BL3 -Database audit files ETL

Table of Contents

4.1 1.1. Management Summary 7

4.2 1.2. Glossary 7

4.3 1.3. Architecture goals and restrictions 7

4.3.1 1.3.1 Applicability of Secure Software Development 7

4.3.2 1.3.2 Known vulnerability in previous versions. 7

4.4 1.4. System Requirements View 8

4.4.1 1.4.1. Use Cases 8

4.4.2 1.4.2. Use Case Diagram 8

4.4.3 1.4.4. Presentation and Application delivery requirements 9

5.1 2.1 Vista Macro 10

5.2 2.1.1 Integrations & Services 11

6.1 2.2.1 Extract AUD files 12

6.2 2.2.1 Activity report generator 12

6.3 2.4. Development View 13

7.1 3.1. Infrastructure base requirements 14

7.2 3.2. Technology Description 15

**Blueprint Level 3 - Software Architecture**

Version 2023 1.0

# Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Autor |
| 29/04/2024 | 1.0 | First Version | Victor Hugo Gonzales |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Approval History

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Revised by | Role | Date | Approved/Rejected | Observations |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Software Architecture

# 1. SOLUTION DESCRIPTION

## 1.1. Management Summary

For security area, is necessary to upgrade an application "Database audit files ETL" that currently works for CBS platform, R5.5 version and now, must work with R23 version.

This ETL application must continue report all audited activities from CBS R23 database users, like DBAs or support team. The database audited activities are: Insert, Update, Delete, Truncate and Drop.

## 1.2. Glossary

|  |  |
| --- | --- |
| Term | Definition |
| ETL | Extract Transform and Load |
|  |  |
|  |  |

## 1.3. Architecture goals and restrictions

Architecture goals

* All ETL process must be orchestrated. This characteristic could improve current architecture.

Restrictions

* Audit files were changed, before, in CBS R23 version, was XML files for each SQL instruction. Now, in CBS R5.5 version, audit files with SQL instructions will come in files with 10MB or less.

### 1.3.1 Applicability of Secure Software Development

|  |  |  |
| --- | --- | --- |
|  | YES | NO |
| Internet facing application |  | X |
| Application for end customers |  | X |
| Will process personally identifiable information (PII)? |  | X |
| Will process authentication information? |  | X |
| Will process other confidential information (eg financial, medical information, others)? |  | X |

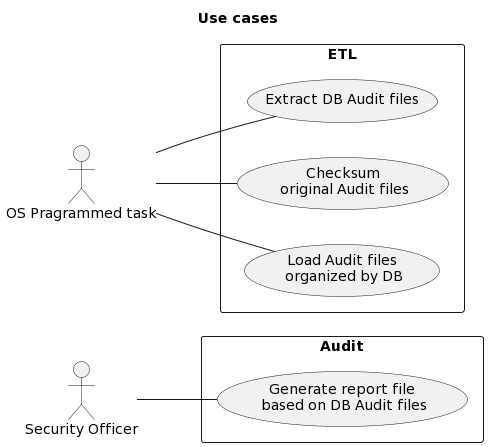
### 1.3.2 Known vulnerability in previous versions.

None.

## 1.4. System Requirements View

### 1.4.1. Use Cases

### 1.4.2. Use Case Diagram



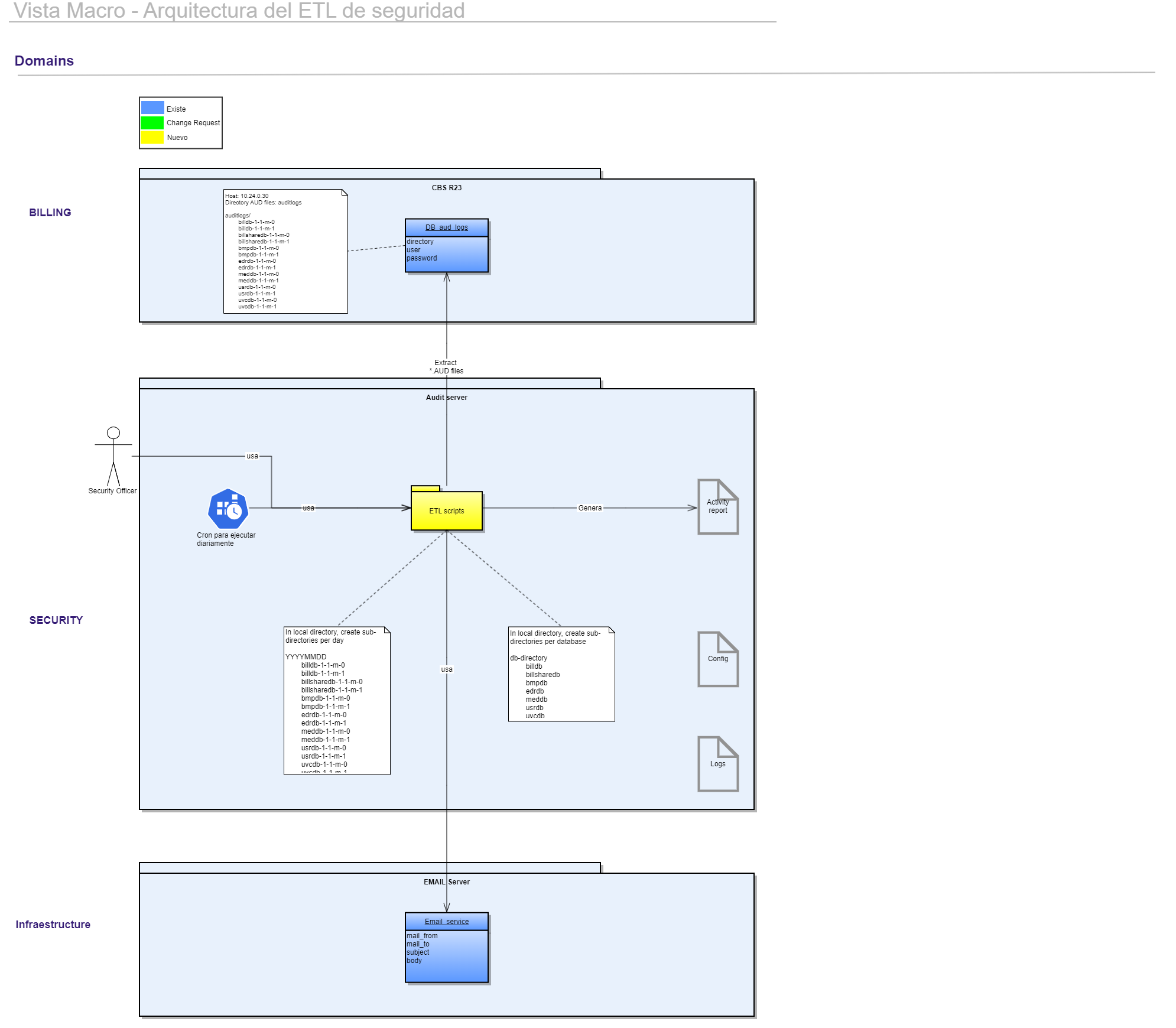
|  |  |  |
| --- | --- | --- |
| Use Case Name | Functionality Description | Use Case Confluence Route |
| Generate report file based on DB Audit files | AUD files must be parsed looking for audited activities (Insert, Update, Delete, Truncate and  Drop) that are in SQL statements.  This report must consider all AUD files from a defined month.  Report must contain the following data:   * Fecha y Hora: SQL execution date * Usuario de BD: SQL execution user * Hostname: Server address * Linea: Line number in a parsed file where is SQL. * Actividad: Audit activity found parsing SQL (Insert, Update, Delete, Truncate and Drop) * Schema: Database schema where SQL were executed. * Table: Table name involved in SQL statement * Query: SQL statement. * Archivo: AUD File name parsed. |  |
| Extract DB Audit files | Daily copy AUD files from CBS R23 server in a local server (where resides ETL scripts)  Copy process must be logged |  |
| Checksum original Audit files | A checksum for each copied file must be generated and saved in a log file |  |
| Load Audit files organized by DB | Daily copied AUD must be organized, in another directory in local server, by database |  |

### 1.4.4. Presentation and Application delivery requirements

The ETL application does not have a user interface. Scripts will be executed by shell on demand or programmed job.

# 2. SOLUTION ARCHITECTURE

## 2.1 Vista Macro

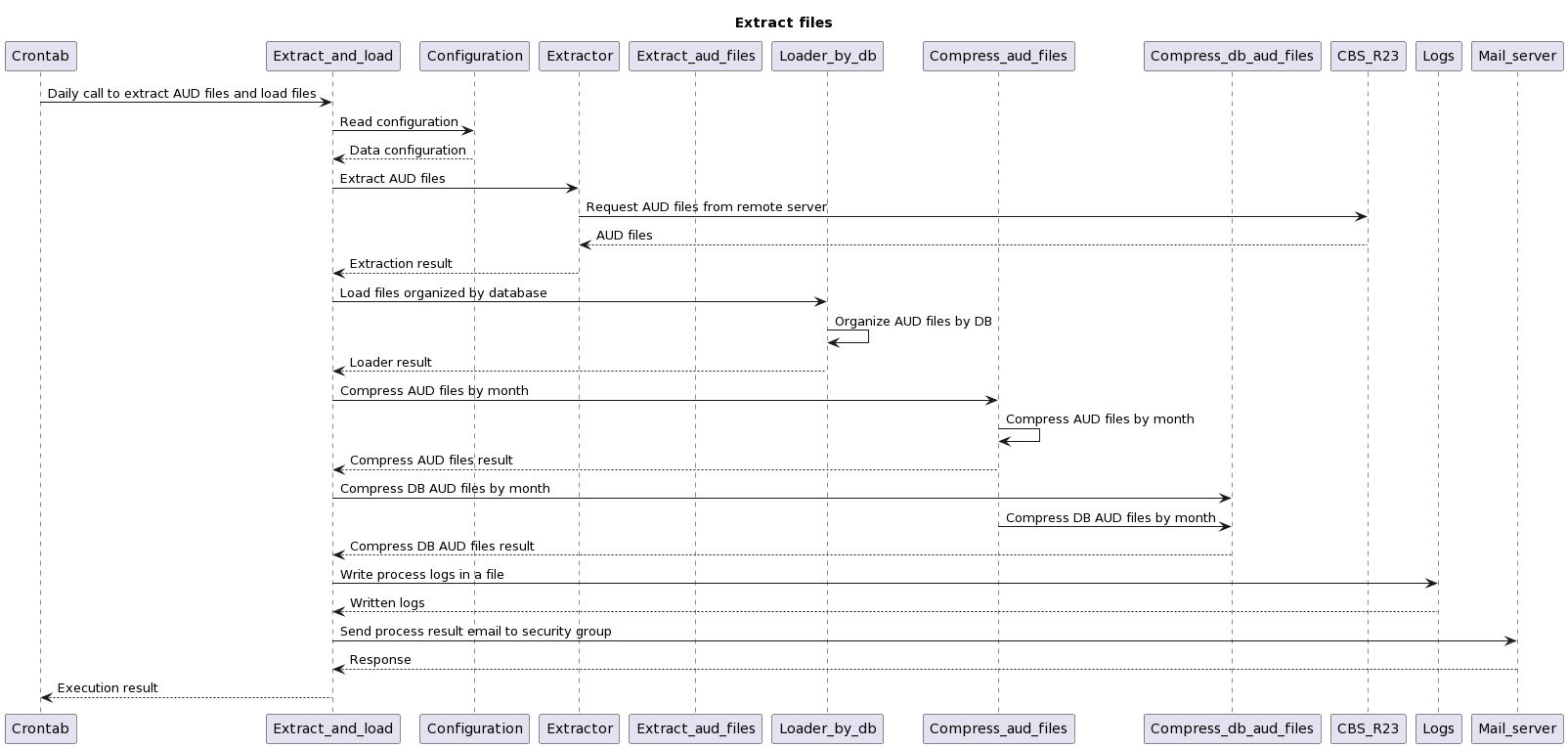


## 2.1.1 Integrations & Services

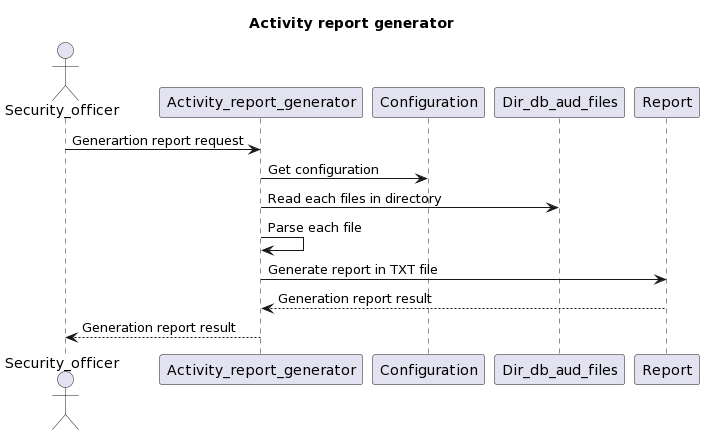
|  |  |  |  |
| --- | --- | --- | --- |
| Name | Functional Description | Technology (Web Service, ISO8583, Text…) | Integration document: Confluence route |
| Extractor | Extract \*.aud files from remote server CBS R23 | SSH, port 22. SCP command |  |
| Mail | Send mail after extraction process finished, reporting the result | SMTP using mail server.  millicomhq.relay.tmes.trendmicro.com |  |

# 2.2 Process View

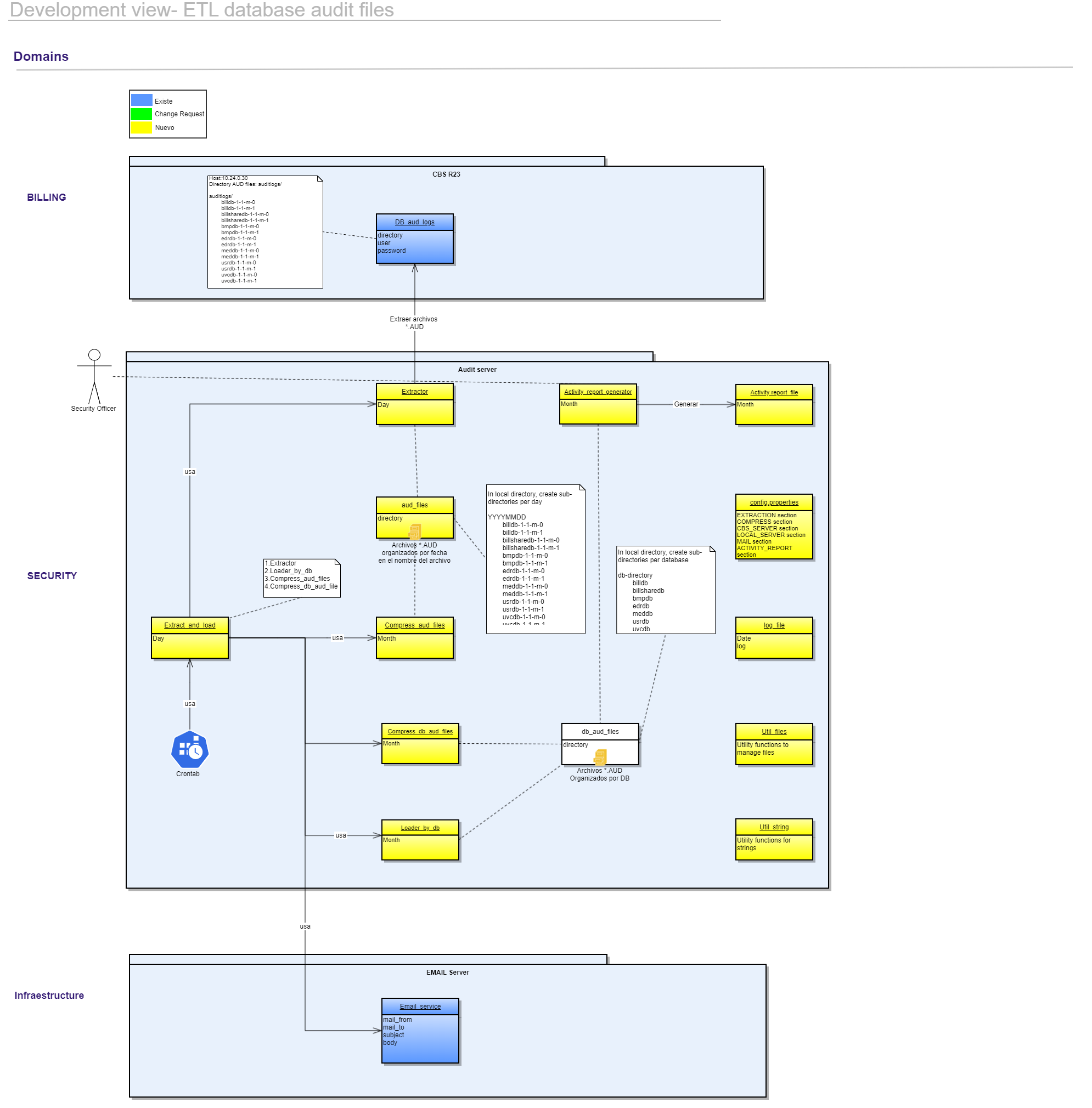
## 2.2.1 Extract AUD files



## 2.2.1 Activity report generator



## 2.4. Development View



# 3. Physical View

## 3.1. Infrastructure base requirements

|  |  |
| --- | --- |
| Performance and maintenance | |
| Quantity of transactions (Annual) |  |
| Number or application users |  |
| Frequency of data application backup, volume and retention |  |
| **Infrastructure Requirements** | |
| Architecture application type |  |
| Application availability level |  |
| Estimated growth rate |  |
| Application peak processing capacity |  |
| Connectivity and type of connectivity with other systems |  |
| Require file server |  |
| Client installation type |  |
| Client stations geographic placing |  |
| Requires email accounts or SMS Center |  |
| Management dedicated stations |  |
| **Network Requirements and Signaling** | |
| Is there a requirement for new connection links to the Telecel network? |  |
| It is required remote connection, through firewall, either for the project, testing or later support? |  |
| Define the required availability for communication links involved in service to implement. Or the total expected Service availability. |  |
| Number of signaling links and used protocol |  |

## 

## 3.2. Technology Description

|  |  |
| --- | --- |
| Definition about technologies that will be used to implement the solution | |
| Development Platform |  |
| Development language | **Python 3.12.3** |
| IDE | Visual Studio Code |
| Framework | None |
| Presentation schema | Interaction by console |