Metacat - Bug #6403

Command-line user management does not handle hashed passwords

01/31/2014 02:39 PM - ben leinfelder

Status:ClosedStart date:Priority:NormalDue date:Assignee:Jing Tao% Done:0%

Category:

Target version: 2.4.0 Spent time: 0.00 hour

Bugzilla-ld:

Description

From original ticket in the identity service redmine instance (https://projects.nceas.ucsb.edu/nceas/issues/862):

When i tried to add a user by running this command:

./authFileManager.sh useradd -h \$2a\$04\$csilPspPJdMx8zt7L9XKXeUxZjkPgKZd.o7TTPC0oJOFmT2kQ/E92 -dn uid=jing2,o=NCEAS,dc=ecoinformatics,dc=org

Estimated time:

0.00 hour

It showed the creation succeeded. However, the password filed is not

"\$2a\$04\$csilPspPJdMx8zt7L9XKXeUxZjkPgKZd.o7TTPC0oJOFmT2kQ/E92". So the loging in can't be successful.

The API - authFile.addUser works since the junit test can set the hashed password correctly.

This is a problem in the Metacat code base so I'm moving this here so we can more easily track the 2.4.0 release.

History

#1 - 01/31/2014 02:41 PM - ben leinfelder

- Description updated
- Assignee set to Jing Tao

#2 - 01/31/2014 02:42 PM - ben leinfelder

I dug around and found that the shell script decoded the bcrypt hash code. If the input (argument) is \$2a\$04\$csilPspPJdMx8zt7L9XKXeUxZjkPgKZd.o7TTPC0oJOFmT2kQ/E92, the shell script will change it to a-bash4.o7TTPC0oJOFmT2kQ/E92 (because the shell script doesn't like \$)?

I found the only way to escape the string is to add two single quotes around the hash code. But, double quotes doesn't work.

Here is the format of bcrypt hash:

\$2\$, \$2a\$ or \$2y\$ identifying the hashing algorithm and format.

A two digit value denoting the cost parameter, followed by \$.

A 53 characters long base-64-encoded value (they use the alphabet ., /, 0-9, A-Z, a-z that is different to the standard Base 64 Encoding alphabet) consisting of:

22 characters of salt (effectively only 128 bits of the 132 decoded bits)

31 characters of encrypted output (effectively only 184 bits of the 186 decoded bits)

#3 - 01/31/2014 02:42 PM - ben leinfelder

I confirmed that the script doesn't like the "\$" as a part of the argument. It will work if we remove the dollar sign part. However, we have to keep them.

#4 - 01/31/2014 02:43 PM - ben leinfelder

- Status changed from New to In Progress

#5 - 01/31/2014 02:54 PM - Jing Tao

I added note to let user know that the hashed password should be surround by single quotes.

#6 - 02/07/2014 03:52 PM - ben leinfelder

- Status changed from In Progress to Closed

03/13/2024 1/2

Tested this on my localhost and it works with single quotes.

03/13/2024 2/2