992-"Database audit files ETL" Installation manual

Table of Contents

3.1 Step 1: Downloading the Software 5

3.2 Step 2: Install Python scripts 5

3.3 Step 3: Configuring the Installation 6

3.4 Step 4: Completing the Installation 7

# Introduction

This manual provides detailed instructions for installing "Database audit files ETL". Please ensure to follow each step carefully to ensure a successful installation.

# System Requirements

Before beginning the installation, make sure your system meets the following minimum requirements:

* Operating System: Windows 10 or higher. Linux that supports Python 3.12.3
* Processor: Intel Core i5, CPU 1.60GHz - 1.80GHz
* RAM: 16.0 GB
* Disk Space: 5 GB available at least.
* **Python 3.12.3 installed.**
  + You could verify Python version get in python console for example:
    - *>py*  
      *Python 3.12.3 (tags/v3.12.3:f6650f9, Apr  9 2024, 14:05:25) [MSC v.1938 64 bit (AMD64)] on win32*  
      *Type "help", "copyright", "credits" or "license" for more information.*
* Internet Connection: Just for Python installation modules

# Installation Procedure

## Step 1: Downloading the Software

1. Access the official website of
2. Navigate to the downloads section.
3. Download Python scripts.

## Step 2: Install Python scripts

1. Once the download is complete, locate scripts files on your system and verify this files exists
   1. config.properties
   2. Extract\_and\_load.py
   3. Activity\_report\_generator.py
   4. Extractor.py
   5. Loader\_by\_db.py
   6. Compress\_aud\_files.py
   7. Compress\_db\_aud\_files.py
   8. Util\_files.py
   9. Util\_string.py
   10. Validate\_modules.py
2. Copy scripts files on a directory:
   1. Example 1, for windows: d:/projects/67-992-CBS-UPGRADE/06Scripts/desarrollo/new-scripts
   2. Example 2, for Linux: **/root/Scripts**
3. It is necessary validate Python installed modules, so, execute using Python the file Validate\_modules.py
   1. Example 1, for windows: *C:/Users/gonzalesv/AppData/Local/Programs/Python/Python312/****python.exe*** *d:/projects/67-992-CBS-UPGRADE/06Scripts/desarrollo/new-scripts/****Validate\_modules.py***
   2. Example 2, for linux: ***python3*** *“****/root/Scripts****/****Validate\_modules.py****”*
4. Result execution for success is (Realize that "NOK modules" section is empty):
   1. *OK modules:*  
      *1. Yes module named os*  
      *2. Yes module named logging*  
      *3. Yes module named configparser*  
      *4. Yes module named re*  
      *5. Yes module named datetime*  
      *6. Yes module named traceback*  
      *7. Yes module named glob*  
      *8. Yes module named sys*  
      *9. Yes module named shutil*  
      *10. Yes module named hashlib*  
      *11. Yes module named smtplib*  
      *12. Yes module named paramiko*  
      *13. Yes module named tarfile*  
      *14. Yes module named base64*  
      *15. Yes module named from Util\_string import getAuditedActivity, getDataBetween, getObjectNameFromQuery*  
      *16. Yes module named from scp import SCPClient*  
      *17. Yes module named from Util\_files import deleteDirContent, createSSHClient, read\_config, createAudFilesInLocalDir, writeScriptsChecksumInLog, getFilesQuantityInRemoteDir, getParamikoSSHCLient, getFilesQuantityInDir, compressFiles*  
      *18. Yes module named from Extractor import extractor*  
      *19. Yes module named from Loader\_by\_db import loader\_by\_db*  
      *20. Yes module named from Compress\_aud\_files import compress\_aud\_files*  
      *21. Yes module named from os.path import basename*  
      *22. Yes module named from email.mime.application import MIMEApplication*  
      *23. Yes module named from email.mime.multipart import MIMEMultipart*  
      *24. Yes module named from email.mime.text import MIMEText*  
      *25. Yes module named from email.utils import COMMASPACE, formatdate*

***NOK modules****:*

1. If some Python module is missing, then it will be listed in "NOK modules" section, for example.
   1. *NOK modules:*  
      *1.* ***No module named*** *'module\_example'*
2. Missing modules must be installed. You could follow official python guide in <https://docs.python.org/3/installing/index.html>
   1. Example: *python -m pip install SomePackage*

## Step 3: Configuring the Installation

1. Open file config.properties for edit. Review value of each parameter and change it according to your preferences and guide comments:
   1. *[EXTRACTION]*  
      *# AUD files will be extracted N days after they are created in remote server*  
      *old\_files\_in\_days\_to\_be\_extracted = 2*  
      *# 1: Delete destiny dir content before copy new data. 0: Does not delete destiny dir content before copy new data*  
      *delete\_destiny\_dir\_content = 1*  
      *# 1: Generate chesksum files. 0: Does not generate checksum files*  
      *generate\_checksum\_files = 0*  
      *# 1: Generate chesksum logs. 0: Does not generate checksum logs*  
      *generate\_chesksum\_log = 1*

*[COMPRESS]*  
*# Compress N months age imported AUD files*  
*compress\_imported\_aud\_files\_n\_months\_after = 2*  
*# Compress N months age organized by DB AUD files*  
*compress\_aud\_files\_organized\_by\_db\_n\_months\_after = 1*  
*# Compress log files where created last N month*  
*compress\_logs\_files\_n\_months\_after = 2*  
*# 1: Compress activity reports inmediatly. 0: Does not compress*  
*compress\_activity\_report\_inmedtaly = 2*

*[CBS\_SERVER]*  
*host = 10.24.0.30*  
*port = 22*  
*user = auditfiles*  
*password = XXXYYZZZ*  
*cbs\_base\_dir\_audit\_files = /auditlogs*  
*cbs\_sub\_dir\_list\_audit\_files =*  
*billdb-1-1-m-0*  
*billdb-1-1-m-1*  
*billsharedb-1-1-m-0*  
*billsharedb-1-1-m-1*  
*bmpdb-1-1-m-0*  
*bmpdb-1-1-m-1*  
*edrdb-1-1-m-0*  
*edrdb-1-1-m-1*  
*meddb-1-1-m-0*  
*meddb-1-1-m-1*  
*usrdb-1-1-m-0*  
*usrdb-1-1-m-1*  
*uvcdb-1-1-m-0*  
*uvcdb-1-1-m-1*

*[LOCAL\_SERVER]*  
*# Local directories*  
*local\_dir\_audit\_files = /home/arcsight/auditCBS*  
*local\_dir\_audit\_files\_by\_db =  /home/arcsight/auditCBS\_Processed*  
*local\_dir\_scripts =   /root/Scripts*  
*local\_dir\_logs =   /root/Scripts/logs*  
*local\_dir\_reports = /root/Scripts/reports*

*[MAIL]*  
*mailFrom = cbsaudit@domain.com*  
*mailTo =* [*informationsecurity@domain.com*](mailto:informationsecurity@domain.com)  
*mailSubject = "CBS Audit Trail LOG"*  
*mailBody = "Job Success"*  
*mailServer =* [*mailserver.com*](http://millicomhq.relay.tmes.trendmicro.com)  
*mailPort = 25*

*[ACTIVITY\_REPORT]*  
*# 1: Add summary report at the end of report. 0: Does not add summary report at the end of report*  
*add\_summary\_report = 0*

## Step 4: Completing the Installation

1. To verify installation, execute the following scripts:
   1. Example for windows: *C:/Users/gonzalesv/AppData/Local/Programs/Python/Python312/****python.exe*** *d:/projects/67-992-CBS-UPGRADE/06Scripts/desarrollo/new-scripts/****Extract\_and\_load.py***
   2. Example for windows: *C:/Users/gonzalesv/AppData/Local/Programs/Python/Python312/****python.exe*** *d:/projects/67-992-CBS-UPGRADE/06Scripts/desarrollo/new-scripts/****Activity\_report\_generator.py***
2. Review log file and report file in sub-directories "logs/" and "reports/" that there are no errors.
3. In case of errors, depending on error, correct configuration and return to step 1.
4. You could affirm that installation is finished if there are no errors in log file and report file.

# Technical Support

If you encounter any issues during the installation that you can't resolve or have any additional questions, feel free to contact our technical support team at vicogo@gmail.com.