Dashboard / … / Consumer IAM Design

Password Policy - Directory Services

Created by Suresh Chinta, last modified on Apr 24, 2019

Ways to define password policies in Directory Services ?

Copied from Forgerock Article provided in reference section

> - Use the pwdPolicy object class to assign subentry based password policies - this method is appropriate (and the simplest) for applying a password policy to all members of a branch.
> - Use a collectiveAttributeSubentry object to assign password policies - this method is appropriate for applying a password policy to LDAP group members or to a subset of users in a specific branch that meet the criteria, for example, base "ou=People".

As all consumers belong to the same category, although they have varying views depending on borrower / guarantor etc., the password policy is uniformly applicable.

Goal

- Create a password policy and make it applicable to all user's in dev1-aes branch (integrate into build script enforcing same policy for each backend)
- Make use of PHEAA-PBKDF2 password scheme and allow pre-encoded passwords (for credential migration)
- Set maximum password failure attempts to 4
- Set lockout duration and self-unlock duration to 5 minutes

Implementation and Testing

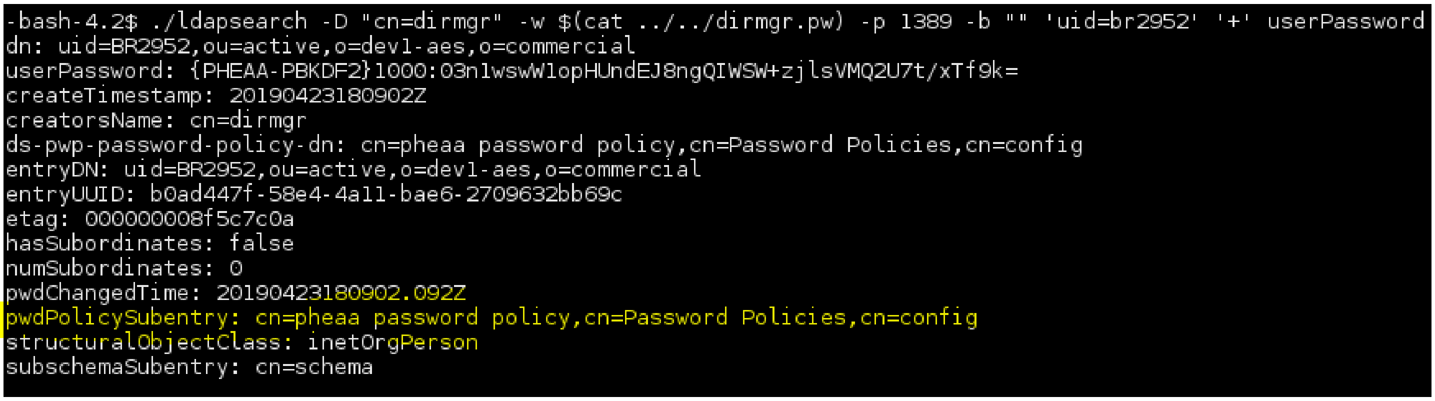
Create a password policy.

```
./dsconfig create-password-policy \
 --set default-password-storage-scheme:PHEAA-PBKDF2 \
 --set password-attribute:userpassword \
 --type password-policy \
 --policy-name "pheaa password policy" \
 --hostname $(hostname -f).pheaacloud.org \
 --port 4444 \
 --bindDN cn=dirmgr \
 --bindPassword supersecret \
 -X -n
```

Make it applicable to user's in dev1-aes backend

```
./dsconfig create-virtual-attribute \
 --set attribute-type:ds-pwp-password-policy-dn \
 --set enabled:true \
 --set value:"cn=pheaa password policy,cn=Password Policies,cn=config" \
 --set base-dn:o=dev1-aes,o=commercial \
 --set filter:\(objectClass=person\) \
 --type user-defined \
 --name "Custom PP Assignment" \
 --hostname $(hostname -f).pheaacloud.org \
 --port 4444 \
 --bindDN cn=dirmgr \
 --bindPassword supersecret \
 -X -n
```

Verify user has a 'pwdPolicySubEntry' attribute associated



```
-bash-4.2$ ./ldapsearch -D "cn=dirmgr" -w $(cat ../../dirmgr.pw) -p 1389 -b "" 'uid=br2952' '+' userPassword
dn: uid=BR2952,ou=active,o=dev1-aes,o=commercial
userPassword: {PHEAA-PBKDF2}1000:03n1wswW1opHUndEJ8ngQIWSW+zjlsVMQ2U7t/xTf9k=
createTimestamp: 20190423180902Z
creatorsName: cn=dirmgr
ds-pwp-password-policy-dn: cn=pheaa password policy,cn=Password Policies,cn=config
entryDN: uid=BR2952,ou=active,o=dev1-aes,o=commercial
entryUUID: b0ad447f-58e4-4a11-bae6-2709632bb69c
etag: 000000008f5c7c0a
hasSubordinates: false
numSubordinates: 0
pwdChangedTime: 20190423180902.092Z
pwdPolicySubentry: cn=pheaa password policy,cn=Password Policies,cn=config
structuralObjectClass: inetOrgPerson
subschemaSubentry: cn=schema
```

Password Policy Configuration

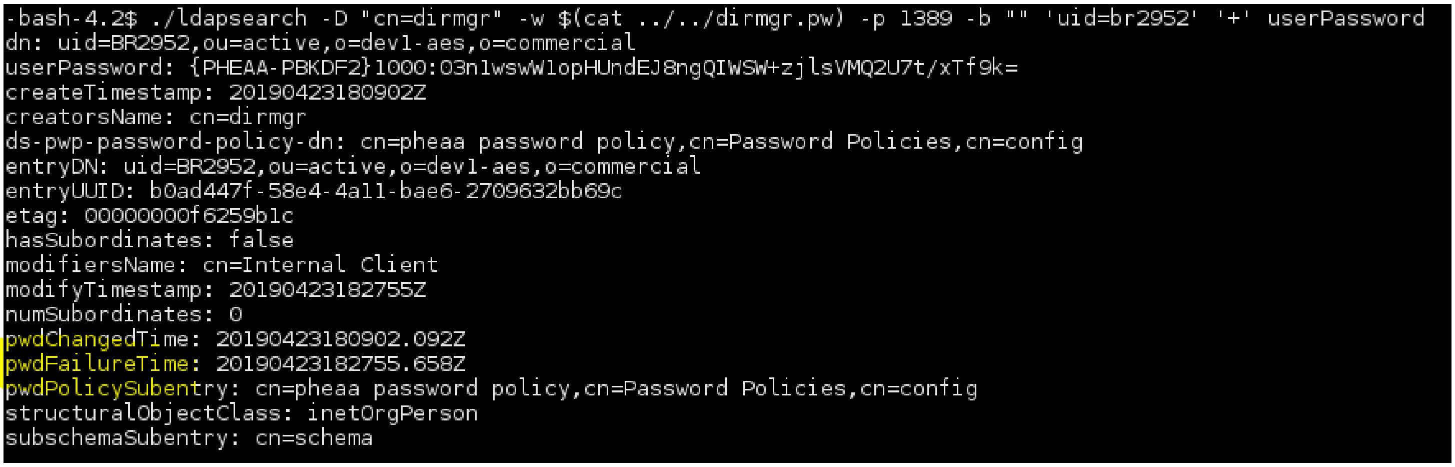
- Max failure attempts to 4
- password lockout and unlock duration to 5 minutes

```
./dsconfig set-password-policy-prop \
 --policy-name pheaa\ password\ policy \
 --set lockout-failure-count:4 \
 --set lockout-duration:300\ s \
 --set lockout-failure-expiration-interval:300\ s \
 --hostname devforgedssrvb.pheaacloud.org \
 --port 4444 \
 --bindDn cn=dirmgr \
 --bindPassword supersecret \
 --trustAll \
 --no-prompt
```

Bind with invalid credentials:

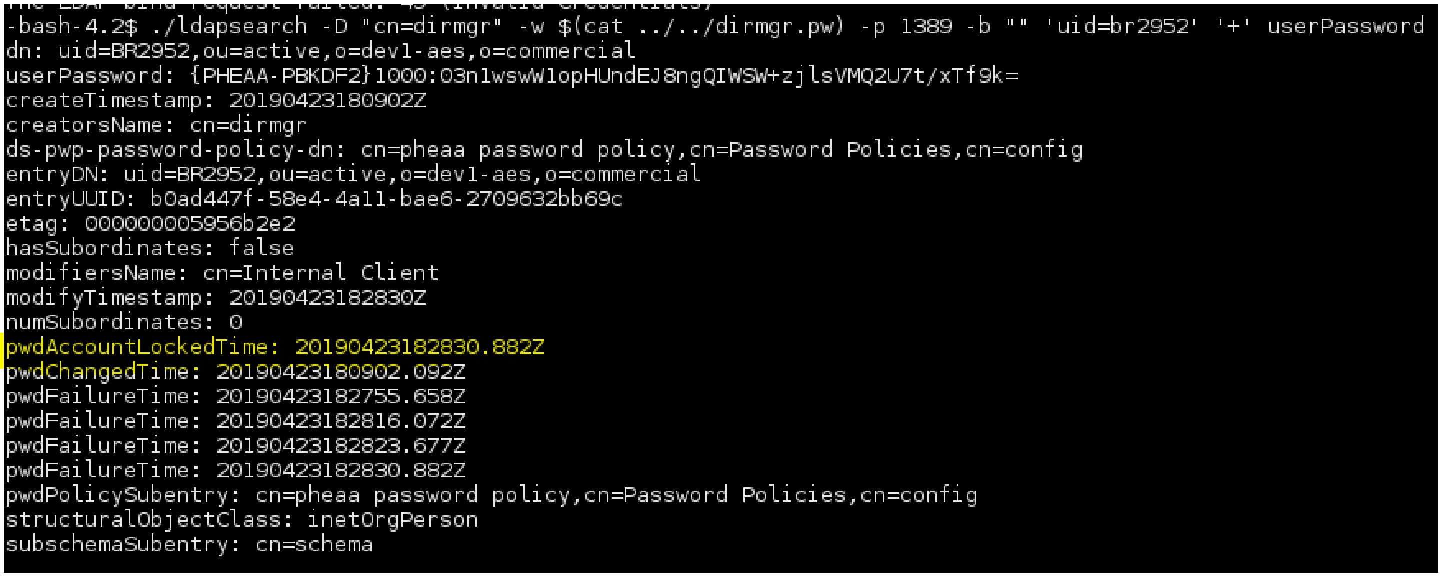
```
./ldapsearch --hostname $(hostname -f).pheaacloud.org \
 --port 1389 \
 --bindDN "uid=br2952,ou=active,o=dev1-aes,o=commercial" \
 --bindPassword incorrectpassword \
 --baseDN o=dev1-aes,o=commercial "uid=br2952" + userPassword
```

Verify 'pwdFailureTime' attribute in user profile after an un-successful bind



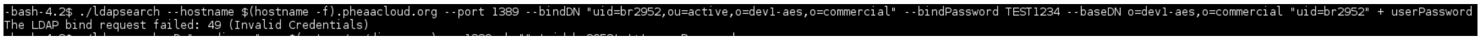
```
-bash-4.2$ ./ldapsearch -D "cn=dirmgr" -w $(cat ../../dirmgr.pw) -p 1389 -b "" 'uid=br2952' '+' userPassword
dn: uid=BR2952,ou=active,o=dev1-aes,o=commercial
userPassword: {PHEAA-PBKDF2}1000:03n1wswW1opHUndEJ8ngQIWSW+zjlsVMQ2U7t/xTf9k=
createTimestamp: 20190423180902Z
creatorsName: cn=dirmgr
ds-pwp-password-policy-dn: cn=pheaa password policy,cn=Password Policies,cn=config
entryDN: uid=BR2952,ou=active,o=dev1-aes,o=commercial
entryUUID: b0ad447f-58e4-4a11-bae6-2709632bb69c
etag: 00000000f6259b1c
hasSubordinates: false
modifiersName: cn=Internal Client
modifyTimestamp: 20190423182755Z
numSubordinates: 0
pwdChangedTime: 20190423180902.092Z
pwdFailureTime: 20190423182755.658Z
pwdPolicySubentry: cn=pheaa password policy,cn=Password Policies,cn=config
structuralObjectClass: inetOrgPerson
subschemaSubentry: cn=schema
```

Verify 'pwdAccountLockedTime' attribute after max (4) un-successful bind along-with 4 'pwdFailureTime' attributes



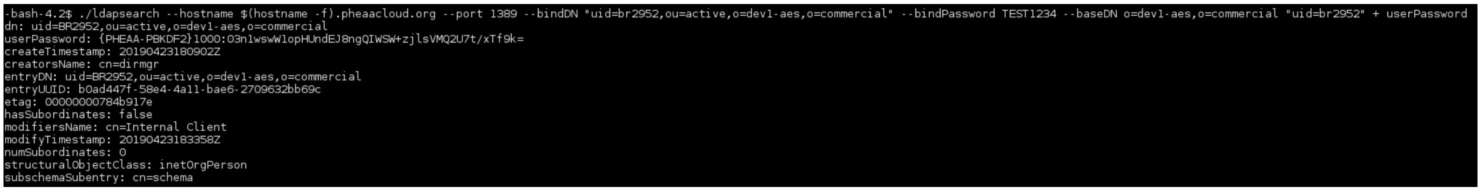
```
The LDAP bind request failed: 49 (Invalid Credentials)
-bash-4.2$ ./ldapsearch -D "cn=dirmgr" -w $(cat ../../dirmgr.pw) -p 1389 -b "" 'uid=br2952' '+' userPassword
dn: uid=BR2952,ou=active,o=dev1-aes,o=commercial
userPassword: {PHEAA-PBKDF2}1000:03n1wswW1opHUndEJ8ngQIWSW+zjlsVMQ2U7t/xTf9k=
createTimestamp: 20190423180902Z
creatorsName: cn=dirmgr
ds-pwp-password-policy-dn: cn=pheaa password policy,cn=Password Policies,cn=config
entryDN: uid=BR2952,ou=active,o=dev1-aes,o=commercial
entryUUID: b0ad447f-58e4-4a11-bae6-2709632bb69c
etag: 000000005956b2e2
hasSubordinates: false
modifiersName: cn=Internal Client
modifyTimestamp: 20190423182830Z
numSubordinates: 0
pwdAccountLockedTime: 20190423182830.882Z
pwdChangedTime: 20190423180902.092Z
pwdFailureTime: 20190423182755.658Z
pwdFailureTime: 20190423182816.072Z
pwdFailureTime: 20190423182823.677Z
pwdFailureTime: 20190423182830.882Z
pwdPolicySubentry: cn=pheaa password policy,cn=Password Policies,cn=config
structuralObjectClass: inetOrgPerson
subschemaSubentry: cn=schema
```

Login before lockout expiration with valid credentials - should fail login



```
-bash-4.2$ ./ldapsearch --hostname $(hostname -f).pheaacloud.org --port 1389 --bindDN "uid=br2952,ou=active,o=dev1-aes,o=commercial" --bindPassword TEST1234 --baseDN o=dev1-aes,o=commercial "uid=br2952" + userPassword
The LDAP bind request failed: 49 (Invalid Credentials)
```

Login after lockout expiration with valid credentials - successful login



```
-bash-4.2$ ./ldapsearch --hostname $(hostname -f).pheaacloud.org --port 1389 --bindDN "uid=br2952,ou=active,o=dev1-aes,o=commercial" --bindPassword TEST1234 --baseDN o=dev1-aes,o=commercial "uid=br2952" + userPassword
dn: uid=BR2952,ou=active,o=dev1-aes,o=commercial
userPassword: {PHEAA-PBKDF2}1000:03n1wswW1opHUndEJ8ngQIWSW+zjlsVMQ2U7t/xTf9k=
createTimestamp: 20190423180902Z
creatorsName: cn=dirmgr
entryDN: uid=BR2952,ou=active,o=dev1-aes,o=commercial
entryUUID: b0ad447f-58e4-4a11-bae6-2709632bb69c
etag: 00000000784b917e
hasSubordinates: false
modifiersName: cn=Internal Client
modifyTimestamp: 20190423183358Z
numSubordinates: 0
structuralObjectClass: inetOrgPerson
subschemaSubentry: cn=schema
```

References

- https://backstage.forgerock.com/docs/opendj/2.6/admin-guide/#assign-pwp-to-individual
- https://ludopoitou.com/2012/06/20/assigning-a-custom-password-policy-to-a-subtree/
- https://backstage.forgerock.com/knowledge/kb/article/a91487886

No labels

2 Comments

Suresh Chinta

@Jennifer Miller , did we arrive at any number for following:

- Maximum allowed password tries
- Timeout, if any, after max password tries ?
- Self-unlock (only applicable if there's a timeout)

Jennifer Miller

@Suresh Chinta - I've set a short meeting for tomorrow morning to come to a final decision on the default values. At this time, we are not providing a true 'unlock' feature, however, we are allowing users to access recovery options during the account restriction period, which would then remove the account restriction if successful.

CC - @Matthew Stoner