OANA-ALEXANDRA COICA

510, SECURITY AND APPLIED LOGIC

Database Security

Project

(Password Vault Management System)

Contents

I. Introduction

a. Short presentation of the designed database model and its rules

The designed database model is corresponding to a collaborative password vault management system, where users can offer access permissions to their credentials or/and choose to keep them private from other users.

When thinking outside the database, at the application linked to it, it is important to mention that a user's private/ personal passwords (passwords that are not shared with anyone) are supposed to be encrypted with a key that's derived from their unhashed password to the vault, while their shared passwords are encrypted with a random key that is meant to be kept on a separate server.

The model will comprise of 4 main tables and a table for auditing vault access, which I will describe below, also enumerating their rules / constraints.

1. Platforms:

- platform_id = primary key (unique & not null); NUMBER;
- platform_name = not null; VARCHAR2;
- platform_description = VARCHAR2;
- access details = VARCHAR2;

2. Credentials:

- credential_id = primary key (unique & not null); NUMBER;
- platform_id = foreign key (from the Platforms table); not null; NUMBER;
- username = not null; VARCHAR2;
- password = encrypted value; VARCHAR2;
- created = not null; DATE;
- last_changed = not null; DATE;
- expiration_date = DATE;
- location_of_encryption_key = unique, VARCHAR2;

3. Rights Management:

- credential_id = part of the primary key; foreign key (from the Credentials table); not null; NUMBER;

- employee_id = part of the primary key; foreign key (from the Employees table); not null; NUMBER;

- rights = VARCHAR2; VIEW / EDIT / OWNER;

4. Employees:

- employee_id = primary key (unique, not null); NUMBER;

- email_address = unique, not null; %@%.%, VARCHAR2;

- vault_password = hashed value; VARCHAR2;

- first_name = not null; VARCHAR2;

- last_name = not null; VARCHAR2;

- job_title = not null; VARCHAR2;

- hiring_date = not null; DATE;

- end date = DATE;

- personal_numerical_code = not null, unique, 13 characters, must be valid; VARCHAR2;

5. Vault Access Audit

- log_id = primary key (unique & not null); NUMBER;

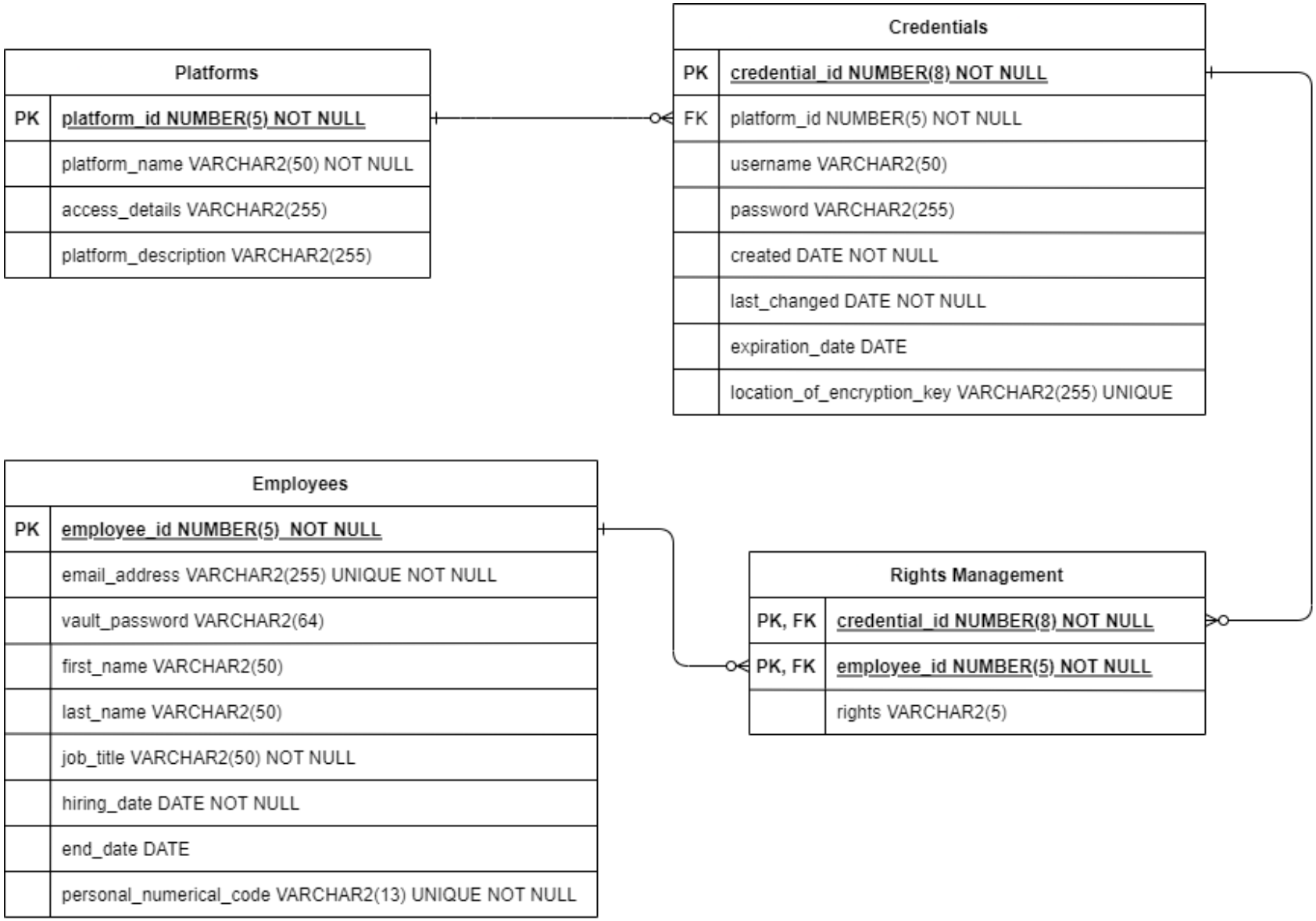
- employee_id = foreign key (from the Employees table); not null; NUMBER;

- credential_id = foreign key (from the Credentials table); not null; NUMBER;

- time = not null, DATETIME;

- action = not null, VARCHAR2;

b. Conceptual diagram



The audit table is going to look like this:

Vault Access Audit	
PK	log_id NUMBER(10) NOT NULL
FK	employee_id NUMBER(5) NOT NULL
FK	credential_id NUMBER(8) NOT NULL
	time DATETIME NOT NULL action VARCHAR2(255) NOT NULL

c. Relational schemes

platforms (#platform_id, platform_name, platform_description, access_details)

credentials (#credential_id, platform_id, username, password, created, last_changed, expiration_date, location_of_encryption_key);

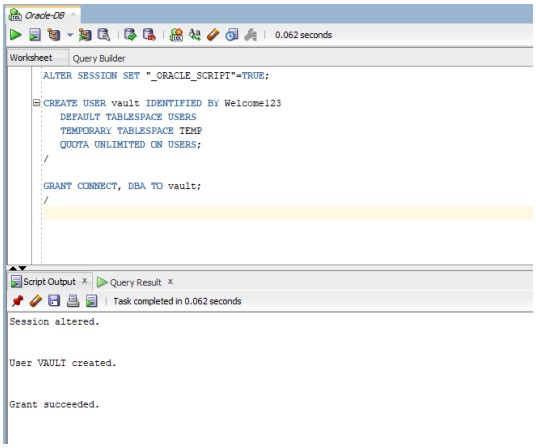
rights_management (#credential_id, #employee_id, rights);

employees (#employee_id, email_address, vault_password, first_name, last_name, job_title, hiring_date, end_date, personal_numerical_code);

vault_access_audit (#log_id, employee_id, credential_id, time, action);

d. Tables creation

The SQL code used to create the tables and insert data into them can be found in the *Coica_Oana_510-create_insert.txt* file. The user "vault" is going to be created and granted permissions - its schema is going to hold the tables.



Oracle-DB

Worksheet | Query Builder

```sql
CREATE TABLE platforms(
    platform_id NUMBER(5) NOT NULL,
    platform_name VARCHAR2(50) NOT NULL,
    access_details VARCHAR2(255),
    platform_description VARCHAR2(255),
    CONSTRAINT pk_platforms PRIMARY KEY(platform_id)
);

INSERT ALL
    INTO platforms VALUES (10001, 'Microsoft Office 365', 'https://www.office.com/', 'cloud-based productivity and collaboration applications')
    INTO platforms VALUES (10002, 'TeamPass', 'https://192.168.123.123/', 'our old collaborative password manager')
    INTO platforms VALUES (10003, 'Trend Micro Cloud App Security', 'https://admin-eu.tmcas.trendmicro.com/', 'security solution for cloud applications')
    INTO platforms VALUES (10004, 'Linkedin', 'https://linkedin.com/', 'social network focused on professional networking')
    INTO platforms VALUES (10005, 'Tufin', 'https://192.168.123.120/', 'firewall management solution')
    INTO platforms VALUES (10006, 'Trend Micro Deep Security', 'https://10.10.108.106/', 'security solution for servers')
    INTO platforms VALUES (10007, 'Symantec Data Loss Prevention', 'https://10.10.108.107/', 'DLP solution')
    INTO platforms VALUES (10008, 'Veritas Data Insight', 'https://10.10.108.109', 'data classification solution')
    INTO platforms VALUES (10009, 'Pluralsight', 'https://www.pluralsight.com', 'learning platform')
    INTO platforms VALUES (10010, 'Notion', 'https://www.notion.so/', 'collaborative note-taking application')
SELECT * FROM dual;
```

Script Output | Task completed in 0.028 seconds

```
Table PLATFORMS created.


10 rows inserted.
```

Oracle-DB | 0.211 seconds

Worksheet | Query Builder

```sql
CREATE TABLE employees(
    employee_id NUMBER(5) NOT NULL,
    email_address VARCHAR2(255) UNIQUE NOT NULL,
    vault_password VARCHAR2(64),
    first_name VARCHAR2(50),
    last_name VARCHAR2(50),
    job_title VARCHAR2(50) NOT NULL,
    hiring_date DATE NOT NULL,
    end_date DATE,
    personal_numerical_code VARCHAR2(13) UNIQUE NOT NULL,
    CONSTRAINT pk_employees PRIMARY KEY(employee_id)
);

INSERT ALL
    INTO employees VALUES (10000, 'mhuckerbe@thisisfake.com', 'password123',  'Mathian', 'Huckerbe', 'Network Engineer', TO_DATE('2021-03-16', 'YYYY-MM-DD'), NULL, '1950114246001')
    INTO employees VALUES (11111, 'djanczewski@thisisfake.com', 'password123',  'Doralin', 'Janczewski', 'Human Resources Assistant', TO_DATE('2021-01-19', 'YYYY-MM-DD'), NULL, '1921007134712')
    INTO employees VALUES (22222, 'rmulliner@thisisfake.com', 'password123',  'Ram', 'Mulliner', 'Infrastructure Architect', TO_DATE('2019-07-16', 'YYYY-MM-DD'), NULL, '1901112028549')
    INTO employees VALUES (33333, 'arobbe@thisisfake.com', 'password123',  'Ambrose', 'Robbe', 'Recruiting Specialist', TO_DATE('2017-05-13', 'YYYY-MM-DD'), NULL, '1890409527209')
    INTO employees VALUES (44444, 'gtoffanelli@thisisfake.com', 'password123',  'Georgetta', 'Toffanelli', 'Network Engineer', TO_DATE('2009-12-12', 'YYYY-MM-DD'), NULL, '2990311407435')
    INTO employees VALUES (55555, 'eyanuk@thisisfake.com', 'password123',  'Eveline', 'Yanuk', 'Human Resources Manager', TO_DATE('2014-02-27', 'YYYY-MM-DD'), NULL, '2880315304490')
    INTO employees VALUES (66666, 'carenaguise@thisisfake.com', 'password123',  'Carena', 'de Guise', 'Security Specialist', TO_DATE('2012-09-09', 'YYYY-MM-DD'), NULL, '2981010411887')
    INTO employees VALUES (77777, 'edanskinela@thisisfake.com', 'password123',  'Evelina', 'Danskine', 'Information Security Manager', TO_DATE('2017-07-03', 'YYYY-MM-DD'), NULL, '2910822053015')
    INTO employees VALUES (88888, 'atown@thisisfake.com', 'password123',  'Alec', 'Towner', 'System Administrator', TO_DATE('2011-03-05', 'YYYY-MM-DD'), NULL, '1900725150301')
    INTO employees VALUES (99999, 'elytyt@thisisfake.com', 'password123',  'Elyssa', 'Tyt', 'Internal Auditor', TO_DATE('2019-04-23', 'YYYY-MM-DD'), NULL, '2990920449782')
SELECT * FROM dual;
```

Script Output | Task completed in 0.211 seconds

```
Table EMPLOYEES created.


10 rows inserted.
```

```oracle-db
CREATE TABLE credentials(
    credential_id NUMBER(8) NOT NULL,
    platform_id NUMBER(5) NOT NULL,
    username VARCHAR2(50),
    password VARCHAR2(255),
    created DATE NOT NULL,
    last_changed DATE NOT NULL,
    expiration_date DATE,
    location_of_encryption_key VARCHAR2(255) UNIQUE,
    CONSTRAINT pk_credentials PRIMARY KEY(credential_id),
    CONSTRAINT fk_platforms FOREIGN KEY(platform_id)
        REFERENCES platforms(platform_id)
);

INSERT ALL
    INTO credentials VALUES (100, 10001, 'eyanuk@thisisfake.com', 'MicrosoftPassword', TO_DATE('2022-01-01', 'YYYY-MM-DD'), TO_DATE('2022-01-01', 'YYYY-MM-DD'), NULL, NULL)
    INTO credentials VALUES (101, 10002, 'eyanuk@thisisfake.com', 'TeamPassPassword', TO_DATE('2022-01-01', 'YYYY-MM-DD'), TO_DATE('2022-01-01', 'YYYY-MM-DD'), NULL, NULL)
    INTO credentials VALUES (102, 10009, 'eyanuk@thisisfake.com', 'PluralsightPassword', TO_DATE('2022-01-01', 'YYYY-MM-DD'), TO_DATE('2022-01-01', 'YYYY-MM-DD'), NULL, NULL)
    INTO credentials VALUES (103, 10003, 'MasterAdmin', 'thisisfake123', TO_DATE('2022-01-01', 'YYYY-MM-DD'), TO_DATE('2022-01-01', 'YYYY-MM-DD'), NULL, NULL)
    INTO credentials VALUES (104, 10006, 'MasterAdmin', 'thisisfake123', TO_DATE('2022-01-01', 'YYYY-MM-DD'), TO_DATE('2022-01-01', 'YYYY-MM-DD'), NULL, NULL)
    INTO credentials VALUES (105, 10007, 'Administrator', 'thisisfake123', TO_DATE('2022-01-01', 'YYYY-MM-DD'), TO_DATE('2022-01-01', 'YYYY-MM-DD'), NULL, NULL)
    INTO credentials VALUES (106, 10005, 'admin', 'tufin123', TO_DATE('2022-01-01', 'YYYY-MM-DD'), TO_DATE('2022-01-01', 'YYYY-MM-DD'), NULL, NULL)
    INTO credentials VALUES (107, 10004, 'hr@thisisfake.com', 'LinkedinPassword', TO_DATE('2022-01-01', 'YYYY-MM-DD'), TO_DATE('2022-01-01', 'YYYY-MM-DD'), NULL, NULL)
SELECT * FROM dual;
```

```
Table CREDENTIALS created.

8 rows inserted.
```

```oracle-db
CREATE TABLE rights_management(
    credential_id NUMBER(8) NOT NULL,
    employee_id NUMBER(5) NOT NULL,
    rights VARCHAR2(5),
    CONSTRAINT pk_rights PRIMARY KEY(credential_id, employee_id),
    CONSTRAINT fk_credentials FOREIGN KEY(credential_id)
        REFERENCES credentials(credential_id),
    CONSTRAINT fk_employees FOREIGN KEY(employee_id)
        REFERENCES employees(employee_id),
    CONSTRAINT chk_rights CHECK (rights IN ('VIEW', 'EDIT', 'OWNER'))
);

INSERT ALL
    INTO rights_management VALUES (100, 55555, 'OWNER')
    INTO rights_management VALUES (101, 55555, 'OWNER')
    INTO rights_management VALUES (102, 55555, 'OWNER')
    INTO rights_management VALUES (103, 77777, 'OWNER')
    INTO rights_management VALUES (103, 66666, 'EDIT')
    INTO rights_management VALUES (103, 22222, 'VIEW')
    INTO rights_management VALUES (103, 88888, 'VIEW')
    INTO rights_management VALUES (104, 77777, 'OWNER')
    INTO rights_management VALUES (104, 66666, 'VIEW')
    INTO rights_management VALUES (104, 22222, 'VIEW')
    INTO rights_management VALUES (104, 88888, 'VIEW')
    INTO rights_management VALUES (105, 77777, 'OWNER')
    INTO rights_management VALUES (105, 66666, 'VIEW')
    INTO rights_management VALUES (105, 22222, 'VIEW')
    INTO rights_management VALUES (106, 22222, 'OWNER')
    INTO rights_management VALUES (106, 10000, 'VIEW')
    INTO rights_management VALUES (106, 44444, 'VIEW')
    INTO rights_management VALUES (106, 66666, 'VIEW')
    INTO rights_management VALUES (107, 55555, 'OWNER')
    INTO rights_management VALUES (107, 33333, 'EDIT')
    INTO rights_management VALUES (107, 11111, 'VIEW')
SELECT * FROM dual;
```

```
Table RIGHTS_MANAGEMENT created.

21 rows inserted.
```

```oracle-db
CREATE SEQUENCE log_seq
    START WITH 10
    INCREMENT BY 1
    NOCACHE
    NOCYCLE;

CREATE TABLE vault_access_audit(
    log_id NUMBER(10) NOT NULL,
    employee_id NUMBER(5) NOT NULL,
    credential_id NUMBER(8) NOT NULL,
    time TIMESTAMP NOT NULL,
    action VARCHAR2(255) NOT NULL,
    CONSTRAINT pk_logs PRIMARY KEY(log_id),
    CONSTRAINT fk_vault_employees FOREIGN KEY(employee_id)
        REFERENCES employees(employee_id),
    CONSTRAINT fk_vault_credentials FOREIGN KEY(credential_id)
        REFERENCES credentials(credential_id)
);
```

```
Sequence LOG_SEQ created.

Table VAULT_ACCESS_AUDIT created.
```

e. Presentation of the security rules applied to the model

Credentials(username, password, created, last_changed, expiration_date, location_of_encryption_key) = secret for the users with no rights to those credentials; => content-based constraint

Employees(vault_password) = secret for everyone except the admin; => simple constraint

Employees(personal_numerical_code) = secret for everyone except HR; => content-based constraint

Vault_access_audit = secret for everyone except audit and admin; => content-based constraint

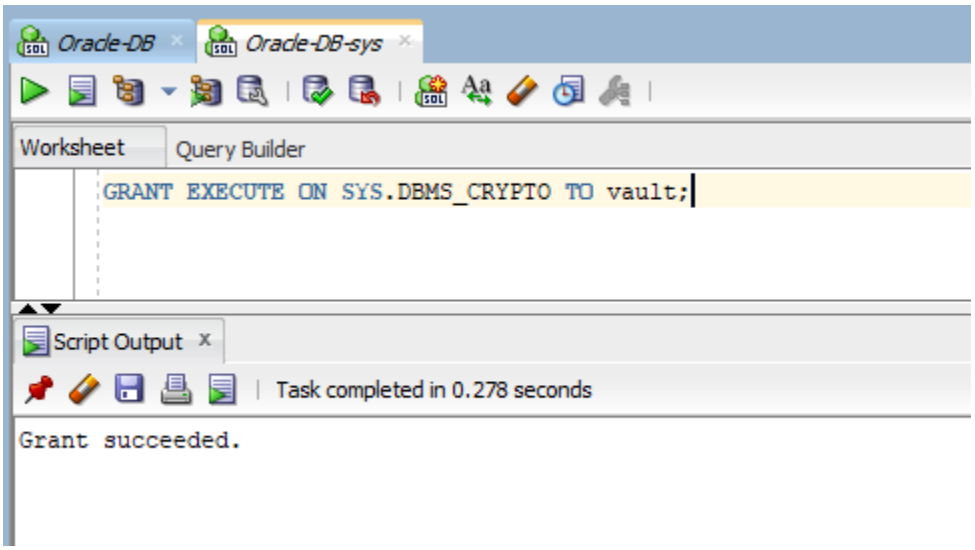
II. Data Encryption

As previously mentioned, the private credentials are going to be encrypted (using the AES algorithm) with a key that's derived from their owner's unhashed password to the vault, while their shared passwords are going to be encrypted (still using the AES algorithm) with a random key that is meant to be kept on a separate server - hence the location_of_encryption_key field in the Credentials table -, but for simplicity's sake, the encryption key it's going to be extractable from the location link itself (although it isn't secure to do so and the database isn't meant to ever be in production environments with this configuration!).

After encrypting the data with the established keys, vault_password is hashed using SHA-256 (without salt & pepper, also for simplicity).

The PL/SQL code used to encrypt the data can be found in the *Coica_Oana_510-encryption.txt* file.

To be able to use the DBMS_CRYPTO, the sys account has to be used to grant execute permissions to the package for the vault user.



Oracle-DB

Worksheet | Query Builder

```
UPDATE credentials
    SET location_of_encryption_key =
        CASE credential_id
            WHEN 103 THEN 'https://192.168.10.10/TUnJuzfycy.txt'
            WHEN 104 THEN 'https://192.168.10.10/keNMJxU62l.txt'
            WHEN 105 THEN 'https://192.168.10.10/W8iBlMkXod.txt'
            WHEN 106 THEN 'https://192.168.10.10/nxf2HN1rlC.txt'
            WHEN 107 THEN 'https://192.168.10.10/SWVrUM5GMK.txt'
        END
    WHERE credential_id >=103 AND credential_id <=107;
```

Script Output | Task completed in 0.135 seconds

```
5 rows updated.
```

Oracle-DB

Worksheet | Query Builder

```
-- function that computes the key that's going to be used for encryption
CREATE OR REPLACE FUNCTION get_encryption_key
    (id_of_the_credential_i_want_to_encrypt credentials.credential_id%TYPE)
RETURN VARCHAR2
AS
    encryption_key VARCHAR2(255);
    how_many_people_have_access NUMBER(5);
BEGIN
    SELECT COUNT(credential_id)
    INTO how_many_people_have_access
    FROM rights_management
    WHERE credential_id = id_of_the_credential_i_want_to_encrypt;

    IF how_many_people_have_access > 1
        THEN
            SELECT SUBSTR(location_of_encryption_key, LENGTH(location_of_encryption_key) - 13, 10)
            INTO encryption_key
            FROM credentials
            WHERE credential_id = id_of_the_credential_i_want_to_encrypt;
        ELSE
            SELECT vault_password
            INTO encryption_key
            FROM employees JOIN rights_management USING (employee_id)
            WHERE credential_id = id_of_the_credential_i_want_to_encrypt AND rights = 'OWNER';
    END IF;
    RETURN encryption_key;
END;
/
BEGIN -- testing
  DBMS_OUTPUT.PUT_LINE(get_encryption_key(102)); -- encryption key for 102 should be password123, because that's its owner unhashed vault password
  DBMS_OUTPUT.PUT_LINE(get_encryption_key(103)); -- encryption key for 103 should be TUnJuzfycy, because that's the key indicated by location_of_encryption_key
END;
/
```

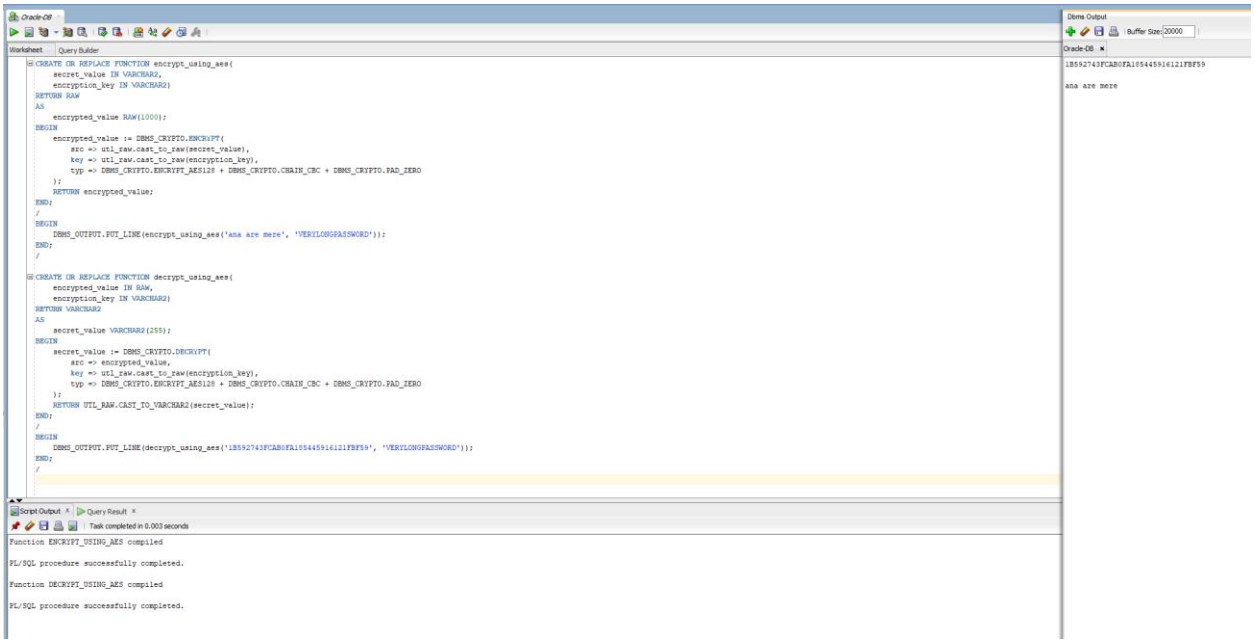
Dbms Output | Buffer Size: 20000

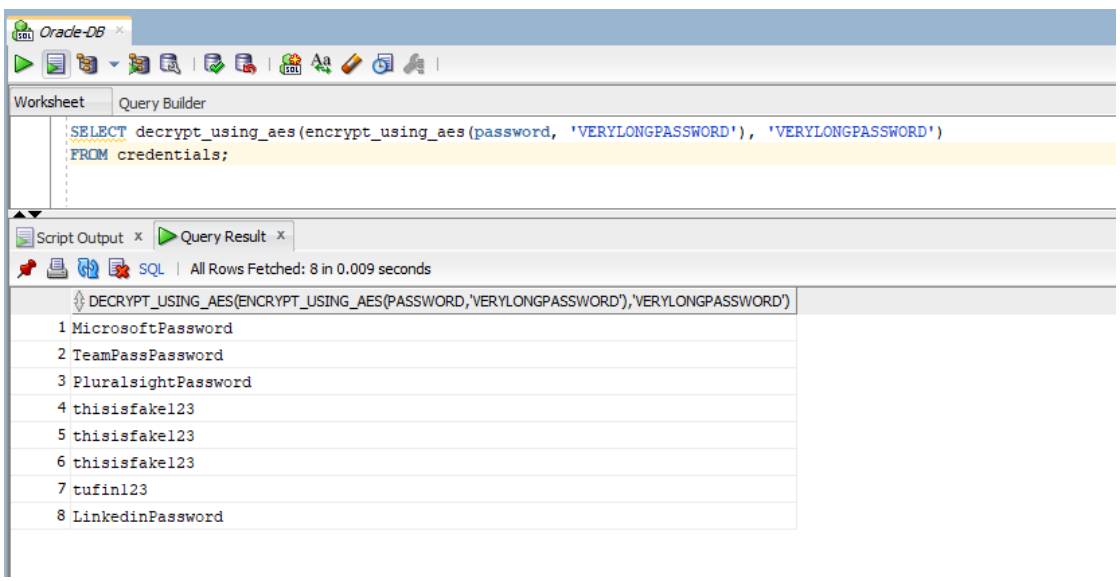
Oracle-DB

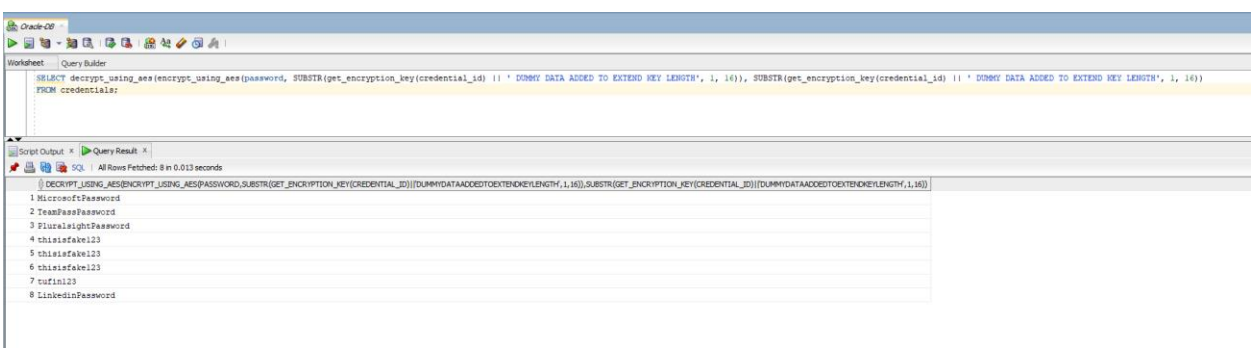
```
password123
TUnJuzfycy
```

Script Output | Query Result | Task completed in 0.005 seconds

```
Function GET_ENCRYPTION_KEY compiled

PL/SQL procedure successfully completed.
```


Oracle-DB
Worksheet
Query Builder
CREATE OR REPLACE FUNCTION encrypt_using_aes(
secret_value IN VARCHAR2,
encryption_key IN VARCHAR2)
RETURN RAW
AS
encrypted_value RAW(1000);
BEGIN
encrypted_value := DBMS_CRYPTO.ENCRYPT(
src => utl_raw.cast_to_raw(secret_value),
key => utl_raw.cast_to_raw(encryption_key),
typ => DBMS_CRYPTO.ENCRYPT_AES128 + DBMS_CRYPTO.CHAIN_CBC + DBMS_CRYPTO.PAD_ZERO
);
RETURN encrypted_value;
END;
/
BEGIN
DBMS_OUTPUT.PUT_LINE(encrypt_using_aes('ana are mere', 'VERYLONGPASSWORD'));
END;
/
CREATE OR REPLACE FUNCTION decrypt_using_aes(
encrypted_value IN RAW,
encryption_key IN VARCHAR2)
RETURN VARCHAR2
AS
secret_value VARCHAR2(255);
BEGIN
secret_value := DBMS_CRYPTO.DECRYPT(
src => encrypted_value,
key => utl_raw.cast_to_raw(encryption_key),
typ => DBMS_CRYPTO.ENCRYPT_AES128 + DBMS_CRYPTO.CHAIN_CBC + DBMS_CRYPTO.PAD_ZERO
);
RETURN UTL_RAW.CAST_TO_VARCHAR2(secret_value);
END;
/
BEGIN
DBMS_OUTPUT.PUT_LINE(decrypt_using_aes('1B592743FCAB0FA185445916121FBF59', 'VERYLONGPASSWORD'));
END;
/
Dbms Output
Buffer Size: 20000
Oracle-DB
1B592743FCAB0FA185445916121FBF59
ana are mere
Script Output
Query Result
Task completed in 0.003 seconds
Function ENCRYPT_USING_AES compiled
PL/SQL procedure successfully completed.
Function DECRYPT_USING_AES compiled
PL/SQL procedure successfully completed.


Oracle-DB
Worksheet
Query Builder
SELECT decrypt_using_aes(encrypt_using_aes(password, 'VERYLONGPASSWORD'), 'VERYLONGPASSWORD')
FROM credentials;
Script Output
Query Result
SQL
All Rows Fetched: 8 in 0.009 seconds
DECRYPT_USING_AES(ENCRYPT_USING_AES(PASSWORD,'VERYLONGPASSWORD'),'VERYLONGPASSWORD')
1 MicrosoftPassword
2 TeamPassPassword
3 PluralsightPassword
4 thisisfake123
5 thisisfake123
6 thisisfake123
7 tufin123
8 LinkedinPassword


Oracle-DB
Worksheet
Query Builder
SELECT decrypt_using_aes(encrypt_using_aes(password, SUBSTR(get_encryption_key(credential_id) || ' DUMMY DATA ADDED TO EXTEND KEY LENGTH', 1, 16)), SUBSTR(get_encryption_key(credential_id) || ' DUMMY DATA ADDED TO EXTEND KEY LENGTH', 1, 16))
FROM credentials;
Script Output
Query Result
SQL
All Rows Fetched: 8 in 0.013 seconds
DECRYPT_USING_AES(ENCRYPT_USING_AES(PASSWORD,SUBSTR(GET_ENCRYPTION_KEY(CREDENTIAL_ID)||'DUMMYDATAADDEDTOEXTENDKEYLENGTH',1,16)),SUBSTR(GET_ENCRYPTION_KEY(CREDENTIAL_ID)||'DUMMYDATAADDEDTOEXTENDKEYLENGTH',1,16))
1 MicrosoftPassword
2 TeamPassPassword
3 PluralsightPassword
4 thisisfake123
5 thisisfake123
6 thisisfake123
7 tufin123
8 LinkedinPassword

Oracle-DB

Worksheet | Query Builder

```
UPDATE credentials
    SET password = encrypt_using_aes(password, SUBSTR(get_encryption_key(credential_id) || ' DUMMY DATA ADDED TO EXTEND KEY LENGTH', 1, 16));
```

Script Output | Query Result

Task completed in 0.21 seconds

```
8 rows updated.
```

Oracle-DB

Worksheet | Query Builder

```
SELECT * FROM credentials;
```

Script Output | Query Result

SQL | All Rows Fetched: 8 in 0.002 seconds

	CREDENTIAL_ID	PLATFORM_ID	USERNAME	PASSWORD	CREATED	LAST_CHANGED	EXPIRATION_DATE	LOCATION_OF_ENCRYPTION_KEY
1	100	10001	eyanuk@thisisfake.com	7E26A5AE2F3278709366C71945D1600414319232C87F7CA1D667599E7BC4F303	01-JAN-22	01-JAN-22	(null)	(null)
2	101	10002	eyanuk@thisisfake.com	ED5615BCD603641A14097B326790EA74	01-JAN-22	01-JAN-22	(null)	(null)
3	102	10009	eyanuk@thisisfake.com	ADEB45951F7A99D50DF018DB87026E3C58BC0E29114A1734AAC5F2E3076A654C	01-JAN-22	01-JAN-22	(null)	(null)
4	103	10003	MasterAdmin	2E72122D1586DBA9382B9440248B0D1E	01-JAN-22	01-JAN-22	(null)	https://192.168.10.10/TUnJuzfycy.txt
5	104	10006	MasterAdmin	ECFD38DCCE984A6FCE0B016AC41BCDA3	01-JAN-22	01-JAN-22	(null)	https://192.168.10.10/keNMJxU621.txt
6	105	10007	Administrator	B6DF45ACB78DB008A48D643934439AB4	01-JAN-22	01-JAN-22	(null)	https://192.168.10.10/W8iBlMkXod.txt
7	106	10005	admin	3E4A7EC9412DD2959D6CA8318FDFB8E8	01-JAN-22	01-JAN-22	(null)	https://192.168.10.10/nxf2HN1r1C.txt
8	107	10004	hr@thisisfake.com	71B7A97B2334B9DE109A0C272E537A95	01-JAN-22	01-JAN-22	(null)	https://192.168.10.10/SWVrUM5GMK.txt

Oracle-DB

Worksheet | Query Builder

```
CREATE OR REPLACE FUNCTION hash_using_sha256(
    secret_value IN VARCHAR2
)
RETURN RAW
AS
    hashed_value RAW(32);
BEGIN
    hashed_value := DBMS_CRYPTO.HASH(utl_i18n.string_to_raw(secret_value, 'AL32UTF8'), DBMS_CRYPTO.HASH_SH256);
    RETURN hashed_value;
END;
/
BEGIN
    DBMS_OUTPUT.PUT_LINE(hash_using_sha256('ana are mere'));
END;
/
```

Script Output | Query Result

Task completed in 0.002 seconds

```
Function HASH_USING_SHA256 compiled

PL/SQL procedure successfully completed.
```

Dbms Output

Buffer Size: 20000

Oracle-DB

```
A3B5AC0C302D9CB2A0AE1EFBFF61C609953D63466D6AC62609DD030448A83607
```

Oracle-DB

Worksheet | Query Builder

```
SELECT vault_password, hash_using_sha256(vault_password)
FROM employees;
```

Script Output | Query Result

SQL | All Rows Fetched: 10 in 0.007 seconds

	VAULT_PASSWORD	HASH_USING_SHA256(VAULT_PASSWORD)
1	password123	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F
2	password123	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F
3	password123	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F
4	password123	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F
5	password123	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F
6	password123	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F
7	password123	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F
8	password123	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F
9	password123	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F
10	password123	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F

Oracle-DB

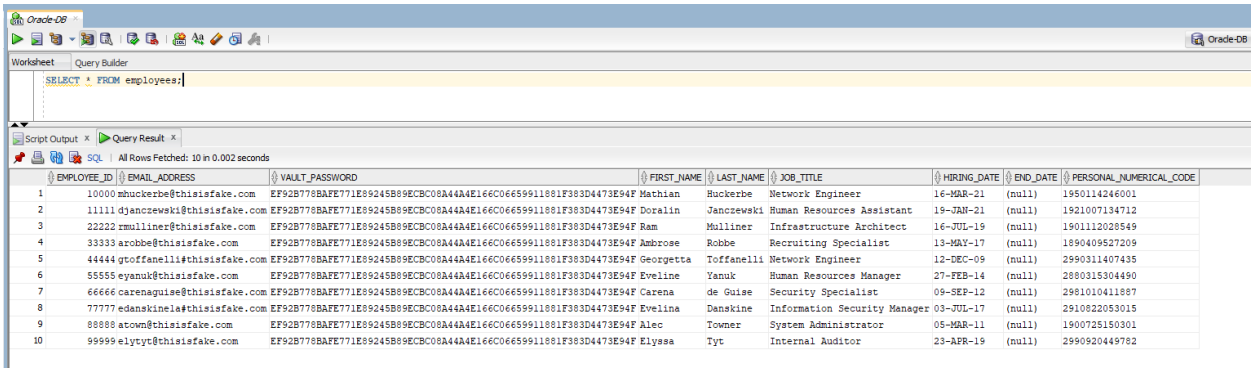
Worksheet | Query Builder

```
UPDATE employees
    SET vault_password = hash_using_sha256(vault_password);
```

Script Output | Query Result

Task completed in 0.007 seconds

```
10 rows updated.
```



```
SELECT * FROM employees;
```

Script Output | Query Result

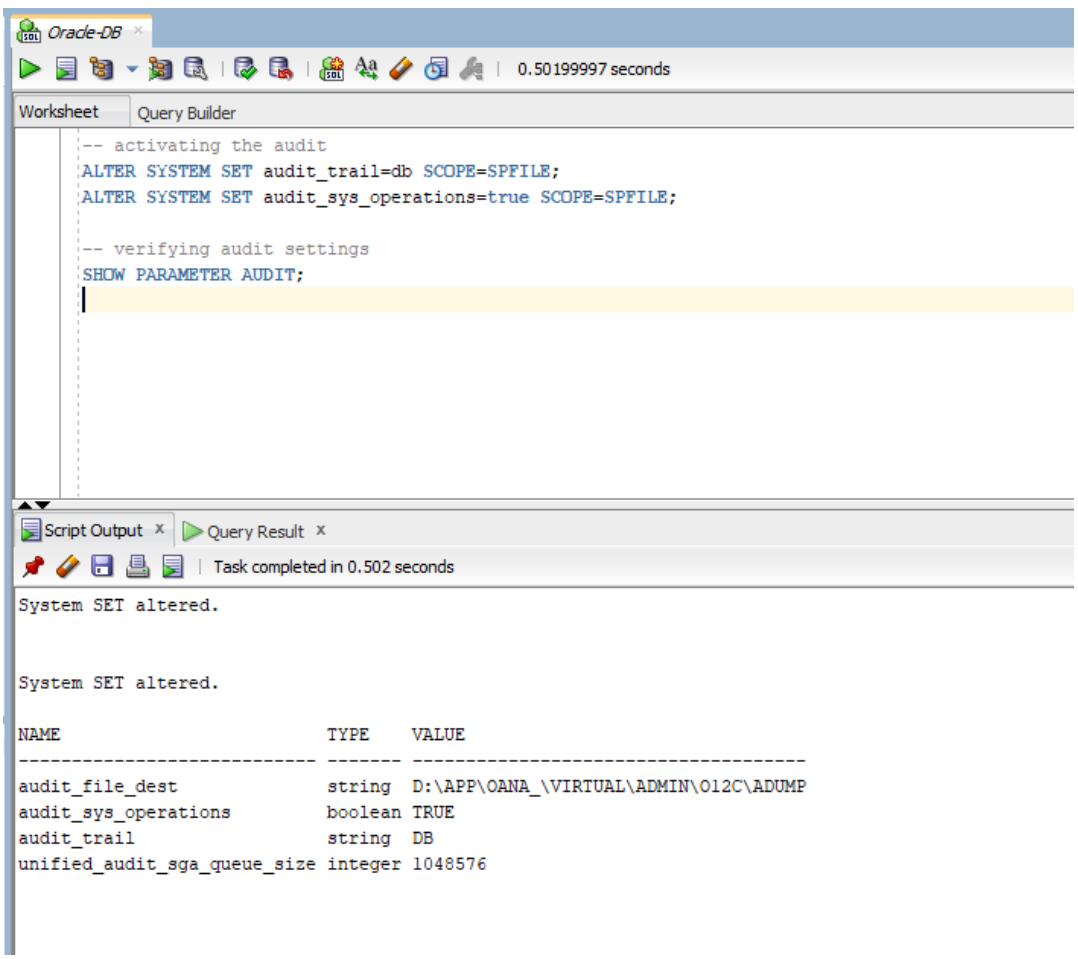
SQL | All Rows Fetched: 10 in 0.002 seconds

	EMPLOYEE_ID	EMAIL_ADDRESS	VAULT_PASSWORD	FIRST_NAME	LAST_NAME	JOB_TITLE	HIRING_DATE	END_DATE	PERSONAL_NUMERICAL_CODE
1	10000	mhuckerbe@thisisfake.com	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Mathian	Huckerbe	Network Engineer	16-MAR-21	(null)	1950114246001
2	11111	djanczewski@thisisfake.com	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Doralin	Janczewski	Human Resources Assistant	19-JAN-21	(null)	1921007134712
3	22222	rmulliner@thisisfake.com	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Ram	Mulliner	Infrastructure Architect	16-JUL-19	(null)	1901112028549
4	33333	arobbe@thisisfake.com	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Ambrose	Robbe	Recruiting Specialist	13-MAY-17	(null)	1890409527209
5	44444	gtoffanelli#thisisfake.com	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Georgetta	Toffanelli	Network Engineer	12-DEC-09	(null)	2990311407435
6	55555	eyanuk@thisisfake.com	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Eveline	Yanuk	Human Resources Manager	27-FEB-14	(null)	2880315304490
7	66666	carenaguise@thisisfake.com	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Carena	de Guise	Security Specialist	09-SEP-12	(null)	2981010411887
8	77777	edanskinela#thisisfake.com	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Evelina	Danskine	Information Security Manager	03-JUL-17	(null)	2910822053015
9	88888	atown@thisisfake.com	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Alec	Towner	System Administrator	05-MAR-11	(null)	1900725150301
10	99999	elytyt@thisisfake.com	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Elyssa	Tyt	Internal Auditor	23-APR-19	(null)	2990920449782

III. Database Activity Audit

The PL/SQL code used to audit the database activity can be found in the *Coica_Oana_510-audit.txt* file.

a. Standard audit



```
-- activating the audit
ALTER SYSTEM SET audit_trail=db SCOPE=SPFILE;
ALTER SYSTEM SET audit_sys_operations=true SCOPE=SPFILE;

-- verifying audit settings
SHOW PARAMETER AUDIT;
```

Script Output | Query Result

Task completed in 0.502 seconds

```
System SET altered.


System SET altered.

NAME                         TYPE    VALUE
---------------------------- ------- ------------------------------------
audit_file_dest              string  D:\APP\OANA_\VIRTUAL\ADMIN\O12C\ADUMP
audit_sys_operations         boolean TRUE
audit_trail                  string  DB
unified_audit_sga_queue_size integer 1048576
```

After modifying the settings, the database has to be restarted.

Command Prompt

```
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\oana_>net stop OracleServiceo12c
The OracleServiceO12C service is stopping..................
The OracleServiceO12C service was stopped successfully.


C:\Users\oana_>net start OracleServiceo12c
The OracleServiceO12C service is starting.....................................................
The OracleServiceO12C service was started successfully.
```

Oracle-DB

0.086 seconds

Worksheet | Query Builder

```
-- activating standard audit for schema objects (rights_management)
AUDIT SELECT, INSERT, UPDATE, DELETE
ON rights_management
BY ACCESS WHENEVER NOT SUCCESSFUL;

-- triggering an action that should be audited
INSERT INTO rights_management
VALUES (9999999999, 999999999999, 'test');
```

Script Output | Query Result

Task completed in 0.086 seconds

```
Audit succeeded.


Error starting at line : 7 in command -
INSERT INTO rights_management
VALUES (9999999999, 999999999999, 'test')
Error report -
SQL Error: ORA-01438: value larger than specified precision allowed for this column
01438. 00000 -  "value larger than specified precision allowed for this column"
*Cause:    When inserting or updating records, a numeric value was entered
           that exceeded the precision defined for the column.
*Action:   Enter a value that complies with the numeric column's precision,
           or use the MODIFY option with the ALTER TABLE command to expand
           the precision.
```

Oracle-DB

Worksheet | Query Builder

```
-- verifying the audit
SELECT * FROM SYS.AUD$
WHERE obj$name = 'RIGHTS_MANAGEMENT';
```

Script Output | Query Result

SQL | All Rows Fetched: 1 in 0.008 seconds

	SESSIONID	ENTRYID	STATEMENT	TIMESTAMP#	USERID	USERHOST	TERMINAL	ACTION#	RETURNCODE	OBJ$CREATOR	OBJ$NAME	AUTH$PRIVILEGES	AUTH$GRANTEE	NEW$OWNER	NEW$NAME	SES$ACTIONS	SES$TID	LOGOFF$LF
1	60522	2	1039	(null)	VAULT	DESKTOP-F7C58AV	unknown	2	1438	VAULT	RIGHTS_MANAGEMENT	(null)	(null)	(null)	(null)	(null)	(null)	(n

b. Audit triggers

The audit trigger is going to add entries into the vault_access_audit table regarding the actions towards the credentials table.

```oracle-db
CREATE OR REPLACE FUNCTION is_number (given_string IN VARCHAR2)
    RETURN INTEGER
IS
    given_number NUMBER;
BEGIN
    given_number := TO_NUMBER(given_string);
    RETURN 1;
EXCEPTION
    WHEN VALUE_ERROR THEN
        RETURN 0;
END is_number;
/

CREATE OR REPLACE TRIGGER credentials_audit_trigger
    AFTER INSERT OR DELETE OR UPDATE ON credentials
    FOR EACH ROW
DECLARE
    user_that_wants_modification VARCHAR2(100);
    is_it_user INTEGER;
BEGIN
    -- detecting the user that inserts/ deletes/ updates a password
    user_that_wants_modification := SUBSTR(USER, 2, LENGTH(USER)-1);

    IF is_number(user_that_wants_modification) = 1 THEN -- verifying that the user is an employee
        SELECT COUNT(employee_id)
        INTO is_it_user
        FROM employees
        WHERE employee_id = TO_NUMBER(user_that_wants_modification);

        IF is_it_user = 1 THEN
            IF INSERTING THEN
                INSERT INTO vault_access_audit VALUES (log_seq.NEXTVAL, TO_NUMBER(user_that_wants_modification), :NEW.credential_id, CURRENT_TIMESTAMP, 'added new credential');
            ELSIF UPDATING THEN
                INSERT INTO vault_access_audit VALUES (log_seq.NEXTVAL, TO_NUMBER(user_that_wants_modification), :NEW.credential_id, CURRENT_TIMESTAMP, 'updated credential');
            ELSIF DELETING THEN
                INSERT INTO vault_access_audit VALUES (log_seq.NEXTVAL, TO_NUMBER(user_that_wants_modification), :OLD.credential_id, CURRENT_TIMESTAMP, 'deleted credential');
            END IF;
        END IF;
    END IF;
END;
/
```

```
Function IS_NUMBER compiled


Trigger CREDENTIALS_AUDIT_TRIGGER compiled
```

Oracle-DB | Oracle-DB-sys

0.479 seconds

Worksheet | Query Builder

```
-- creating a new user for employee 55555 to test the audit trigger
ALTER SESSION SET "_ORACLE_SCRIPT"=TRUE;

CREATE USER E55555 IDENTIFIED BY Welcome123
   DEFAULT TABLESPACE USERS
   TEMPORARY TABLESPACE TEMP
   QUOTA UNLIMITED ON USERS;
/

GRANT CONNECT TO E55555;
GRANT INSERT ON vault.credentials TO E55555;
```

Script Output

Task completed in 0.479 seconds

```
Session altered.

User E55555 created.

Grant succeeded.


Grant succeeded.
```

Oracle-DB | Oracle-DB-sys | Oracle-DB-E55555

Worksheet | Query Builder

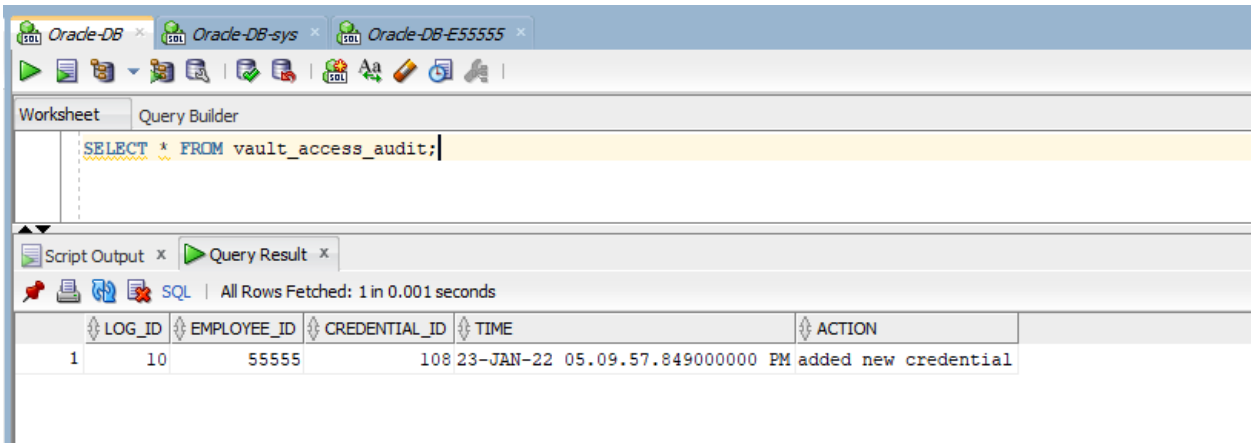
```
INSERT INTO vault.credentials
VALUES (108, 10004, 'hr@thisisfake.com', 'LinkedinPassword', TO_DATE('2022-01-01', 'YYYY-MM-DD'), TO_DATE('2022-01-01', 'YYYY-MM-DD'), NULL, NULL);
```

Script Output

Task completed in 0.442 seconds

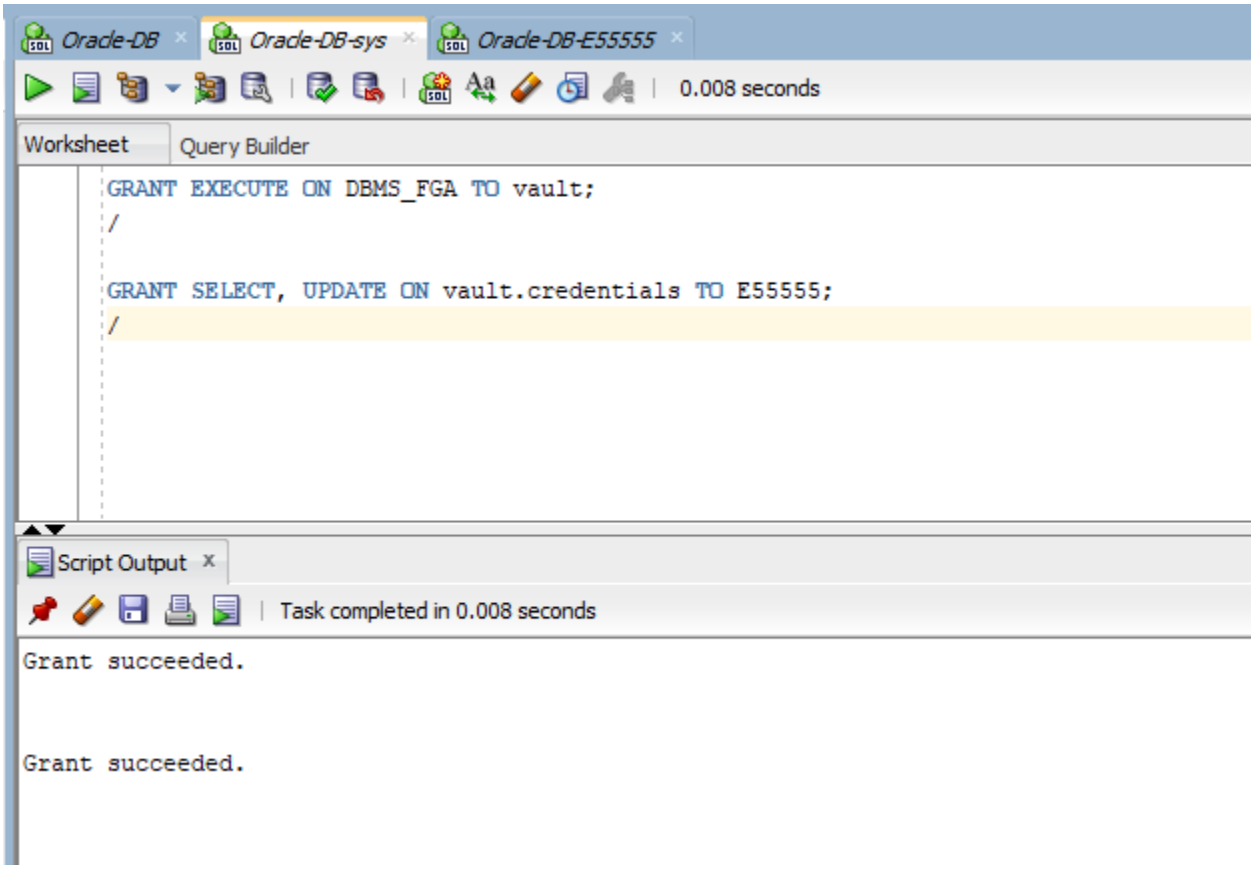
```
1 row inserted.
```

(Commit.)



c. Audit policies

The policy is going to log when a user is changing a credential but (s)he doesn't update the last_changed field (or at least not properly).



Oracle-DB | Oracle-DB-sys

0.449 seconds

Worksheet | Query Builder

```
-- creating and enabling the policy that logs when a user changes a credential but (s)he doesn't update the last_changed field (at least not properly)
BEGIN
    DBMS_FGA.ADD_POLICY(
        object_schema   => 'vault',
        object_name     => 'credentials',
        policy_name     => 'changed_credential_but_no_update_on_last_changed',
        audit_condition => 'CAST(last_changed as DATE) < CAST(CURRENT_TIMESTAMP as DATE)',
        audit_column    => 'username, password',
        enable          =>  FALSE,
        statement_types => 'UPDATE'
    );

    DBMS_FGA.ENABLE_POLICY(
        object_schema   => 'vault',
        object_name     => 'credentials',
        policy_name     => 'changed_credential_but_no_update_on_last_changed'
    );
END;
/
```

Script Output | Query Result

Task completed in 0.449 seconds

```
PL/SQL procedure successfully completed.
```

Oracle-DB | Oracle-DB-sys | Oracle-DB-E55555

Worksheet | Query Builder

```
UPDATE vault.credentials
    SET password = 'Microsoft'
    WHERE credential_id = 100;

COMMIT;
```

Script Output

Task completed in 0.021 seconds

```
1 row updated.

Commit complete.
```

Oracle-DB | Oracle-DB-sys | Oracle-DB-E55555

Worksheet | Query Builder

```
SELECT db_user, userhost, policy_name, timestamp, sql_text
FROM dba_fga_audit_trail;
```

Script Output | Query Result

SQL | All Rows Fetched: 1 in 0.004 seconds

	DB_USER	USERHOST	POLICY_NAME	TIMESTAMP	SQL_TEXT
1	E55555	DESKTOP-F7C58AV	CHANGED_CREDENTIAL_BUT_NO_UPDATE_ON_LAST_CHANGED	23-JAN-22	UPDATE vault.credentials SET password = 'Microsoft' WHERE credential_id = 100

IV. User & access to computational resources management

a. Identity management configuration design

(process-user, entity-process, entity-user matrixes)

Processes list

P1: Configure (add, edit) platforms information

P2: View platforms information

P3: Configure (add, edit, delete) credentials

P4: View credentials

P5: View & configure rights to credentials

P6: Add employees

P7: View and configure profile / account information of employees

P8: View vault logs

P9: Create accounts

User categories list

Human Resources Personnel

Information Technology Administrators

Audit Analysts

Vault Users

Ex-employees

Application & Database Administrator

Process-User Matrix

	P1	P2	P3	P4	P5	P6	P7	P8	P9
Human Resources Personnel						X	X		
Information Technology Administrators	X	X							
Audit Analysts		X						X	
Vault Users		X	X	X	X				
Ex-employees		X		X					
Application & Database Administrator		X					X	X	X

Entity-Process Matrix

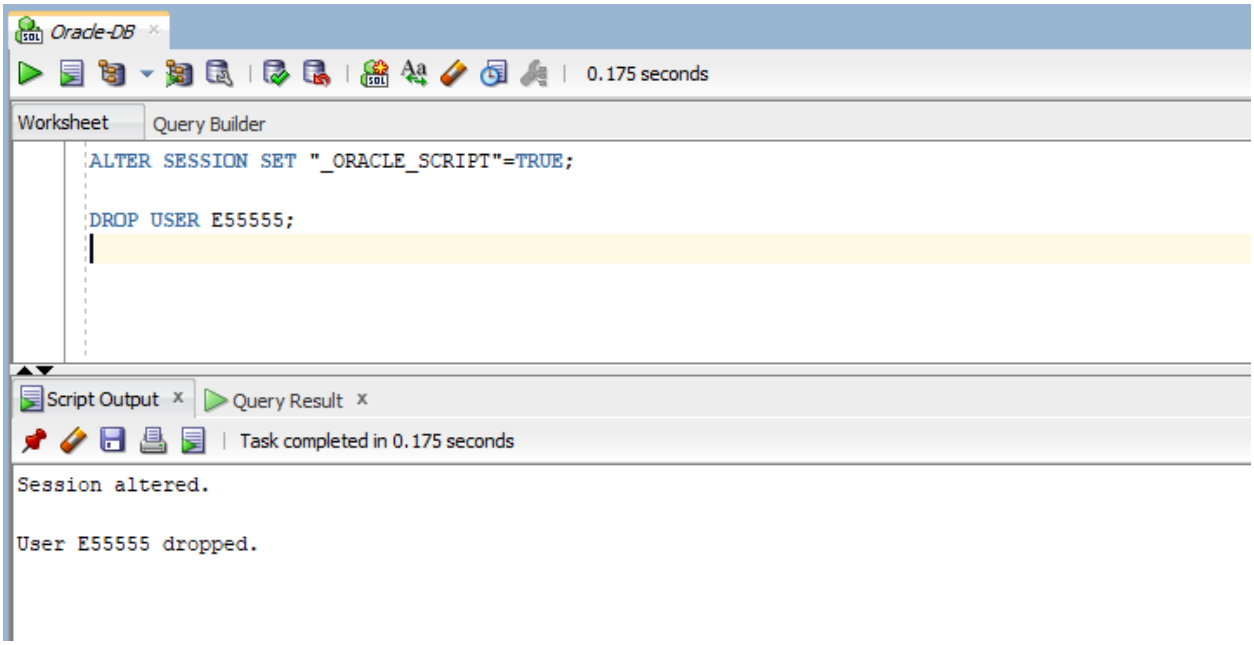
	P1	P2	P3	P4	P5	P6	P7	P8	P9
PLATFORMS	I, U	S	S	S					
EMPLOYEES			S		S	I	S, U		S
CREDENTIALS			I, U, D	S	S				
RIGHTS_MANAGEMENT					S, I, U, D				
VAULT_ACCESS_INFORMATION								S	

Entity-User Matrix

	HR	IT	Audit	Vault Users	Ex-emp	A&DBA
PLATFORMS		S, I, U	S	S	S	S
EMPLOYEES	S, I, U			S		S, U
CREDENTIALS				S, I, U, D	S	
RIGHTS_MANAGEMENT				S, I, U, D		
VAULT_ACCESS_INFORMATION			S			S

b. Identity management configuration implementation

The PL/SQL code used to implement the identity and resources management can be found in the *Coica_Oana_510-manag_ident_res_comp.txt* file.



Oracle-DB

0.033 seconds

Worksheet | Query Builder

```
-- creating user profiles
CREATE PROFILE HR_PERSONNEL LIMIT
    SESSIONS_PER_USER 2
    CONNECT_TIME 60
    IDLE_TIME 10
    PASSWORD_LIFE_TIME 30
    PASSWORD_GRACE_TIME 3
    PASSWORD_LOCK_TIME 2/3
    FAILED_LOGIN_ATTEMPTS 10;

CREATE PROFILE IT_PERSONNEL LIMIT
    SESSIONS_PER_USER 3
    CONNECT_TIME 30
    IDLE_TIME 5
    PASSWORD_LIFE_TIME 90
    PASSWORD_GRACE_TIME 10
    PASSWORD_LOCK_TIME 1/24
    FAILED_LOGIN_ATTEMPTS 3;

CREATE PROFILE AUDIT_ANALYSTS LIMIT
    SESSIONS_PER_USER 1
    CPU_PER_CALL 500
    CONNECT_TIME 120
    IDLE_TIME 30
    FAILED_LOGIN_ATTEMPTS 3
    PASSWORD_LOCK_TIME 1;

CREATE PROFILE OTHER_USERS LIMIT
    SESSIONS_PER_USER 5
    CONNECT_TIME 480
    IDLE_TIME 60
    FAILED_LOGIN_ATTEMPTS 10
    PASSWORD_LOCK_TIME 7;
```

Script Output | Query Result

Task completed in 0.033 seconds

```
Profile HR_PERSONNEL created.


Profile IT_PERSONNEL created.


Profile AUDIT_ANALYSTS created.


Profile OTHER_USERS created.
```

Oracle-DB

0.38100001 seconds

Worksheet | Query Builder

```
-- creating user accounts and assigning profiles
CREATE USER THEADMIN IDENTIFIED BY password123
PROFILE IT_PERSONNEL;

CREATE USER E10000 IDENTIFIED BY password123
PROFILE OTHER_USERS;

CREATE USER E11111 IDENTIFIED BY password123
PROFILE HR_PERSONNEL;

CREATE USER E22222 IDENTIFIED BY password123
PROFILE IT_PERSONNEL;

CREATE USER E33333 IDENTIFIED BY password123
PROFILE HR_PERSONNEL;

CREATE USER E44444 IDENTIFIED BY password123
PROFILE OTHER_USERS;

CREATE USER E55555 IDENTIFIED BY password123
PROFILE HR_PERSONNEL;

CREATE USER E66666 IDENTIFIED BY password123
PROFILE IT_PERSONNEL;

CREATE USER E77777 IDENTIFIED BY password123
PROFILE IT_PERSONNEL;

CREATE USER E88888 IDENTIFIED BY password123
PROFILE IT_PERSONNEL;

CREATE USER E99999 IDENTIFIED BY password123
PROFILE AUDIT_ANALYSTS;
```

Script Output | Query Result

Task completed in 0.381 seconds

```
User THEADMIN created.

User E10000 created.

User E11111 created.

User E22222 created.

User E33333 created.

User E44444 created.

User E55555 created.

User E66666 created.

User E77777 created.

User E88888 created.

User E99999 created.
```

V. Privileges and roles

The PL/SQL code used to implement privileges and roles can be found in the *Coica_Oana_510-privs_roles.txt* file.

```
-- creating the role used for HR
-- granting privileges:
-- HR can SELECT data on the employees table (except the vault_password field) using only the employees_hr_view;
-- HR can INSERT and UPDATE data directly on the employees table (except the vault_password field);
CREATE ROLE HR_Management;

GRANT CONNECT
TO HR_Management;

CREATE VIEW employees_hr_view AS
SELECT employee_id, email_address, first_name, last_name, job_title, hiring_date, end_date, personal_numerical_code
FROM employees;

GRANT SELECT
ON employees_hr_view
TO HR_Management;

GRANT INSERT(employee_id, email_address, first_name, last_name, job_title, hiring_date, end_date, personal_numerical_code),
      UPDATE(employee_id, email_address, first_name, last_name, job_title, hiring_date, end_date, personal_numerical_code)
ON vault.employees
TO HR_Management;
```

```
Role HR_MANAGEMENT created.


Grant succeeded.

View EMPLOYEES_HR_VIEW created.


Grant succeeded.


Grant succeeded.
```

Oracle-DB

0.033 seconds

Worksheet | Query Builder

```
-- creating the role used for IT
-- granting privileges:
-- IT can SELECT, INSERT and UPDATE data on the platforms table
CREATE ROLE IT_Administration;

GRANT CONNECT
TO IT_Administration;

GRANT SELECT, INSERT, UPDATE
ON vault.platforms
TO IT_Administration;
```

Script Output | Query Result

Task completed in 0.033 seconds

```
Role IT_ADMINISTRATION created.


Grant succeeded.


Grant succeeded.
```

Oracle-DB

0.061 seconds

Worksheet | Query Builder

```
-- creating the role used for Audit
-- granting privileges:
-- Audit can SELECT data on the platforms table
-- Audit can SELECT data on the vault_access_audit table
CREATE ROLE CS_Audit;

GRANT CONNECT
TO CS_Audit;

GRANT SELECT
ON vault.platforms
TO CS_Audit;

GRANT SELECT
ON vault.vault_access_audit
TO CS_Audit;
```

Script Output | Query Result

Task completed in 0.061 seconds

```
Role CS_AUDIT created.


Grant succeeded.


Grant succeeded.


Grant succeeded.
```

Oracle-DB

0.96200001 seconds

Worksheet | Query Builder

```sql
-- creating the role used for vault users
-- granting privileges:
-- vault users can SELECT data on the platforms table
-- vault users can SELECT data on the employees table using only the employees_user_view
-- vault users can SELECT, INSERT, UPDATE and DELETE data on the credentials table
-- vault users can SELECT, INSERT, UPDATE and DELETE data on the rights_management table
CREATE ROLE Vault_User;

GRANT CONNECT
TO Vault_User;

GRANT SELECT
ON vault.platforms
TO Vault_User;

CREATE VIEW employees_user_view AS
SELECT employee_id, email_address, first_name, last_name, job_title, hiring_date, end_date
FROM employees;

GRANT SELECT
ON employees_user_view
TO Vault_User;

GRANT SELECT, INSERT, UPDATE, DELETE
ON vault.credentials
TO Vault_User;

GRANT SELECT, INSERT, UPDATE, DELETE
ON vault.rights_management
TO Vault_User;
```

Script Output | Query Result

Task completed in 0.962 seconds

```
Role VAULT_USER created.


Grant succeeded.


Grant succeeded.

View EMPLOYEES_USER_VIEW created.


Grant succeeded.


Grant succeeded.


Grant succeeded.
```

Oracle-DB

0.035 seconds

Worksheet | Query Builder

```
-- creating the role used for ex_employees
-- granting privileges:
-- ex-employees can SELECT data on the platforms table
-- ex-employees can SELECT data on the credentials table
CREATE ROLE Ex_Employee;

GRANT CONNECT
TO Ex_Employee;

GRANT SELECT
ON vault.platforms
TO Ex_Employee;

GRANT SELECT
ON vault.credentials
TO Ex_Employee;
```

Script Output | Query Result

Task completed in 0.035 seconds

```
Role EX_EMPLOYEE created.


Grant succeeded.


Grant succeeded.


Grant succeeded.
```

Oracle-DB

Worksheet | Query Builder

```
-- granting privileges to theadmin user:
-- the admin can SELECT data on the platforms table
-- the admin can SELECT data on the employees table using only the employees_user_view
-- the admin can UPDATE data on the employees table (except the personal_numerical_code field)
-- the admin can SELECT data on the credentials table
-- the admin can SELECT data on the vault_access_audit table
GRANT CONNECT, CREATE USER, ALTER USER
TO THEADMIN;

GRANT SELECT
ON vault.platforms
TO THEADMIN;

GRANT SELECT
ON employees_user_view
TO THEADMIN;

GRANT UPDATE(employee_id, email_address, first_name, last_name, vault_password, job_title, hiring_date, end_date)
ON vault.employees
TO THEADMIN;

GRANT SELECT
ON vault.credentials
TO THEADMIN;

GRANT SELECT
ON vault.vault_access_audit
TO THEADMIN;
```

Script Output | Query Result

Task completed in 0.012 seconds

```
Grant succeeded.

Grant succeeded.

Grant succeeded.

Grant succeeded.

Grant succeeded.

Grant succeeded.
```

Oracle-DB

0.207 seconds

Worksheet | Query Builder

```
-- assigning roles to users
GRANT Vault_User TO E10000;
GRANT Vault_User, HR_Management TO E11111;
GRANT Vault_User, IT_Administration TO E22222;
GRANT Vault_User, HR_Management TO E33333;
GRANT Vault_User TO E44444;
GRANT Vault_User, HR_Management TO E55555;
GRANT Vault_User, IT_Administration TO E66666;
GRANT Vault_User, IT_Administration TO E77777;
GRANT Vault_User, IT_Administration TO E88888;
GRANT Vault_User, CS_Audit TO E99999;
```

Script Output | Query Result

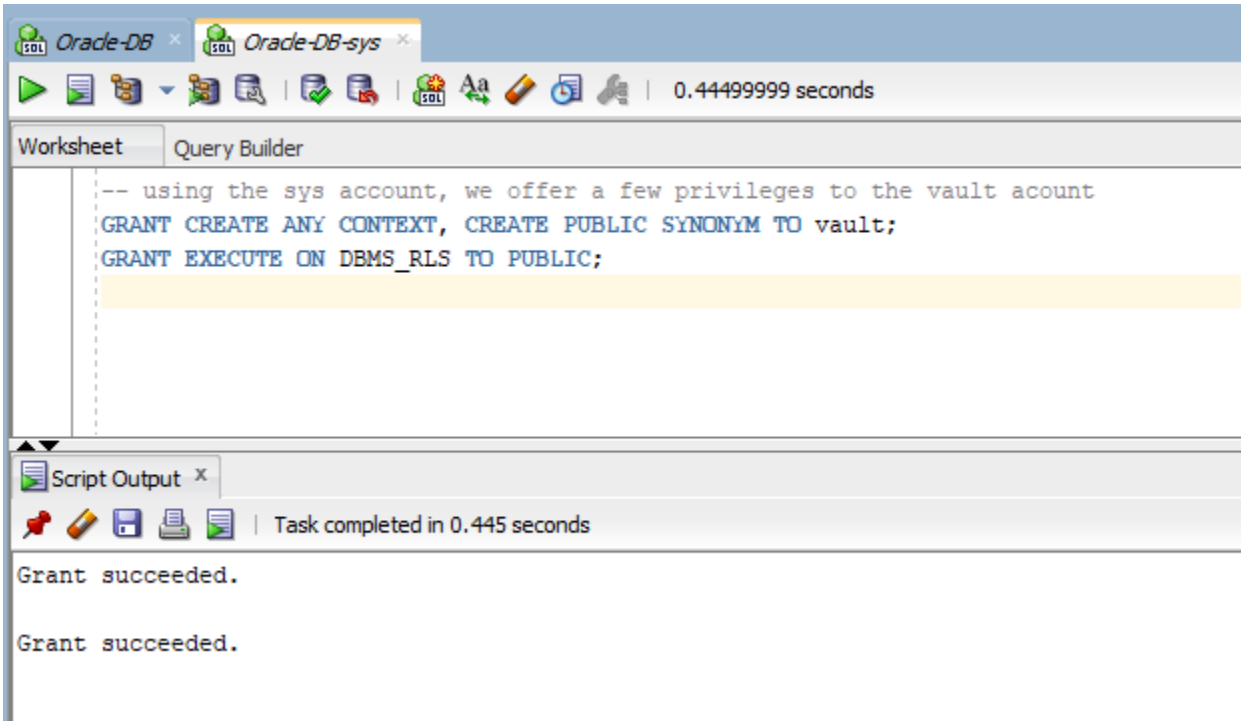
Task completed in 0.207 seconds

```
Grant succeeded.

Grant succeeded.

Grant succeeded.

Grant succeeded.

Grant succeeded.

Grant succeeded.

Grant succeeded.

Grant succeeded.

Grant succeeded.

Grant succeeded.
```

VI. Database application and data security

The PL/SQL code used to implement data security can be found in the *Coica_Oana_510-app_security.txt* file.

a. Application context



Oracle-DB | Oracle-DB-sys

1.28100002 seconds

Worksheet | Query Builder

```
-- creating an application context
CREATE CONTEXT vault_context USING vault.context_package;

-- creating the package associated to the context
CREATE OR REPLACE PACKAGE context_package AS
    PROCEDURE set_context;
END;
/

CREATE OR REPLACE PACKAGE BODY context_package IS
    PROCEDURE set_context IS
        v_employee_id NUMBER(5);
        v_connected_user VARCHAR2(255);
    BEGIN
        v_connected_user := SYS_CONTEXT('USERENV','SESSION_USER');
        IF is_number(SUBSTR(v_connected_user, 2, LENGTH(v_connected_user)-1)) = 1
            THEN v_employee_id := TO_NUMBER(SUBSTR(v_connected_user, 2, LENGTH(v_connected_user)-1));
        ELSE v_employee_id := NULL;
        END IF;
        DBMS_SESSION.set_context('vault_context', 'connected_employee_id', v_employee_id);
    END set_context;
END context_package;
/

-- granting execution rights on the package functions for everyone
GRANT EXECUTE ON vault.context_package TO PUBLIC;
CREATE PUBLIC SYNONYM context_package FOR vault.context_package;
```

Script Output | Query Result

Task completed in 1.281 seconds

```
Context VAULT_CONTEXT created.

Package CONTEXT_PACKAGE compiled

Package body CONTEXT_PACKAGE compiled

Grant succeeded.

Public synonym CONTEXT_PACKAGE created.
```

Oracle-DB | Oracle-DB-sys

0.39700001 seconds

Worksheet | Query Builder

```oracle
-- creating a trigger that sets the context at logon
CREATE OR REPLACE TRIGGER set_security_context
AFTER LOGON ON DATABASE
BEGIN
    context_package.set_context;
END;
/

CREATE OR REPLACE PACKAGE security_package AS
    FUNCTION credentials_security(owner VARCHAR2, objname VARCHAR2)
        RETURN VARCHAR2;
END security_package;
/

CREATE OR REPLACE PACKAGE BODY security_package IS
    FUNCTION credentials_security(owner VARCHAR2, objname VARCHAR2) RETURN VARCHAR2 IS
        predicate VARCHAR2(2000);
    BEGIN
        IF SYS_CONTEXT('vault_context', 'connected_employee_id') = NULL
            THEN predicate := '1!=1';
        ELSE
            predicate := 'credential_id IN (SELECT credential_id
                      FROM rights_management
                      WHERE employee_id = SYS_CONTEXT(''vault_context'', ''connected_employee_id''))';
        END IF;
        RETURN predicate;
    END credentials_security;
END security_package;
/
```

Script Output | Query Result

Task completed in 0.397 seconds

```
Trigger SET_SECURITY_CONTEXT compiled

Package SECURITY_PACKAGE compiled


Package body SECURITY_PACKAGE compiled
```

Oracle-DB | Oracle-DB-sys

0.16 seconds

Worksheet | Query Builder

```oracle
ALTER SYSTEM SET "_allow_insert_with_update_check"=TRUE scope=spfile;
```

Script Output | Query Result

Task completed in 0.16 seconds

```
System SET altered.
```

Oracle-DB

1.12300003 seconds

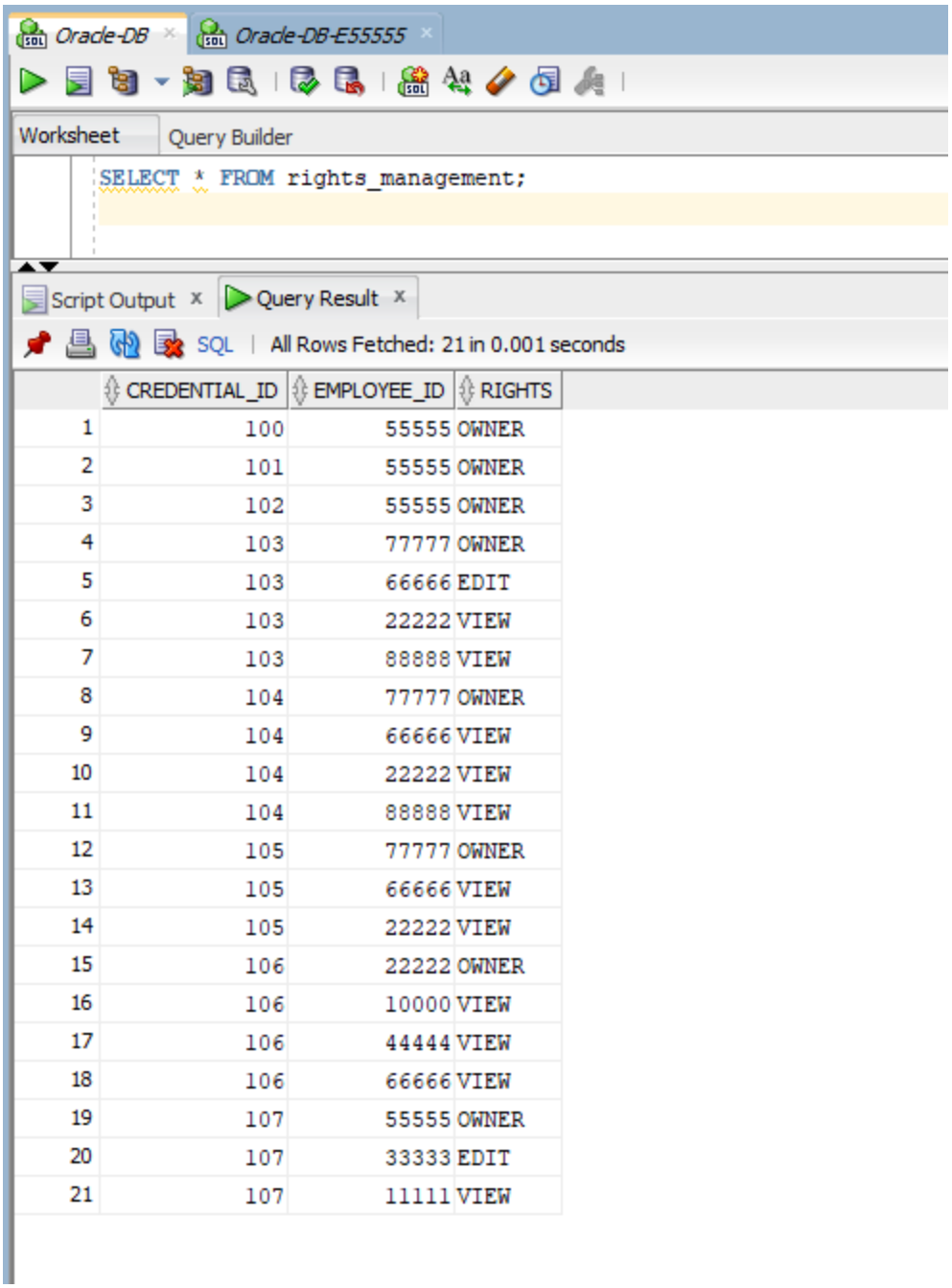
Worksheet | Query Builder

```
-- all users need execution rights on the security_package
GRANT EXECUTE ON vault.security_package TO PUBLIC;
CREATE PUBLIC SYNONYM security_package FOR vault.security_package;
/

-- adding policy
BEGIN
    DBMS_RLS.add_policy(
        object_schema => 'vault',
        object_name => 'credentials',
        policy_name => 'credentials_policy',
        function_schema => 'vault',
        policy_function => 'security_package.credentials_security',
        statement_types => 'SELECT, INSERT, UPDATE, DELETE');
END;
/
```

Script Output

Task completed in 1.123 seconds

```
Grant succeeded.

Public synonym SECURITY_PACKAGE created.

PL/SQL procedure successfully completed.
```



	CREDENTIAL_ID	EMPLOYEE_ID	RIGHTS
1	100	55555	OWNER
2	101	55555	OWNER
3	102	55555	OWNER
4	103	77777	OWNER
5	103	66666	EDIT
6	103	22222	VIEW
7	103	88888	VIEW
8	104	77777	OWNER
9	104	66666	VIEW
10	104	22222	VIEW
11	104	88888	VIEW
12	105	77777	OWNER
13	105	66666	VIEW
14	105	22222	VIEW
15	106	22222	OWNER
16	106	10000	VIEW
17	106	44444	VIEW
18	106	66666	VIEW
19	107	55555	OWNER
20	107	33333	EDIT
21	107	11111	VIEW

From E55555's account, only credentials 100, 101, 102 and 107 should be accessible, while from E11111's account, only credential 107 should be accessible. Verification:

Oracle-DB | Oracle-DB-E55555

Worksheet | Query Builder

```
SELECT * FROM vault.credentials;
```

Query Result

SQL | All Rows Fetched: 4 in 0.29 seconds

	CREDENTIAL_ID	PLATFORM_ID	USERNAME	PASSWORD	CREATED	LAST_CHANGED	EXPIRATION_DATE	LOCATION_OF_ENCRYPTION_KEY
1	100	10001	eyanuk@thisisfake.com	Microsoft	01-JAN-22	01-JAN-22	(null)	(null)
2	101	10002	eyanuk@thisisfake.com	TeamPassPassword	01-JAN-22	01-JAN-22	(null)	(null)
3	102	10009	eyanuk@thisisfake.com	PluralsightPassword	01-JAN-22	01-JAN-22	(null)	(null)
4	107	10004	hr@thisisfake.com	LinkedinPassword	01-JAN-22	01-JAN-22	(null)	https://192.168.10.10/SWVrUM5GMK.txt

Oracle-DB | Oracle-DB-E55555 | Oracle-DB-E11111

Worksheet | Query Builder

```
SELECT * FROM vault.credentials;
```

Query Result

SQL | All Rows Fetched: 1 in 0.123 seconds

	CREDENTIAL_ID	PLATFORM_ID	USERNAME	PASSWORD	CREATED	LAST_CHANGED	EXPIRATION_DATE	LOCATION_OF_ENCRYPTION_KEY
1	107	10004	hr@thisisfake.com	LinkedinPassword	01-JAN-22	01-JAN-22	(null)	https://192.168.10.10/SWVrUM5GMK.txt

b. SQL Injection

Oracle-DB | 0.30399999 seconds

Worksheet | Query Builder

```
CREATE OR REPLACE PROCEDURE VERIFY_LOGIN (used_username VARCHAR2, used_password VARCHAR2) AS
    v_login_status NUMBER(2) :=-1;
BEGIN
    EXECUTE IMMEDIATE 'SELECT COUNT(*) FROM employees WHERE employee_id=''' || SUBSTR(used_username, 2, LENGTH(used_username)-1) || '''
        AND vault_password=hash_using_sha256(''' || used_password ||''')' INTO v_login_status;
    DBMS_OUTPUT.PUT_LINE('SELECT COUNT(*) FROM employees WHERE employee_id=''' || SUBSTR(used_username, 2, LENGTH(used_username)-1) || '''
        AND vault_password=hash_using_sha256(''' || used_password ||''')');
    IF v_login_status=0 THEN
        DBMS_OUTPUT.PUT_LINE('Login failed');
    ELSE
        DBMS_OUTPUT.PUT_LINE('Login successful');
    END IF;
END;
/
EXEC VERIFY_LOGIN('E10000', 'password123');
EXEC VERIFY_LOGIN('E10000', 'wrongpassword');
EXEC VERIFY_LOGIN('E10000''--','wrongpassword');
EXEC VERIFY_LOGIN('123'' OR 1=1 --', 'SOMETHING');
```

Script Output | Task completed in 0.304 seconds

```
Procedure VERIFY_LOGIN compiled


PL/SQL procedure successfully completed.


PL/SQL procedure successfully completed.


PL/SQL procedure successfully completed.


PL/SQL procedure successfully completed.
```

Dbms Output | Buffer Size: 20000

Oracle-DB

```
SELECT COUNT(*) FROM employees WHERE employee_id='10000'
        AND vault_password=hash_using_sha256('password123')
Login successful

SELECT COUNT(*) FROM employees WHERE employee_id='10000'
        AND vault_password=hash_using_sha256('wrongpassword')
Login failed

SELECT COUNT(*) FROM employees WHERE employee_id='10000'--'
        AND vault_password=hash_using_sha256('wrongpassword')
Login failed

SELECT COUNT(*) FROM employees WHERE employee_id='23' OR 1=1 --'
        AND vault_password=hash_using_sha256('SOMETHING')
Login failed
```

VII. Data masking in Oracle

The PL/SQL code used to implement data masking can be found in the *Coica_Oana_510-data_masking.txt* file.

```
CREATE OR REPLACE PACKAGE masking_package IS
    FUNCTION f_masking_name (name_to_mask VARCHAR2) RETURN VARCHAR2;
    FUNCTION f_masking_email (email_to_mask VARCHAR2) RETURN VARCHAR2;
    FUNCTION f_masking_pnc (pnc_to_mask VARCHAR2) RETURN VARCHAR2;
END;
/

CREATE OR REPLACE PACKAGE BODY masking_package IS
    FUNCTION f_masking_name (name_to_mask VARCHAR2) RETURN VARCHAR2
    IS
        v_masked_name VARCHAR2(100);
        v_length NUMBER;
    BEGIN
        v_masked_name := SUBSTR(name_to_mask, 1, 2);
        SELECT LENGTH(name_to_mask)
        INTO v_length
        FROM DUAL;

        v_masked_name := RPAD(v_masked_name, v_length, '*');
        RETURN v_masked_name;
    END f_masking_name;

    FUNCTION f_masking_email (email_to_mask VARCHAR2) RETURN VARCHAR2
    IS
        v_masked_email VARCHAR2(100);
    BEGIN
        SELECT REGEXP_REPLACE(email_to_mask, '(\w{2})\w+', '\1**')
        INTO v_masked_email
        FROM dual;
        RETURN v_masked_email;
    END f_masking_email;

    FUNCTION f_masking_pnc (pnc_to_mask VARCHAR2) RETURN VARCHAR2
    IS
        v_masked_pnc VARCHAR2(13);
    BEGIN
        SELECT RPAD('*' || SUBSTR(pnc_to_mask, 2, 6), 13, '*')
        INTO v_masked_pnc
        FROM dual;

        RETURN v_masked_pnc;
    END f_masking_pnc;
END;
/
```

```
Package MASKING_PACKAGE compiled


Package body MASKING_PACKAGE compiled
```

Oracle-DB

0.186 seconds

Worksheet | Query Builder

```
CREATE OR REPLACE DIRECTORY DIREXP AS 'D:\SECBD';
```

Script Output | Query Result

Task completed in 0.186 seconds

```
Directory DIREXP created.
```

Command Prompt

```
C:\Users\oana_>expdp vault/Welcome123@o12c tables=employees remap_data=vault.employees.first_name:masking_package.f_masking_name rema
p_data=vault.employees.last_name:masking_package.f_masking_name remap_data=vault.employees.email_address:masking_package.f_masking_em
ail remap_data=vault.employees.personal_numerical_code:masking_package.f_masking_pnc directory=DIREXP dumpfile=EXPORT_FILE.dmp

Export: Release 12.2.0.1.0 - Production on Tue Jan 25 21:49:32 2022

Copyright (c) 1982, 2017, Oracle and/or its affiliates.  All rights reserved.

Connected to: Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production

Warning: Oracle Data Pump operations are not typically needed when connected to the root or seed of a container database.

Starting "VAULT"."SYS_EXPORT_TABLE_01":  vault/********@o12c tables=employees remap_data=vault.employees.first_name:masking_package.f
_masking_name remap_data=vault.employees.last_name:masking_package.f_masking_name remap_data=vault.employees.email_address:masking_pa
ckage.f_masking_email remap_data=vault.employees.personal_numerical_code:masking_package.f_masking_pnc directory=DIREXP dumpfile=EXPO
RT_FILE.dmp
Processing object type TABLE_EXPORT/TABLE/TABLE_DATA
Processing object type TABLE_EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS
Processing object type TABLE_EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
Processing object type TABLE_EXPORT/TABLE/STATISTICS/MARKER
Processing object type TABLE_EXPORT/TABLE/TABLE
Processing object type TABLE_EXPORT/TABLE/GRANT/OWNER_GRANT/OBJECT_GRANT
Processing object type TABLE_EXPORT/TABLE/CONSTRAINT/CONSTRAINT
. . exported "VAULT"."EMPLOYEES"                          9.984 KB      10 rows
Master table "VAULT"."SYS_EXPORT_TABLE_01" successfully loaded/unloaded
******************************************************************************
Dump file set for VAULT.SYS_EXPORT_TABLE_01 is:
  D:\SECBD\EXPORT_FILE.DMP
Job "VAULT"."SYS_EXPORT_TABLE_01" successfully completed at Tue Jan 25 21:50:23 2022 elapsed 0 00:00:50


C:\Users\oana_>
```

Command Prompt

```
C:\Users\oana_>impdp vault/Welcome123@o12c directory=DIREXP dumpfile=EXPORT_FILE.DMP TABLES=employees remap_table=employees:emp1

Import: Release 12.2.0.1.0 - Production on Tue Jan 25 21:53:02 2022

Copyright (c) 1982, 2017, Oracle and/or its affiliates.  All rights reserved.

Connected to: Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production

Warning: Oracle Data Pump operations are not typically needed when connected to the root or seed of a container database.

Master table "VAULT"."SYS_IMPORT_TABLE_01" successfully loaded/unloaded
Starting "VAULT"."SYS_IMPORT_TABLE_01":  vault/********@o12c directory=DIREXP dumpfile=EXPORT_FILE.DMP TABLES=employees remap_table=e
mployees:emp1
Processing object type TABLE_EXPORT/TABLE/TABLE
Processing object type TABLE_EXPORT/TABLE/TABLE_DATA
. . imported "VAULT"."EMP1"                              9.984 KB      10 rows
Processing object type TABLE_EXPORT/TABLE/GRANT/OWNER_GRANT/OBJECT_GRANT
Processing object type TABLE_EXPORT/TABLE/CONSTRAINT/CONSTRAINT
ORA-31684: Object type CONSTRAINT:"VAULT"."PK_EMPLOYEES" already exists

Processing object type TABLE_EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS
Processing object type TABLE_EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
Processing object type TABLE_EXPORT/TABLE/STATISTICS/MARKER
Job "VAULT"."SYS_IMPORT_TABLE_01" completed with 1 error(s) at Tue Jan 25 21:53:24 2022 elapsed 0 00:00:22


C:\Users\oana_>
```

Oracle-DB

Worksheet | Query Builder

```
SELECT * FROM emp1;
```

Script Output | Query Result

SQL | All Rows Fetched: 10 in 0.026 seconds

	EMPLOYEE_ID	EMAIL_ADDRESS	VAULT_PASSWORD	FIRST_NAME	LAST_NAME	JOB_TITLE	HIRING_DATE	END_DATE	PERSONAL_NUMERICAL_CODE
1	10000	mh**@th**.co**	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Ma*****	Hu******	Network Engineer	16-MAR-21	(null)	*950114******
2	11111	dj**@th**.co**	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Do*****	Ja********	Human Resources Assistant	19-JAN-21	(null)	*921007******
3	22222	rm**@th**.co**	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Ra*	Mu******	Infrastructure Architect	16-JUL-19	(null)	*901112******
4	33333	ar**@th**.co**	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Am*****	Ro***	Recruiting Specialist	13-MAY-17	(null)	*890409******
5	44444	gt**#th**.co**	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Ge*******	To********	Network Engineer	12-DEC-09	(null)	*990311******
6	55555	ey**@th**.co**	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Ev*****	Ya***	Human Resources Manager	27-FEB-14	(null)	*880315******
7	66666	ca**@th**.co**	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Ca****	de******	Security Specialist	09-SEP-12	(null)	*981010******
8	77777	ed**#th**.co**	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Ev*****	Da******	Information Security Manager	03-JUL-17	(null)	*910822******
9	88888	at**@th**.co**	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	Al**	To****	System Administrator	05-MAR-11	(null)	*900725******
10	99999	el**@th**.co**	EF92B778BAFE771E89245B89ECBC08A44A4E166C06659911881F383D4473E94F	El****	Ty*	Internal Auditor	23-APR-19	(null)	*990920******