1. Introdução ao Software

O Nemesys® é uma nova geração de software de gerência de rede desenvolvido pela TSDA para atender as crescentes demandas e necessidades de seus clientes.

Uma aplicação WEB baseada na arquitetura SOA (Service Oriented Arquitectures) e possui a característica de um sistema escalável.

2. Visão Geral do Sistema

A imagem abaixo apresenta o sistema de maneira geral, mostrando sua funcionalidade e operabilidade.

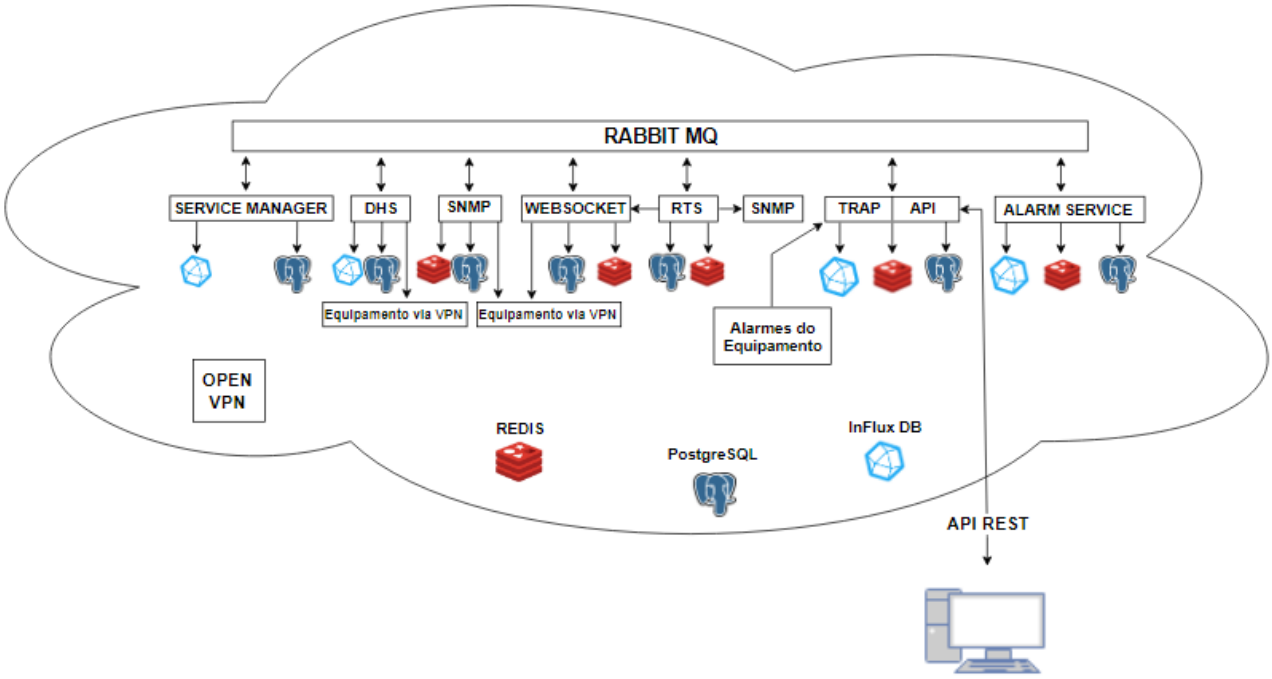

FIGURA 1 – VISÃO GERAL NEMESYS®

3. Detalhes do Sistema

3.1. Bancos de Dados

O sistema utiliza três bancos de dados, sendo eles, REDIS, PostgreSQL e InFlux DB. Cada banco de dados é responsável por armazenar dados diferentes.

- **REDIS:** É utilizado para cache de dados em tempo real e tokens;
- **PostgreSQL:** É utilizado para configuração de usuários, times, equipamentos e etc;
- **InFlux DB:** É utilizado para armazenar histórico de dados, por exemplo, métricas, históricos de alarme, logs do sistema e etc.

3.2. RabbitMQ

O RabbitMQ é um distribuidor de mensagens utilizado para a comunicação entre os serviços. Ele é responsável por intermediar toda comunicação do sistema.

3.3. API Manager

O API Manager é uma API Rest responsável por toda comunicação com o usuário final, realizando toda configuração de usuários e equipamentos e também é entrada para busca de dados de métricas.

3.4. Service Manager

O Service Manager é responsável por controlar os demais serviços e escutar os Logs.

3.5. Alarm Service

O serviço de alarme escuta mensagens de alarme e validação de alarmes através do RabbitMQ e as processa, notificando os usuários finais de acordo com a configuração do sistema.

3.6. DHS

O Data History Service (DHS) é responsável por buscar os dados de histórico de todos os container armazenando-os no banco de histórico de dados.

3.7. RTS

O Real Time Services (RTS) é responsável por manter os dados de tempo real do equipamento atualizado no cache enquanto for necessário.

3.8. SNMP

O serviço SNMP é responsável por fazer a comunicação com os equipamentos utilizando o protocolo SNMP, servindo como uma ferramenta de comunicação para os outros serviços.

3.9. Websocket

É um serviço responsável por fazer a comunicação com equipamentos utilizando Websocket, mais especificamente com a nova linha FLEX da TSDA.

3.10. Traps

É uma característica do SNMP que possibilita que o equipamento gerenciado envie informações ao servidor em situações previamente programadas de alarmes.

3.11. Open VPN

Para um acesso seguro e criptografado a seus equipamentos, é utilizado o Cliente Open VPN.

4. Segurança do Sistema

A segurança do sistema é apresentada abaixo através dos fluxogramas.

4.1. Criação de Login

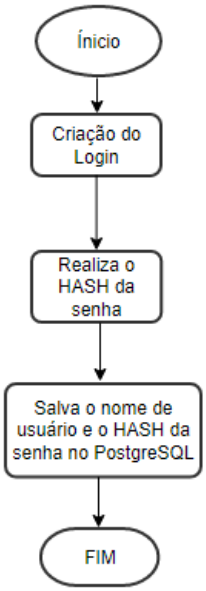

FIGURA 2 – FLUXOGRAMA CRIAÇÃO DE LOGIN

Observação: A comunicação entre o cliente e a API é feita pelo protocolo HTTPS.

4.2. Requisição de Login

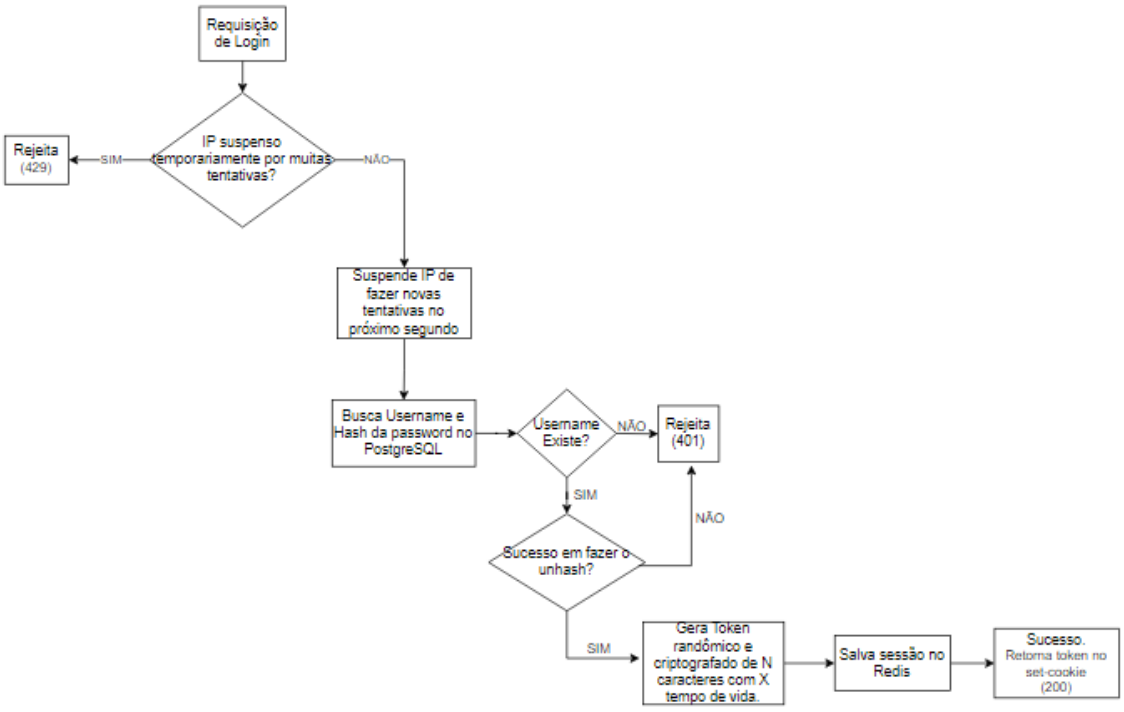

FIGURA 3 – FLUXOGRAMA REQUISIÇÃO DE LOGIN

Observações:

- O tamanho do token e seu tempo de vida podem ser configurados na inicialização do servidor. O padrão é 64 caracteres e uma semana de tempo de vida;
- Se outra sessão já estiver salva, ela será sobrescrita e seu token se torna inválido.