FCBHifence software UNIX installation and user guide

Table of contents

CONCEPT

FCBHIFENCE software doesn't reinvent wheel and uses GNU Privacy Guard software (GnuPG). GnuPG (or compatible to IETF standards-track specification of OpenPGP software) must be installed as on server side so on user computer. Key management operations, i.e. creation, deletion, expiration, import, export are performed by GnuPG only. Data operations as encryption and decryption are performed by the GnuPG also. FCBHIFENCE software can be considered as a bridge between the GnuPG (or software with the similar functionality) and Oracle database. Data Operations. Without being lost in too much details asymmetrical encryption bases on two kinds of security keys: public and private. Public key is used to encrypt data. Private key is used to decrypt data. They both is the pair. User, who authorized is to decrypt and therefore to read data, stores private key in GnuPG key storage on the user computer. Public key is stored on the server or on the user computer in the GnuPG key storage also. Keys can be exported and imported to/from the GnuPG key storage. Thus any cell level data in an Oracle table can be encrypted by the different public keys to provide data separation, i.e. one column can contain differently encrypted data. Only application having access to the local key storage where paired private key is stored can decrypt data.

BEGINNING

FCBHIFENCE software is provided as a binary self-extracting archive file. Its name looks like **fcbhifence-1.2.40.run** where 1 is a version number, 2 is a subversion number and 40 is a build number. FCBHIFENCE software installation supposes Korn shell[1] (ksh) is installed, valid and available as /usr/bin/ksh[2]. **fcbhifence-**

1 Korn shell is one of prerequisites for Oracle database installation. See Installation and Upgrade Guide for Linux, Installation Guide for IBM AIX, Installation Guide for Oracle Solaris, Installation Guide for HP-UX Itanium

2 if /usr/bin as a catalog for ksh is absolutely unacceptable for you, please either make a symbolic link or change #!/usr/bin/ksh value in fcbhifence/bin/install.sh file

1.2.40.run file can be run on UNIX like operating systems (IBM AIX, SUN/Oracle Solaris, Linux, HP HP-UX)[3], i.e.

```
$ ./fcbhifence-1.2.40.run

FCBHifence software. Copyright 2019 Olexandr Siroklyn. All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:
...
```

As it can be seen from above there is an End User License Agreement you must accept to continue or reject to cancel installation. In case you accept End User License Agreement unpacking starts,

```
Please type y to accept, n otherwise: y
Creating directory fcbhifence
Verifying archive integrity...  100%   All good.
Uncompressing installer for fcbhifence software  100%..
```

fcbhifence directory is created

```
$ ls -ltr
total 56K
drwxrwxr-x. 6 oracle dba 160 Apr 17 10:22 fcbhifence/
-rwxr-xr-x. 1 oracle dba 53K Apr 17 14:56 fcbhifence-1.1.22.run*
```

```
$ ls -la fcbhifence
total 8.0K
drwxrwxr-x. 6 oracle dba  160 Apr 17 10:22 ./
drwxr-xr-x. 3 oracle dba   80 Apr 17 14:56 ../
drwxrwxr-x. 2 oracle dba  140 Apr 17 10:06 bin/
-rw-r--r--. 1 oracle dba  724 Apr 17 10:22 .dbvariables
drwxr-xr-x. 2 oracle dba  120 Apr 17 10:17 exm/
-rw-r--r--. 1 oracle dba 2.1K Apr 17 10:22 .osvariables
drwxrwxr-x. 2 oracle dba  120 Apr 17 10:56 sql/
drwxrwxr-x. 2 oracle dba  120 Apr 17 10:17 test/
```

and FCBHIFENCE software installation starts via

```
$ cd fcbhifence/bin; ./install.sh

...
Hello,

You are starting installation of FCBHifence software v.1.1.22.
...
```

3 it wasn't tested on HP HP-UX, but it should work

PREREQUISITES

There are prerequisites to continue installation

a) fcbhifence/.osvariables file
b) fcbhifence/.dbvariables file
c) Oracle database 11g (excepting Express Edition[4]), 12c or 18c
d) $ORACLE_HOME environment variable
e) Oracle listener service
f) $ORACLE_HOME/bin/sqlplus utility
g) database user privileges
h) Oracle database Java subsystem[5]

a) **.osvariables** file contains a small shell scripts to detect paths to the common UNIX utilities like ls, cat, diff and so on. Also .osvariables file contains directory aliases for FCBHIFENCE software installation. In common case you don't need to change anything inside this file.

b) .**dbvariables** file contains database related environment variables. Most of their values are wrong for your database case. **You must manually adjust .dbvariables file values relating to you needs and database parameters.**

- **l_DB_SERVICE**=orcl sets a database service name to be used in connection process.
- **l_DB_HOST**=localhost sets a host name to be used in connection process.
- **l_DB_PORT**=1521 sets a port number to be used in connection process.
- **l_PACKAGE_OWNER**=system sets a database schema where FCBHIFENCE software will be installed.
- **l_PACKAGE_OWNER_PASS**=system sets a password for the database schema where FCBHIFENCE software will be installed.
- **GG_TEMP_DIR**=DATA_PUMP_DIR sets a database directory (not an operating system directory!) name where temp files will be placed. Please refer to the ALL_DIRECTORIES view for details.
- **l_DB_CONNECTION**=${l_PACKAGE_OWNER}/${l_PACKAGE_OWNER_PASS}@${l_DB_HOST}:${l_DB_PORT}/${l_DB_SERVICE} simply joins together some previous variables to get a database connection string to be used by SQL*Plus utility.

d) **$ORACLE_HOME** environment variable must be setup to provide a correct work of SQL*Plus utility.

e) **Oracle listener service** must be setup and started. Also **l_DB_SERVICE** value should be registered in listener service.

f) **$ORACLE_HOME/bin/sqlplus** utility must be available via **$PATH** environment variable. **$ORACLE_HOME/bin/sqlplus** is used in FCBHIFENCE software installation process to run SQL scripts.

4 Oracle Database 11g Express Edition
5 a standard database cross-version and cross-edition component or How to Add the JVM Component to an Existing Oracle Database (Doc ID 1461562.1)

g) A database user where FCBHIFENCE software is going to be installed (see **I_PACKAGE_OWNER** variable from **.dbvariables** file) must have following grants

- create table
- create procedure
- create type
- create session
- alter session
- read/write on **GG_TEMP_DIR** (see **.dbvariables** file) directory

h) Java database component is installed and valid, otherwise [5]

CRYPTOGRAPHY

As it was mentioned above FCBHIFENCE is a “bridge” providing possibility to asymmetrically encrypt/decrypt SQL or PL/SQL data, i.e. string, varchar2, nvarchar2, clob, nclob, via GnuPG software. Also this guide’s purpose is not to describe how GnuPG software works. For that please refer to the GnuPG main site. But the main concept of GnuPG software, asymmetrical cryptography and FCBHIFENCE software is a pair of the keys: public key and private key. We use public key to encrypt data. We distribute public key to the others. We use private key to decrypt data only. Private key can be a real private or “conditionally” private, i.e. accessible for the group of persons with the same data security level access. Both kinds of the keys can be exported, imported and expired. Both keys are stored in GnuPG key storage. Every key or data operations are performed by GnuPG software only. Also please have a note FCBHIFENCE doesn’t support pass-phrase protected keys.

GNUPG

GnuPG software v2 (or software with the similar functionality) must be installed prior FCBHIFENCE installation. How to check that out? Here is a common example:

```
$ whoami
oracle

$ gpg2 --version
gpg (GnuPG) 2.2.8
libgcrypt 1.8.3
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /home/oracle/.gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2
```

FCBHIFENCE interacts with GnuPG via:

- Java based “bridge” module, i.e. **fcbhifence/sql/cre_jsr_fcbhifence.sql**
- server side UNIX shell scripts:
  - to decrypt data, i.e. **fcbhifence/bin/fcbhifence_decr.sh**
  - to encrypt data, i.e. **fcbhifence/bin/fcbhifence_encr.sh**
  - to import public key, i.e. **fcbhifence/bin/fcbhifence_imppkey.sh**

But interaction is not possible till special grants provided. To do this please do following:

a) examine **fcbhifence/sql/cre_pkg_fcbhifence.pks** file and adjust file paths, i.e.

```
gg_encrbin_name varchar2(1024):='full_path_to/fcbhifence_encr.sh';
gg_decrbin_name varchar2(1024):='full_path_to/fcbhifence_decr.sh';
gg_impkbin_name varchar2(1024):='full_path_to/fcbhifence_imppkey.sh';
 gg_gpgbin_name varchar2(1024):='/usr/bin/gpg2';
    gg_temp_dir varchar2(64)  :='DATA_PUMP_DIR';
```

b) if your database is 12c or 11g and 19721304 patch was applied please make sure Java Development feature (if it is) is allowed

```
SQL> select upper(JAVA_DEV_ALLOWED) from sys.java_dev_status;

UPP
---
YES
```

If it’s not allowed please allow it

```
SQL> exec dbms_java_dev.enable;
```

Without allowed Java Development feature, (if it is) Java based “bridge” module doesn’t work on 12c at least.

c) grant rights via

```
 SQL> call dbms_java.grant_permission(upper('package owner'),
'SYS:java.io.FilePermission','/usr/bin/gpg2','execute');

 SQL> call dbms_java.grant_permission(upper('package owner'),
'SYS:java.io.FilePermission','/fcbhifence/bin/fcbhifence_decr.sh',
'execute');

 SQL> call dbms_java.grant_permission(upper('package owner'),
'SYS:java.io.FilePermission','/fcbhifence/bin/fcbhifence_encr.sh',
'execute');

 SQL> call dbms_java.grant_permission( upper('package owner'),
'SYS:java.io.FilePermission','/fcbhifence/bin/fcbhifence_imppkey.sh',
'execute');
```

```
SQL> grant read,write on directory DATA_PUMP_DIR to 'package owner';
```

INSTALLATION

```
$ ./install.sh

Hello,

You are starting installation of FCBHifence software v.1.1.22. It's very
recommended to do that under Oracle database binaries' operating system owner
account. Your current account is 'oracle:dba'. You can press Ctrl-C anytime to
stop installation. You can re-run installation via cd /fcbhifence/bin/../bin;
./install.sh call. Before the next step please make sure following items are
filled/setup/working correctly:

  a. /fcbhifence/bin/../.dbvariables file
  b. $ORACLE_HOME environment variable
  c. Oracle listener service
  d. $ORACLE_HOME/bin/sqlplus utility

Continue? (y/n)y

> Hereafter following connection credentials will be used: system/**@***:1521/ee18

> Java component is presented and valid.

> Detecting 19721304 patch presence via ${ORACLE_HOME}/OPatch/opatch lsinventory
call

> ...not found.

> GnuPG v2 detected.

Please look at ../sql/cre_pkg_fcbhifence.pks file, adjust file paths and grant
according rights via

SQL> call
dbms_java.grant_permission(upper('system'),'SYS:java.io.FilePermission','/usr/bin/
gpg2','execute');
SQL> call
dbms_java.grant_permission(upper('system'),'SYS:java.io.FilePermission','/ora01/
fcbhifence/bin/fcbhifence_decr.sh','execute');
SQL> call
dbms_java.grant_permission(upper('system'),'SYS:java.io.FilePermission','/ora01/
fcbhifence/bin/fcbhifence_encr.sh','execute');
SQL> call
dbms_java.grant_permission(upper('system'),'SYS:java.io.FilePermission','/ora01/
fcbhifence/bin/fcbhifence_imppkey.sh','execute');
SQL> grant read, write on directory 'DATA_PUMP_DIR' to 'lab_pt27';
```

```
Also please check out
create session, alter session, create type, create procedure, read/write on
DATA_PUMP_DIR directory
grants have been provided to the package owner, i.e. system

Do you want to modify ../sql/cre_pkg_fcbhifence.pks file automatically? (y/n)y

Next actions are creations of database objects under system/**@**:1521/ee18
credentials.

Continue? (y/n)y

> @../sql/cre_jsr_fcbhifence.sql

Java created.

No errors.

> @../sql/cre_typ_fcbhifence.sql

Type created.

No errors.

> @../sql/cre_pkg_fcbhifence.pks

Package created.

No errors.

> @../sql/cre_pkg_fcbhifence.pkb

Package body created.

No errors.

Package body altered.

FCBHifence software v.1.1.22
Copyright (c) 2019, Olexandr Siroklyn. All rights reserved.

PL/SQL procedure successfully completed.

If you see no errors above this means installation has finished successfully.
```

AFTER INSTALLATION

When installation finishes you have following objects in FCBHIFENCE software schema

- **PKG_ FCBHIFENCE** package[6]
- **JSR_ FCBHIFENCE** java source

6 **PKG_ FCBHIFENCE** package validity depends on the all objects below

- **TYP_FCBHIFENCE** type

PKG_ FCBHIFENCE package is a main part of FCBHIFENCE software. **FCBHIFENCE** package consists of two parts: a package specification and a wrapped package body.

Correspondent files:

- **fcbhifence/sql/cre_pkg_fcbhifence.pks**
- **fcbhifence/sql/cre_pkg_fcbhifence.pkb**

FCBHIFENCE package provides following encryption, decryption routines:

CHAR, VARCHAR2, STRING

- function fnc_encrstring (l_string in varchar2, l_receiver_list in typ_fcbhifence, l_mode in varchar2 default 'email') return varchar2
- function fnc_decrstring (l_string in varchar2) return varchar2

NCHAR, NVARCHAR2

- function fnc_encrnstring (l_string in nvarchar2, l_receiver_list in typ_fcbhifence, l_mode in varchar2 default 'email') return nvarchar2
- function fnc_decrstring (l_string in nvarchar2) return nvarchar2

CLOB

- function fnc_encrclob (l_clob in clob, l_receiver_list in typ_fcbhifence, l_mode in varchar2 default 'email') return clob;
- function fnc_decrclob (l_clob in clob) return clob;

NCLOB

- function fnc_encrnclob (l_nclob in nclob, l_receiver_list in typ_fcbhifence, l_mode in varchar2 default 'email') return nclob;
- function fnc_decrnclob (l_nclob in nclob) return nclob;

Please look at the **fcbhifence/test** and **fcbhifence/exm** directories for examples how crypto routines could be used.

DATA ACCESS SEPARATION

In FCBHIFENCE context's data access separation means possibility to have a table with, for example, clob type column the column related rows encrypted by the different public keys. Therefore only correct paired private key can decrypt relating rows. To simplify data ownership detection every FCBHIFENCE encryption function has **l_mode** input parameter. If **l_mode** = 'db' then encrypted data look like

```
to:scotttiger@localhost.com,phi@hospital.com,person12@localhost.com,

-----BEGIN PGP MESSAGE-----

hQIMA1+7rgLa3qUAAQ/8DSCEC6c47CLulyTTIO2UrmUKWU0sthiOgE3bf8P3OdfD
....
```

```
68J8nppZDqhX5+HIwEY6sm6tCsICTtnpv+5FdZwYz0WmzRaU
=FZmE
-----END PGP MESSAGE-----
```

where at the top you can see a list of persons and groups whose public keys were used to encrypt data. Therefore data can be decrypted only by those persons' or groups' private keys.

If **l_mode** = 'email' then encrypted data look like

```
-----BEGIN PGP MESSAGE-----

hQIMA1+7rgLa3qUAAQ/8DSCEC6c47CLulyTTIO2UrmUKWU0sthiOgE3bf8P3OdfD
....
68J8nppZDqhX5+HIwEY6sm6tCsICTtnpv+5FdZwYz0WmzRaU
=FZmE
-----END PGP MESSAGE-----
```

Decryption private key rules are the same.

RESTRICTIONS

There are no ways to store asymmetrically encrypted data in Oracle table data types like date, timestamp, float, number.

DATA COMPRESSION

FCBHIFENCE software provides indirect data compression possibility via GnuPG software. Please examine **fcbhifence/bin/fcbhifence_encr.sh** file. **"-z 9"** option is for compression.

TESTS AND EXAMPLES

Please look at the **fcbhifence/test, fcbhifence/exm** directories and **readme.first** file:

```
$ ls -la test
total 32K
drwxrwxr-x. 2 oracle dba 4.0K Apr 17 10:17 ./
drwxrwxr-x. 6 oracle dba 4.0K Apr 17 10:22 ../
-rw-rw----. 1 oracle dba  100 Apr 16 14:17 about.sql
-rwxrwx---. 1 oracle dba 6.6K Apr 17 10:16 clob_test.sh
drwxr-xr-x. 2 oracle dba 4.0K Apr 17 08:12 keys/
-rwxrwx---. 1 oracle dba 5.5K Apr 17 10:17 nclob_test.sh
-rwxrwx---. 1 oracle dba 2.3K Apr 17 10:16 string_test.sh
-rw-r--r--. 1 osir   dba 3.1K Apr 19 09:27 readme.first
-rwxrwx---. 1 oracle dba 2.4K Apr 17 10:16 nstring_test.sh

$ ls -la exm
total 24K
```

```
drwxr-xr-x. 2 oracle   dba 4.0K Apr 17 10:17 ./
drwxrwxr-x. 6 oracle   dba 4.0K Apr 17 10:22 ../
-rwxrwxr--. 1 oracle   dba 1.5K Apr 17 10:16 decr_clob_local.sh
-rwxrwxr--. 1 oracle   dba  576 Apr 11 17:59 exp_pubkey_local.sh
-rwxrwxr--. 1 oracle   dba  198 Apr 11 18:00 list_localpubkey.sh
-rwxrwxr--. 1 oracle   dba  703 Apr 17 10:17 upload_localpubkey.sh
```

VERSION

```
$ sqlplus ******/******
...
SQL> set serveroutput on
SQL> exec pkg_fcbhifence.prc_about;

FCBHifence software v.1.1.22
Copyright (c) 2019, Olexandr Siroklyn. All rights reserved.
```

COPYRIGHTS

CONTACTS

Olexandr Siroklyn, Ukraine, Dnipo city, +380505771900