

Metacat - Bug #3765

Backup configured passwords as encrypted values

01/22/2009 10:11 AM - Michael Daigle

Status:	New	Start date:	01/22/2009
Priority:	Normal	Due date:	
Assignee:	Michael Daigle	% Done:	0%
Category:	metacat	Estimated time:	0.00 hour
Target version:	Unspecified	Spent time:	0.00 hour
Bugzilla-Id:	3765		

Description

Currently, the user has to add the passwords for the db, skins and metacat ldap web every time they upgrade. This should use the EncryptionUtil class to save encrypted passwords in the backup files.

Note, the EncryptionUtil class has been implemented with triple-DES encryption, but has not been used or tested yet.

History

#1 - 01/22/2009 10:36 AM - Shaun Walbridge

Along these lines of reasoning, security practices dictate never storing the plaintext password at all. Perhaps once you've began using this class we can switch over to a salted hash model of passwords in Metacat, and then passwords can be embedded the same way in the backup as they are within Metacat.

A salted hash psuedo-code example:

```
password = 'foo'  
salt = random()  
hash_string = password + 'ajk890askjl' + salt  
encrypted_password = SHA1.hexdigest(hash_string)
```

Then the 'encrypted_password' and 'salt' values are stored, and can be backed up safely.

#2 - 03/27/2013 02:24 PM - Redmine Admin

Original Bugzilla ID was 3765