1. Software Introduction

Nemesys® is a new generation of network management software developed by TSDA to meet the growing demands and needs of its customers.

A WEB application based on SOA architecture (Service Oriented Architectures) and has the characteristic of a scalable system.

2. System Overview

The image below presents the system in general, showing its functionality and operability.

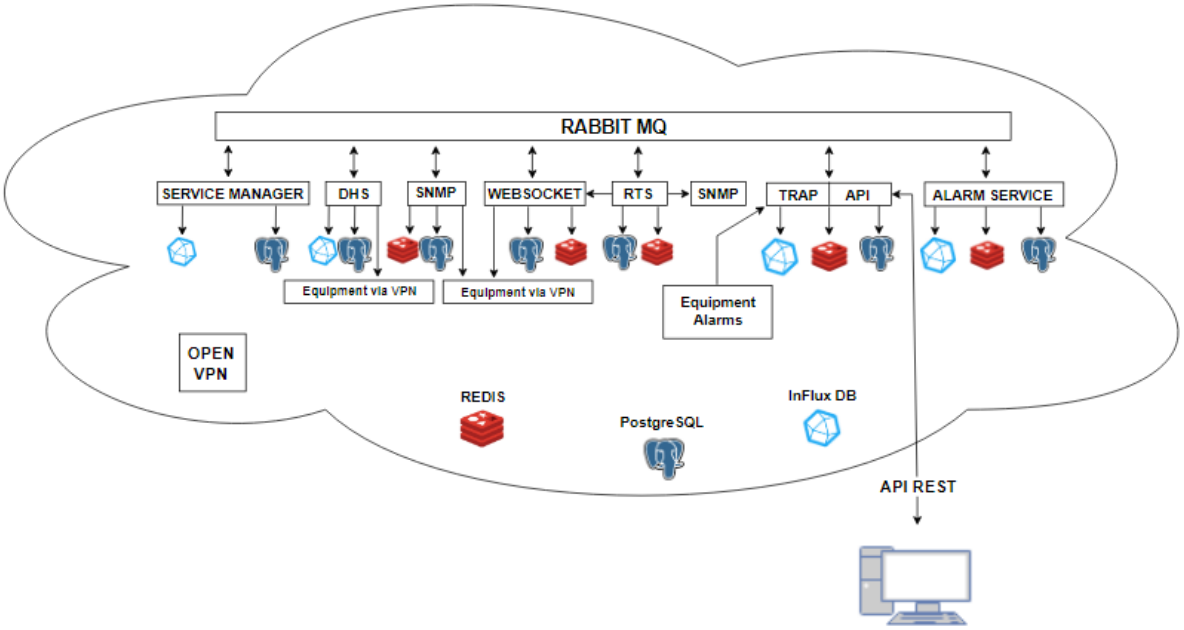

FIGURE 1 – NEMESYS® OVERVIEW

3. System Details

3.1. Database

The system uses three databases, namely, REDIS, PostgreSQL and InFlux DB. Each database is responsible for storing different data.

- **REDIS:** It is used for caching real-time data and tokens;
- **PostgreSQL:** It is used to configure users, teams, equipment, etc;
- **InFlux DB:** It is used to store historical data, for example, metrics, alarm histories, system logs, etc.

3.2. RabbitMQ

RabbitMQ is a message broker used for communication between services. It is responsible for mediating all system communication.

3.3. API Manager

The API Manager is a Rest API responsible for all communication with the end user, performing all configurations of users and equipment and is also an input for searching metric data.

3.4. Service Manager

The Service Manager is responsible for controlling the other services and listening to the Logs.

3.5. Alarm Service

The Alarm Service listens for alarm and alarm validation messages through RabbitMQ and processes them, notifying end users according to the system configuration.

3.6. DHS

The Data History Service (DHS) is responsible for fetching the historical data of all containers by storing them in the historical database.

3.7. RTS

The Real Time Services (RTS) is responsible for keeping the equipment's real-time data updated in the cache as long as necessary.

3.8. SNMP

The SNMP service is responsible for communicating with equipment using the SNMP protocol, serving as a communication tool for others services.

3.9. Websocket

It is a service responsible for communicating with equipment using Websocket, more specifically with TSDA's new FLEX line.

3.10. Traps

It is a feature of SNMP that allows the managed equipment to send information to the server in previously programmed alarm situations.

3.11. Open VPN

For secure and encrypted access to your equipment, the Open VPN Client is used.

4. System Security

The system security is presented below through the flowcharts.

4.1. Login Creation

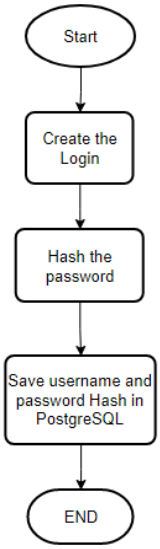

FIGURE 2 – LOGIN CREATION FLOWCHART

Note: Communication between the client and the API is done using the HTTPS protocol.

4.2. Login Request

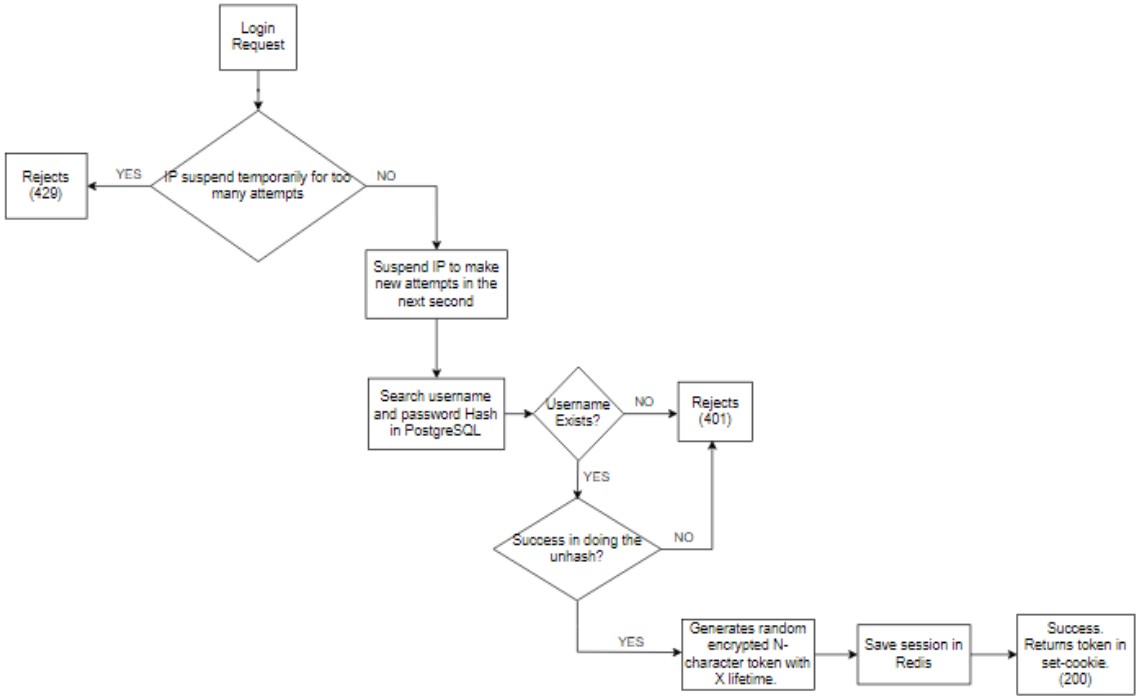

FIGURE 3 – LOGIN REQUEST FLOWCHART

Notes:

- Token size and lifetime can be configured at server startup. Default is 64 characters and one week to live;
- If another session is already saved, it will be overwritten and its token becomes invalid.