Oracle数据库透明加密实验

- xiabee

0x00 实验目的

- 了解`Oracle`

0x01 实验过程

创建表

```
create table t_clear
    ( id           varchar2(30) primary key,
      ssn          varchar2(11),
      address      varchar2(80),
      credit_card  varchar2(30)
    )
    tablespace in_the_clear;
  insert into t_clear (id, ssn, address, credit_card )
    values ( 'Look for me', '123-45-6789',
            '123 Main Street', '1234-5678-9876-5432' );
```

测试

```
 select a.member
     from v$logfile a, v$log b
    where a.group# = b.group#
     and b.status = 'CURRENT'
      and rownum = 1;
```

透明加密:

```
create table t_clear
    ( id           varchar2(30) primary key,
      ssn          varchar2(11),
      address      varchar2(80),
      credit_card  varchar2(30)  encrypt
    )
tablespace in_the_clear;
credit_card  varchar2(30)  encrypt ----缺省情况下采用192位密钥长度的AES算法。
```

Md5算法:

```
CREATE OR REPLACE FUNCTION md5_digest1(input_string IN VARCHAR2) RETURN
VARCHAR2
IS
        l_hash raw(32);
BEGIN
         l_hash := dbms_crypto.hash(
                    src=>input_string,
                    typ=>dbms_crypto.hash_md5);
        dbms_output.put_line('digest2=='||l_hash);
        RETURN l_hash;
END;
```

DES:

```
DECLARE
 l_credit_card_no VARCHAR2(19) := '1234-5678-9012-3456';
 l_ccn_raw RAW(128) := utl_raw.cast_to_raw(l_credit_card_no);
 l_key     RAW(128) := utl_raw.cast_to_raw('abcdefgh');
 l_encrypted_raw RAW(2048);
 l_decrypted_raw RAW(2048);
BEGIN
  dbms_output.put_line('Original : ' || l_credit_card_no);
  l_encrypted_raw := dbms_crypto.encrypt(l_ccn_raw,
  dbms_crypto.des_cbc_pkcs5, l_key);
  dbms_output.put_line('Encrypted : ' ||
  RAWTOHEX(utl_raw.cast_to_raw(l_encrypted_raw)));
  l_decrypted_raw := dbms_crypto.decrypt(src => l_encrypted_raw,
  typ => dbms_crypto.des_cbc_pkcs5, key => l_key);
  dbms_output.put_line('Decrypted : ' ||
  utl_raw.cast_to_varchar2(l_decrypted_raw));
END;
```