

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

```
1 create table t_clear
2   ( id          varchar2(30) primary key,
3     ssn          varchar2(11),
4     address      varchar2(80),
5     credit_card  varchar2(30)
6   )
7   tablespace in_the_clear;
8 insert into t_clear (id, ssn, address, credit_card )
9   values ( 'Look for me', '123-45-6789',
10          '123 Main Street', '1234-5678-9876-5432' );
```

测试

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

透明加密:

```
1 create table t_clear
2   ( id          varchar2(30) primary key,
3     ssn          varchar2(11),
4     address      varchar2(80),
5     credit_card  varchar2(30) encrypt
6   )
7   tablespace in_the_clear;
8 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:

```

1 CREATE OR REPLACE FUNCTION md5_digest1(input_string IN VARCHAR2) RETURN
  VARCHAR2
2 IS
3     l_hash raw(32);
4 BEGIN
5     l_hash := dbms_crypto.hash(
6         src=>input_string,
7         typ=>dbms_crypto.hash_md5);
8     dbms_output.put_line('digest2=='||l_hash);
9     RETURN l_hash;
10 END;

```

DES:

```

1 DECLARE
2     l_credit_card_no VARCHAR2(19) := '1234-5678-9012-3456';
3     l_ccn_raw RAW(128) := utl_raw.cast_to_raw(l_credit_card_no);
4     l_key RAW(128) := utl_raw.cast_to_raw('abcdefgh');
5     l_encrypted_raw RAW(2048);
6     l_decrypted_raw RAW(2048);
7 BEGIN
8     dbms_output.put_line('Original : ' || l_credit_card_no);
9     l_encrypted_raw := dbms_crypto.encrypt(l_ccn_raw,
10     dbms_crypto.des_cbc_pkcs5, l_key);
11     dbms_output.put_line('Encrypted : ' ||
12     RAWTOHEX(utl_raw.cast_to_raw(l_encrypted_raw)));
13     l_decrypted_raw := dbms_crypto.decrypt(src => l_encrypted_raw,
14     typ => dbms_crypto.des_cbc_pkcs5, key => l_key);
15     dbms_output.put_line('Decrypted : ' ||
16     utl_raw.cast_to_varchar2(l_decrypted_raw));
17 END;

```