User Management: How do I define a password policy in LDAP?

How do I define a password policy in LDAP?

Changing the default password hash algorithm

(Tested on RHEL6. For RHEL7 some steps may not be valid)

passwd-hash configures one or more hashes to be used in generation of user passwords stored in the userPassword attribute during processing of LDAP Password Modify Extended Operations (RFC 3062). This allows the directory server to handle hashing instead of the client. The password hash to use for new passwords must be one of SSHA, SHA, SMD5, MD5, CRYPT, and CLEARTEXT. When the password-hash directive is not specified, the default is SSHA.

Including this option in the configuration file conforms to best practices and will be specified in this guide using the SSHA hashing algorithm.

Change the password-hash global variable in /cm/local/apps/openldap/etc/slapd.conf :

```
# Set password hashing algorithm to use by default
password-hash {CRYPT}
password-crypt-salt-format "$6$%.12s"
```

The salt format here is '$6$' which invokes a SHA512-based hash method and provides 12 characters (72 bits) of salt. It uses the default 5000 iterations. The table on Hashcat's home page suggests that this is around 50,000 times stronger than the simple SSHA1 hash.

Configure the LDAP server to use a password policy

Edit the file /cm/local/apps/openldap/etc/slapd.conf

```
- Include a policy schema:
```

```
include         /cm/local/apps/openldap/etc/schema/ppolicy.schema
```

- Load the password policy module:

```
moduleload ppolicy.la
```

- Add the following to the Access Control Policy:

```
access to *
 by self write
 by * read
```

- Add the following overlay policy after the auto-generated section:

```
overlay ppolicy
ppolicy_default "cn=default,ou=policies,dc=cm,dc=cluster"
ppolicy_use_lockout
```

Create and import a password policy

```
# cat /cm/local/apps/openldap/etc/password-policy.ldif



dn: ou=policies,dc=cm,dc=cluster
ou: policies
objectClass: top
objectClass: organizationalUnit


dn: cn=default,ou=policies,dc=cm,dc=cluster
objectClass: top
objectClass: device
objectClass: pwdPolicy
cn: default
pwdAttribute: userPassword
pwdMaxAge: 7776002
pwdExpireWarning: 432000
pwdInHistory: 3
pwdCheckQuality: 1
pwdMinLength: 8
pwdMaxFailure: 5
pwdLockout: TRUE
pwdLockoutDuration: 900
pwdGraceAuthNLimit: 0
pwdFailureCountInterval: 0
pwdMustChange: TRUE
pwdAllowUserChange: TRUE
pwdSafeModify: FALSE
```

This sets the following policies:

- password expiration at 90 days
- password lockout on 5 failures and lockout duration of 15 mintues
- minimum password length of 8
- 3 earlier password in history

To import the policy:

```
ldapadd  -D "cn=root,dc=cm,dc=cluster" -W -x  -f /cm/local/apps/openld
ap/etc/password-policy.ldif
```

You will be prompted for the password of rootdn ("cn=root,dc=cm,dc=cluster"). See the slapd.conf. To view the imported policy:

```
ldapsearch  -x -D "cn=root,dc=cm,dc=cluster" -W -b "dc=cm,dc=cluster"
```

Configure the clients

Edit the file /etc/pam_ldap.conf on all the headnode and all the software images (/cm/images//etc/pam_ldap.conf) and uncomment the lines:

```
# Search the root DSE for the password policy (works
# with Netscape Directory Server)

pam_lookup_policy yes

# Use the OpenLDAP password change
# extended operation to update the password.

pam_password exop
```

More on password policies

- The user is allowed to change his own password. Note that the directory ACLs for this attribute can also affect this ability (pwdAllowUserChange: TRUE).
- The name of the password attribute is "userPassword" (pwdAttribute: userPassword). Note that this is the only value that is accepted by OpenLDAP for this attribute.
- The server will check the syntax of the password. If the server is unable to check the syntax (i.e., it was hashed or otherwise encoded by the client) it will return an error refusing the password (pwdCheckQuality: 2).
- When a client includes the Password Policy Request control with a bind request, the server will respond with a password expiration warning if it is going to expire in ten minutes or less (pwdExpireWarning: 600). The warnings themselves are returned in a Password Policy Response control.
- When the password for a DN has expired, the server will allow five additional "grace" logins (pwdGraceAuthNLimit: 5).
- The server will maintain a history of the last five passwords that were used for a DN (pwdInHistory: 5).
- The server will lock the account after the maximum number of failed bind attempts has been exceeded (pwdLockout: TRUE).
- When the server has locked an account, the server will keep it locked until an administrator unlocks it (pwdLockoutDuration: 0)
- The server will reset its failed bind count after a period of 30 seconds.
- Passwords will not expire (pwdMaxAge: 0).
- Passwords can be changed as often as desired (pwdMinAge: 0).
- Passwords must be at least 5 characters in length (pwdMinLength: 5).
- The password does not need to be changed at the first bind or when the administrator has reset the password (pwdMustChange: FALSE)
- The current password does not need to be included with password change requests (pwdSafeModify: FALSE)
- The server will only allow five failed binds in a row for a particular DN (pwdMaxFailure: 5).

The full slapd.conf configuration file

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
include         /cm/local/apps/openldap/etc/schema/core.schema
include         /cm/local/apps/openldap/etc/schema/cosine.schema
include         /cm/local/apps/openldap/etc/schema/inetorgperson.schema
include         /cm/local/apps/openldap/etc/schema/nis.schema
include         /cm/local/apps/openldap/etc/schema/ppolicy.schema

# Allow LDAPv2 client connections.  This is NOT the default.
allow bind_v2

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral       ldap://root.openldap.org

pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args


#password-hash {CRYPT}
#password-crypt-salt-format "$6$%.12s"
```

```
# Load dynamic backend modules:
# modulepath    /cm/local/apps/openldap/sbin/openldap
# moduleload    back_bdb.la
# moduleload    back_ldap.la
# moduleload    back_ldbm.la
# moduleload    back_passwd.la
# moduleload    back_shell.la
moduleload ppolicy.la

# The next three lines allow use of TLS for encrypting connections usi
ng a
# dummy test certificate which you can generate by changing to
# /usr/share/ssl/certs, running "make slapd.pem", and fixing permissio
ns on
# slapd.pem so that the ldap user or group can read it.  Your client s
oftware
# may balk at self-signed certificates, however.
# TLSCACertificateFile /usr/share/ssl/certs/ca-bundle.crt
# TLSCertificateFile /usr/share/ssl/certs/slapd.pem
# TLSCertificateKeyFile /usr/share/ssl/certs/slapd.pem

# Sample security restrictions
#       Require integrity protection (prevent hijacking)
#       Require 112-bit (3DES or better) encryption for updates
#       Require 63-bit encryption for simple bind
# security ssf=1 update_ssf=112 simple_bind=64

# Sample access control policy:
#       Root DSE: allow anyone to read it
#       Subschema (sub)entry DSE: allow anyone to read it
#       Other DSEs:
#               Allow self write access
#               Allow authenticated users read access
#               Allow anonymous users to authenticate
#       Directives needed to implement policy:
# access to dn.base="" by * read
# access to dn.base="cn=Subschema" by * read
# access to *
#       by self write
#       by users read
#       by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn.  (e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!
# the "rogroup" contains user with a read-only access to the directory
access to attrs=userPassword
 by group.exact="cn=rogroup,dc=cm,dc=cluster" read
 by self write
 by anonymous auth
 by * none

access to dn=""
 by group.exact="cn=rogroup,dc=cm,dc=cluster" read
 by * read

access to attrs=loginShell,shadowLastChange
 by group.exact="cn=rogroup,dc=cm,dc=cluster" read
 by self write
 by * read

access to *
 by group.exact="cn=rogroup,dc=cm,dc=cluster" read
 by * read


#access to *
# by self write
# by * read
#access to *
# by self write
# by users read
# by anonymous auth
#Note that for some of the attributes you may have to enable write
#access for the users:
#
#access to attrs=shadowLastChange,userPassword,...,...
#      by self write
#      by * read
#      by anonymous auth



#######################################################################
#
# ldbm and/or bdb database definitions
#######################################################################
#

database        bdb
suffix          "dc=cm,dc=cluster"
rootdn          "cn=root,dc=cm,dc=cluster"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw          {SSHA}s60Jgj36WxG9oInPntUOEQ3IE70tECEM
# rootpw                {crypt}ijFYNcSNctBYg
#rootpw                         secret

# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory       /var/lib/ldap

# Indices to maintain for this database
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index uniqueMember                      eq,pres
index nisMapName,nisMapEntry            eq,pres,sub

# Replicas of this database
#replogfile /var/lib/ldap/openldap-master-replog
#replica host=ldap-1.example.com:389 starttls=critical
#     bindmethod=sasl saslmech=GSSAPI
#     authcId=host/ldap-master.example.com@EXAMPLE.COM

# Kill inactive connections after 101 seconds
idletimeout 101

# Maintain 10000 entries in memory, increase if number of records is f
ar greater
cachesize 10000

# Checkpoint the database every 5 minutes, or after 128Kb of writes (w
hichever comes first)
checkpoint 128 5

# Do not log debugging output
loglevel 0

# Allow unlimited result-sets to be returned
sizelimit unlimited

#Explicitly disable monitoring to prevent annoying warning
monitoring off


# This section of this file was automatically generated by cmd. Do not
 edit manually!
```

```
# BEGIN AUTOGENERATED SECTION -- DO NOT REMOVE
index entryCSN,entryUUID eq
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
# END AUTOGENERATED SECTION   -- DO NOT REMOVE

overlay ppolicy
ppolicy_default "cn=default,ou=policies,dc=cm,dc=cluster"
ppolicy_use_lockout
```

Unique solution ID: #1225
Author: Panos Labropoulos
Last update: 2016-05-06 10:49