Externalize and encrypt grouper passwords morphString morph

⚠ Note, if you are not on Grouper 2.2.3+ or not on a fully patched 2.2.2, you need to make sure your sources.xml does not have any passwords in it. GRP-1227.

You should encrypt and externalize Grouper LDAP and database passwords especially in production. Grouper has a morphString utility that uses a system key to symmetrically encrypt/decrypt sensitive data.

If you have slashes in your passwords and are not externalizing them, set morphString.properties encrypt.disableExternalFileLookup=true

The goal is to improve password security:

1. config files should be able to be emailed around without having to cleanse them
2. config files (and warfiles) should not contain passwords so they can be stored in version control etc
3. only people who have permissions on the production box will need to know the password, not developers who send them the war to deploy
4. If someone finds a config file, they cannot see the password, and there is no documented way to unencrypt it

Setup externalized encrypted passwords in 2.5

```
grouperPassEncrypt $ wget https://repo1.maven.org/maven2/edu/internet2/middleware/grouper/grouperClient/2.5.XX
/grouperClient-2.5.XX.jar

... note, in v2.5.23- you need the morphString.base.properties in this dir, in v2.5.24+ you do not ...
... put your morphString.properties in this dir with your secret ...

grouperPassEncrypt $ echo 'encrypt.key = *********' > morphString.properties
grouperPassEncrypt $ java -cp .:grouperClient-2.5.23.jar edu.internet2.middleware.morphString.Encrypt
Type the string to encrypt (note: pasting might echo it back):
The encrypted string is: qN28V6C3Qt7ffqI4lSf/iQ==
grouperPassEncrypt $
```

you can script this in a command (with morphString.properties in dir)

```
java -cp .:grouperClient-2.5.46.jar edu.internet2.middleware.morphString.Encrypt dontMask <<< "somePass" | sed -
n '2p' | sed 's/The encrypted string is: //'
```

Setup externalized encrypted passwords POST 2.4.0 API patch #76

1. In morphString.properties, set the encrypt.key entry to a random alphanumeric string, or a pathname of a file containing the alphanumeric string, or a scriptlet (encrypt.key.elConfig instead)
2. In subject.properties, and grouper.hibernate.properties, encrypt the passwords with:

   Windows: (from grouper API dir)

   ```
   C:\mchyzer\isc\dev\grouper-qs-1.2.0\grouper>java -cp conf;build;lib/* edu.internet2.middleware.
   morphString.Encrypt
   Enter the location of morphString.properties: conf/morphString.properties
   Type the string to encrypt (note: pasting might echo it back):
   The encrypted string is: ede9aa3fe38e68d811107f886a941cc6
   ```

Unix:

```
/opt/grouper-qs-1.2.0/grouper>java -cp conf:build:lib/* edu.internet2.middleware.morphString.Encrypt
Enter the location of morphString.properties: conf/morphString.properties
Type the string to encrypt (note: pasting might echo it back):
The encrypted string is: ede9aa3fe38e68d811107f886a941cc6
```

Script

```
[tomcat@ed083ed08743 temp]$ ls
grouperClient-2.5.42.jar  morphString.properties
[tomcat@ed083ed08743 temp]$ java -cp .:grouperClient-2.5.42.jar edu.internet2.middleware.morphString.
Encrypt dontMask <<< "somePass" | sed -n '2p' | sed 's/The encrypted string is: //'
Ev3sDTJm0evgFaQsE69WHA==
[tomcat@ed083ed08743 temp]$
```

3. Put results in a file, and put the file path where the passwords were in sources.xml or grouper.hibernate.properties (absolute file path must contain a slash)

   Windows:

   ```
   hibernate.connection.password = c:/pass/myGrouper/mySource.pass
   ```

   Unix:

   ```
   hibernate.connection.password = /opt/pass/myGrouper/mySource.pass
   ```

   Note: an absolute path is required. The configuration will use the "/" directory delimiter to distinguish between an external file reference and a literal password string.

Setup externalized encrypted passwords PRE 2.4.0 API patch #76

1. In morphString.properties, set the encrypt.key entry to a random alphanumeric string, or a pathname of a file containing the alphanumeric string
2. In sources.xml, and grouper.hibernate.properties, encrypt the passwords with:

   Windows:

   ```
   C:\mchyzer\isc\dev\grouper-qs-1.2.0\grouper>java -jar lib\morphString.jar
   Enter the location of morphString.properties: conf/morphString.properties
   Type the string to encrypt (note: pasting might echo it back):
   The encrypted string is: ede9aa3fe38e68d811107f886a941cc6
   ```

   Unix:

   ```
   /opt/grouper-qs-1.2.0/grouper>java -jar lib/morphString.jar
   Enter the location of morphString.properties: conf/morphString.properties
   Type the string to encrypt (note: pasting might echo it back):
   The encrypted string is: ede9aa3fe38e68d811107f886a941cc6
   ```

3. Put results in a file, and put the file path where the passwords were in sources.xml or grouper.hibernate.properties (absolute file path must contain a slash)

   Windows:

   ```
   hibernate.connection.password = c:/pass/myGrouper/mySource.pass
   ```

   Unix:

   ```
   hibernate.connection.password = /opt/pass/myGrouper/mySource.pass
   ```

   Note: an absolute path is required. The configuration will use the "/" directory delimiter to distinguish between an external file reference and a literal password string.

Example

e.g. Here is my morphString.properties

Put a random alphanumeric string (Case sensitive) for the password encryption. e.g. fh43IRJ4Nf5
or put a filename where the random alphanumeric string is. e.g. c:/whatever/key.txt
encrypt.key = C:/mchyzer/isc/dev/grouper/grouperDecryptKey.txt
set this to true if you have slashes in your passwords and dont want to look in external files
encrypt.disableExternalFileLookup = false

In the file: C:/mchyzer/isc/dev/grouper/grouperDecryptKey.txt is a key like: fur43MD2kl

Then I take my db password from sources.xml and grouper.hibernate.properties, and I encrypt like this (note, two ways to do it, the default which masks the input [though kind of shady due to java], and one the doesnt mask in case masking has problems... note both show the same output):

C:\mchyzer\isc\dev\grouper-qs-1.2.0\grouper>java -jar lib\morphString.jar
Enter the location of morphString.properties: conf/morphString.properties
Type the string to encrypt (note: pasting might echo it back):
The encrypted string is: 2aac86f12aexxxxxx81144b5b1e4ba

C:\mchyzer\isc\dev\grouper-qs-1.2.0\grouper>java -jar lib\morphString.jar dontMask
Enter the location of morphString.properties: conf/morphString.properties
Type the string to encrypt (note: pasting might echo it back): test
The encrypted string is: 2aac86f12aexxxxxx81144b5b1e4ba

Then write that encrypting string to the password file, in my case:
C:/mchyzer/isc/dev/grouper/grouperLocalPass.txt

And in grouper.hibernate.properties and sources.xml, replace the password with that file location:

hibernate.connection.password = C:/mchyzer/isc/dev/grouper/grouperLocalPass.txt

<init-param>
<param-name>dbPwd</param-name>
<param-value>C:/mchyzer/isc/dev/grouper/grouperLocalPass.txt</param-value>
</init-param>

this requires morphString.jar

The ldap source adapter supports encrypted passwords as of version 2.1.0. (4 years later)

For example, ldap.properties may contain :

edu.vt.middleware.ldap.bindDn=cn=Manager,dc=example,dc=edu
edu.vt.middleware.ldap.bindCredential=/grouper.apiBinary/conf/ldap.pwd

Where ldap.pwd contains the encrypted password.

grouper.apiBinary> java -jar lib/grouper/morphString.jar
Enter the location of morphString.properties: conf/morphString.properties
Type the string to encrypt (note: pasting might echo it back):
The encrypted string is: l3hr1pI0A+Dd6HP/5BUCDw==

grouper.apiBinary> echo l3hr1pI0A+Dd6HP/5BUCDw== > ldap.pwd