LICENSEAUDIT.COM

Encryption Script manual

Version 1.1

Introduction

This document is created for database and system administrators for the purpose of executing License Audit script's output data encryption. Basic understanding of working with Linux shell is highly recommended.

Technical Requirements
This script is written in PERL and requires following perl modules to be available on server:

- POSIX;
- Term::ANSIColor;
- MIME::Base64;
- Crypt::Mode::CBC;
- Text::ParseWords;
- Data::Dumper;

If any of these modules are missing, please install it using cpan. You can read more about cpan here: http://www.cpan.org/modules/INSTALL.html

Execution permissions
To execute this encryption perl script regular Linux user permissions are enough.

Output Files Encryption Process

To encrypt previously collected audit scripts output, you have to do the following steps:

Unzip files.
Unzip lca-output-masking.zip archive into some location
i.e. /home/user/lca-output-masking/ folder
After extracting you should have following files and folders structure;

outputs - folder where you should place collected outputs from your databases, which you have previously collected with LCA Audit sql script.
outputs_encrypted - folder where files with encrypted data will be located
MaskFiles.pl - perl script for data encryption

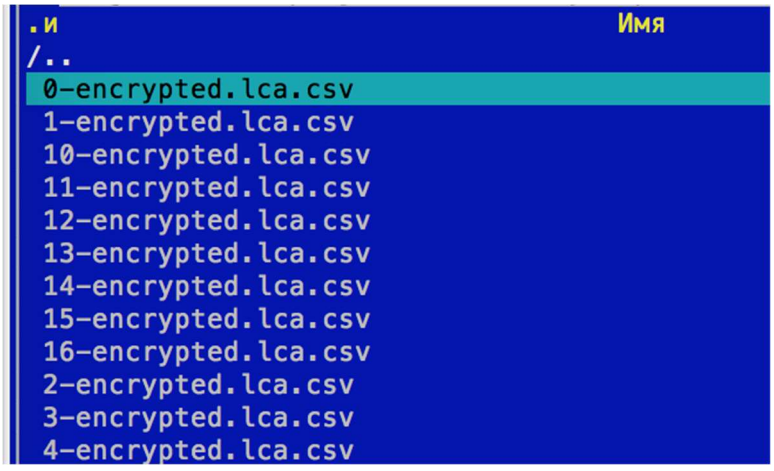
Encrypt outputs.
After you have placed database outputs into the 'outputs' folder, you can run **MaskFiles.pl** file using command **./MaskFiles.pl**. You should see a screen like this:

```
bash-3.2$ ./MaskFiles.pl

                Welcome to LICENSEAUDIT.COM encryption tool.


This tool is designed to encrypt all sensitive data in outputs you got after runing audit sql script on your databases.
In order to encrypt your data with AES-256 encryption method, you have to provide encryption key and initialization vector.

Encryption key length should be 32 characters.
Initialization vector length should be 16 characters.
You can use auto for key and initialization vector values, in that case they will be automatically generated randomly.

NOTE:Store encryption key and initialization vector in safe place.


Please choose desired action below:
1 - Encrypt outputs
2 - Decrypt  string

Choose Action [1] >
```

Please press 1 to encrypt outputs. Enter your encryption key and initialization vector values.

```
Choose Action [1] > 1
Please provide your secret key and initialization vector values below:
Please enter your Secret Key (32 chars) [auto] > type-your-secret-key-here-32-chr
Please enter your initialization vector (16 chars)  [auto] > type-your-init-v


Your Encryption Parameters:
Secret Key: type-your-secret-key-here-32-chr
Initialization Vector: type-your-init-v


Starting encryption process. Please wait...

Status: Processed 17 from 17. 100% Completed.

Encryption finished successfully!
```

All done. Now your **outputs_encrypted** folder contains masked outputs.



If you open any file you should see masked data, like this:

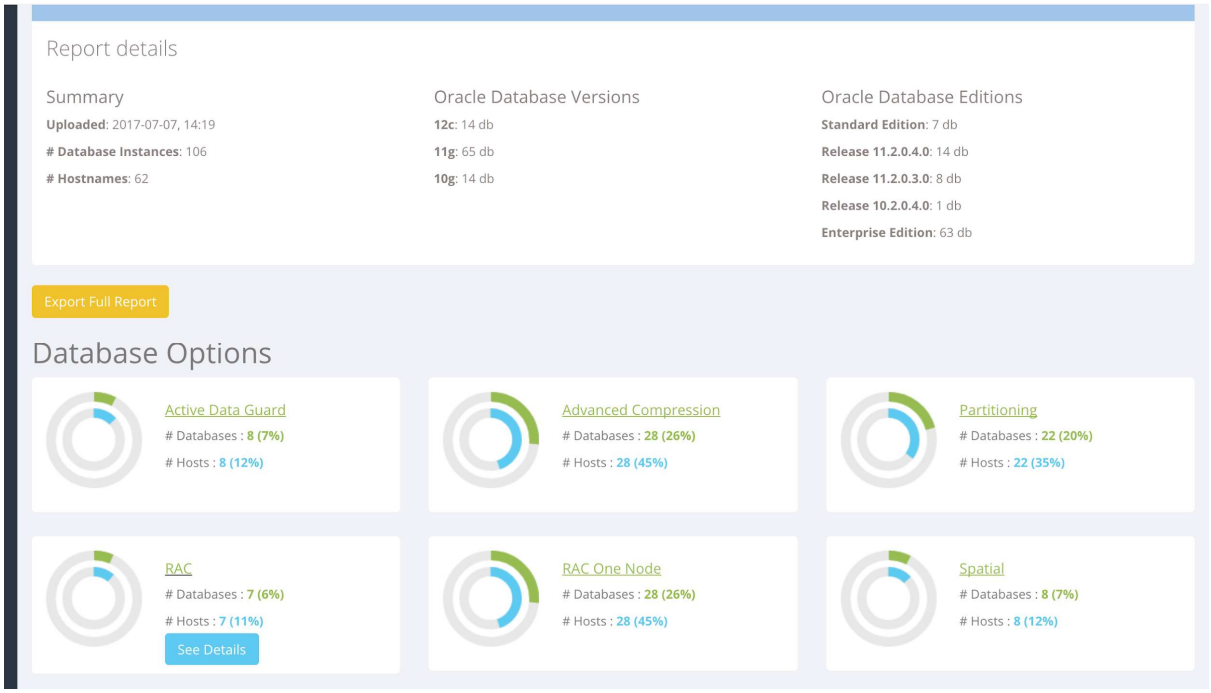
```
SECTION:STBY_C,V$DATAGUARD_CONFIG
"3f82f95b7f4319bce9c8d65d6a880fd5","<LCA>"
SECTION:STBY_C,V$ARCHIVE_DEST_STATUS
SECTION:ACTIVE_DATA_GUARD,11gr1
SECTION:ACTIVE_DATA_GUARD,V$DATABASE
"17717","3f82f95b7f4319bce9c8d65d6a880fd5","3f82f95b7f4319bce9c8d65d6a880fd5","READ WRITE","PRIMARY","ENA
SECTION:ACTIVE_DATA_GUARD,V$BLOCK_CHANGE_TRACKING
SECTION:RAC
"3f82f95b7f4319bce9c8d65d6a880fd5","d777f7efa32249dc9fa6b48d36a72730","1","OPEN","<LCA>"
```

Zip folder and upload
Now you can zip the **outputs_encrypted** folder and upload it to LicenseAudit.com

Uploading your output to licenseaudit.com

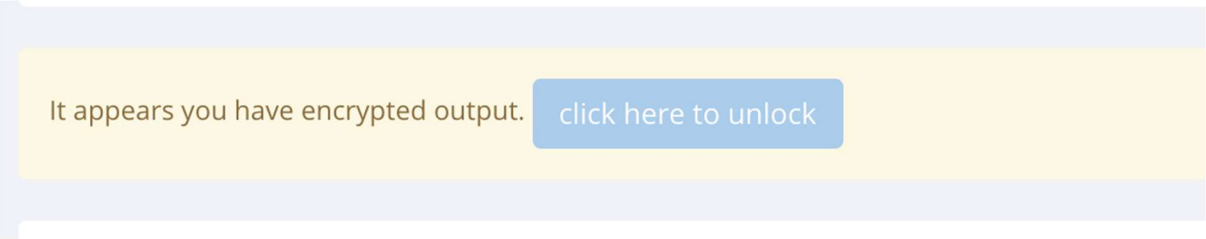
After data collection, upload it to https://oracle.licenseaudit.com to get detailed information about your packs, options and features usage. If you don't have an account yet, you can create it for free and then use the 'Upload' button to upload your data. If you already have an account, you can upload your data in your own Dashboard.

After analyzing your data, you will see the results similar to this example:

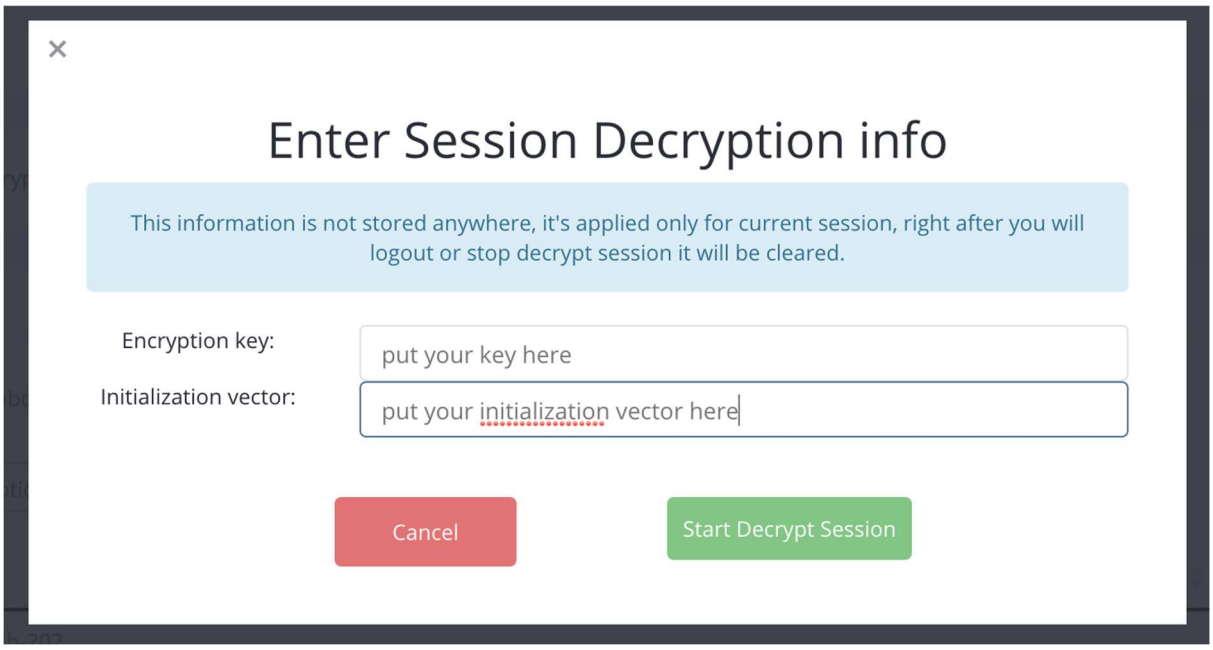


Furthermore, you will be able to see detailed info about databases and hosts which are using particular features and detailed explanation why this option has been marked as 'in use'.

Since you have uploaded encrypted output on details page you will see a notice like this:



If you want to see the analysis results online, click at the unlock button. Enter your encryption key and initialization vector values in the modal window:



Then click ‘Start Decrypt Session’, you’re now able to see decoded output online.

We do not store your encryption key and initialization vector values anywhere.

What if I don't want to enter my encryption key and initialization vector values anywhere?

We understand that your privacy matters, so there are other options to decrypt data on your end:

1) Translation table.
After you have ran the **./MaskFiles.pl** file, a new file appeared called **raw-encrypted-table.csv.** This is an automatically generated translation table, which contains
a table with raw and encrypted values for hosts, database names and it looks like this:

	A	B	C	D	E	F
1	Host Name	Istance Name	Database Unique Name	Host Name	Istance Name	Database Unique Name
2	host-204	db-204	db-204	324543d02b2277b106f4f36e61f165ce	bc9db7f432518ff6550b71306dfe38f3	bc9db7f432518ff6550b71306dfe38f3
3	host-146	db-146	db-uniq-146	d09c9b62f33e3eda0231fc528b1b68a0	a9f6f4a0ec8542112eaeb0aa88782132	0eb73d13038289359d4a7b792a97b5d5
4	host-101	db-101	db-101	5a07a3a0920f9f8fc84c9105135874e5	ed90223b32ae192556eaa8a75392d8f1	ed90223b32ae192556eaa8a75392d8f1
5	host-347	db-347	db-347	52332aa02eb76398cc0a10d09e70371d	76212a1e2e841dbfe4ac8a1fbc009507	76212a1e2e841dbfe4ac8a1fbc009507
6	host-202	db-202	db-202	de77ddd51bb7106ed668afb979722b6c	c20f40af5c0e678c23ef0b4195261bb1	c20f40af5c0e678c23ef0b4195261bb1
7	host-481	db-481	db-uniq-481	751986bc735e0100663e1f783791d735	74cb7d90e55401f172d9cc21ecadfdf2	5e7d568aba6005b3f68c85bd31e5d2ee
8	host-341	db-341	db-341	df94ec8263795a9c32ea9c2671f8f53d	fbe2a223266092e3bdeccb01ed8d67e6	fbe2a223266092e3bdeccb01ed8d67e6

You can open it in Excel, use the VLOOKUP functionality in Excel to connect it with encrypted xls report output you can get from https://oracle.licenseaudit.com

2) Decrypt any text using ./MaskFiles.pl functionality

Run the **./MaskFiles.pl** file and in desired action enter 2, like shown below:

```
bash-3.2$ ./MaskFiles.pl

                Welcome to LICENSEAUDIT.COM encryption tool.


This tool is designed to encrypt all sensitive data in outputs you got after runing audit sql script on your databases.
In order to encrypt your data with AES-256 encryption method, you have to provide encryption key and initialization vector.

Encryption key length should be 32 characters.
Initialization vector length should be 16 characters.
You can use auto for key and initialization vector values, in that case they will be automatically generated randomly.

NOTE:Store encryption key and initialization vector in safe place.


Please choose desired action below:
1 - Encrypt outputs
2 - Decrypt  string

Choose Action [1] > 2
```

Then enter your encryption key, initialization vector values and text to decrypt:

```
Choose Action [1] > 2
Please provide your secret key and initialization vector values below:
Please enter your Secret Key (32 chars) [auto] > type-your-secret-key-here-32-chr
Please enter your initialization vector (16 chars)  [auto] > type-your-init-v


Your Encryption Parameters:
Secret Key: type-your-secret-key-here-32-chr
Initialization Vector: type-your-init-v
Please enter text to decrypt > 3f82f95b7f4319bce9c8d65d6a880fd5
Decoded string: db-204
```

If you have any questions or comments, please feel free to contact us by e-mail
contact@licenceaudit.com