Gather DBlink passwords

How to extract the password of database links

From Oracle Database 11gR2 version 11.2.0.4, DBMS_METADATA.GET_DDL does not show the password hash value needed to create database links any more.Instead, a bind variable is displayed.

```
SQL> select * from dba_db_links
OWNER          DB_LINK      USERNAME        HOST     CREATED
-------------- ------------ --------------- -------- -------
SYS            TEST_LINK    DBLINK_ACCOUNT  TNSALIAS 05-JUN-14

SQL> SELECT OWNER, DB_LINK, DBMS_METADATA.GET_DDL('DB_LINK',DB_LINK,OWNER) as DDL FROM
DBA_DB_LINKS
OWNER          DB_LINK      DDL
-------------- ------------ -------------------------------------------------------------
SYS            TEST_LINK    CREATE DATABASE LINK "TEST_LINK"
                            CONNECT TO "DBLINK_ACCOUNT" IDENTIFIED BY VALUES ':1'
                            USING 'TNSALIAS'
```

Nevertheless, the password ~~hash~~ value is stored in SYS.LINK$.

A complete list can be generated as:

```
SQL> select
 name,
 userid,
 utl_raw.cast_to_varchar2(dbms_crypto.decrypt((substr(passwordx,19)), 4353, (substr(passwordx,
3,16))))
from sys.link$
;
```

This DBMS_CRYPTO syntax only works with 50-byte-values. On 256-byte values, you get:

```
ORA-28817: PL/SQL-Funktion hat einen Fehler zurückgegeben.
ORA-06512: in "SYS.DBMS_CRYPTO_FFI", Zeile 67
ORA-06512: in "SYS.DBMS_CRYPTO", Zeile 44
ORA-06512: in Zeile 1
28817. 00000 -  "PL/SQL function returned an error."
*Cause:    A PL/SQL function returned an error unexpectedly.
*Action:   This is an internal error. Contact Oracle customer support.
```

And when trying to use values, you either get:

```
ORA-02153: invalid VALUES password string
```

for short values or

```
ORA-600 [kzdlk_zt2]
```

for long values.

As stated in MOS article Doc ID 1309705.1, the "BY VALUES" syntax is not supported any more and "reserved for internal Oracle use only".

Oracle Support writes on this:

> "This is expected and the correct output
> *Per bug 18461318 this was changed for security reasons.*
>
> Because of this, unfortunately we can't make it possible to output a complete db-link creation DDL command which will automatically re-create the database link with it's current password, as we used to do in the past.
>
> *From now on we recommend that only Data Pump should be used to move database links between databases while preserving their current password. Internally, Data Pump replaces the ":1" with the correct obfuscated database link password when it runs the DDL on the target system.*
> Or manually replace with password."

Update: Meanwhile, there is a possibility to reverse engineer database link passwords, which make the above obsolete in most cases.

See also:

- oracleforensics.com
- Loopback Blog Post (German)
- https://mahmoudhatem.wordpress.com/2016/12/08/reverse-engineering-db-link-password-decryption-in-plsql/
- https://www.doag.org/formes/servlet/DocNavi?action=getFile&did=9611800&key=
- https://github.com/hatem-mahmoud/scripts/blob/master/db_link_password_decrypt.sql