



Relatório de Estágio

Serviço de Monitorização

Diogo Alexandre Cambão Pinto

N.º 18844 – Regime Pós-laboral

Orientação

Doutor Luís Gonzaga Martins Ferreira

Ano letivo 2022/2023

Licenciatura em Engenharia de Sistemas Informáticos

Escola Superior de Tecnologia

Instituto Politécnico do Cávado e do Ave

Identificação do Aluno

Diogo Alexandre Cambão Pinto

Aluno número 18844, regime pós-laboral

Licenciatura em Engenharia de Sistemas Informáticos

Orientação

Dr. Professor Luís Gonzaga Martins Ferreira

Professor Adjunto

Informação sobre o Estágio

RTU – Ricardo Terleira Unipessoal, LDA

Avenida da Abelheira, N°41

Bloco 3 R/C

4900-926, Viana do Castelo

Orientação de Ricardo Terleira

RESUMO

Este documento descreve as atividades desenvolvidas durante um período de estágio, compreendido entre 6 de fevereiro e 4 de maio de 2023 na empresa Ricardo Terleira, Unipessoal, Lda, doravante descrita como RTU.

A RTU, criada em 2018, está inserida num contexto empresarial geograficamente desafiante e demonstra, quando desafiada, a vontade de compreender e beneficiar as mais recentes novidades ao nível de engenharia em sistemas na área das tecnologias de informação, bem como, compreender de que forma, uma solução, como a que aqui se apresentará, poderia contribuir para responder a uma pergunta tão simples como:

De que forma poderemos enfrentar as dificuldades crescentes do aumento de pedidos de suporte atuando de forma preventiva e aumentando a notoriedade junto dos atuais e potenciais clientes, demonstrando a capacidade de execução e resolução de problemas e, dessa forma, tornando o processo de crescimento ainda mais ágil e economicamente viável?

Após algumas reuniões de contextualização, tornou-se claro, ainda que, de forma hipotética, havia uma necessidade específica.

Foi proposto o desenvolvimento de um programa de monitorização, uma ferramenta, em código aberto, para controlar e gerir um parque informático completo, incluindo também, ativos de rede e servidores de armazenamento de dados permeáveis, capaz de entregar, num formato específico, informação para que a RTU prontamente interprete e dê resposta.

Tendo os pressupostos do projeto alinhados, o presente relatório está estruturado em torno das atividades realizadas durante o período de estágio, com foco especial na implementação de um serviço de controlo. Serão apresentados os objetivos do estágio, a descrição do serviço de monitorização proposto, a metodologia utilizada na implementação do serviço, os resultados obtidos e as considerações finais.

AGRADECIMENTOS

Gostaria de expressar a minha sincera gratidão a todas as pessoas que tornaram possível a realização deste estágio e, conseqüentemente, a conclusão deste relatório. Em primeiro lugar, agradeço a Ricardo Terleira, o meu mentor durante todo o estágio, por estar sempre presente, disponível e por proporcionar uma experiência profissional enriquecedora. Agradeço também ao Professor Luís Ferreira, pela orientação, pelo apoio e pela partilha de conhecimentos e ideias que foram fundamentais para o desenvolvimento do projeto.

Não posso deixar de agradecer aos meus pais, Adélio e Silvia, pelo apoio incondicional que me deram ao longo de todo o meu percurso universitário. Agradeço também aos meus avós, por estarem sempre presentes e por serem uma fonte de inspiração.

Agradeço à equipa da empresa em que estagiei, em especial ao Rodolfo Moreira, por fazerem parte deste percurso e por contribuírem para o meu crescimento profissional.

Um agradecimento especial é reservado para os meus amigos e, particularmente, para a Daniela, cujo apoio foi essencial durante este percurso.

A todos, o meu sincero obrigado!

ÍNDICE

1.	Introdução.....	1
1.1.	Objetivos	2
1.2.	Contexto.....	3
1.3.	Estrutura do documento	4
2.	Estado da Arte	5
2.1.	Soluções Existentes.....	5
2.1.1.	Critérios de comparação das soluções	6
2.2.	Zabbix	6
2.2.1.	Zabbix Server.....	7
2.2.2.	Zabbix Proxy	8
2.2.3.	Zabbix Agent.....	9
2.2.4.	Zabbiz Hosts	10
2.2.5.	Zabbix Templates.....	10
2.3.	Infraestrutura do Servidor Zabbix.....	11
2.3.1.	Servidor Virtual Privado	11
3.	Análise e especificação de requisitos	12
3.1.	Requisitos funcionais	12
3.2.	Requisitos não funcionais	13
3.3.	Entidades e relações.....	14
3.3.1.	Entidades Críticas.....	14
3.3.2.	Engenharia Reversa da Base de Dados	16
4.	Implementação	17
4.1.	Primeira Fase.....	19
4.1.1.	A001 – Ambiente de Instalação	19
4.1.2.	A002 – Firewall e Ligações Externas.....	19

4.1.3.	A003 – Requisitos para Instalação	20
4.2.	Segunda Fase	21
4.2.1.	B001 – Análise da Documentação	21
4.2.2.	B002 – Instalação do Zabbix	21
4.2.3.	B003 - Arranque Inicial	22
4.3.	Terceira Fase	24
4.3.1.	C001 – Estudo de Clientes	24
4.3.2.	C002 - Sistemas Críticos	24
4.3.3.	C003 - Proxies	26
4.3.4.	C004 – Integração Clientes	27
4.3.5.	C005 – Integração dos Proxies	30
4.3.6.	C006 – Integração dos Sistemas	32
4.3.7.	C007 – Métricas dos Sistemas	34
	C008 – Alertas e Notificações	36
5.	Análise de Resultados	38
5.1.	Análise de Métricas Específicas	38
5.2.	Histórico de Dados	39
6.	Conclusões e Trabalhos Futuros	41
6.1.	Plano de Formação	41
6.2.	Configuração do Painel de Cliente	41
6.3.	Políticas de Segurança – Retenção e Integridade dos Dados	42
6.4.	Análise de Padrões, Predição de Comportamentos e I.A.	42

ÍNDICE DE FIGURAS

Figura 1 - Módulo Proxy em produção.....	8
Figura 2 - Módulo Zabbix Proxy.....	9
Figura 3 – Esquema de entidades do Zabbix	14
Figura 4 - Processo Desenvolvimento	17
Figura 5 - Paineil boas-vindas	22
Figura 6 - Configuração Ligação BD.....	23
Figura 7 - Visão Global Zabbix	23
Figura 8 - Servidor Cliente B - Host	29
Figura 9 - Configuração módulo Agente em ambiente Windows	30
Figura 10 - Configuração Proxy	31
Figura 11 - Configuração Encriptação Proxy	31
Figura 12 - Configurações Servidor Cliente B.....	32
Figura 13 - Inserção de Macros	32
Figura 14 – Encriptação do Host	33
Figura 15 - Métricas CPU – Dispositivo Servidor Cliente B	35
Figura 16 - Métricas Rede - Dispositivo AP-IW Cliente A	35
Figura 17 - Métricas Disponibilidade - Dispositivo AP-U6PRO Cliente A.....	35
Figura 18 - Triggers Dispositivo AP-IW Cliente A	36
Figura 19 - Configuração Telegram na Interface Web	37
Figura 20 - Código QR.....	38
Figura 21 - Relatório de Disponibilidade	39
Figura 22 - Gráfico de Clientes AP-U6PRO.....	39
Figura 23 - Configuração da retenção de dados.....	40

ÍNDICE DE TABELAS

Tabela 1 – Ferramentas existentes	5
Tabela 2 - Critérios decisivos das soluções	6
Tabela 3 - Requisitos funcionais	12
Tabela 4 - Requisitos não funcionais	13
Tabela 5 - Descrição Primeira Fase	18
Tabela 6 - Descrição Segunda Fase	18
Tabela 7 - Descrição Terceira Fase	18
Tabela 8 - Sistemas Críticos Cliente A.....	25
Tabela 9 - Sistemas Críticos Cliente B.....	25
Tabela 10 - Protocolos usados nos Sistemas Críticos	25
Tabela 11 – Parâmetros Configuração Host	33
Tabela 12 - Parâmetros dos Sistemas Críticos	34

Glossário

Agent – Software que recolhe informações de um sistema ou rede e as envia para um servidor central.

Apache – Um servidor web de código aberto que é um dos mais utilizados para entregar conteúdo web.

Backup - Cópia que se destina a guardar dados armazenados no caso de uma eventual perda de informação.

Firewall – Sistema de segurança que controla o tráfego de entrada e saída numa rede com base em regras pré-determinadas. Ajuda a proteger redes contra acessos não autorizados.

Hosts – Computadores ou outros dispositivos conectados a uma rede que são identificados por um endereço IP único.

Macros – No contexto do Zabbix, são utilizadas como variáveis configuráveis que permitem a personalização de configurações e notificações de forma dinâmica.

MySQL – Sistema de gestão de base de dados.

PostgreSQL – Sistema de gestão de base de dados.

Proxies – Servidores intermediários entre um utilizador e a internet, utilizados para filtrar solicitações, melhorar a segurança e armazenar conteúdos em cache para acelerar o acesso.

Proxy – Versão singular de Proxies; um servidor que atua como intermediário para pedidos de recursos por parte de um cliente à procura de recursos de outro servidor.

Templates – No Zabbix, referem-se a conjuntos predefinidos de elementos de monitorização, como itens, triggers, gráficos, e descobertas de rede, que podem ser aplicados a múltiplos hosts ou aplicações de forma a padronizar e facilitar a configuração.

Token API – Chave de segurança utilizada na comunicação entre aplicações e APIs. Serve para autenticar e autorizar acessos ou transações.

Triggers – Mecanismos automáticos ativados por eventos específicos dentro de um sistema de base de dados, usados para assegurar a integridade dos dados ou automatizar tarefas.

Siglas e Acrónimos

BD – Base de Dados

CPU – Central Processing Unit (Unidade Central de Processamento)

IP – Internet Protocol (Protocolo de Internet)

ODBC – Open Database Connectivity (Conexão Aberta de Base de Dados)

PVE – Proxmox Virtual Environment (Ambiente Virtual Proxmox)

PSK – Pre-Shared Key (Chave Pré-Partilhada)

SNMP – Simple Network Management Protocol (Protocolo Simples de Gestão de Rede)

SSH – Secure Shell (Shell Seguro)

TCP – Transmission Control Protocol (Protocolo de Controlo de Transmissão)

TI – Tecnologias da Informação

VPS – Virtual Private Server (Servidor Privado Virtual)

1. Introdução

A RTU é uma empresa criada em Viana do Castelo em 2018. O seu promotor considerava existir uma falta de resposta com qualidade na indústria TI da região e em alguns casos, empresas de maior dimensão. Muitas vezes a solução era salvaguardada por empresas de outras regiões que, inadvertidamente, criam um desequilíbrio maior nas balanças de desenvolvimento social e económico desta região. A retenção e a criação de valor na região foram uma das premissas que levaram ao desenvolvimento do projeto colocado em discussão de seguida.

Durante o período de estágio na RTU, uma das principais preocupações por parte do promotor deste trabalho foi sempre garantir uma gestão de tempo adequada ao desenvolvimento do projeto.

Identificaram-se algumas lacunas com potencial resolução, contudo, optou-se por intervir na área da monitorização/controlo de sistemas; a necessidade de uma solução eficiente para monitorização ativa criava atrasos nos processos existentes e, em alguns casos, até a falha de resposta em tempo útil nos pedidos efetuados pelos clientes. Portanto, o propósito da criação da RTU começava a perder força com a perda de capacidade de resposta. A empresa, embora especializada em TI, enfrentava dificuldades com o aumento dos pedidos de suporte e a falta de dimensão humana. Esse volume, frequentemente, originava atrasos na resposta aos problemas dos clientes, em vez de promover uma ação preventiva, promovia uma ação reativa.

Assim sendo, procurou-se uma solução que transformasse a abordagem da empresa relativamente à monitorização, elevando o seu nível de engenharia e imagem qualitativa para o exterior.

1.1. Objetivos

No âmbito do estágio, definiram-se objetivos específicos, tanto a nível técnico quanto empresarial, em concordância com as exigências e características do contexto socioeconómico e geográfico em que a RTU opera. Estes objetivos estão alinhados com o modelo ADKAR (Jeff Hiatt, 2006), que enfatiza a importância das iniciativas de mudança.

Objetivos Técnicos:

1. **Implementação do Zabbix:** Equipar a RTU com uma ferramenta eficaz e adaptável - o Zabbix – responde ao aumento de pedidos dos clientes atuais e potenciais. Esta ferramenta destaca-se pela sua capacidade de controlo abrangente e pela flexibilidade em adaptar-se às necessidades dinâmicas da empresa.
2. **Integração com o Telegram:** Desenvolver competências nos colaboradores para a utilização eficiente do programa de controlo Telegram como interface de gestão. Este objetivo visa capacitar a equipa para intervir de forma cirúrgica na resolução de problemas, utilizando esta ferramenta como um meio de comunicação rápida e eficaz.
3. **Aumentar a eficiência nos Processos de Monitorização:** Assegurar que os processos de monitorização implementados são eficazes e que existe uma operação fluída entre o Zabbix e o Telegram, garantindo assim uma resposta célere e uma gestão rápida às situações monitorizadas.

Objetivos Empresariais:

1. **Aumento da Notoriedade da RTU:** Fomentar o reconhecimento da RTU no mercado, capacitando-a na resolução eficiente de problemas. Isto envolve mudar práticas e procedimentos que estavam em vigor desde a fundação da empresa, adaptando-os para métodos mais modernos e eficientes.
2. **Otimização de Tempo e Recursos:** Melhorar a gestão do tempo e recursos da empresa para lidar com o volume crescente de pedidos, permitindo tomar decisões estratégicas sem comprometer as responsabilidades fiscais, legais e sociais da organização.

Estes objetivos foram delineados especificamente para responder às necessidades particulares da RTU, tendo em vista a sua progressão e ajuste às exigências do mercado.

1.2. Contexto

A Ricardo Terleira Unipessoal, LDA (RTU), foi criada em 2018 e tem sede em Viana do Castelo. Destaca-se no mercado em que se insere pela capacidade de resposta ao nível de telecomunicações, mais especificamente, em sistemas TI. Com mais de 10 anos de experiência, a RTU é especializada na revenda de produtos de telecomunicações para empresas e particulares, bem como, no comércio de equipamentos e oferta de soluções relacionadas com TI. Opera num espaço geográfico difícil e, em alguns casos, com necessidades complexas.

A necessidade de manter-se atualizada com tendências emergentes e a necessidade de dar respostas cada vez mais rápidas nos sistemas dos clientes emergiram como um ponto crítico, dificultando a capacidade da empresa de prestar um serviço proativo e eficiente.

Durante o estágio na RTU, constatou-se que a empresa carecia de um sistema de monitorização eficiente, o que resultava em desafios na supervisão e no controlo do parque informático dos clientes. Assim, o principal objetivo do estágio foi implementar uma solução abrangente para a monitorização dos sistemas, recorrendo à ferramenta Zabbix.

O Zabbix é uma solução de software em código aberto para a monitorização de sistemas. A escolha baseou-se em duas publicações que demonstraram a sua eficácia e versatilidade, o artigo "Zabbix Monitoring Software In-Depth Review" (Paulo Gardini Miguel, 2023), que destacou as especificações e a opinião profissional relativa ao Zabbix e também a publicação "Top 5 reasons to choose Zabbix for network monitoring" (Dmitry Lambert, 2021), fornecendo uma visão valiosa sobre as suas capacidades.

Este projeto envolveu um estudo do Zabbix, com o intuito de assegurar a sua eficaz integração nos sistemas existentes da empresa. Colaborou-se com clientes da RTU para testar e implementar a solução de monitorização.

Como resultado, a RTU está a absorver um sistema de monitorização eficiente, que proporciona métricas e notificações adequadas para um controlo mais preciso do parque informático dos clientes.

1.3. Estrutura do documento

Este relatório está organizado em várias secções, cada uma dedicada a um aspeto específico do desenvolvimento do trabalho. A seguir, apresenta-se um resumo da estrutura e conteúdo de cada capítulo:

- **Introdução:** Este capítulo inicial oferece um resumo conciso dos objetivos e metas do projeto, estabelecendo as bases para os capítulos seguintes.
- **Estado da Arte:** Neste capítulo, a análise aprofundada das soluções existentes no mercado para a monitorização de equipamentos, permitirá não só compreender o panorama atual das ferramentas disponíveis, mas também destacar as características distintivas que tornam a plataforma Zabbix a escolha acertada.
- **Análise e Especificação de Requisitos:** Neste terceiro capítulo, a definição minuciosa dos requisitos para a implementação da ferramenta de monitorização na RTU é crucial para assegurar uma integração harmoniosa com os sistemas já em produção, salvaguardando a disponibilidade e a integridade dos sistemas existentes.
- **Implementação:** Este capítulo detalha o processo de implementação do Zabbix, seguindo uma abordagem por fases. Descreve os passos principais e as decisões técnicas, oferecendo uma visão direta da implementação da ferramenta.
- **Análise de Resultados:** Neste capítulo, apresenta-se uma análise dos resultados alcançados com a implementação do Zabbix. Foca-se na avaliação do desempenho, na eficácia das soluções adotadas e no impacto nas operações diárias da RTU.
- **Conclusões e Trabalhos Futuros:** São expostos alguns procedimentos que devem ser analisados no futuro para uma implementação mais segura e de fácil compreensão.

Cada capítulo foi elaborado para fornecer uma visão compreensiva e detalhada de cada etapa do projeto, desde a conceção inicial até à sua implementação e avaliação.

2. Estado da Arte

Esta secção pretende apresentar o conjunto de soluções existentes para a monitorização de equipamentos. A segunda parte desta secção descreve detalhadamente a plataforma Zabbix, pois foi a plataforma escolhida para este trabalho.

Outras tecnologias utilizadas¹, tais como MySQL, SNMP, Apache são minimamente identificadas, pois são comuns e estão bem documentadas na literatura e informação das respetivas empresas.

2.1. Soluções Existentes

No âmbito do mercado atual, existe um leque variado de soluções de monitorização, cada uma com as suas características distintas. Foi realizada uma pesquisa, com o intuito de analisar várias soluções existentes e avaliar os benefícios e limitações inerentes a cada uma. Este estudo possibilitou uma compreensão dos diversos sistemas, fornecendo uma base sólida para a seleção da ferramenta mais adequada às necessidades da empresa.

Tabela 1 – Ferramentas existentes²

Recurso	Custo	Suporte	Instalação
Zabbix	Gratuito	Comunidade, Fórum e Suporte Comercial	Simples
Prometheus	Gratuito	Comunidade e Suporte Comercial	Simples
PRTG	Licenciamento	Comunidade e Suporte Comercial	Complexa
Solar Winds	Licenciamento	Comunidade, Fórum e Suporte Comercial	Simples

¹ Tecnologias identificadas no glossário.

² Eventualmente alguns dados das tabelas 1 e 2, poderão não corresponder de todo a realidade, pois assentam em informações retiradas de websites mencionados na Bibliografia.

2.1.1. Critérios de comparação das soluções

Na tabela 2 são apresentados critérios de funcionalidades com interesse para a implementação da ferramenta.

Tabela 2 - Critérios decisivos das soluções

Recurso	Visualização de Dados	Alertas	Escalabilidade	Proxy
Zabbix	Interface Web	✓	Alta	✓
Prometheus	Expression Console	✓	Alta	N/A
PRTG	Interface Web	✓	Alta	✓
Solar Winds	Interface Web	✓	Alta	✓

A seguir, descreve-se com mais detalhe o Zabbix, plataforma utilizada para a implementação.

2.2. Zabbix

O *Zabbix* é uma solução *open-source* para diversos tipos de infraestruturas, incluindo redes, servidores, máquinas virtuais, computadores e serviços *cloud*. A capacidade de escalar para grandes ambientes, a flexibilidade na configuração, a parametrização, a robustez na deteção de problemas e a geração de alertas, foram decisivas para a utilização desta ferramenta.

Destaca-se pela sua arquitetura modular, composta pelo núcleo central do sistema, o *Zabbix Server*, o *Zabbix Proxy*, que recolhe e armazena dados provenientes das infraestruturas para posterior envio ao servidor, e pelo *Zabbix Agent*, instalado nos sistemas operativos dos equipamentos compatíveis para recolher dados.

O *Zabbix* oferece funcionalidades tais como: (Zabbix, 2023h)

- **Monotorização de Desempenho e Disponibilidade:** Fornece dados em tempo real sobre o estado e o desempenho dos sistemas.
- **Deteção Avançada de Problemas:** Utiliza um mecanismo de deteção baseado em limiares e dependências.

- **Visualização de Dados:** Apresenta informações por meio de painéis customizáveis e relatórios.
- **Alertas e Notificações:** Envia notificações personalizadas, com base nos critérios definidos pelo administrador, e para várias plataformas³.
- **Previsão e Tendência:** Através de estatísticas e dados históricos, prevê possíveis interrupções, problemas ou indisponibilidade dos sistemas.

2.2.1. Zabbix Server

Sendo o *Zabbix* um sistema modular, o *Server* é o módulo principal da ferramenta. É responsável por centralizar todos os dados e processos de monitorização. Recolhe e processa informações de performance, disponibilidade, verifica a integridade dos sistemas e dispara alertas e notificações. Disponibiliza também a interface web onde são geridas todas as configurações e parametrizações.

As principais características deste módulo são: (Zabbix, 2023e)

- **Processamento de Dados:** Recebe e processa dados de monitorização de outros módulos, consolidando-os numa base de dados central para análise e armazenamento.
- **Deteção de Anomalias:** Utiliza um motor de regras complexas e altamente customizáveis para detetar padrões anormais e potenciais falhas nos equipamentos monitorizados.
- **Geração de Alertas:** Envia notificações com base nos eventos detetados que correspondem a critérios previamente definidos.
- **Interface Web:** Oferece uma interface web completa para configuração e gestão de toda a ferramenta, bem como para visualização de dados em tempo real e históricos.
- **Base de Dados:** Utiliza *MySQL* ou *PostgreSQL*⁴ para garantir o registo de todos os dados recolhidos.

³ Telegram, WhatsApp, SMS, Email.

⁴ Tecnologias de Base de Dados

- **Escalabilidade:** Desenhado para funcionar eficientemente em ambientes mais pequenos e com possibilidade de escalar para monitorizar infraestruturas com maior nível de equipamentos sem perda significativa de performance.

2.2.2. Zabbix Proxy

O módulo *proxy* atua como um intermediário que recolhe dados e informações dos dispositivos monitorizados e envia para o módulo *server*. É útil em ambientes distribuídos, como a RTU, onde existem vários parques informáticos e a comunicação direta dos dispositivos com o módulo *server* poderia ser ineficiente ou limitada, por motivos de largura de banda e segurança.

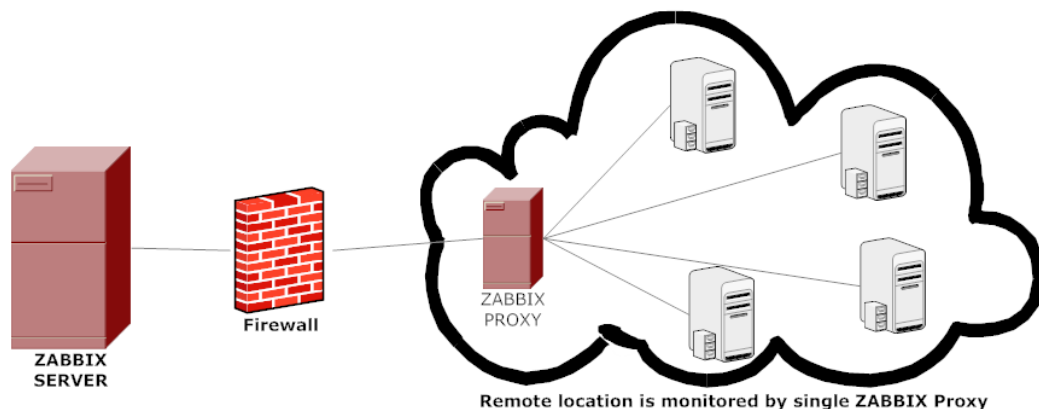


Figura 1 - Módulo Proxy em produção

(Fonte: (Zabbix, 2023c))

A função do módulo proxy envolve: (Zabbix, 2023d)

- **Recolha de Dados:** Recolhe dados dos equipamentos monitorizados, com ou sem uso, do módulo *agent*.
- **Armazenamento Temporário:** Mantém os dados recolhidos localmente antes de enviar para o módulo *server*, o que pode ajudar na redução da carga de rede e do processamento do servidor principal.

- **Autonomia e Disponibilidade:** Pode monitorizar os equipamentos mesmo quando a ligação com o servidor principal está indisponível, garantindo a continuidade da monitorização.
- **Escalabilidade e Redundância:** Através deste módulo, pode ser implementado o serviço em diversos parques informáticos em localizações distintas.
- **Comunicação Ativa e Passiva:** Suporta dois tipos de comunicações para o servidor. Isto permite melhorar o desempenho e o tempo de resposta para certos parâmetros, dependendo das necessidades da implementação.

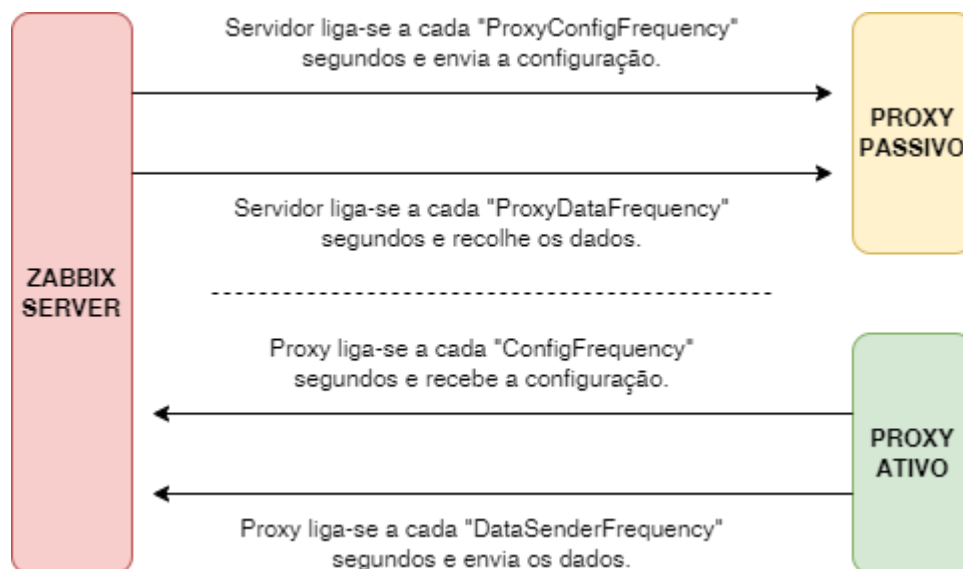


Figura 2 - Módulo Zabbix Proxy

(Fonte: Adaptado de (Rajesh Kumar, 2023))

2.2.3. Zabbix Agent

Desempenha um papel vital no ecossistema do *Zabbix*, atuando como o componente diretamente instalado nos sistemas operativos dos equipamentos que requerem monitorização. Este agente recolhe dados de desempenho tais como, uso do processador, uso da memória, espaço em disco, tráfego de rede e estado de serviços.

As principais características deste modulo são: (Zabbix, 2023a)

- **Comunicação Segura:** Suporta ligação criptografada entre o agente e o servidor ou proxy, garantindo que os dados transmitidos são protegidos.
- **Monitorização Ativa e Passiva:** Pode ser configurado para o modo ativo, no qual o agente inicia a ligação entre o servidor/*proxy*, ou passivo, onde aguarda por instruções do servidor para enviar dados.
- **Multiplataforma:** Este módulo está disponível para diversos sistemas operativos, desde Windows, Linux, *macOS* e outros.

2.2.4. Zabbix Hosts

O conceito de *host* (Zabbix, 2023b) é fundamental, pois é nele que os itens de monitorização são configurados e as estatísticas são recolhidas. No Zabbix, um “*host*” é um dispositivo que através dos módulos anteriormente mencionados se liga ao servidor principal, como, por exemplo um computador.

Cada *host* é identificado por um nome único e pode ser organizado em grupos para simplificar a administração e a visualização de dispositivos similares ou relacionados. Através da interface web, é possível adicionar, configurar e gerir os *hosts*.

Um *host* pode conter inúmeras métricas de monitorização. Se existir um agente instalado num servidor com o sistema operativo Windows Server, é possível extrair informações de performance, uso da memória, estado do serviço de SQL, caso se aplique, entre outros.

2.2.5. Zabbix Templates

Na plataforma existem modelos (Zabbix, 2023f) que contêm um conjunto de entidades de monitorização pré-definidas, como itens, *triggers*, gráficos e notificações. Estes modelos são usados para padronizar a monitorização de *hosts* que possuem configurações semelhantes, permitindo assim uma implementação rápida e consistente.

Através dos modelos é possível reutilizar as paramétricas definidas para um tipo de serviço ou dispositivo, e quaisquer alterações no modelo, são propagadas pelos *hosts* associados. Permite também a exportação e importação graças à capacidade de serem exportados e importados como arquivos XML.

2.3. Infraestrutura do Servidor Zabbix

Existem diversas abordagens para a instalação do servidor *Zabbix*, refletindo a sua flexibilidade e adaptabilidade. As opções incluem a instalação direta em sistemas operativos com base em Linux, utilizando pacotes distribuídos oficialmente, e também o uso de imagens pré-configuradas e prontas para serem implementadas.

As variedades de métodos de instalação permitem que o *Zabbix* adapte a diferentes ambientes e necessidades específicas. A escolha do método de instalação depende dos requisitos, dos recursos disponíveis e dos objetivos da implementação.

Na secção seguinte, descrevem-se as tecnologias que foram seguidas neste trabalho.

2.3.1. Servidor Virtual Privado

O uso de um servidor virtual privado (SVP) para hospedar o servidor *Zabbix* oferece uma combinação de flexibilidade, escalabilidade e controlo total dos recursos da infraestrutura. Proporciona um ambiente isolado, através do qual é fácil escalar recursos conforme a necessidade, ajustando a capacidade de processamento, memória e armazenamento sem interrupções significativas. (Ionos, 2023)

Sendo hospedado na nuvem, o servidor *Zabbix* é acessível em qualquer lugar, facilitando a monitorização e gestão remota dos equipamentos. O servidor virtual privado expõe melhor garantia de segurança e disponibilidade em comparação com servidores locais, especialmente quando hospedados por revendedores certificados e de renome.

Com uma solução implementada virtualmente, a empresa evita o custo de aquisição e manutenção de hardware físico, pagando apenas pelos recursos que usa, o que pode ser mais económico a longo prazo.

3. Análise e especificação de requisitos

Este capítulo é dedicado à definição dos requisitos essenciais para a implementação da ferramenta de monitorização na RTU. A compreensão aprofundada e precisa dos requisitos é um pilar crucial no desenvolvimento deste projeto. Analisando meticulosamente estas necessidades, conseguimos captar as expectativas dos utilizadores finais e assegurar que a solução proposta não só responda as suas funções básicas, mas também esteja em sintonia com os objetivos estratégicos da RTU. Este processo abrange a identificação minuciosa dos requisitos funcionais e não funcionais, assim como a análise de fatores críticos como a usabilidade, a eficiência no desempenho e a capacidade de integração harmoniosa com os sistemas já em operação.

De seguida são enumerados e descritos os requisitos funcionais da ferramenta. Inclui tarefas específicas que a ferramenta deve ser capaz de realizar.

3.1. Requisitos funcionais

Tabela 3 - Requisitos funcionais

RF01	Monitorização de dispositivos em rede	Capacidade de monitorizar equipamentos ativos de rede, tais como, servidores, workstations, firewalls, routers e outros. Deve incluir parâmetros como o tráfego, uso do processador, memória e espaço em disco.
RF02	Deteção de falhas e alertas	O sistema deve ser capaz de detetar falhas nos dispositivos e enviar alertas em tempo real para os administradores.
RF03	Monitorização de aplicações	Atualizações constantes do desempenho de aplicações críticas como base de dados e serviços web.
RF04	Suporte a protocolos	Suporte para vários protocolos, incluindo SNMP, ICMP, SSH e TCP/IP.

Descrevem-se a seguir os requisitos não funcionais, cruciais para garantir que a ferramenta não só funciona corretamente, mas também cumpra padrões de qualidade e desempenho.

3.2. Requisitos não funcionais

Tabela 4 - Requisitos não funcionais

RNF01	Desempenho	Monitorizar a rede e os dispositivos em tempo real, com um tempo de resposta rápido, mesmo sob carga elevada.
RNF02	Escalabilidade	Capacidade de se adaptar ao crescimento da infraestrutura, podendo monitorizar um número crescente de dispositivos e aplicações sem perda de desempenho.
RNF03	Hardware	A eficácia da escalabilidade da ferramenta depende diretamente das capacidades do hardware sobre o qual é executada. Para assegurar que é possível aumentar o nível de carga da infraestrutura, é crucial que o hardware seja adequadamente dimensionado.
RNF04	Segurança	Implementação de protocolos de segurança para proteger os dados e comunicação entre a ferramenta e os dispositivos monitorizados.
RNF05	Disponibilidade	Garantir disponibilidade do sistema, minimizando tempos de inatividade e assegurar a continuidade do funcionamento da ferramenta.
RNF06	Integridade	Precisão dos dados para que os alertas e relatórios sejam baseados em informações corretas.

3.3. Entidades e relações

No contexto do uso da ferramenta, é importante compreender a interação e o papel de cada entidade dentro da sua arquitetura. Este estudo é fundamental para a configuração eficaz e o uso eficiente da aplicação. Nas secções seguintes será dada uma explicação detalhada do processo e das entidades críticas envolvidas.

3.3.1. Entidades Críticas

Antes de utilizar a ferramenta, é essencial estabelecer um entendimento claro das entidades fundamentais e como elas interagem. Isso envolve a familiarização com o princípio de funcionamento do serviço. Através do seguinte diagrama é possível identificar como as entidades estão ligadas entre si.

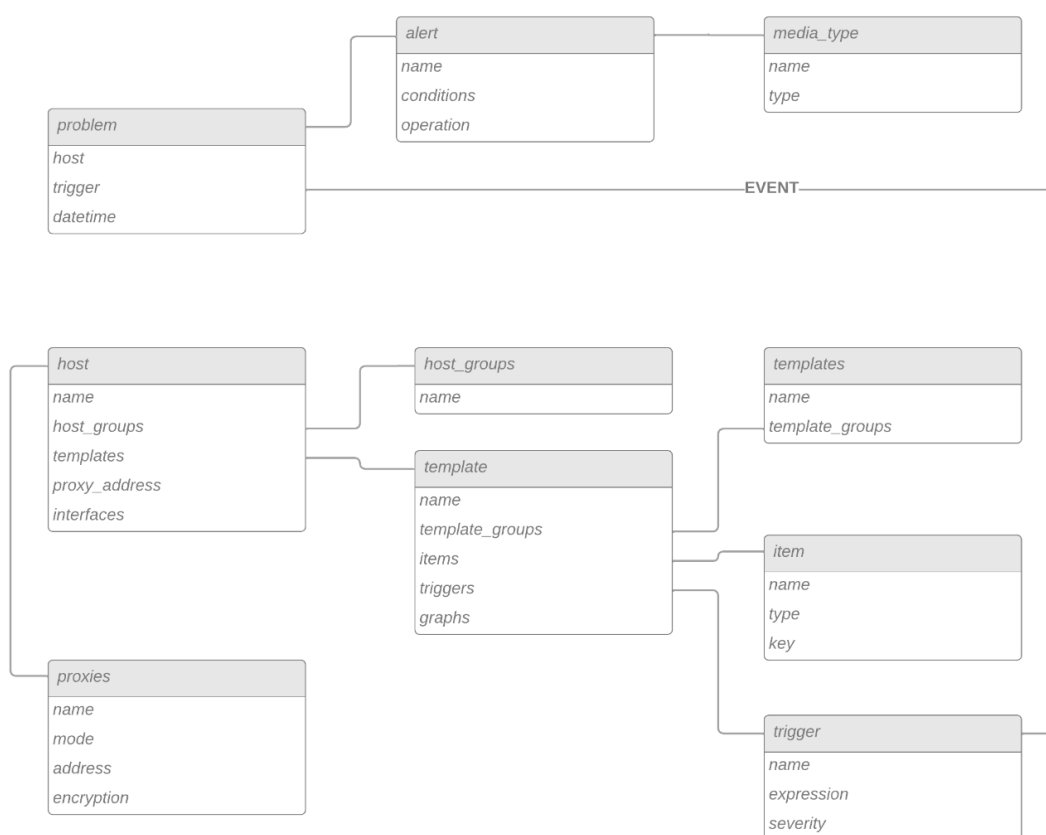


Figura 3 – Esquema de entidades do Zabbix

Após análise do diagrama da Figura 3 identificamos as entidades que alimentam o modelo de dados da ferramenta de forma a tornar possível todo o processo de monitorização. Os aspetos mais relevantes são:

- **Hosts** - A entidade host representa os dispositivos ou sistemas monitorizados pelo Zabbix. Cada host está associado a uma variedade de outras entidades, como items, triggers, e events, que detêm a riqueza dos dados de monitorização. Por exemplo, items podem incluir métricas específicas, como o uso do processador ou espaço em disco, enquanto triggers definem condições sob as quais os alertas devem ser gerados.
- **Templates** - Os templates oferecem uma forma poderosa de aplicar configurações pré-definidas a múltiplos hosts, garantindo consistência e eficiência. Eles contêm items, triggers, e graphs standardizados, que podem ser herdados por qualquer host vinculado a esse template, conforme ilustrado no diagrama (Figura 3), pelas ligações entre host e templates.
- **Triggers e Problems** - No Zabbix, os triggers são condições lógicas definidas para identificar potenciais problemas em hosts monitorizados. Quando as condições de um trigger são cumpridas, um problema (problem) é registado, indicando uma situação anormal ou de falha. Estes problems levam à geração de alertas (alerts), dependendo da sua severidade ou configuração do sistema.
- **Alerts** - A entidade alerts representa as ações tomadas em resposta a eventos, como o envio de notificações para as plataformas previamente configuradas. Estes alertas são gerados com base no estado dos triggers e na gravidade dos events, destacando a importância das relações entre estas entidades.
- **Integridade Referencial** - Dada a natureza interligada destas entidades, a integridade referencial é de suma importância. Ao inserir ou editar um host, deve-se assegurar que todas as entidades relacionadas estejam corretamente configuradas. Isso garante que qualquer ação - monitorização de desempenho ou resposta a incidentes - seja realizada com base em dados precisos e confiáveis.

3.3.2. Engenharia Reversa da Base de Dados

Através da engenharia reversa aplicada à base de dados do Zabbix, foi possível desvendar a rede de entidades e as suas ligações. O “cérebro” desta base de dados é a entidade *host*, que serve como núcleo central para várias outras entidades importantes e reflete a capacidade modular e extensível do Zabbix.

Esta base de dados encontra-se em anexo, identificada como Anexo A por motivos de legibilidade.

4. Implementação

Neste capítulo, descreve-se detalhadamente o processo de implementação, nomeadamente os passos seguidos, as decisões tomadas e as metodologias aplicadas.

As decisões tomadas durante o processo de implementação foram influenciadas quer pelo estudo de manuais (Nathan Liefting & Brian van Baekel, 2022) e análise das soluções existentes (Seyed Tahaghoghi & Hugh E. Williams, 2007), quer pela familiaridade com determinadas tecnologias. Esta experiência pré-existente levou à escolha de soluções já conhecidas, garantindo uma implementação mais eficiente e segura.

Apresenta-se uma estrutura organizada, dividida em fases. Para garantir uma compreensão clara do processo de implementação. Nas tabelas seguintes, servindo de guia para o procedimento, são enumerados os pontos executados, ordenados de forma lógica e sequencial, no sentido de facilitar o acompanhamento da execução das tarefas.

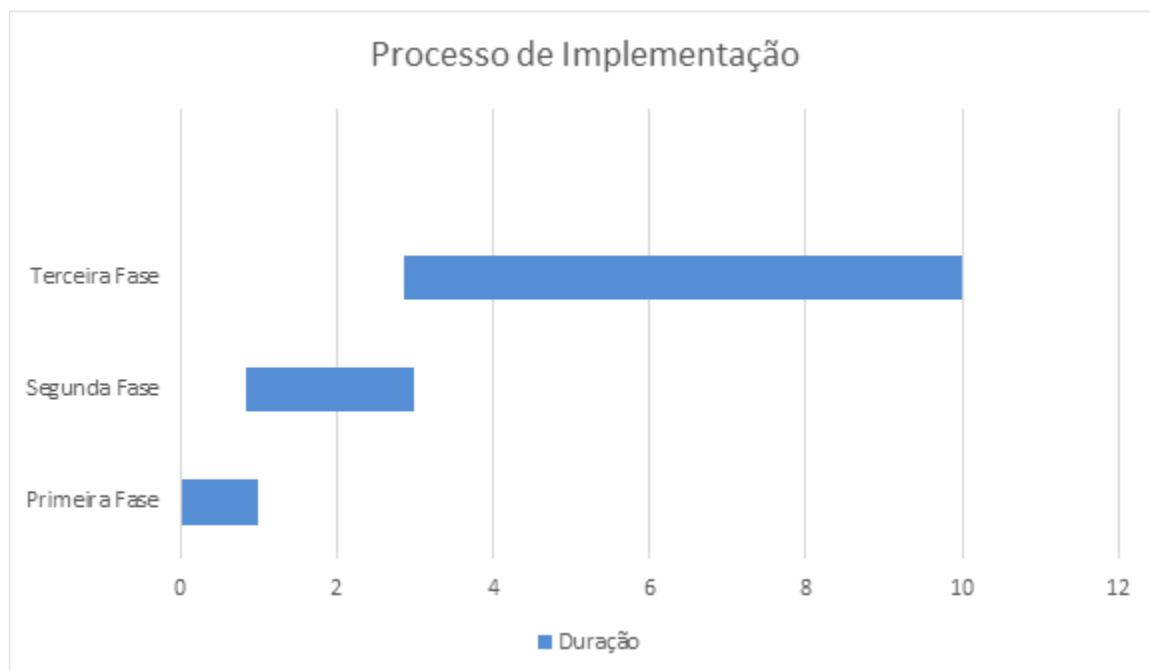


Figura 4 - Processo Desenvolvimento

Primeira Fase – Preparação e Configuração do Ambiente [1 semana]*Tabela 5 - Descrição Primeira Fase*

Código	Descrição
A001	Ambiente de Instalação
A002	Firewall e Ligações Externas
A003	Requisitos para Instalação

Segunda Fase – Instalação e Inicialização [2 semanas]*Tabela 6 - Descrição Segunda Fase*

Código	Descrição
B001	Análise de Documentação
B002	Instalação da Ferramenta
B003	Arranque Inicial

Terceira Fase – Integração de Sistemas [6 semanas]*Tabela 7 - Descrição Terceira Fase*

Código	Descrição
C001	Estudo de Clientes
C002	Sistemas Críticos
C003	<i>Proxies</i>
C004	Integração Clientes
C005	Integração dos Proxies
C006	Integração dos Sistemas
C007	Métricas dos Sistemas
C008	Alertas e Notificações

4.1. Primeira Fase

Nesta fase o foco principal recaiu no estabelecimento das bases técnicas essenciais para uma implementação segura e estável. Foi preparado o ambiente de instalação, assegurando que toda a infraestrutura de hardware e software esteja configurada e otimizada conforme as necessidades. Paralelamente, foi configurada a firewall e ligações externas, com o intuito de salvaguardar a segurança dos dados.

4.1.1. A001 – Ambiente de Instalação

Como introduzido na secção 2.3.1, a implementação foi direcionada para um servidor virtual privado, uma opção avaliada como adequada para este projeto. A escolha deste tipo de servidor, oferecido pela OVH, uma empresa reconhecida pelas suas soluções de cloud pública e privada, visa atender aos requisitos não funcionais identificados como RNF02, RNF03 e RNF05.

Relativamente à instalação do Zabbix Server, embora seja compatível com diversos sistemas operativos, optou-se por utilizar o Ubuntu Server, versão 22.04 (Jammy). Esta decisão foi baseada em critérios técnicos e práticos. A escolha do Ubuntu como sistema operativo alinha-se perfeitamente com as necessidades do projeto.

4.1.2. A002 – Firewall e Ligações Externas

Para melhorar a segurança do servidor, foi crucial ativar e configurar a firewall logo após o início do sistema, especialmente considerando que, por padrão, vem desativada.

Inicialmente foi aberta a porta TCP 22 para acesso via SSH, tecnologia que faculta acesso à linha de comandos por meio de credenciais autorizadas, e bloqueadas as restantes portas.

Antes de iniciar qualquer instalação de pacotes oficialmente distribuídos pelo repositório do Ubuntu, foi essencial garantir que o sistema esteja atualizado. Isto

implicou atualizar a lista de pacotes disponíveis e as próprias versões dos pacotes instalados, assegurando que o sistema e as suas aplicações estavam na versão mais recente e segura.

Esta prática foi fundamental para manter a integridade do sistema e evitar problemas de compatibilidade ou falhas de segurança, que podem ocorrer com pacotes desatualizados ou acessos não controlados, respeitando o requisito não funcional, RNF04.

4.1.3. A003 – Requisitos para Instalação

Através da documentação existente na página oficial do Zabbix⁵, identificou-se que a instalação do Zabbix Server requer:

- i. Uma base de dados.
- ii. Um servidor web.

O conhecimento de algumas tecnologias, permitiu agilizar o processo e tornar-se um fator decisivo nas opções sugeridas pela ferramenta.

Para a base de dados optou-se pelo MySQL, um sistema de gestão de base de dados relacional, que utiliza a linguagem SQL para gerir dados. Esta escolha foi influenciada não só pela familiaridade com o MySQL, mas também pelo seu desempenho comprovado em ambientes de produção. (Seyed Tahaghoghi & Hugh E. Williams, 2007)

Para o servidor web, decidiu-se utilizar o Apache, uma das opções mais populares e bem testadas no mercado. Esta decisão baseou-se na sua estabilidade, segurança e compatibilidade comum com o MySQL. (Seyed Tahaghoghi & Hugh E. Williams, 2007)

A combinação entre ambas as soluções, reflete uma escolha estratégica, orientada pela experiência e pela procura de uma solução tecnicamente sólida e confiável. Juntas oferecem uma base consistente, garantindo desempenho e segurança ao longo da sua utilização.

⁵ <https://www.zabbix.com/download>

4.2. Segunda Fase

Prosseguindo a partir da premissa definida no ponto 4.1, a implementação avança para o núcleo da instalação do Zabbix, um processo metódico que requer atenção aos detalhes e rigor no cumprimento dos requisitos predefinidos. A documentação fornecida pelo Zabbix não é só abrangente, mas também uma fonte importante, servindo como um guia crucial para este percurso.

4.2.1. B001 – Análise da Documentação

Procedeu-se à consulta da documentação existente referente à versão 6.4 do Zabbix (Zabbix, 2023i), versão que na data do projeto era a mais recente. A documentação, disponibilizada oficialmente, oferece um conjunto detalhado de instruções, como a instalação e configuração inicial da ferramenta.

4.2.2. B002 – Instalação do Zabbix

Através do Ubuntu foram realizados os seguintes processos:

1. Configuração do repositório oficial do Zabbix.
2. Instalação, a partir de um script, dos módulos:
 - a. Zabbix Server;
 - b. Zabbix Frontend;
 - c. Zabbix Agent;
3. Criação de uma base de dados identificada por “zabbix”.
4. Criação de um utilizador identificado por “zabbix”, com todas as permissões relativas à base de dados previamente criada.
5. Importar o esquema inicial SQL, transferido da instalação do módulo Server, para a base de dados criada.
6. Editar o ficheiro de configuração do módulo Server, localizado em:
`/etc/zabbix/zabbix_server.conf` para editar as configurações da base de dados criada.
7. Reiniciar os módulos do Zabbix e o servidor Apache.

Após o processo de instalação é necessário a abertura de portas para permitir o acesso à página web externamente. Para tal, foi configurada a firewall do sistema, habilitando assim a porta TCP 80.

4.2.3. B003 - Arranque Inicial

Depois de executar as etapas anteriores passou a estar disponível o endereço web <http://ipdoservidor/zabbix>, (Figura 5) que permitiu a configuração inicial do sistema.

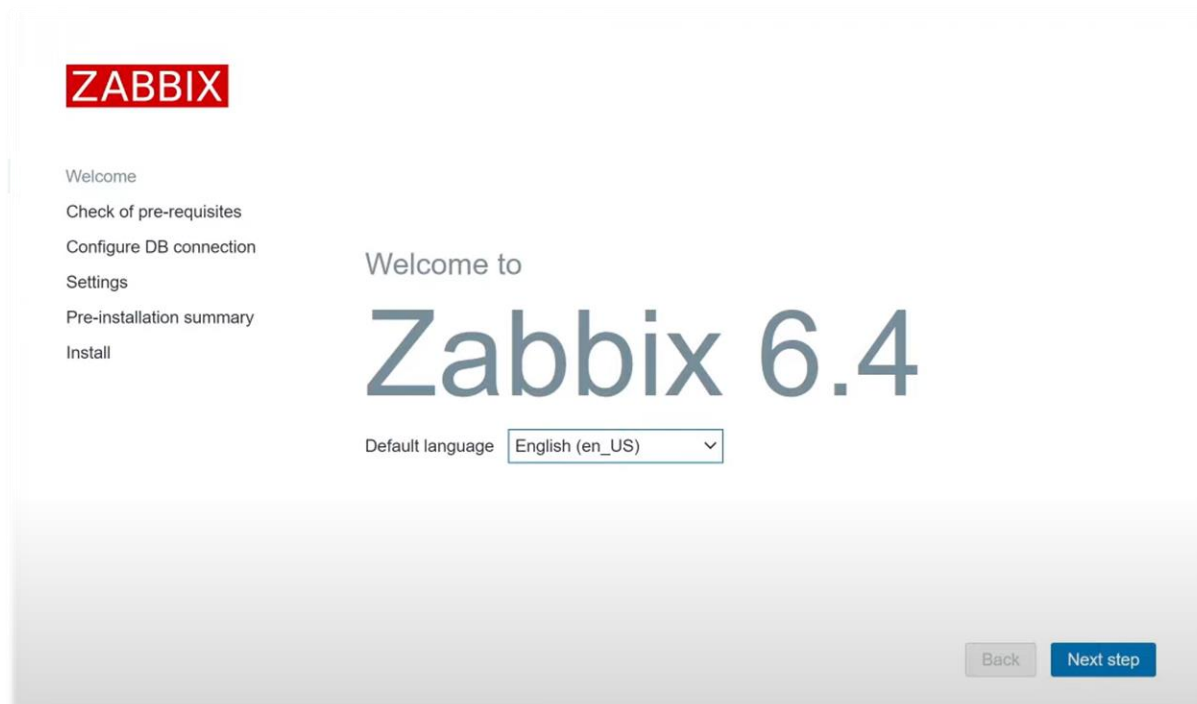


Figura 5 - Painel boas-vindas

Neste menu inicial (Figura 5) verifica-se se o servidor cumpre os pré-requisitos e configura-se alguns aspetos importantes, tais como a ligação à base de dados, o nome do servidor e o fuso horário.

WELCOME

Check of pre-requisites

Configure DB connection

Settings

Pre-installation summary

Install

Database type

MySQL

Database host

localhost

Database port

0

0 - use default port

Database name

zabbix

Store credentials in

Plain text

HashiCorp Vault

CyberArk Vault

User

zabbix

Password

Database TLS encryption

Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows).

Back

Next step

Figura 6 - Configuração Ligação BD

Sendo a instalação da base de dados local, usamos o *localhost* para identificar a conexão com a BD (Figura 6). As credenciais de acesso são previamente configuradas na secção 4.2.2.

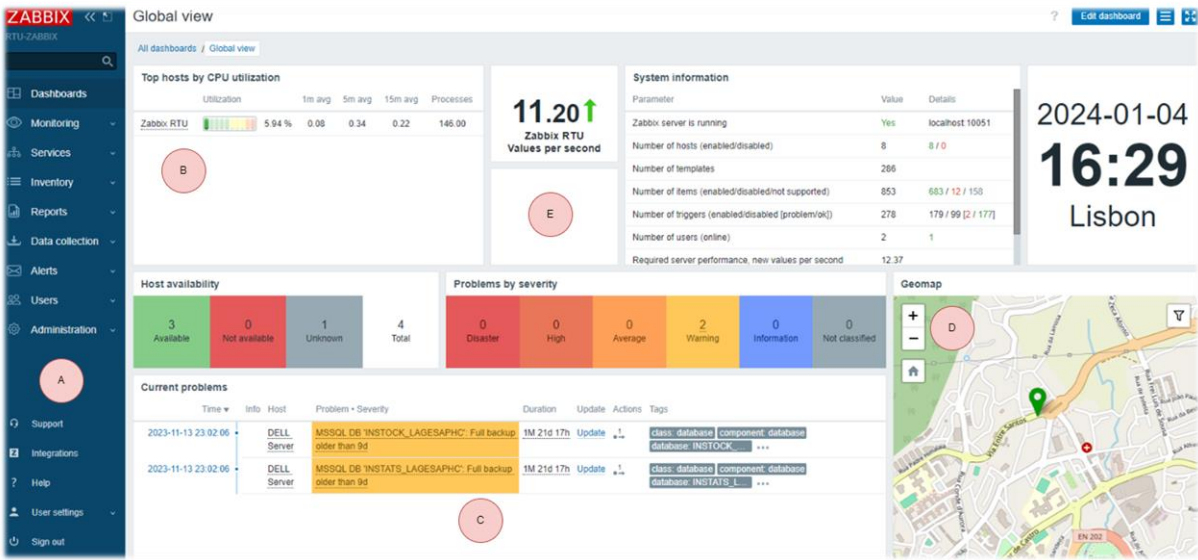


Figura 7 - Visão Global Zabbix

No painel inicial, é possível visualizar um menu vertical com ligações para as várias opções do Zabbix (Figura 6 (A)), métricas relacionadas com os dispositivos configurados (Figura 6 (B)), os problemas e a sua severidade (Figura 6 (C)), um mapa com a localização geográfica dos dispositivos (Figura 6 (D)) e também informações do sistema (Figura 6 (C)).

4.3. Terceira Fase

Durante esta fase, foi feita uma análise dos clientes e dos seus sistemas críticos. Esta avaliação serve de base para os subsequentes processos de implementação das tecnologias necessárias. Enfatizando a importância de uma abordagem personalizada, esta etapa assegura que as soluções adotadas estejam alinhadas com os objetivos específicos dos clientes.

4.3.1. C001 – Estudo de Clientes

O objetivo desta fase foi conduzir um estudo para identificar e selecionar dois clientes potenciais, cujas necessidades e contextos sejam adequados para a integração da ferramenta adotada.

Após a análise, foram identificados dois possíveis clientes. Por questões de privacidade e proteção de dados, ambos serão referenciados como cliente A e cliente B.

Contextualizando os dois clientes:

- Cliente A – Empresa de *coworking* e aluguer de salas de formação/reuniões.
- Cliente B - Empresa de importação, exportação e distribuição de ferragens.

4.3.2. C002 - Sistemas Críticos

Após análise e escolha dos clientes procedeu-se à identificação dos respetivos sistemas críticos e às necessidades específicas de cada um. Nas tabelas seguintes (Tabela 9 e 10) são enumerados e descritos os sistemas críticos e a sua descrição.

Tabela 8 - Sistemas Críticos Cliente A

Cliente	Dispositivo	Serviços	Descrição
A	UDM PRO SE	Router, Firewall, Gateway, Controladora	Gestão de todo o tráfego da empresa, acessos e regras.
	IW & U6 PRO	Pontos de Acesso WiFi	Distribuição de WiFi pelo espaço físico.
	PVE	Plataforma de virtualização	Gestão de máquinas virtuais.

Tabela 9 - Sistemas Críticos Cliente B

Cliente	Dispositivo	Serviços	Descrição
B	Servidor	SQL Server	Base de dados do programa de gestão operam neste servidor.
	Impressora	Contador de Cópias	Para efeitos de controlo de qualidade, cliente necessita do histórico de número cópias semanal, mensal e anual.

Posteriormente à análise dos requisitos do cliente e à identificação dos sistemas críticos, os protocolos compatíveis com o *Zabbix* entram em ação para permitir a integração destes sistemas com a ferramenta de monitorização. Na tabela 10 é possível identificar os protocolos usados para cada um dos dispositivos.

Tabela 10 - Protocolos usados nos Sistemas Críticos

Cliente	Dispositivo	Protocolo/s
A	UDM PRO SE	SSH
	IW	SNMP v3
	U6 PRO	SNMP v3
	PVE	Agente e API
B	Servidor	Agente e ODBC
	Impressora	SNMP v2

Na secção seguinte será demonstrado o processo de comunicação dos clientes com a ferramenta alojada no servidor virtual privado.

4.3.3. C003 - Proxies

Nesta implementação adotou-se uma abordagem de reaproveitamento de recursos. Uma escolha não apenas económica, mas também sustentável. Em ambos os clientes, decidiu-se utilizar servidores antigos que anteriormente estiveram em produção. Esta decisão revelou-se vantajosa, permitindo tirar partido de equipamento já existente e reduzir os custos associados à aquisição de novo hardware.

O processo de instalação dos servidores foi idêntico ao método utilizado na primeira fase. Após validar todos os requisitos, foram realizados os seguintes procedimentos:

1. Configuração do repositório oficial do Zabbix.
2. Instalação, a partir de um script, dos módulos:
 - a. Zabbix Proxy;
3. Criação de uma base de dados identificada por “zabbix_proxy”.
4. Criação de um utilizador identificado por “zabbix”, com todas as permissões relativas à base de dados previamente criada.
5. Importar o esquema inicial SQL, transferido da instalação do módulo Server, para a base de dados criada.
6. Editar o ficheiro de configuração do módulo Proxy, localizado em: `/etc/zabbix/zabbix_proxy.conf` para editar as configurações da base de dados criada.
7. Reiniciar o módulo Proxy.

Na configuração padrão do módulo Proxy, a comunicação entre o módulo Server e o módulo Proxy é realizada sem encriptação, o que significa que, por defeito, a comunicação ocorre em texto legível. Esta abordagem pode representar uma vulnerabilidade em termos de segurança, especialmente em ambientes onde a confidencialidade e a integridade das informações são críticas

Para mitigar este risco e aumentar a segurança da comunicação entre módulos, adotou-se a opção de encriptação baseada em uma chave pré partilhada (PSK). A utilização desta encriptação é uma medida preventiva que protege a comunicação, garantindo que os dados transmitidos sejam encriptados. Detalhes pormenorizados

sobre a configuração da encriptação PSK encontram-se disponíveis no manual oficial. (Zabbix, 2023g)

O processo de configuração da ligação entre os módulos inicia-se com a geração de uma chave PSK de 256 bit através da linha de comandos:

- `openssl rand -hex 32 > /etc/zabbix/secret.psk`

De seguida, altera-se o ficheiro de configuração do módulo localizado em: `/etc/zabbix/zabbix_proxy.conf` para editar e adicionar os seguintes parâmetros:

1. `Server=xxx.xxx.xxx.xxx6`
2. `Hostname=Zabbix Proxy Cliente A`
3. `TLSConnect=psk`
4. `TLSAccept=psk`
5. `TLSPSKFile=/etc/zabbix/secret.psk`
6. `TLSPSKIdentity=ZBX-PSK-CLIENTEA`

Com a conclusão da configuração da conexão, empregando a PSK, asseguramos a segurança na comunicação entre os módulos. Esta medida essencial encripta os dados, garantindo que a comunicação esteja protegida contra acessos não autorizados e vulnerabilidades externas.

Este aprimoramento na segurança é de suma importância e cumpre integralmente com os requisitos não funcionais RNF05 e RNF06.

4.3.4. C004 – Integração Clientes

Tendo em consideração os dispositivos do cliente, realizou-se um estudo visando otimizar o processo de monitorização e gestão dos mesmos através do Zabbix.

Primeiramente, verificou-se a existência de templates oficiais do Zabbix para cada dispositivo. De seguida, analisaram-se as métricas relevantes para cada

⁶ Endereço IP Público do Módulo Server

dispositivo, identificando aquelas que seriam cruciais para monitorizar, com o intuito de fornecer uma visão detalhada e útil do seu desempenho e estado.

Para ambos os clientes, identificou-se a presença de um dispositivo compatível para receber o módulo Agente. Esta capacidade permitiu uma integração mais direta e proporcionou uma camada adicional de visibilidade, permitindo assim o acesso a uma gama mais ampla de métricas e dados.

Sistemas do Cliente A:

- No caso do cliente A, existiam equipamentos da marca Ubiquiti que careciam de *templates* oficiais, contudo, através da comunidade ampla do Zabbix recorreu-se a soluções alternativas de *templates* criados por membros da comunidade, garantindo assim a cobertura de todos os dispositivos.
- Para a infraestrutura específica do cliente A, a análise focou-se no servidor PVE (*Proxmox Virtual Environment*), que opera sobre uma base Linux. A natureza deste sistema possibilitou a instalação direta do módulo agente, facilitando a recolha de métricas vitais do sistema operativo.
- Paralelamente, tirou-se partido de um template oficial desenhado especificamente para *Proxmox*, que opera através da API para agregar informações adicionais.

Sistemas do Cliente B (Figura 8):

- Adicionalmente, no contexto do cliente B, especificamente no servidor equipado com o sistema operativo Windows Server 2019, revelou-se também compatível com o módulo Agente.
- Através de um template oficial complementou-se o módulo Agente com uma ligação através do protocolo ODBC ao serviço de SQL instalado no servidor, fornecendo um leque variado de informações, métricas e alertas.

The screenshot shows the Zabbix 'Host' configuration page for a host named 'BLADE-SQL'. The 'Host' tab is selected, showing fields for 'Host name' (BLADE-SQL) and 'Visible name' (DELL Server). Below these are 'Templates' with a table listing 'MSSQL by ODBC' and 'Windows by Zabbix agent', each with 'Unlink' and 'Unlink and clear' actions. There is a search bar for templates. The 'Host groups' section shows 'Cliente B', 'Databases', and 'Servers' as selected groups, with a 'Select' button and a search bar.

Figura 8 - Servidor Cliente B - Host

A dualidade desta abordagem proporcionou uma perspetiva ampla dos servidores, oferecendo dados relativos e específicos às tecnologias instaladas em cada um. Desta forma, permite à RTU localizar e identificar possíveis problemas, de maneira mais clara e sucinta.

De seguida, será demonstrado o processo de instalação do módulo agente em ambos os dispositivos dos clientes.

Configuração do Cliente A:

O processo de instalação do módulo Agente no sistema operativo Linux segue o registo dos outros módulos, excluindo a instalação da base de dados. Após validar todos os requisitos, foram realizados os seguintes procedimentos:

1. Configuração do repositório oficial do Zabbix.
2. Instalação, a partir de um script, dos módulos:
 - a. Zabbix Agent;
3. De seguida, altera-se o ficheiro de configuração do módulo localizado em: `/etc/zabbix/zabbix_agentd.conf` para editar os seguintes parâmetros:

- a. `Server=xxx.xxx.xxx.xxx7`
- b. `ServerActive=xxx.xxx.xxx.xxx`

⁷ Endereço IP Local da Proxy

Configuração do Cliente B:

O procedimento de instalação do módulo Agente no sistema operativo Windows Server realiza-se através de um executável, disponível na página oficial do Zabbix, com as configurações presentes na Figura 9.

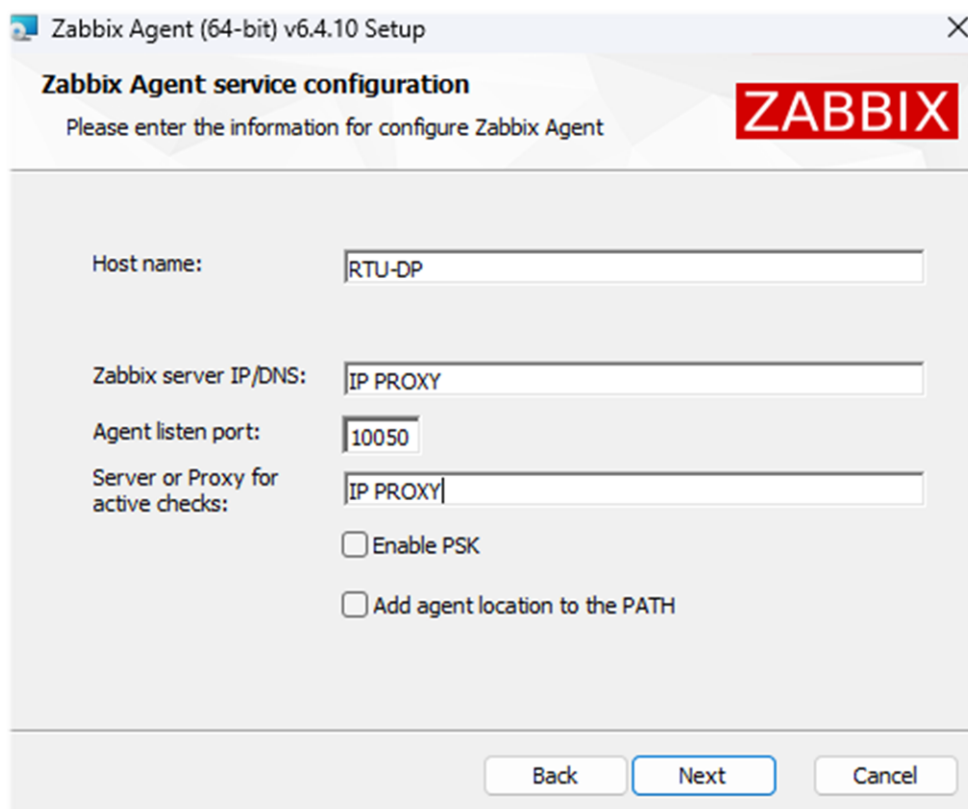


Figura 9 - Configuração módulo Agente em ambiente Windows

4.3.5. C005 – Integração dos Proxies

Nesta etapa do projeto, com os proxies já ativos nos clientes e os dispositivos aptos para o módulo Agente configurados, a atenção centra-se na integração das proxies com o módulo Server. Optou-se por configurar os proxies em modo ativo, de forma a não sobrecarregar o servidor virtual privado.

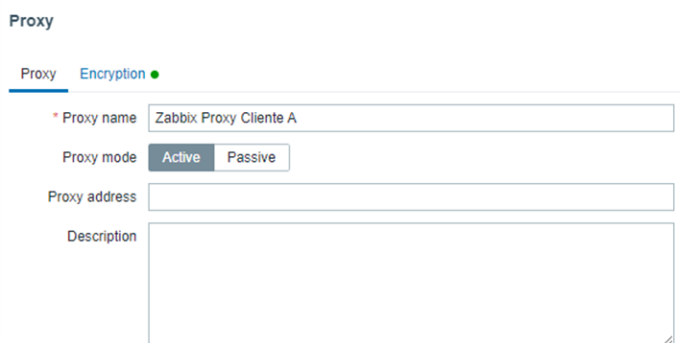
Salienta-se que ambos os clientes possuem um endereço IP público fixo, um detalhe crucial no aumento da segurança da implementação. Esta particularidade permite a implementação de medidas de segurança mais rigorosas, como a definição de regras na firewall do servidor virtual privado.

Neste contexto, estabeleceram-se na firewall regras que permitem apenas ligações nas portas TCP 10051 e 10050, provenientes desses endereços públicos, reforçando significativamente a segurança, restringindo o acesso ao módulo Server exclusivamente aos clientes autorizados.

Após a configuração das regras na firewall, a integração dos proxies com o módulo Server foi realizada da seguinte forma:

1. Na interface web do Zabbix, acedeu-se à secção 'Administration', seguida de 'Proxies'.
2. Adicionou-se cada proxy, identificadas pelo Hostname.
3. Configurou-se a encriptação.

Nas figuras 10 e 11 destacam-se os parâmetros utilizados na configuração de cada proxy, respeitando os dados previamente configurados na altura da instalação em cada cliente.



Proxy

Proxy Encryption

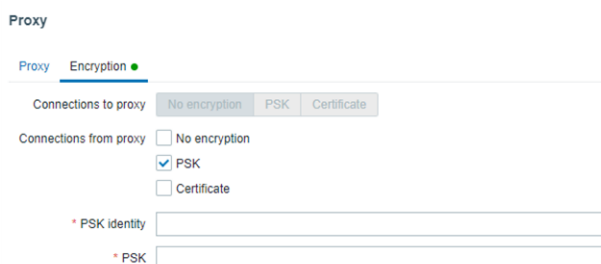
* Proxy name Zabbix Proxy Cliente A

Proxy mode Active Passive

Proxy address

Description

Figura 10 - Configuração Proxy



Proxy

Proxy Encryption

Connections to proxy No encryption PSK Certificate

Connections from proxy ☐ No encryption ☒ PSK ☐ Certificate

* PSK identity

* PSK

Figura 11 - Configuração Encriptação Proxy

Através da encriptação da conexão e das regras estabelecidas na firewall garantimos o cumprimento dos requisitos não funcionais RNF04 e RNF06.

4.3.6. C006 – Integração dos Sistemas

Através da interface web, acede-se à secção de gestão de hosts, localizada em 'Monitoring -> Hosts'. Este acesso permite aos utilizadores entrar na área específica onde podem criar e gerir hosts (Figura 12).

Host

Host IPMI Tags Macros 4 Inventory Encryption Value mapping

* Host name: BLADE-SQL

Visible name: DELL Server

Templates

Name	Action
MSSQL by ODBC	Unlink Unlink and clear
Windows by Zabbix agent	Unlink Unlink and clear

type here to search Select

* Host groups: Cliente B x Databases x Servers x

type here to search Select

Interfaces

Type	IP address	DNS name	Connect to	Port
Agent	10.0.150.25		IP DNS	10050

Add

Description

Monitored by proxy: Zabbix Proxy Cliente B

Enabled ☒

Update

Figura 12 - Configurações Servidor Cliente B

Analisando a figura 13, identificamos os seguintes parâmetros na configuração do host (Tabela 11):

Host macros Inherited and host macros

Macro	Value	Description
{\$MSSQL.DSN}	value	System data source name.
{\$MSSQL.INSTANCE}	value	The instance name for the default instance is SQLServer. For named instance set the macro value as MSSQLInstance name.
{\$MSSQL.PASSWORD}	value	MSSQL user password.
{\$MSSQL.USER}	value	MSSQL username.

Figura 13 - Inserção de Macros

Tabela 11 – Parâmetros Configuração Host

Host Name	Replicado conforme configuração original.
Visible Name	Nome visível dentro da interface.
Templates	Modelos compatíveis com o dispositivo.
Host Groups	Grupos aos quais o host pertence.
Interfaces	Detalhes da interface de rede do host.
Monitored by proxy	Indica se o host é monitorizado por meio de um proxy.

Na secção 'Macros', da figura 13, observa-se a presença de campos que necessitam de ser preenchidos manualmente. Esta exigência decorre das especificidades do template utilizado no host, que requer a definição de parâmetros específicos para estabelecer a ligação por meio do protocolo ODBC.

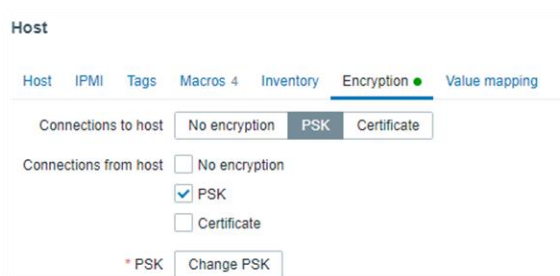


Figura 14 – Encriptação do Host

Na secção 'Encryption', da figura 14, assume a mesma metodologia que a proxy. Neste caso em específico, foi configurada encriptação entre host e módulo Server mesmo sendo intermediado pela Proxy.

Os restantes dispositivos foram configurados com os parâmetros especificados na tabela 12:

Tabela 12 - Parâmetros dos Sistemas Críticos

Host Name	Template	Interface	Host Groups
AP-IW	UBQT UNIFI SNMP V3 HN	SNMP	Cliente A
AP-U6PRO	UBQT UNIFI SNMP V3 HN	SNMP	Cliente A
PVE-ClienteA	Proxmox VE by HTTP & Linux by Zabbix agent	Agent	Cliente A
UDMPRO-SE	Template UniFi UDMP SSH	Agent	Cliente A
Printer Kyocera	Kyocera SNMP V2	SNMP	Cliente B

Posteriormente à configuração dos sistemas críticos no módulo Server, foi imperativo proceder à configuração individual dos dispositivos envolvidos. Este passo incluiu o acesso às configurações de cada dispositivo para habilitar protocolos de comunicação, como o SNMP para equipamentos de rede e Token API para o PVE. Após a ativação destes protocolos, gerou-se credenciais em cada dispositivo para possibilitar a comunicação segura com autenticação.

4.3.7. C007 – Métricas dos Sistemas

Após configuração dos sistemas críticos, torna-se fundamental monitorizar o seu desempenho e disponibilidade. A interface web do Zabbix oferece uma visão abrangente e detalhada das métricas dos sistemas, permitindo uma gestão eficaz e proactiva.

Métricas de Desempenho (Figura 15): Métricas relacionadas com o desempenho do sistema, como a utilização do CPU, memória em uso e espaço em disco.

<input type="checkbox"/> Host	Name ▲	Last check	Last value	Change
<input type="checkbox"/> DELL Server	Context switches per second ?	33s	2412.7626	-466.9446
<input type="checkbox"/> DELL Server	CPU DPC time ?	37s	0 %	
<input type="checkbox"/> DELL Server	CPU interrupt time ?	36s	0 %	
<input type="checkbox"/> DELL Server	CPU privileged time ?	35s	0 %	-0.07694 %
<input type="checkbox"/> DELL Server	CPU queue length ?	32s	0	
<input type="checkbox"/> DELL Server	CPU user time ?	34s	0.3847 %	+0.07693 %
<input type="checkbox"/> DELL Server	CPU utilization ?	29s	0.4881 %	-0.04226 %
<input type="checkbox"/> DELL Server	Number of cores ?	16s	20	

Figura 15 - Métricas CPU – Dispositivo Servidor Cliente B

Métricas de Rede (Figura 16): Visão detalhada sobre o tráfego de rede, incluindo a velocidade da interface, o tráfego de chegada e o tráfego de saída, endereço MAC do dispositivo e endereço IP do dispositivo.

<input type="checkbox"/> Host	Name ▲	Last check	Last value	Change
<input type="checkbox"/> AP-IW	Interface Speed (Mbit/s)	13m 3s	1000	
<input type="checkbox"/> AP-IW	IP Address	3m 3s	10.10.100.50	
<input type="checkbox"/> AP-IW	LAN Traffic Incoming	3s	647 Bps	-416 Bps
<input type="checkbox"/> AP-IW	LAN Traffic Incoming Errors	3s	0 Error(s)	
<input type="checkbox"/> AP-IW	LAN Traffic Outgoing	3s	500 Bps	-94 Bps
<input type="checkbox"/> AP-IW	LAN Traffic Outgoing Errors	3s	0 Error(s)	
<input type="checkbox"/> AP-IW	MAC Address	13m 3s	D0 21 F9 26 7D 74	

Figura 16 - Métricas Rede - Dispositivo AP-IW Cliente A

Métricas de Disponibilidade (Figura 17): Informações sobre o tempo de atividade dos sistemas, destacando qualquer período de inatividade.

<input type="checkbox"/> Host	Name ▲	Last check	Last value	Change
<input type="checkbox"/> AP-U6PRO	ICMP Check	6s	1	
<input type="checkbox"/> AP-U6PRO	Uptime	3m 43s	12 days, 01:22:24	+00:05:00

Figura 17 - Métricas Disponibilidade - Dispositivo AP-U6PRO Cliente A

Tendo em consideração os requisitos dos clientes, procedeu-se à verificação da compatibilidade dos itens monitorizados com as necessidades apresentadas. Esta etapa assegurou que todos os parâmetros monitorizados, desde a performance até

aos indicadores de rede, estavam alinhados com as expectativas e exigências dos clientes. Após esta verificação, foram implementados gatilhos, configurados para alertar a RTU em caso de mudanças significativas nos valores ou na deteção de falhas. Estes gatilhos são essenciais para uma resposta rápida e eficaz (Figura 18).

Severity	Value	Name ▲	Expression
Warning	OK	UBQT UNIFI SNMP V3 HN: Channel utilization 2G on {HOST.NAME} high	<code>avg(/AP-IW/unifiRadioCuTotal.1,300s)=80</code>
Average	OK	UBQT UNIFI SNMP V3 HN: Channel utilization 2G on {HOST.NAME} very high	<code>avg(/AP-IW/unifiRadioCuTotal.1,300s)=90</code>
Warning	OK	UBQT UNIFI SNMP V3 HN: Channel utilization 5G on {HOST.NAME} high	<code>avg(/AP-IW/unifiRadioCuTotal.2,300s)=80</code>
Average	OK	UBQT UNIFI SNMP V3 HN: Channel utilization 5G on {HOST.NAME} very high	<code>avg(/AP-IW/unifiRadioCuTotal.2,300s)=90</code>
Disaster	OK	UBQT UNIFI SNMP V3 HN: Check Device Status	<code>last(/AP-IW/icmpping)=0</code>
Average	OK	UBQT UNIFI SNMP V3 HN: Processor load is too high on {HOST.NAME}	<code>avg(/AP-IW/laLoad.1,5m)>1</code>
High	OK	UBQT UNIFI SNMP V3 HN: Processor load is very high on {HOST.NAME}	<code>avg(/AP-IW/laLoad.1,5m)>3</code>

Figura 18 - Triggers Dispositivo AP-IW Cliente A

C008 – Alertas e Notificações

Nesta fase do projeto, um dos objetivos primordiais foi a implementação de notificações em tempo real para dispositivos móveis, especificamente para os telemóveis utilizados pela RTU. Entre as várias opções disponíveis, a escolha recaiu sobre o Telegram. Sendo uma aplicação não tão comum, esta estratégia visa evitar confusões com outras mensagens do dia a dia, assegurando que as notificações da ferramenta se destaquem e sejam prontamente identificadas e atendidas. Na interface web do Zabbix, essa funcionalidade é implementada através dos 'Alerts -> Media Types'.

A integração do Telegram com o Zabbix utiliza uma API que pode ser gerada através da aplicação e configurada para enviar mensagens para um grupo dentro da aplicação, identificado por um token (Figura 19).

Media type Message templates 5 Options

* Name Telegram BOT

Type Webhook

Parameters	Name	Value	Action
	Message	{ALERT.MESSAGE}	Remove
	ParseMode	markdown	Remove
	Subject	{ALERT.SUBJECT}	Remove
	To	{ALERT.SENDTO}	Remove
	Token	6169294313:AAEnhdeZww08Van	Remove
	Add		

* Script var Telegram = {...

* Timeout 10s

Process tags ☐

Include event menu entry ☐

* Menu entry name

* Menu entry URL

Description <https://git.zabbix.com/projects/ZBX/repos/zabbix/browse/templates/media/telegram>

1. Register bot: send "/newbot" to @BotFather and follow instructions
 2. Copy and paste the obtained token into the "Token" field above
 3. If you want to send personal notifications, you need to get chat id of the user you want to send messages to:

Enabled ☒

[Update](#) [Clone](#) [Delete](#) [Cancel](#)

Figura 19 - Configuração Telegram na Interface Web

Existe também a possibilidade de personalizar as mensagens, consoante o tipo e severidade. Se o alerta gerado for um problema, a mensagem enviada tem como conteúdo:

```
Device/Host: {HOST.NAME}
Problem started at {EVENT.TIME} on {EVENT.DATE}
Problem name: {EVENT.NAME}
Host: {HOST.NAME}
Severity: {EVENT.SEVERITY}
Original problem ID: {EVENT.ID}
```

Identificando desta forma o dispositivo, a data e hora do acontecimento, o problema, a severidade e uma identificação do problema através de um código, gerado automaticamente, de forma a tornar cada problema único.

5. Análise de Resultados

Para proporcionar uma compreensão mais ampla e tangível do impacto da ferramenta implementada, procedeu-se à gravação de três vídeos que documentam o funcionamento do sistema em tempo real na RTU. Este registo audiovisual visa captar a eficácia e a fluidez do sistema em operação, oferecendo uma perspetiva prática sobre a sua utilidade e desempenho. A gravação inclui uma entrevista com o orientador do estágio, demonstrações de como as notificações são recebidas e tratadas, e a interação dos utilizadores com o sistema. Estes vídeos são uma ferramenta valiosa para ilustrar os benefícios e a funcionalidade do sistema de uma forma que complementa a descrição textual. Para aceder aos vídeos, basta utilizar o código QR fornecido abaixo.



Figura 20 - Código QR

5.1. Análise de Métricas Específicas

Esta análise é crucial para compreender a indisponibilidade dos equipamentos durante o período em questão, oferecendo uma visão clara sobre a fiabilidade e a eficiência do dispositivo. Através destes dados, é possível identificar padrões, prever tendências e, conseqüentemente, tomar medidas preventivas para melhorar o desempenho e a disponibilidade do equipamento. Ao focarmos num período temporal definido, que neste caso corresponde à duração do estágio, é possível avaliar, por exemplo, o relatório de disponibilidade ilustrado na figura 21.

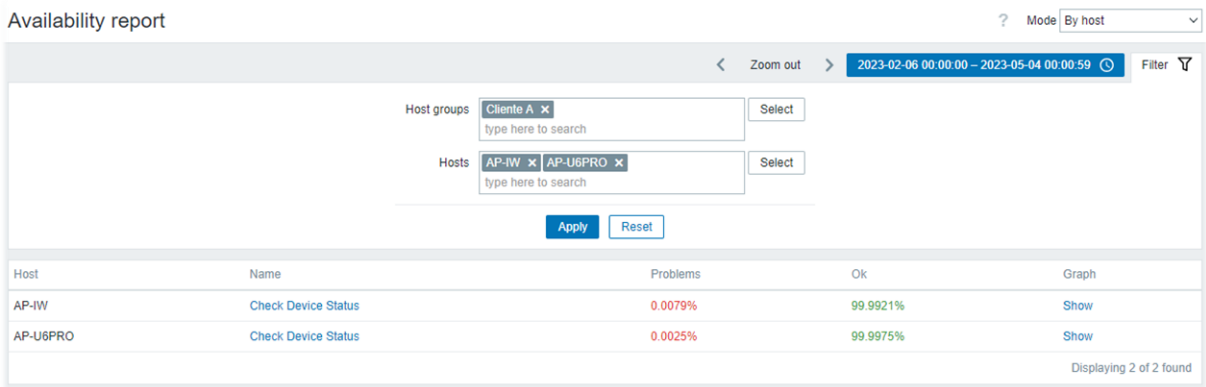


Figura 21 - Relatório de Disponibilidade

A interface web permite uma visualização simplificada e acessível dos gráficos gerados pelo Zabbix, destacando o número de utilizadores ligados ao equipamento AP-U6PRO. Esta funcionalidade facilita o controlo em tempo real da utilização do equipamento (Figura 22).

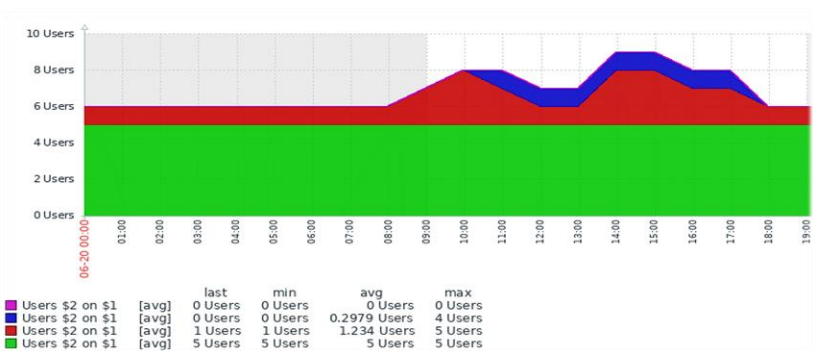


Figura 22 - Gráfico de Clientes AP-U6PRO

5.2. Histórico de Dados

Explora-se a funcionalidade de 'Housekeeping' do Zabbix, um mecanismo para a gestão do histórico de dados. Por defeito, esta função está configurada para reter dados por um período de 365 dias. Dada a incerteza quanto ao volume de dados que a ferramenta gerará e as necessidades específicas da RTU relativamente ao histórico, optou-se por manter esta configuração padrão.

Este período de retenção oferece um equilíbrio entre a manutenção de um histórico de dados suficientemente extenso e a capacidade de armazenamento do servidor.

Salienta-se a flexibilidade do Zabbix nesta matéria. Os parâmetros da função podem ser ajustados e adaptados a qualquer momento, permitindo uma resposta ágil a mudanças nas necessidades de retenção de dados ou na política de gestão de dados da RTU como ilustrado na figura 23.

Housekeeping

Events and alerts

Enable internal housekeeping ☒

* Trigger data storage period 365d

* Service data storage period 1d

* Internal data storage period 1d

* Network discovery data storage period 1d

* Autoregistration data storage period 1d

Services

Enable internal housekeeping ☒

* Data storage period 365d

User sessions

Enable internal housekeeping ☒

* Data storage period 365d

History

Enable internal housekeeping ☒

Override item history period ☐

* Data storage period 90d

Trends

Enable internal housekeeping ☒

Override item trend period ☐

* Data storage period 365d

Figura 23 - Configuração da retenção de dados

6. Conclusões e Trabalhos Futuros

É fundamental reconhecer que a implementação da ferramenta Zabbix na RTU superou as expectativas iniciais, revelando-se um êxito. Atualmente em plena operação e a recolher dados de forma eficiente, esta ferramenta tem contribuído significativamente para aprimorar a capacidade de resposta e gestão dos sistemas críticos.

Contudo, é importante salientar, que devido a limitações temporais, alguns aspetos previstos não foram totalmente desenvolvidos ou implementados. Estes elementos, que representam oportunidades para desenvolvimentos futuros, serão explorados detalhadamente nos pontos seguintes.

Assim, este capítulo não só faz um resumo do sucesso alcançado até ao momento, mas também traça um caminho claro para a continuação e evolução do projeto, assegurando que a RTU se mantenha na vanguarda da tecnologia de monitorização de sistemas.

6.1. Plano de Formação

Expõe-se a necessidade de continuar a formar os utilizadores da ferramenta Zabbix após o período de estágio. Esta formação contínua é fundamental para garantir que os utilizadores não só compreendam plenamente todas as funcionalidades e potencialidades da ferramenta, mas também sejam capazes de realizar a sua manutenção e prestar suporte de forma eficaz.

Dada a complexidade e a abrangência do sistema, a formação não pode ser vista como um evento isolado, mas sim como um processo contínuo.

O Plano de Formação deverá ser flexível, adaptando-se às necessidades e ao feedback dos utilizadores, garantindo assim uma formação relevante e eficaz.

6.2. Configuração do Painel de Cliente

Na perspetiva do cliente, seria também relevante ter acesso às informações que lhe dizem respeito, para poderem verificar o estado dos seus sistemas. Neste contexto, propõe-se a criação de um ambiente controlado dentro do Zabbix,

especificamente desenhado tendo em conta as necessidades e características de cada cliente.

Este ambiente permitirá que os clientes tenham acesso à visualização dos dados relativos aos seus sistemas, mas sem a possibilidade de realizar quaisquer alterações. Essencialmente, os clientes poderão consultar os dados e análises pertinentes sem que represente um risco para a integridade da ferramenta ou a segurança dos dados.

Através da interface web é possível configurar contas de utilizador, gerir as permissões e dados a visualizar. Deverá também ser melhorada a segurança da autenticação da página web, assegurando a proteção dos dados e a legitimidade dos acessos.

6.3. Políticas de Segurança – Retenção e Integridade dos Dados

Relativamente às políticas de segurança, deve ser adotado um plano rigoroso de cópias da base de dados e da ferramenta, de forma a garantir a máxima segurança e integridade dos dados. Idealmente, estas cópias automáticas serão programadas para ocorrer em intervalos definidos, garantindo, assim, que os dados mais recentes estejam sempre disponíveis e seguros.

Além da regularidade e da automatização, o plano deve abranger protocolos de teste regulares para as cópias de segurança. Estes testes são cruciais para verificar a eficácia do processo de backup e para assegurar que, em caso de falha, os dados possam ser recuperados de forma eficiente e completa.

6.4. Análise de Padrões, Predição de Comportamentos e I.A

A ferramenta permite estudar comportamentos através de cálculos matemáticos, fornecendo previsões de possíveis acontecimentos. No entanto, a integração da Inteligência Artificial (I.A) neste processo abriria um leque ainda mais amplo de possibilidades, elevando significativamente a eficácia e a precisão na previsão dos sistemas.

Adicionalmente, a implementação da I.A no Zabbix, poderia revolucionar a forma como são geridos os eventos, automatizando processos que vão além da mera análise de dados. Um dos aspetos mais promissores desta integração seria a

capacidade da I.A identificar e corrigir falhas automaticamente, sem intervenção humana, aumentando significativamente a eficiência do sistema.

Este objetivo irá constituir uma proposta de trabalho final do Mestrado em Engenharia Informática (MEI) da EST-IPCA.

Bibliografia

- Dmitry Lambert. (2021, August 31). *Top 5 reasons to choose Zabbix for network monitoring*. <https://blog.zabbix.com/top-5-reasons-to-choose-zabbix-for-network-monitoring/15247/>
- Ionos. (2023, January 8). *What are the differences between VPS and dedicated servers?* <https://www.ionos.com/digitalguide/server/know-how/vps-vs-dedicated-servers/>
- Jeff Hiatt. (2006). *ADKAR: A Model for Change in Business, Government, and Our Community* (Prosci Learning Center Publications, Ed.). https://www.google.pt/books/edition/ADKAR/Te_cHbWv-ZgC?hl=pt-PT&gbpv=1&kptab=overview
- Nathan Liefting, & Brian van Baekel. (2022). *Zabbix 6 IT Infrastructure Monitoring Cookbook* (Packt Publishing, Ed.). https://www.google.pt/books/edition/Zabbix_6_IT_Infrastructure_Monitoring_Co/gzIIEAAAQBAJ?hl=pt-PT&gbpv=0
- Paulo Gardini Miguel. (2023). *Zabbix Monitoring Software In-Depth Review*. <https://thectoclub.com/tools/zabbix-review/>
- Rajesh Kumar. (2023, September 3). *Zabbix Tutorials: Install and Configure Zabbix Proxy on Ubuntu 20.x*. <https://www.devopsschool.com/blog/install-and-configure-zabbix-proxy-on-ubuntu-20-x/>
- Seyed Tahaghoghi, & Hugh E. Williams. (2007). *Learning MySQL* (Andy Oram, Ed.; Second Edition). O'Reilly Media, Inc.
- Zabbix. (2023a). *Agent*. Zabbix Documentation. <https://www.zabbix.com/documentation/current/en/manual/concepts/agent>
- Zabbix. (2023b). *Hosts and host groups*. Zabbix Documentation. <https://www.zabbix.com/documentation/current/en/manual/config/hosts>
- Zabbix. (2023c). *Proxies*. Zabbix Documentation. https://www.zabbix.com/documentation/current/en/manual/distributed_monitoring/proxies

- Zabbix. (2023d). *Proxy*. Zabbix Documentation.
<https://www.zabbix.com/documentation/current/en/manual/concepts/proxy>
- Zabbix. (2023e). *Server*. Zabbix Documentation.
<https://www.zabbix.com/documentation/current/en/manual/concepts/server>
- Zabbix. (2023f). *Templates and template groups*. Zabbix Documentation.
<https://www.zabbix.com/documentation/current/en/manual/config/templates>
- Zabbix. (2023g). *Using pre-shared keys*. Zabbix Documentation.
https://www.zabbix.com/documentation/current/en/manual/encryption/using_pre_shared_keys
- Zabbix. (2023h). *Zabbix Features*. Zabbix Documentation.
<https://www.zabbix.com/features>
- Zabbix. (2023i). *Zabbix Manual*. Zabbix Documentation.
<https://www.zabbix.com/documentation/current/en/manual>

ANEXOS

Anexo A – Base de Dados Zabbix 6.4

