Hvrcrypt

Contents

Name

hvrcrypt - Encrypt passwords.

Synopsis

hvrcrypt *key* [*pwd*]

hvrcryptdb [-*options*] *hubdb*

Description

Command **hvrcrypt** can be used to interactively encrypt a password for a hub database when starting HVR on the command line. The second argument *pwd* is optional. If not specified **hvrcrypt** will prompt for it on the command line, not echoing the input. Using **hvrcrypt** is not needed for commands started with the HVR GUI.

Command **hvrcryptdb** will encrypt all unencrypted passwords in column **loc_remote_pwd** and **loc_db_us er** in catalog **hvr_location** of the hub database, using column **loc_name** as key. Passwords entered using the HVR GUI will already be encrypted.

The argument *hubdb* specifies the connection to the hub database. For more information about supported hub databases and the syntax for using this argument, see Calling HVR on the Command Line.

Passwords are encrypted using an encryption key. Each password is encrypted using a different encryption key, so that if two passwords are identical they will be encrypted to a different value. The encryption key used for hub database passwords is the name of the hub database, whereas the key used to encrypt the login passwords and database passwords for HVR location sis the HVR location name. This means that if an HVR location is renamed, the encrypted password becomes invalid.

Regardless of whether **hvrcrypt** is used, **Hvrgui** and **Hvrinit** will always encrypt passwords before saving them or sending them over the network. The passwords will only be decrypted during authorization checking on the remote location.

Options

This section describes the options available for command **hvrcrypt**.

Parameter	Description
-h*class*	Location *class* of the hub database. Valid values for *class* are **db2**, **db2i**, **ingres**, **mys ql**, **oracle**, **postgresql**, **sqlserver**, or **teradata**. For more information, see Calling HVR on the Command Line.

-u _user[/pwd]_	Connect to hub database using DBMS account _user_. For some databases (e.g. SQL Server) a password must also be supplied.

Example

To start the HVR Scheduler at reboot without the password being visible:

Unix & Linux

```
$ DBUSER=<span style="color:blue;"><i>hvrhubaw</i></span>
$ DBPWD=<span style="color:blue;"><i>mypassword</i></span>
$ DBPWD_CRYPT=`hvrcrypt $DBUSER $DBPWD`
$ hvrscheduler $DBUSER/$DBPWD_CRYPT
```

Use of Unix command **ps|grep hvrscheduler** will give the following:

```
hvr 21852 17136 0 15:50:59 pts/tf 00:03 hvrscheduler -i hvrhubaw/!\
{CLCIfCSy6Z7AUUya\}!
```

The above techniques also work for the hub database name supplied to **Hvrinit**.

Notes

Although the password encryption algorithm is reversible, there is deliberately no decryption command supplied.

Secure network encryption of remote HVR connections is provided using command **hvrsslgen** and action **LocationProperties /SslRemoteCertificate**.