cleartext

ppolicy_hash_cleartext
Define si las claves deben guardarse en el repositorio en forma de Hash.

A groso modo se establece que la política por defecto estará definido en la entrada
"cn=Default,ou=Policies,dc=colsanitas,dc=com"
que debe ser un objeto de tipo pwdPolicy del schema ppolicy.schema.

Como atributos importantes de este objeto se encuentan:
pwdExpireWarning: Número de segundos a partir del cual se le hace la advertencia al usuario que su password va a expirar.
pwdMaxAge: Tiempo de vida máximo de una clave en segundos.
pwdInHistory: Cuando se hace validación de claves, es el número de claves inmediatamente anteriores que se comparan para evitar que el usuario las re-use nuevamente.
pwdCheckQuality: Define si se hace validación de la calidad de la clave.
pwdMinLength: Mínima cantidad de caracteres que debe tener una clave.
pwdAllowUserChange: Define si un usuario puede cambiar su propia clave.
Items not currently used.

pwdMinAge: Define el número de segundos que debe esperar un usuario antes de poder usar su clave
pwdGraceAuthnLimit: Número de logins exitosos que puede tener un usuario antes que el sistema lo obligue a cambiar su clave.
pwdLockout: Define si una clave se bloquea por intentos fallidos

pwdLockoutDuration: Tiempo en segundos que demora en desbloquearse una clave.
pwdMaxFailure: Máximo número de intentos que puede hacer un usuario antes que su clave sea bloqueada.
pwdMustChange: Define si el usuario está obligado a cambiar la clave.
pwdSafeModify: Define si el usuario está obligado a suministrar nuevamente su clave para poder realizar un cambio de la misma.

En caso de que para un usuario se deseen establecer otras políticas distintas a las definidas por defecto, se debe hacer uso del atributo pwdPolicySubentry en el usuario especifico y asignarle la referencia a otra política según se considere.

Cabe aclarar que estas restricciones no aplican al administrador del sistema, y por ende, este puede disponer de la información cuando sea conveniente, pero se debe usar con mucha precaución.

3.4. Otros Temas por trabajar

Es posible mejorar el desempeño y las funcionalidades que se usan de OpenLDAP si se profundiza en temas como:

Ajustes de desempeño.
Integridad Referencial.
Creación de esquemas propios.
Caching.
Replicación entre árboles con posibilidad de modificación.

4. Instrucciones de Instalación

Para realizar la instalación de las políticas de seguridad descritas, se debe hacer lo siguiente:

1. Cambiar el usuario y la clave del administrador general en el archivo anexo slapd.conf.
2. Copiar el archivo slapd.conf en la ruta: **/etc/ldap/slapd.conf** cambiando el Password y el nombre del administrador por el del servidor.
3. Inciar el servidor pasando como parámetro la configuración anterior : slapd -d config -f **/etc/ldap/slapd.conf**
4. Autenticarse con la herramienta Jxplorer con el usuario y clave definidos en el numeral 1.
5. En Jxplorer Importar el archivo anexo 2 como un fichero LDIF.

5. Utilizar comandos de línea.

Desde línea de comandos Linux es posible manipular una instancia de un servidor OpenLDAP, a continuación un conjunto de comandos útiles:

- Intentar cambiar la clave de un usuario por él mismo:

```
ldappasswd -H ldap://localhost -D uid=prueba.prest,ou=people,dc=colsanitas,dc=com -W -A -S "uid=prueba.prest,ou=people,dc=colsanitas,dc=com"
```

- Intentar cambiar la clave de un usuario por el administrador:

```
ldappasswd -H ldap://localhost -D cn=Manager,dc=colsanitas,dc=com -w secret -A -S "uid=prueba.prest,ou=people,dc=colsanitas,dc=com"
```

- Busca información en el árbol (requiere binding):

```
ldapsearch -x -D 'uid=prueba.prest,ou=people,dc=colsanitas,dc=com' -b "" -s base -w fuck
```

- Modificar alguna entrada del árbol:

```
ldapmodify -x -W -D cn=Manager,dc=colsanitas,dc=com
```

- Buscar toda la información de un usuario:

```
ldapsearch -LL -x -w secret -D 'cn=Manager,dc=colsanitas,dc=com' '(uid=prueba.prest)'
```

- Subir una instancia adicional de OpenLDAP Con un puert especifico:

```
slapd -d config -f /etc/ldap/slapd.conf -h ldap://192.168.136.221:489
```

6. Referencias

Configuración de OpenLDAP en Ubuntu
https://help.ubuntu.com/10.04/serverguide/C/openldap-server.html

Descripción de las Políticas de Password
http://linux.die.net/man/5/slapo-ppolicy

Descripción de las Políticas de Password
http://www.zytrax.com/books/ldap/ch6/ppolicy.html
Mastering OpenLDAP, Matt Butcher.
http://www.packtpub.com/OpenLDAP-Developers-Server-Open-Source-Linux/book

Información sobre la herramienta Jxplorer
http://jxplorer.org/

Borrador de estandar - Password Policy for LDAP Directories
http://tools.ietf.org/html/draft-behera-ldap-password-policy-10

7. Anexo 1 – sladp.conf

```
# slapd.conf - Configuration file for LDAP SLAPD


##########
# Basics #
##########
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/dyngroup.schema


pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
loglevel any
modulepath /usr/lib/ldap
# modulepath /usr/local/libexec/openldap
moduleload back_hdb.so
moduleload ppolicy.so
moduleload dyngroup.so


############################
# Database Configuration #
############################
```

```
database hdb
suffix "dc=colsanitas,dc=com"
rootdn "cn=Manager,dc=colsanitas,dc=com"
rootpw secret
directory /var/lib/ldap
# directory /usr/local/var/openldap-data
index objectClass,cn eq



########
# ACLs #
########
access to attrs=userPassword
        by anonymous auth
        by self write
        by * none
access to *
        by self write
        by * none



##############################
# Password policy enforcement.   #
##############################

overlay ppolicy
ppolicy_default "cn=Default,ou=Policies,dc=colsanitas,dc=com"
ppolicy_hash_cleartext
#ppolicy_use_lockout
```

8. Anexo 2 – Default.ldif

dn: ou=Policies,dc=colsanitas,dc=com

objectClass: top

objectClass: organizationalUnit

ou: policies

dn: cn=Default,ou=Policies,dc=colsanitas,dc=com

objectClass: top

objectClass: device

objectClass: pwdPolicy

cn: Default

pwdAttribute: userPassword

90 dias (7776000 seg.) para que se venza el password y a partir del 80 días (6912000 seg.)comenzar a avizar.

pwdExpireWarning: 6912000

pwdMaxAge: 7776000

pwdInHistory: 4

pwdCheckQuality: 2

pwdMinLength: 8

pwdAllowUserChange: TRUE

Items not currently used.

pwdMinAge: 0

pwdGraceAuthnLimit: 0

pwdLockout: TRUE

pwdLockoutDuration: 30

pwdMaxFailure: 3

pwdFailureCountInterval: 0

pwdMustChange: TRUE

pwdSafeModify: TRUE

pwdReset: TRUE