# Relatório de Estágio

João Filipe Gonçalves Costa

Curso Técnico Superior Profissional em Cibersegurança

set | 2023

GUARDA
POLI
TÉCNICO

POLI TÉCNICO GUARDA

**Escola Superior de Tecnologia e Gestão**

# RELATÓRIO DE ESTÁGIO

PROJETO EM CONTEXTO DE ESTÁGIO
PARA OBTENÇÃO DO DIPLOMA DE TÉCNICO(A) SUPERIOR PROFISSIONAL
EM CIBERSEGURANÇA

**João Filipe Gonçalves Costa**
**Setembro / 2023**

POLI TÉCNICO GUARDA

**Escola Superior de Tecnologia e Gestão**

# RELATÓRIO DE ESTÁGIO

PROJETO EM CONTEXTO DE ESTÁGIO
PARA OBTENÇÃO DO DIPLOMA DE TÉCNICO(A) SUPERIOR PROFISSIONAL
EM CIBERSEGURANÇA

Professor(a) Orientador(a): Noémio De Jesus Da Encarnação Dória
Supervisor(a): Pedro Manuel Pinto Teixeira

**João Filipe Gonçalves Costa**
**Setembro / 2023**

# Agradecimentos

Aqui vai um pequeno agradecimento a todas as pessoas que me ajudaram e apoiaram durante este período desafiador e gratificante.

Primeiramente, gostaria de expressar minha sincera gratidão às minhas avós, que sempre estiveram ao meu lado, encorajando-me e dando me motivação a dar sempre o meu melhor. A sabedoria, gentileza e amor incondicional que me foi dado foram fundamentais para o meu crescimento pessoal e profissional.

Agradeço também ao meu pai, que sempre foi um modelo de determinação e perseverança. A sua dedicação e luta pelo apoio financeiro tornaram possível a realização deste estágio e a minha formação como profissional.

Não posso deixar de mencionar a minha namorada, que sempre me incentivou a seguir os meus sonhos e me apoiou em todos os momentos. O seu amor, paciência e compreensão deram-me a força necessária para superar os desafios e nunca desistir.

Agradeço a toda a minha família, que esteve sempre presente e me apoiou em cada etapa da minha vida. Todo esse apoio foi fundamental para minha a formação pessoal e profissional.

Quero também agradecer ao Engenheiro Micael Pires e ao meu colega de curso José Albuquerque pela partilha de conhecimentos e pela amizade que fomos criando ao longo do tempo.

Por fim, agradeço também aos meus professores Pedro Pinto e Noémio Dória pela aprendizagem fornecida e por estarem sempre disponíveis para qualquer tipo de situação.

A todos que mencionei acima e a todos os outros que me ajudaram ao longo do caminho, o meu mais profundo agradecimento. Todo este apoio tornou possível a realização deste estágio e ajudou-me a crescer como profissional e como pessoa.

# Ficha de Identificação

Aluno

Nome: João Filipe Gonçalves Costa

Número: 1706909

Curso: CTeSP em Cibersegurança

Estabelecimento de Ensino

Politécnico da Guarda

Escola Superior de Tecnologia e Gestão (ESTG)

Entidade Acolhedora do Estágio

Nome: Centro de Informática (Politécnico da Guarda)

Morada: Av. Dr. Francisco Sá Carneiro 50, 6300-559 Guarda

Contacto Telefónico: 271 220 100

Supervisor de Estágio

Nome: Pedro Manuel Pinto Teixeira

Email: ppinto@ipg.pt

Função: Chief Information Security Officer

Grau Académico: Mestrado

Docente Orientador de Estágio

Nome: Noémio De Jesus Da Encarnação Dória

Email: ndoria@ipg.pt

Função: Especialista de Informática

Grau Académico: Mestrado

# Resumo

No relatório, vai ser apresentada uma introdução sobre a importância da cibersegurança num mundo cada vez mais digital e conectado, destacando como as soluções de monitorização são fundamentais para garantir a segurança e estabilidade dos sistemas de TI (Tecnologias da informação). Vão ser detalhadas as funcionalidades do Zabbix e do Icinga, bem como as diferenças entre as duas soluções.

Ao longo do período de estágio, foram adquiridos conhecimentos sobre as características e benefícios de cada ferramenta, bem como os desafios associados à instalação e utilização das mesmas. Por meio da experiência prática, foram comparadas e avaliadas as vantagens e desvantagens de cada ferramenta, fornecendo habilidades valiosas para aqueles que desejam explorar essas soluções para atender às suas necessidades específicas.

No relatório, é descrito como cada ferramenta é instalada e configurada, bem como a sua capacidade de monitorizar e relatar o desempenho da infraestrutura de TI. Além disso, são apresentados exemplos de casos em que o Zabbix e o Icinga foram utilizados para monitorizar sistemas e identificar problemas antes que afetassem o desempenho ou a segurança.

Em resumo, o relatório fornece uma visão geral sobre o Zabbix e o Icinga, apresentando as suas funcionalidades, benefícios e desafios. São oferecidos habilidades valiosas sobre a instalação e utilização das soluções de monitorização, bem como exemplos práticos de como essas ferramentas podem ser utilizadas para garantir a segurança e estabilidade de sistemas de TI em Linux. O relatório tem como objetivo contribuir para uma melhor compreensão dessas duas ferramentas de monitorização e fornecer informações úteis para aqueles que desejam explorá-las nas suas infraestruturas de TI.

# Abstract

The report will present an introduction to the importance of cybersecurity in an increasingly digital and connected world, highlighting how monitoring solutions are fundamental to ensuring the security and stability of IT systems. The functionalities of Zabbix and Icinga will be detailed, as well as the differences between the two solutions.

Throughout the internship period, knowledge was acquired about the characteristics and benefits of each tool, as well as the challenges associated with their installation and use. Through practical experience, the advantages and disadvantages of each tool were compared and evaluated, providing valuable insights for those who wish to explore these solutions to meet their specific needs.

The report describes how each tool is installed and configured, as well as its ability to monitor and report the performance of the IT infrastructure. In addition, examples are presented of cases where Zabbix and Icinga were used to monitor systems and identify issues before they affected performance or security.

In summary, the report provides an overview of Zabbix and Icinga, presenting their functionalities, benefits, and challenges. Valuable insights are offered on the installation and use of monitoring solutions, as well as practical examples of how these tools can be used to ensure the security and stability of IT systems in Linux. The report aims to contribute to a better understanding of these two monitoring tools and provide useful information for those who wish to explore them in their IT infrastructures.

# Índice

# Índice de figuras

# Glossário de Abreviaturas

| | |
|---|---|
| API | Application Programming Interface |
| BD | Base de Dados |
| CPU | Central Processing Unit |
| CSR | Certificate Signing Request |
| ESTG | Escola Superior de Tecnologia e Gestão |
| IDO | Intelligent Data Object |
| IP | Internet Protocol |
| IPG | Instituto Politécnico da Guarda |
| IPMI | Intelligent Platform Management Interface |
| JMX | Java Management Extensions |
| PSK | Pre-shared key |
| SQL | Structured Query Language |
| SMTP | Simple Mail Transfer Protocol |
| SNMP | Simple Network Management Protocol |
| TFTP | Trivial File Transfer Protocol |
| TI | Tecnologias da Informação |
| VM | Virtual Machine |
| VoIP | Voz sobre IP |
| WEB | World Wide Web |
| URL | Uniform Resource Locator |

# 1 Introdução

Num mundo cada vez mais digital e conectado, a cibersegurança é uma preocupação constante para empresas e utilizadores da tecnologia. Neste sentido, as soluções de monitorização são fundamentais numa infraestrutura, como o Zabbix e o Icinga, ambos têm um papel fundamental na garantia da segurança e estabilidade dos sistemas. Este relatório de estágio tem como objetivo apresentar as minhas experiências ao instalar e utilizar as duas soluções de monitorização de uma infraestrutura em Linux, o Zabbix e o Icinga. Ao longo do período de estágio, pude adquirir conhecimentos sobre as funcionalidades e características de cada uma dessas ferramentas, bem como sobre os benefícios e desafios associados à instalação e utilização das mesmas. Neste relatório, apresentarei uma introdução ao Zabbix e ao Icinga, detalhando as suas principais funcionalidades, bem como as diferenças entre as duas soluções. Além disso, irei comparar e avaliar as vantagens e desvantagens de cada ferramenta, com base na minha experiência pessoal. Irei também mencionar diversas operações realizadas ao longo do meu percurso de estágio. Com este relatório, espero contribuir para uma melhor compreensão dessas duas ferramentas de monitorização, fornecendo informações valiosas para aqueles que desejam explorar estas soluções para responder às suas necessidades específicas. Espero que este relatório seja útil e informativo para todos os leitores.

## 1.1 Motivação

Diversos fatores impulsionaram e despertaram a minha motivação e interesse nesta área específica. Sempre fui fascinado pelo mundo da tecnologia e pelo seu impacto nas organizações. Ao perceber a importância da monitorização adequada dos equipamentos de uma infraestrutura de TI, compreendi que essa é uma tarefa crucial para garantir o bom funcionamento dos sistemas e a disponibilidade dos serviços. O projeto de estágio proporcionou-me a oportunidade de colocar em prática os conhecimentos teóricos adquiridos ao longo da minha formação académica. Poder aplicar os conceitos aprendidos em sala de aula em um contexto real e desafiador foi um estímulo significativo.

## 1.2 Caraterização sumária da instituição

O Politécnico da Guarda é uma instituição de ensino superior pública portuguesa, situada em Portugal, mais concretamente na cidade da Guarda, onde se situam três das quatro escolas superiores (Escola Superior de Educação, Comunicação e Desporto, Escola Superior de Saúde e Escola Superior de Tecnologia e Gestão) e a restante, em Seia (Escola Superior de Turismo e Hotelaria).

A constituição do Politécnico da Guarda ocorreu apenas em 1980, mediante o Decreto-Lei nº 303/80, de 16 de agosto, de onde surgiram também outros politécnicos, nomeadamente: o Politécnico de Leiria, o Politécnico de Portalegre e o Politécnico de Viana do Castelo.

Cinco anos mais tarde, surge a Escola Superior de Tecnologia de Gestão através do Decreto-Lei nº 46/85, de 22 de novembro (PolitecnicoGuarda, 2022).

Atualmente, a mesma dispõe de uma vasta oferta formativa, tendo para oferecer aos novos estudantes: 24 cursos técnicos superiores profissionais, 11 licenciaturas e 5 mestrados.

Inserido no Politécnico da Guarda, está o Centro de Informática, onde o estagiário teve a oportunidade de realizar o seu estágio.

### 1.2.1 Caracterização da entidade acolhedora de estágio

O Centro de Informática da Escola Superior de Tecnologia e Gestão tem como missão garantir o bom funcionamento de toda a infraestrutura informática do Politécnico da Guarda.

A sua área de atuação compreende a manutenção e segurança de toda a infraestrutura de rede, administração de sistemas e serviços, bem como oferecer suporte aos utilizadores de toda a comunidade IPG, visa ainda o desenvolvimento de projetos com o intuito de melhorar a atual infraestrutura.

Este encontra-se situado no Politécnico da Guarda, situado na Avenida Dr. Francisco Sá Carneiro, nº50, 6300-559, Guarda.

## 1.3 Objetivos

O objetivo principal do projeto foi comparar e avaliar as soluções de monitorização Zabbix e Icinga numa infraestrutura de TI. Os objetivos específicos incluíram o estudo da infraestrutura existente, a seleção das soluções de monitorização, a configuração das soluções, a realização de testes de monitorização, a comparação e avaliação dos resultados, e a elaboração de um relatório final com conclusões e recomendações. O projeto visou fornecer informações relevantes para a escolha da solução de monitorização mais adequada.

## 1.4 Estrutura do relatório

A estrutura deste relatório é composta por diversas secções que abrangem desde a motivação inicial até á conclusão das tarefas realizadas. Todas as fontes utilizadas nas figuras estão identificadas na legenda, se a figura não tiver uma fonte será porque se trata de uma fonte própria. A seguir, é apresentada uma breve descrição das secções que compõem este relatório:

### 1.4.1 Introdução (Secção 1):

Nesta secção, são apresentados os principais objetivos e a motivação por trás do estágio, bem como uma caraterização sumária da instituição onde o mesmo foi realizado.

### 1.4.2 Metodologia (Secção 2):

Aqui, é descrevida em detalhes a metodologia adotada para a realização das atividades, incluindo a definição dos critérios de comparação, a captura de dados, a configuração do ambiente de testes, a execução dos testes e a análise dos resultados.

### 1.4.3 Descrição das Soluções (Secção 3):

Esta Secção aborda as duas principais soluções de monitorização, Icinga e Zabbix, detalhando suas características, funcionalidades, vantagens e limitações.

### 1.4.4 Instalação das Soluções (Secção 4):

Nesta Secção, são fornecidas instruções passo a passo para a instalação das soluções Icinga e Zabbix, incluindo informações específicas sobre a instalação do Icinga Director no Debian e a configuração do agente do Zabbix em ambientes Windows.

### 1.4.5 Atualização de Firmwares (Secção 5):

Aqui, descrevemos o processo de atualização de firmwares, destacando sua importância na manutenção da infraestrutura de rede.

### 1.4.6 Outras Operações Realizadas (Secção 6):

Esta secção abrange outras atividades e operações que foram realizadas durante o estágio e que contribuíram para o desenvolvimento das minhas competências e conhecimentos.

### 1.4.7 Conclusão (Secção 7):

Finalmente, na secção de conclusão, discutimos a importância da monitorização de redes numa infraestrutura, destacamos as dificuldades enfrentadas e é apresentada uma conclusão final que resume os principais resultados e aprendizagens obtidas durante o estágio.

# 2 Metodologia

Neste capítulo, descreveremos a metodologia utilizada para realizar a comparação entre as soluções de monitorização Zabbix e Icinga. Dividimos a metodologia em cinco etapas principais: definição dos critérios de comparação, captura de dados, configuração do ambiente de testes, execução dos testes e análise dos resultados.

## 2.1 Definição dos Critérios de Comparação

Antes de iniciar a comparação, foram estabelecidos critérios de comparação para avaliar as soluções de monitorização. Os critérios selecionados foram os seguintes:

- Facilidade de Instalação e Configuração
- Interface e Usabilidade
- Capacidade de Monitorização
- Flexibilidade e Personalização
- Escalabilidade
- Suporte e Comunidade

Estes critérios foram escolhidos com base na importância para o ambiente de monitorização e nas necessidades específicas da organização.

## 2.2 Captura de Dados

Para realizar a comparação, foram obtidos dados relevantes sobre as soluções Zabbix e Icinga. Esses dados incluíram informações sobre as características, funcionalidades, vantagens e limitações de cada solução. Além disso, foram consultadas documentações oficiais, fóruns, blogs e outros recursos online para obter informações atualizadas e confiáveis.

## 2.3 Configuração do Ambiente de Testes

Um ambiente de testes foi configurado para implementar as soluções Zabbix e Icinga. O ambiente de testes consistiu em duas máquinas virtuais para a instalação e configuração das soluções num servidor dedicado, bem como um conjunto de máquinas virtuais onde foram configuradas com Windows para serem monitorizados para efeito de testes.

## 2.4 Execução dos testes

Após a configuração do ambiente de testes, foram realizados testes para avaliar o desempenho e a usabilidade de cada solução. Durante os testes, foram monitorizados diferentes aspetos, como disponibilidade, desempenho de rede, uso de recursos e alertas. Os testes foram executados ao longo de um período de tempo suficiente para obter uma análise abrangente das soluções.

## 2.5 Análise dos Resultados

Os resultados dos testes foram capturados e analisados com base nos critérios estabelecidos. Foram comparados os desempenhos das soluções em relação a cada critério, identificando pontos fortes e fracos de cada uma. Esta análise permitiu uma avaliação das soluções e facilitou a seleção da solução mais adequada às necessidades da organização.

# 3 Descrição das Soluções

## 3.1 Icinga

O Icinga é uma plataforma de monitorização de código aberto que se destaca pela sua flexibilidade e recursos avançados. Ele foi desenvolvido como uma bifurcação do Nagios e oferece várias melhorias e aprimoramentos. Vamos abordar aqui as suas características, funcionalidades, vantagens e limitações.

### 3.1.1 Características e Funcionalidades

**Monitorização de rede e sistemas:** O Icinga permite monitorizar ativos da rede, servidores, serviços e aplicações, fornecendo informações detalhadas sobre o seu estado e desempenho.

**Configuração flexível:** Ele oferece uma configuração flexível baseada em ficheiros de configuração que permite adaptar o Icinga às necessidades específicas do ambiente de TI.

**Visualizações e dashboards:** O Icinga oferece visualizações personalizáveis e *dashboards* que fornecem uma visão geral rápida do estado de monitorização.

**Integração com outros sistemas:** Ele suporta integrações com várias ferramentas e sistemas, permitindo a automação e ação com base nos resultados da monitorização.

### 3.1.2 Vantagens e Limitações

**Vantagens:**

- **Flexibilidade:** O Icinga é altamente flexível e pode ser personalizado para atender às necessidades específicas do ambiente de TI.
- **Comunidade ativa:** O Icinga também possui uma comunidade ativa de utilizadores que contribuem com plugins, extensões e suporte.
- **Interface amigável:** A interface do Icinga é conhecida pela sua usabilidade e facilidade de navegação.

**Limitações:**

- **Instalação complexa:** A instalação e configuração inicial do Icinga podem ser consideradas complexas, exigindo conhecimento técnico avançado e experiência para realizar o processo corretamente.
- **Aprendizagem inicial:** O Icinga pode exigir algum tempo para se familiarizar com a sua configuração e recursos.
- **Documentação:** A documentação oficial do Icinga pode não ser tão abrangente quanto a de outras soluções, mas a comunidade é uma excelente fonte de informações.
- **Necessidade de múltiplas bases de dados:** O Icinga pode exigir a utilização de várias bases de dados, o que pode aumentar a complexidade e a sobrecarga da gestão em comparação com o Zabbix, que utiliza apenas uma base de dados.

## 3.2 Zabbix

O Zabbix é também uma plataforma de monitorização da rede e sistemas de código aberto amplamente utilizada na indústria. Ele fornece recursos abrangentes para monitorizar e gerir ambientes de TI, permitindo a captura de métricas em tempo real, notificações personalizadas e visualizações detalhadas. Com a sua escalabilidade e flexibilidade, o Zabbix é capaz de lidar com ambientes complexos, fornecendo aos administradores uma visão abrangente do desempenho e disponibilidade dos seus sistemas e equipamentos.

### 3.2.1 Características e Funcionalidades

- **Monitorização abrangente:** O Zabbix oferece a capacidade de monitorizar diversos componentes da rede, servidores, dispositivos, aplicações e serviços em tempo real. Ele suporta a captura de métricas como disponibilidade, desempenho, utilização de recursos, eventos e registos de *logs*.
- **Captura de dados flexível:** O Zabbix suporta múltiplas formas de captura de dados, incluindo agentes dedicados, monitorização por SNMP, monitorização de protocolos específicos como IPMI e JMX, além de suportar APIs personalizadas.

- **Notificações e alertas personalizáveis:** O Zabbix permite configurar regras de notificação e alertas personalizados com base em eventos ou condições específicas, garantindo que o utilizador seja notificado de forma proativa sobre qualquer problema que exija atenção imediata.
- **Visualizações e relatórios detalhados:** A plataforma fornece uma interface gráfica intuitiva e personalizável, com painéis de controle e visualizações que apresentam dados em tempo real, permitindo que os utilizadores acompanhem o estado do sistema de maneira eficiente.
- **Monitorização distribuída e escalável:** O Zabbix pode ser dimensionado horizontalmente para monitorizar ambientes distribuídos e complexos, permitindo a adição de servidores *proxy* para captura e processamento distribuídos de dados de monitorização.

### 3.2.2 Vantagens e Limitações

**Vantagens:**

- **Utilização de uma única base de dados:** O Zabbix possui a vantagem de utilizar apenas uma base de dados para armazenar todas as informações de monitorização. Isso simplifica a implementação e a gestão, reduzindo a complexidade em comparação com o Icinga, que requer a utilização de várias bases de dados para diferentes componentes.
- **Interface intuitiva e amigável:** O Zabbix oferece uma interface gráfica intuitiva e fácil de usar, permitindo que os administradores configurem, monitorizem e giram os seus sistemas de forma eficiente. A interface amigável do Zabbix é conhecida pela sua usabilidade, o que facilita a navegação e a configuração da solução.
- **Ampla gama de recursos e funcionalidades:** O Zabbix oferece uma ampla gama de recursos e funcionalidades, como monitorização abrangente de redes, servidores e aplicações, notificações personalizadas, *dashboards* personalizáveis e relatórios detalhados. Esses recursos avançados permitem uma monitorização mais completa e uma análise mais aprofundada do ambiente de TI.

- **Escalabilidade e alta disponibilidade:** O Zabbix é altamente escalável e pode ser dimensionado para atender às necessidades de ambientes complexos e distribuídos. Ele suporta a configuração de servidores proxy para captura e processamento distribuídos de dados de monitorização, garantindo escalabilidade e alta disponibilidade em grande escala.
- **Comunidade ativa e suporte:** O Zabbix possui uma comunidade de utilizadores ativa, o que significa que há um amplo suporte disponível, bem como uma variedade de plugins, extensões e integrações desenvolvidas pela comunidade. Isso proporciona aos utilizadores um acesso a recursos adicionais e conhecimentos compartilhados.

**Limitações:**

- **Curva de aprendizagem inicial:** Assim como qualquer sistema complexo, o Zabbix possui uma curva de aprendizagem inicial. Os administradores podem necessitar de investir algum tempo para se familiarizarem com a configuração e com os recursos do Zabbix. No entanto, uma vez dominado, o Zabbix oferece uma ampla gama de funcionalidades para monitorização eficaz.
- **Configuração inicial mais detalhada:** A configuração inicial do Zabbix pode ser mais detalhada em comparação com o Icinga. É necessário definir *hosts*, itens, *triggers* e outros componentes para começar a monitorizar um ambiente. Isso pode exigir um planeamento cuidadoso e um entendimento claro dos requisitos de monitorização.
- **Gestão de recursos:** O Zabbix, devido às suas extensas funcionalidades, pode exigir mais recursos do hardware e armazenamento em comparação com soluções mais leves, dependendo do tamanho do ambiente de monitorização. É importante garantir que o sistema tenha recursos adequados para lidar com a carga de trabalho e com o volume de dados.
- **Documentação extensa:** A documentação oficial do Zabbix é abrangente, mas às vezes pode ser complexa. Além disso, algumas funcionalidades menos conhecidas ou específicas podem ter menos documentação disponível. No entanto, a comunidade do Zabbix é ativa e pode fornecer suporte adicional.

# 4 A Importância da monitorização da rede de uma infraestrutura

A crescente interligação de sistemas e dispositivos em ambientes empresariais e industriais trouxe consigo inúmeras vantagens, mas também ampliou consideravelmente a superfície de ciberataques. Nesse cenário, a importância da monitorização da rede de uma infraestrutura tornou-se crucial para garantir a segurança. A monitorização de rede é a prática de rastrear e analisar constantemente o tráfego de dados, os sistemas, os dispositivos e outros elementos de uma infraestrutura. Ao adotar soluções de monitorização como o Zabbix ou o Icinga, as organizações ganham a capacidade de identificar e resolver problemas de desempenho, anomalias e ameaças potenciais em tempo real. Esta abordagem pró-ativa exerce um impacto direto na cibersegurança.

Aqui estão algumas das razões pelas quais a monitorização da rede com soluções como o Zabbix ou Icinga é crucial para a cibersegurança:

**Deteção de Intrusões:** Ao monitorizar o tráfego de rede e os padrões de uso, ambas as soluções podem identificar atividades suspeitas que podem indicar tentativas de intrusão. Isto permite que a equipa de segurança responda rapidamente e tome medidas para conter a ameaça.

**Prevenção de Ataques:** A monitorização constante permite a deteção precoce de comportamentos invulgares, como varreduras de portas ou tráfego malicioso. Isto ajuda a impedir ataques antes que eles ganhem um ponto de apoio na rede.

**Identificação de Anomalias:** A capacidade de monitorizar métricas de desempenho, como utilização de CPU, uso de largura de banda e latência, ajuda a identificar anomalias que podem indicar atividade maliciosa ou falhas de sistema decorrentes de ataques.

**Resposta Rápida a Incidentes:** Com alertas em tempo real e painéis de controlo visuais, ambas as soluções permitem que as equipas de segurança reajam prontamente a incidentes cibernéticos, minimizando o impacto e acelerando a resolução.

**Monitorização de Ativos:** A monitorização não se limita apenas ao tráfego. Ambas as soluções também podem ser usadas para controlar a integridade e a segurança de dispositivos, servidores e outros ativos, garantindo que eles estejam atualizados e livres de vulnerabilidades conhecidas.

**Cumprimento de Normas de Segurança:** Muitas indústrias estão sujeitas a regulamentações rígidas de segurança. A monitorização da rede com ferramentas como ambas as soluções ajudam as organizações a cumprirem essas normas, demonstrando que estão a adotar medidas adequadas de proteção.

Resumindo, a monitorização da rede utilizando soluções de monitorização desempenham um papel crítico na manutenção da cibersegurança. Ao permitir uma visão detalhada do ambiente de rede e ao possibilitar a deteção precoce de ameaças, a monitorização ajuda a garantir que as organizações possam antecipar e responder eficazmente a ataques cibernéticos, mantendo assim a integridade e a continuidade das suas operações.

# 5 Instalação das soluções

## 5.1 Icinga

A seguinte solução foi instalada num ambiente Debian, primeiramente vamos atualizar todos os pacotes do Debian através dos seguintes comandos:

```
apt update
apt upgrade
```

Um requisito importante do Icinga é ter o LAMP instalado, para instalarmos o mesmo iremos utilizar o seguinte comando:

```
apt install apache2 mariadb-server mariadb-client mariadb-common php php-mysqli
```

Quando a instalação estiver concluída iremos verificar se todos os serviços estão a correr através dos comandos:

```
systemctl is-active apache2
systemctl is-active mariadb
```

Se os mesmos não estiverem ativos iremos então iniciar ambos os serviços:

```
systemctl start {apache2,mariadb}
```

Por fim antes de prosseguirmos iremos usar o comando "**mysql_secure_installation**" para definir a password da conta da base de dados *root*, mover utilizadores anónimos, desativar o login do *root* remotamente e remover a base de dados teste do MariaDB como podemos ver na figura 1.

```
root@tecmint:~# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] y
Enabled successfully!
Reloading privilege tables..
 ... Success!


You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
 ... Success!


By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y^C
Aborting!

Cleaning up...
root@tecmint:~#
```

*Figura 1 - Script de shell desenvolvido para proteger o MariaDB*

https://www.tecmint.com/install-mariadb-database-in-debian-10/

Para ser possível ter a interface web do Icinga é necessário também que o Apache Web Server esteja instalado, para o instalar utilizamos o comando:

```
apt-get install apache2
```

Agora podemos adicionar módulos de PHP adicionais através do comando:

```
sudo apt install php-gd php-mbstring php-mysqlnd php-curl php-xml php-cli php-soap php-intl php-xmlrpc php-zIP  php-common php-opcache php-gmp php-imagick php-pgsql  -y
```

E iremos também editar o seguinte ficheiro com as respetivas configurações:

```
nano /etc/php/7.4/apache2/php.ini
```

```
memory_limit = 256M
post_max_size = 64M
upload_max_filesize = 100M
max_execution_time = 300
default_charset = "UTF-8"
date.timezone = "Eur/Lisbon"
cgi.fix_pathinfo=0
```

Quando tivermos os passos anteriores todos concluídos iremos então proceder a instalação do Icinga e dos seus plugins de monitorização através do comando:

```
apt install icinga2 monitoring-plugins -y
```

Quando a instalação estiver finalizada iremos iniciar e ativar o Icinga, para isso iremos utilizar os comandos que se seguem:

```
sudo systemctl start icinga2
sudo systemctl enable icinga2
```

Para verificarmos se o Icinga está ativo introduzimos o seguinte comando:

```
systemctl status icinga2
```

De seguida vamos então passar para a instalação do módulo IDO do Icinga que serve para exportar todas as informações de configuração e estado para a base de dados IDO, utilizaremos o seguinte comando para o instalar:

```
apt install icinga2-ido-mysql -y
```

Agora iremos criar uma base de dados para o módulo Icinga-IDO MySQL, para isso iremos fazer login no prompt do MySQL através do comando:

```
sudo mysql -u root -p
```

Para criar a base de dados e o utilizador da mesma utilizamos os seguintes comandos:

```
CREATE DATABASE icinga_ido_db;
GRANT ALL ON icinga_ido_db.* TO 'icinga_ido_user'@'localhost' IDENTIFIED BY
'Password321';
FLUSH PRIVILEGES;
EXIT;
```

Agora é necessário importar o esquema do Icinga2 IDO através do comando:

```
sudo mysql -u root -p icinga_ido_db < /usr/share/icinga2-ido-mysql/schema/mysql.sql
```

Iremos agora ativar o módulo do Icinga-IDO MySQL, para isso entraremos no seguinte ficheiro:

```
nano /etc/icinga2/features-available/ido-mysql.conf
```

E iremos fazer as alterações necessárias como na figura 2 de acordo com os dados que introduzimos:

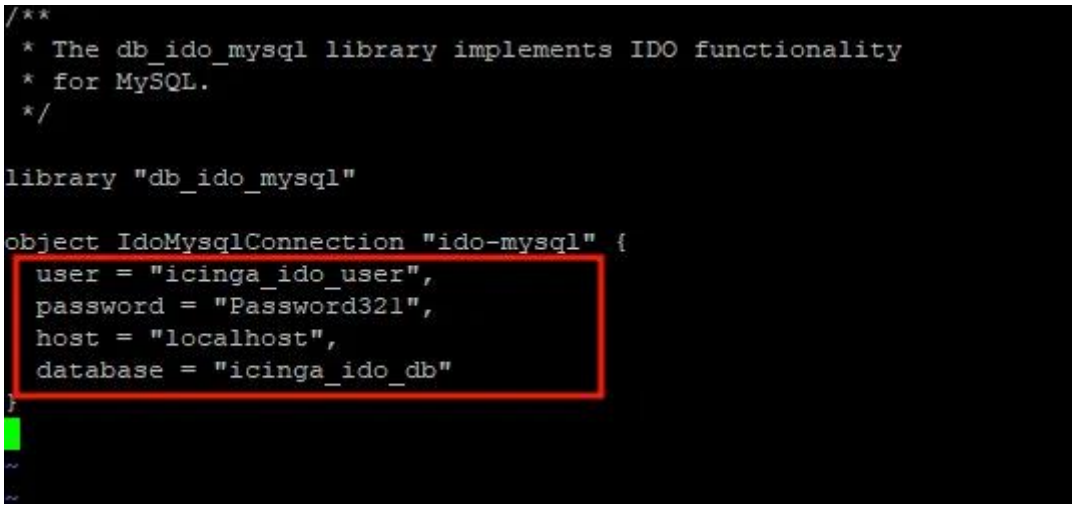


*Figura 2 - Dados a alterar de acordo com as informações da BD IDO*

*Fonte: https://www.tecmint.com/install-icinga2-monitoring-debian/*

Guardamos as configurações efetuadas e logo após ativamos o módulo através do seguinte comando:

```
icinga2 feature enable ido-mysql
```

Para aplicar as alterações efetuadas é necessário reiniciar o Icinga2:

```
systemctl restart icinga2
```

Agora por fim iremos instalar o IcingaWeb2 através do comando:

```
apt install icingaweb2 icingacli -y
```

E vamos também criar uma base de dados para o mesmo:

```
sudo mysql -u root -p
CREATE DATABASE icingaweb2;
GRANT ALL ON icingaweb2.* TO 'icingaweb2user'@'localhost' IDENTIFIED BY
'P@ssword';
FLUSH PRIVILEGES;
```

Para realizar a autenticação ao *setup* do browser vamos agora gerar um *token*:

```
icingacli setup token create
```

```
@debian-11:~$
@debian-11:~$
@debian-11:~$ sudo icingacli setup token create
The newly generated setup token is: b9c2051efef6f486
@debian-11:~$
@debian-11:~$
```

*Figura 3 - Token gerado*

*Fonte: https://www.tecmint.com/install-icinga2-monitoring-debian/*

Podemos finalmente aceder á interface Web do Icinga2 e proceder ao setup do mesmo através do seguinte URL:

```
http://IP-do-server/icingaweb2/setup
```

Iremos por fim colocar a *token* gerada como podemos ver na figura 4 para podermos realizar o *setup*.

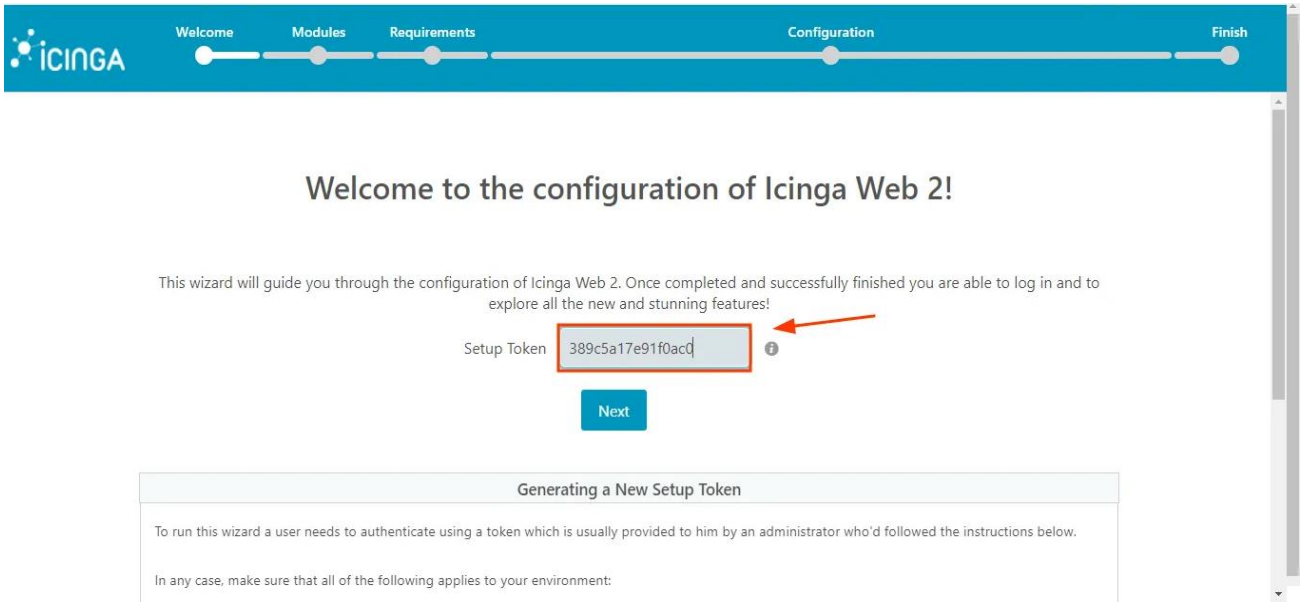


*Figura 4 - Local onde é introduzido o token gerado*

*Fonte: https://www.tecmint.com/install-icinga2-monitoring-debian/*

E está feito, podemos agora monitorizar a infraestrutura e fornecer feedback sobre a disponibilidade e o desempenho dos seus dispositivos tal como na figura 5.

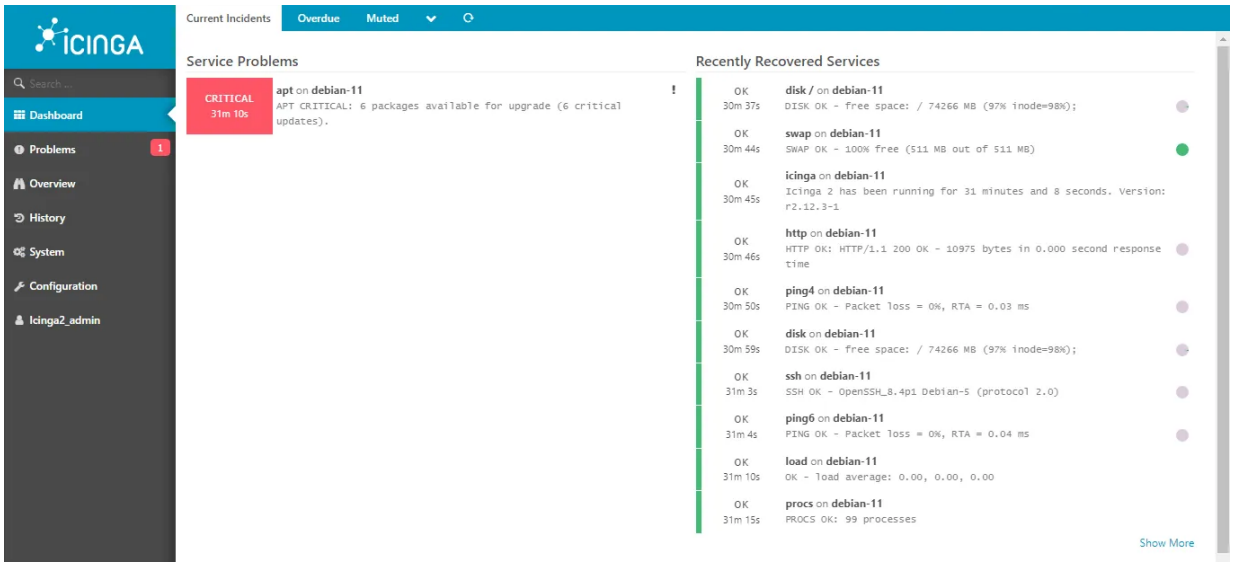


*Figura 5 – Interface web do Icinga*

*Fonte: https://www.tecmint.com/install-icinga2-monitoring-debian/*

### 5.1.1 Instalação do Icinga Director no Debian

O Icinga Director é um poderoso gestor de configuração para o Icinga. Ele permite que os utilizadores configurem e giram os seus sistemas de monitorização de uma maneira mais fácil e eficiente. Com o Icinga Director, os utilizadores podem criar e gerenciar objetos de monitorização, como *hosts* e serviços, sem precisar de editar manualmente os ficheiros de configuração. Em vez disso, eles podem usar a interface gráfica do utilizador do Diretor para criar objetos e definir suas propriedades, tais como os limiares de alerta e ações a serem tomadas em caso de problemas.

Primeiramente vamos adicionar o repositório de pacotes do Icinga através dos seguintes comandos:

```
apt-get -y install apt-transport-https wget gnupg

wget -O - https://packages.icinga.com/icinga.key | apt-key add -

DIST=$(awk -F"[)(]+" '/VERSION=/ {print $2}' /etc/os-release); \
 echo "deb https://packages.icinga.com/debian icinga-${DIST} main" > \
 /etc/apt/sources.list.d/${DIST}-icinga.list
 echo "deb-src https://packages.icinga.com/debian icinga-${DIST} main" >> \
 /etc/apt/sources.list.d/${DIST}-icinga.list
```

Iremos instalar os mesmos pacotes com o seguinte comando:

```
apt-get install icinga-director
```

Irá ser necessária mais uma base de dados para o Icinga Director para isso iremos cria-la através dos comandos que se seguem:

```
mysql -e "CREATE DATABASE director CHARACTER SET 'utf8';
  CREATE USER director@localhost IDENTIFIED BY 'CHANGEME';
  GRANT ALL ON director.* TO director@localhost;"
```

Para finalizar vamos adicionar um novo recurso que será neste caso para a base de dados do Icinga Director, para isso vamos a **Configuration** → **Application** → **Resources** → **Create a New Resource** devemos obter uma página tal como na figura 6.

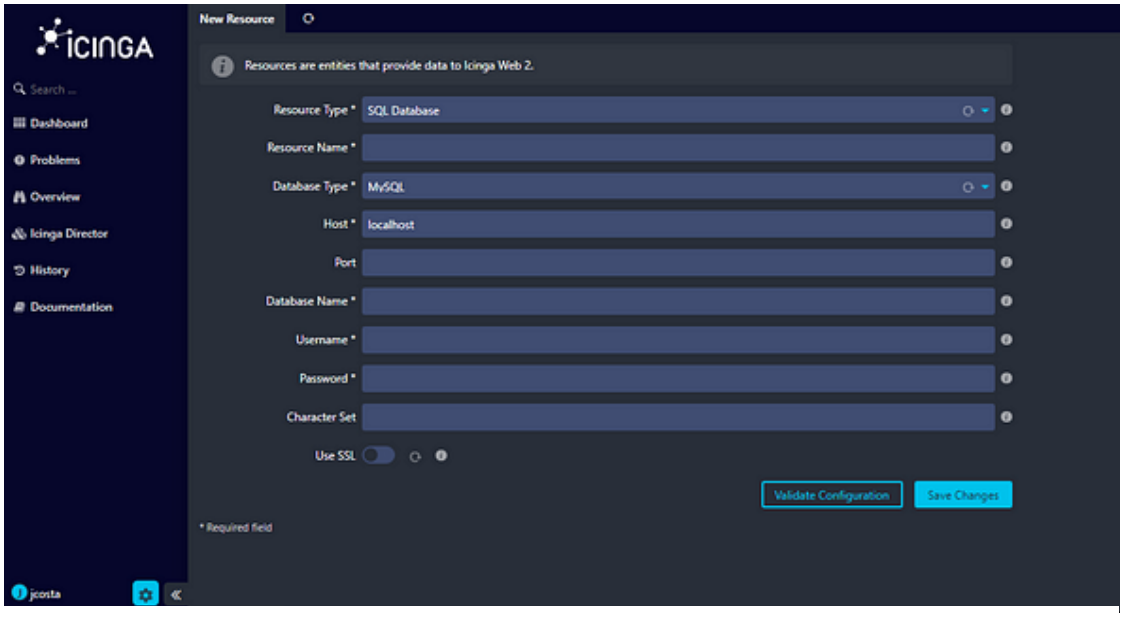


*Figura 6 - Criação de um novo Recurso no Icinga*

E está feito, temos o Icinga Director instalado como podemos ver na figura 7.

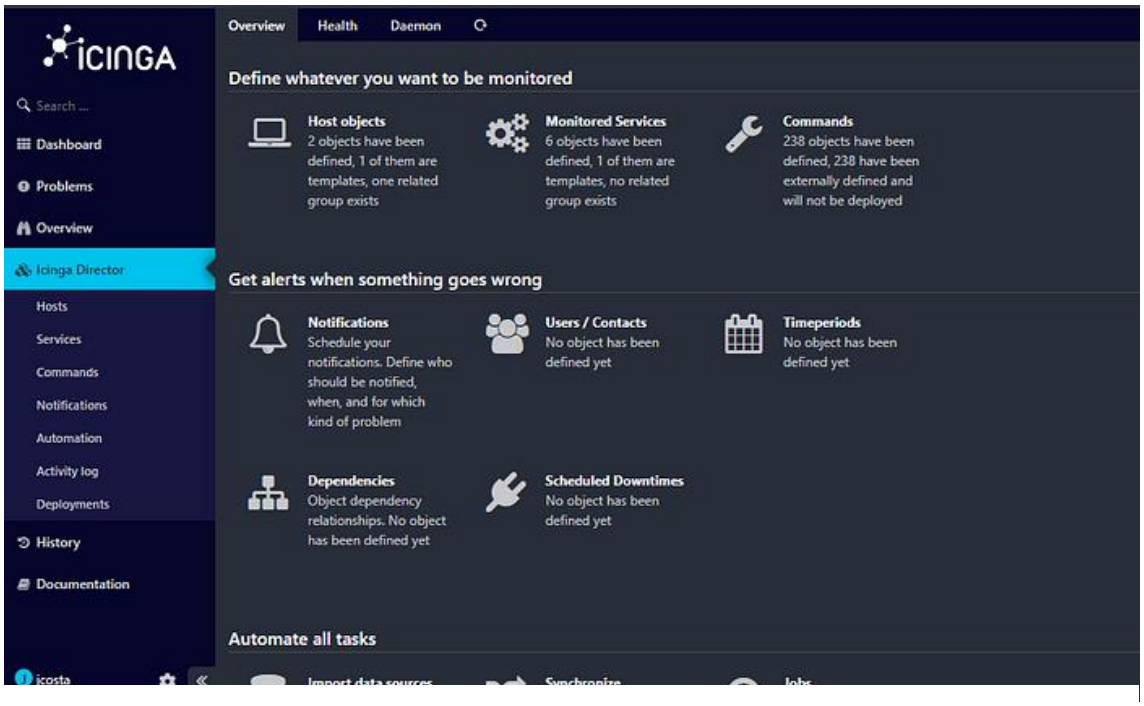


*Figura 7 - Icinga Director instalado*

## 5.1.2 Kickstart Wizard do Icinga Director

Para dar início ao *Kickstart Wizard* do Icinga Diretor iremos primeiramente adicionar o nosso utilizador API na opção "Icinga Api users" como é possível ver na figura 8.

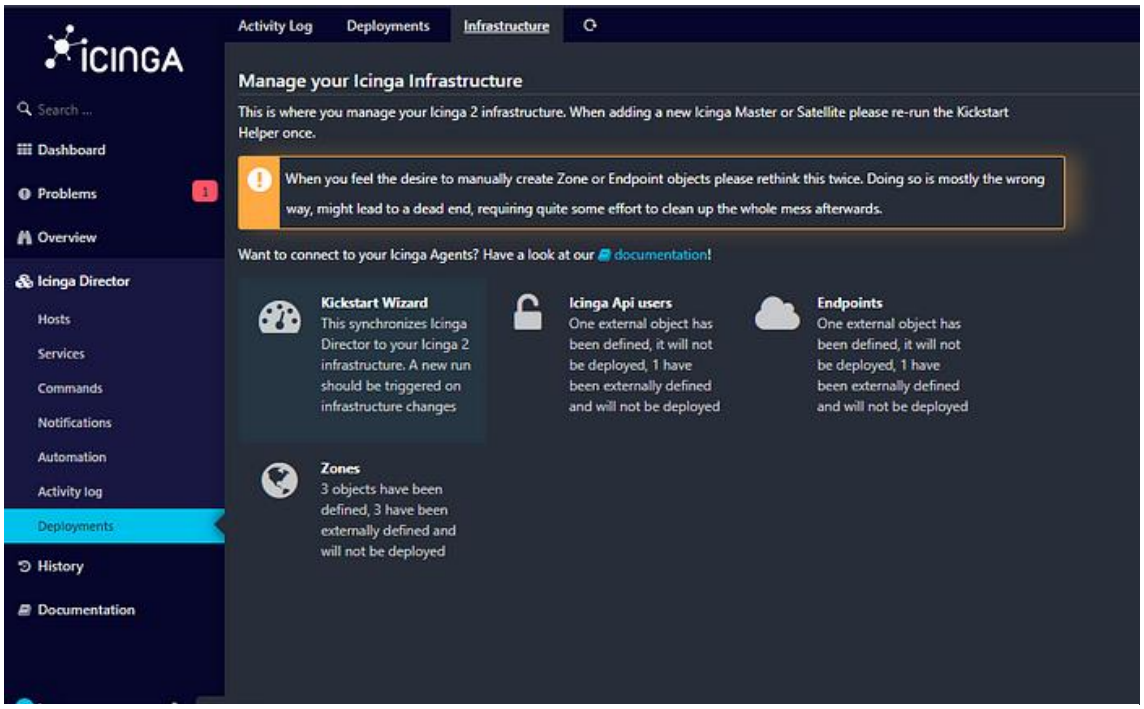


*Figura 8 - Utilizadores API*

Para sabermos qual é o nosso utilizador API iremos aceder ao ficheiro dos utilizadores API no icinga através do seguinte comando:

```
nano /etc/icinga2/conf.d/api-users.conf
```

Na figura 9 podemos ver todos os "Api Users" do Icinga, neste caso iremos utilizar o "root" com a sua devida password:


*Figura 9 - Ficheiro de configuração de utilizadores API*

Após termos adicionado o nosso "Api User" é necessário agora adicionar um *endpoint* como podemos ver na figura 10 onde iremos colocar o nosso endereço do Icinga e vamos utilizar o "Api User" adicionado anteriormente:

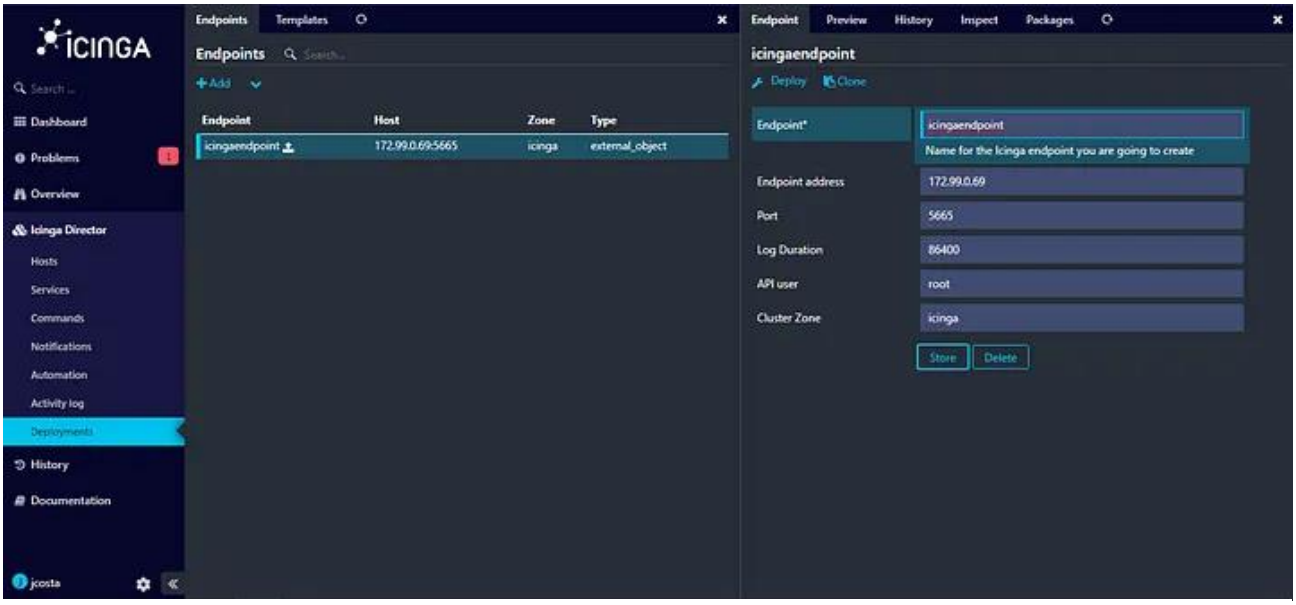


*Figura 10 - Configuração de um Endpoint*

Após adicionados o "Api User" e o "Endpoint" podemos então prosseguir ao *Kickstart Wizard* do Icinga Director

Aqui iremos adicionar o nome do "Endpoint" criado o endereço do Host do Icinga a sua devida porta e por fim o "Api User" com a sua password como é feito na figura 11.

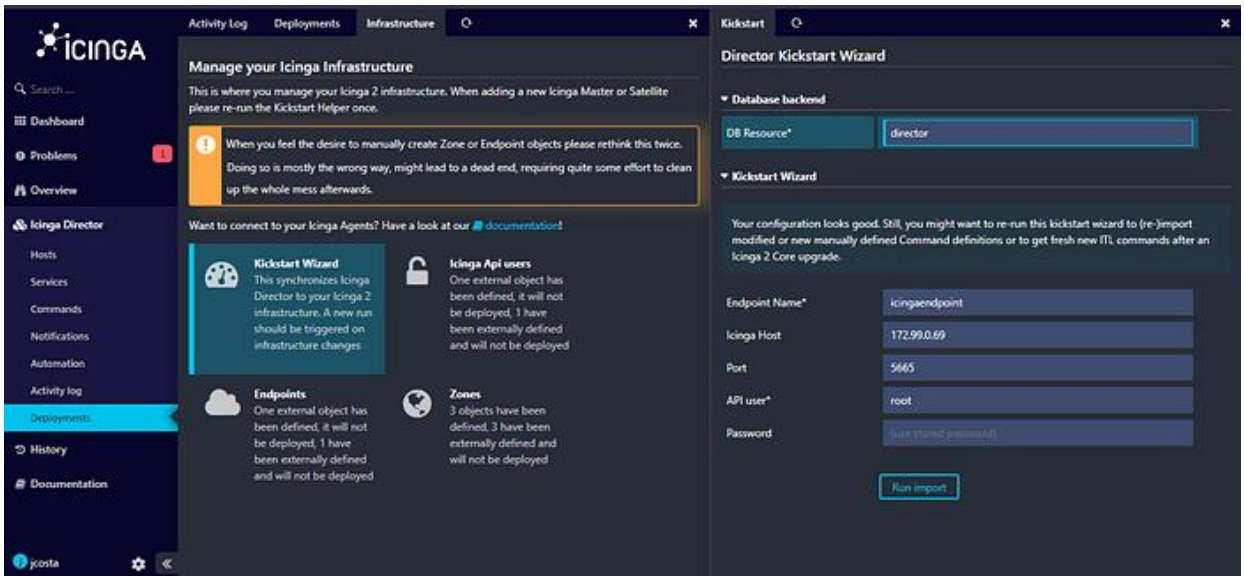


*Figura 11 - Director Kickstart Wizard*

### 5.1.3 Como adicionar Hosts com o Icinga Director

Para exemplo iremos utilizar uma máquina virtual com Windows Server para adicionar como *host* no Icinga. Para adicionar máquinas com Windows no Icinga é necessário que elas tenham o agente do Icinga Instalado nas mesmas, é possível descarregar o *setup* do agente no seguinte link: *https://packages.icinga.com/windows/*

Recomenda-se utilizar a versão *x86_64* para sistemas mais modernos. Para adicionar um *Host* é necessário criar primeiro um ”Host Template” como é feito na figura 12.

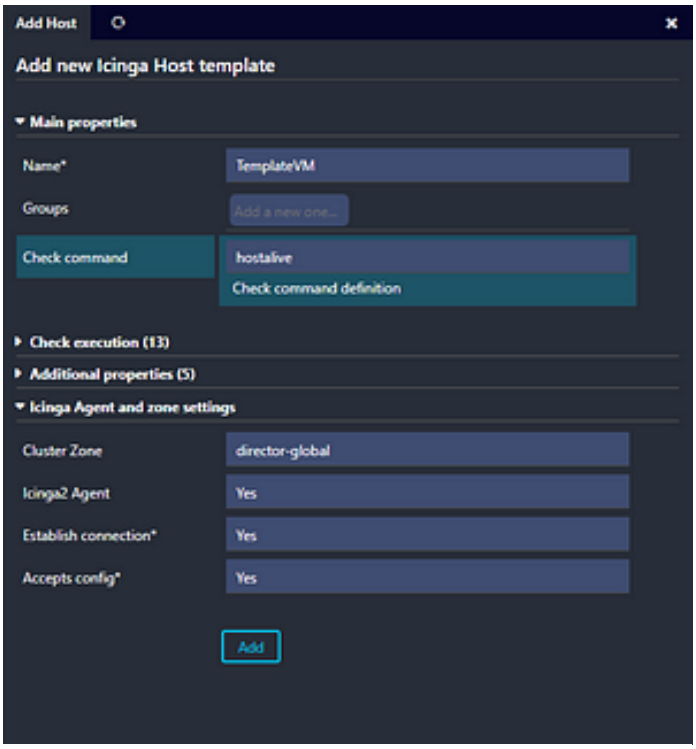


*Figura 12 - Criação de uma Icinga Host Template*

No “Host Template” podemos configurar diferentes parâmetros tais como o “Check Execution” onde configuramos os intervalos de tentativas para executar o comando escolhido neste caso utilizamos o “hostalive” para sabermos sempre se a máquina está ligada ou desligada, dá nos também a possibilidade de ativar as notificações como por exemplo quando a máquina fica desligada. No cluster zone vamos adicionar a nossa zona pretendida para a template. Como vamos utilizar o agente do icinga2 no Windows é necessário colocar “Yes” na opção “Icinga2 Agent” tal como nas outras opções é necessário que esteja tudo “Yes”.

Agora sim iremos adicionar o novo *host* para isso colocamos o *template* criado anteriormente, definimos um *hostname* ao nosso *host*, e colocamos o endereço da máquina que queremos adicionar como na figura 13.

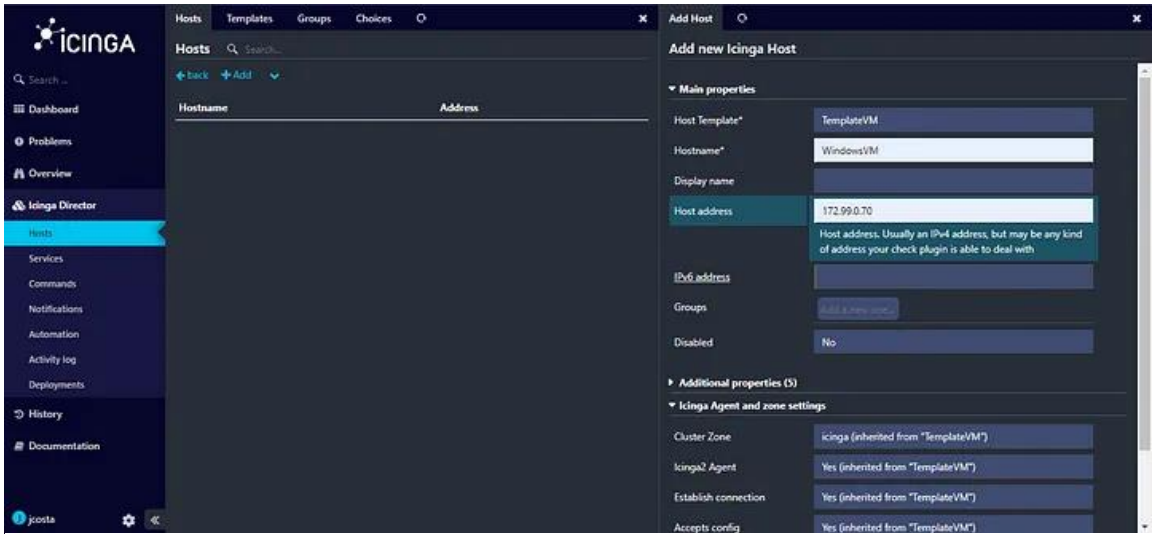


*Figura 13 - Criação de um Host no Icinga*

Lembrando que é necessário sempre fazer *deploy* das modificações efetuadas para o Director aplicar as alterações tal como na figura 14.

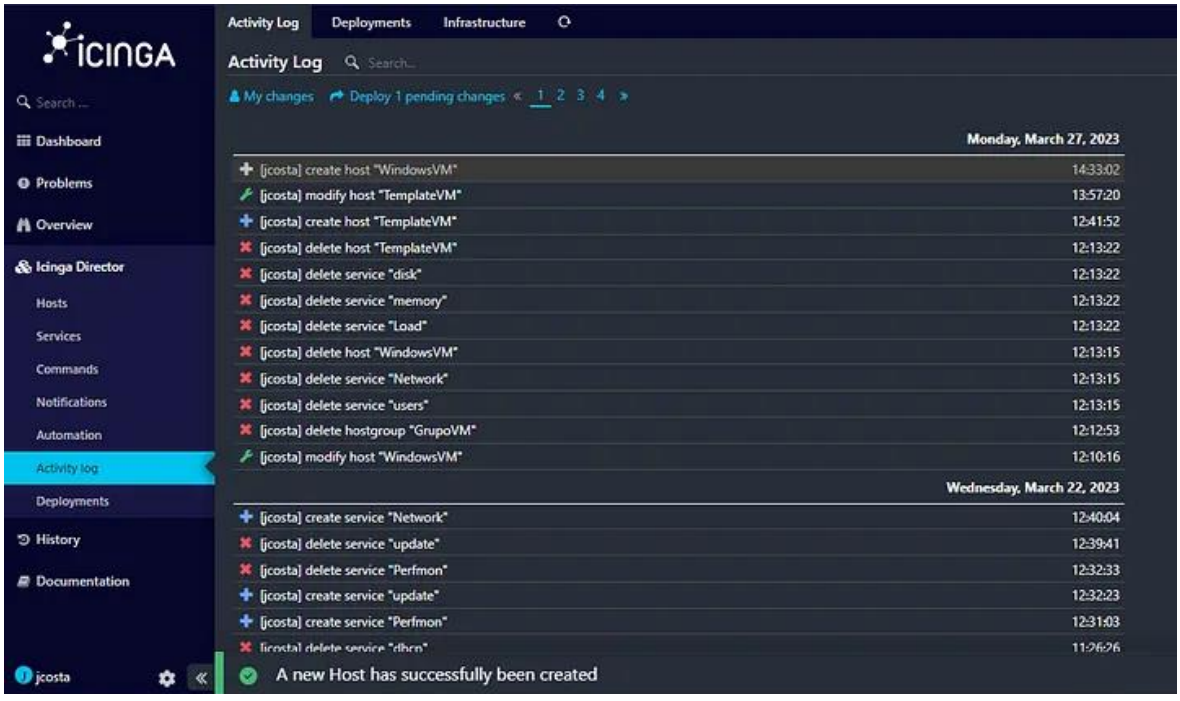


*Figura 14 - Deploy das alterações*

Agora no agente vamos adicionar o mesmo nome da máquina que introduzimos para a nossa VM que neste caso foi "WindowsVM" tal como na figura 15.

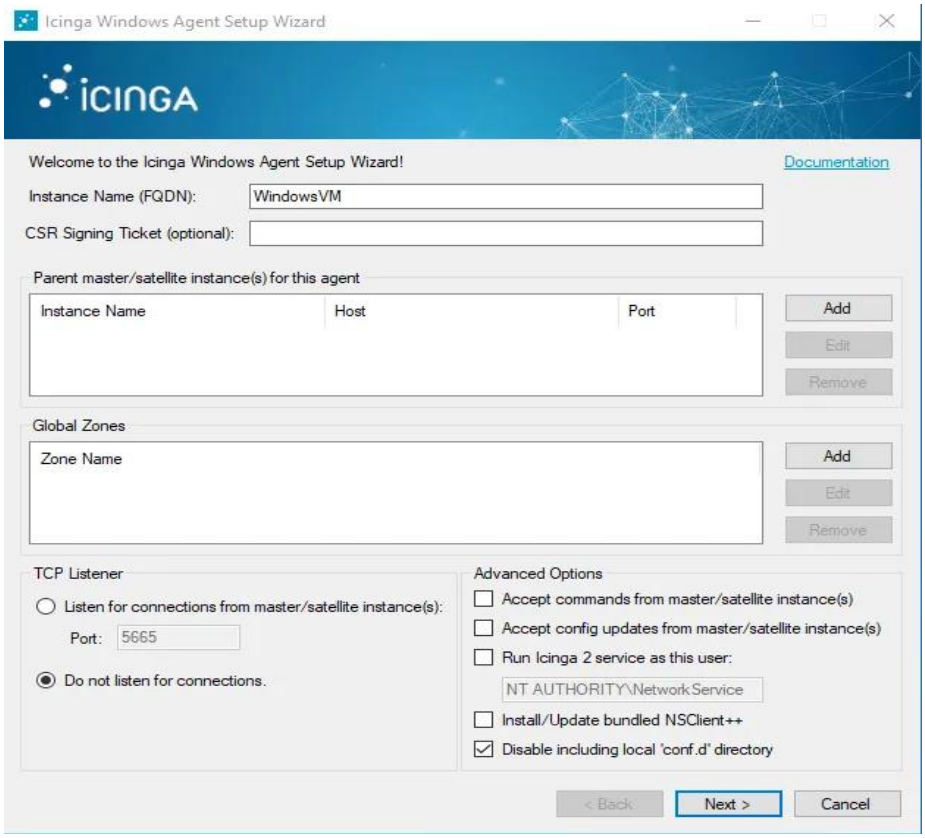


*Figura 15 - Nome de Instância no Setup do Agente*

Vamos agora gerar o nosso ticket CSR através do seguinte comando:

```
icinga2 pki ticket --cn nomedamaquina
```

Podemos ver o ticket que foi gerado na figura 16.

```
root@icinga:~# icinga2 pki ticket --cn WindowsVM
1813d0008caef47142d2e82f72db605570bd4dea
root@icinga:~#
```

*Figura 16 - Ticket gerado*

Colocamos o Nome da instância com o seu devido ticket adicionamos o nome da nossa máquina que contém o Icinga com o seu IP e a zona global que pretendemos criar e depois clicamos em “next”, tal como na figura 17.

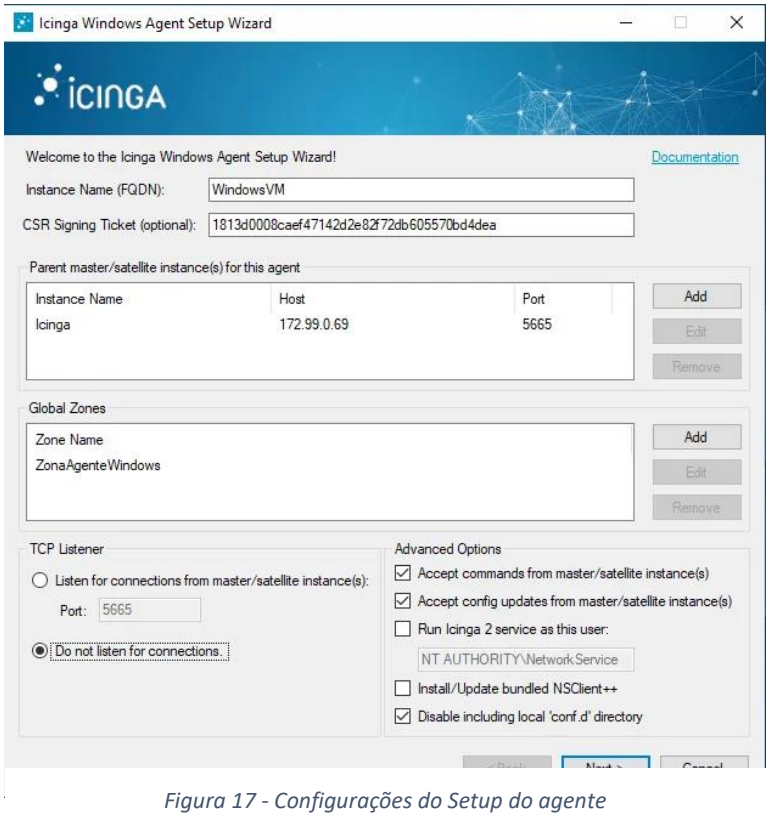


*Figura 17 - Configurações do Setup do agente*

No próximo passo clicamos em *next* novamente e por fim *finish* como podemos ver na figura 18.

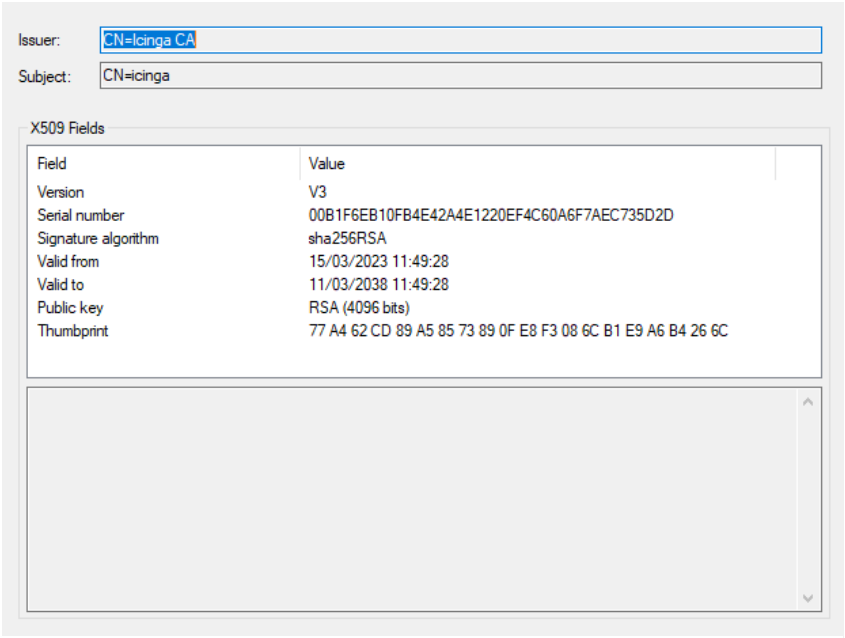


*Figura 18 - Conclusão do Setup do Agente*

Como podemos ver na figura 19 já está disponível a informação da nossa máquina virtual e podemos ver se a mesma está "UP" ou "DOWN".

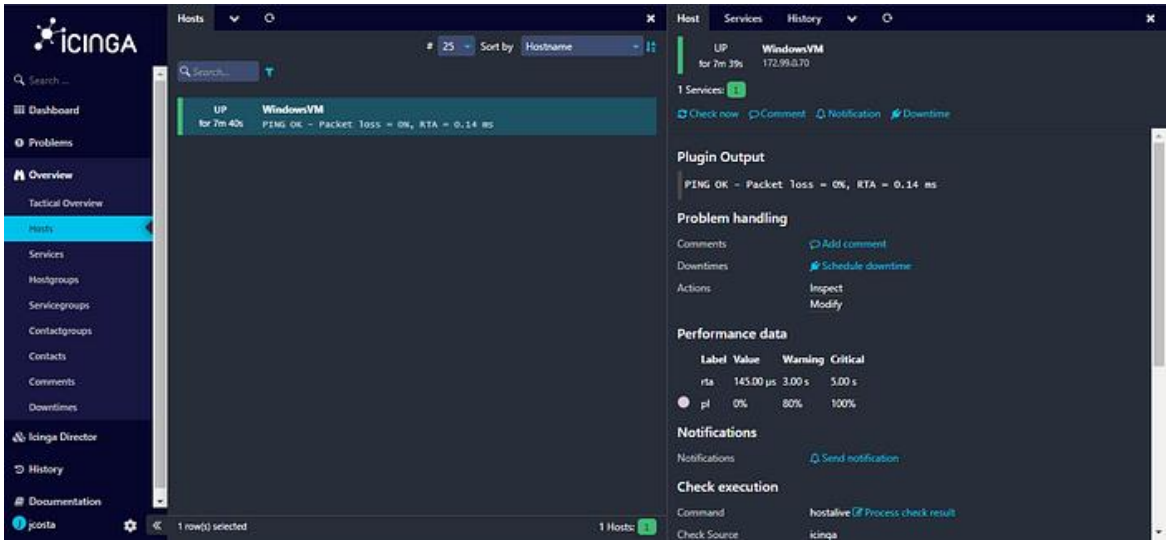


*Figura 19 - Informação da Máquina Virtual adicionada*

### 5.1.4 Adicionar serviços para monitorizar num host no Icinga

Existe uma infinidade de serviços que é possível monitorizar com o Icinga2, eles podem ser todos vistos no seguinte link: [https://icinga.com/docs/icinga-2/latest/doc/10-icinga-template-library/](https://icinga.com/docs/icinga-2/latest/doc/10-icinga-template-library/)

Para adicionar um serviço novo ao nosso *host* é necessário ter uma Template de Serviços criada. Para isso iremos cria-la com a ajuda do Icinga Director como está indicado na figura 20.

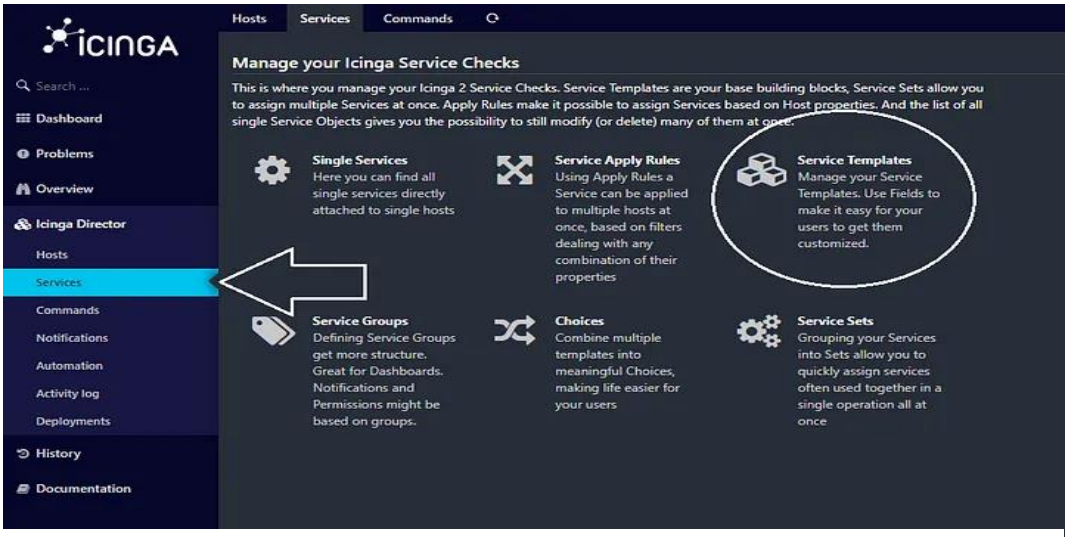


*Figura 20 - Localização dos "Service Templates"*

Quando adicionamos a *template* podemos efetuar enumeras configurações tais como o tempo de intervalo em que vai ser executado o serviço pretendido, o máximo de tentativas, podemos definir as notificações relativas aos serviços e por aí adiante como podemos ver na figura 21.

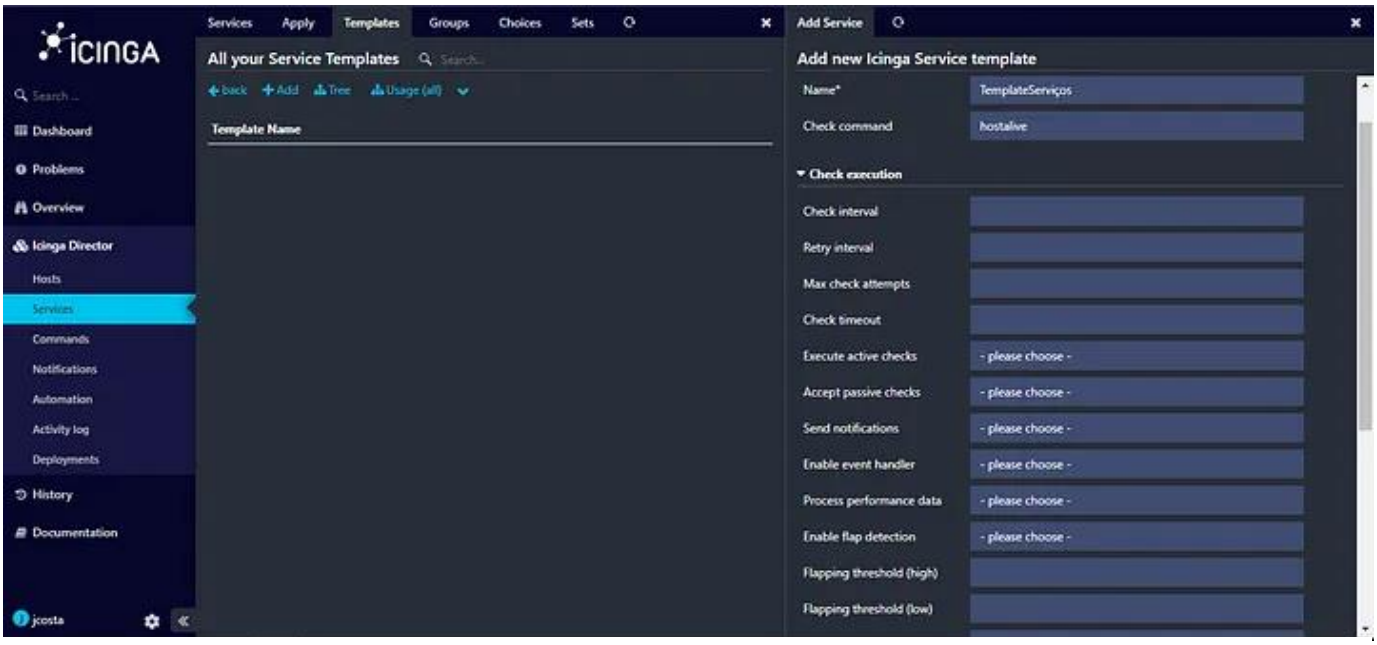


*Figura 21 - Criação de um novo Serviço de Templates*

Como é pretendido que os serviços corram num agente que neste caso está no Windows server é importante na seguinte opção selecionar “yes” tal como na figura 22.

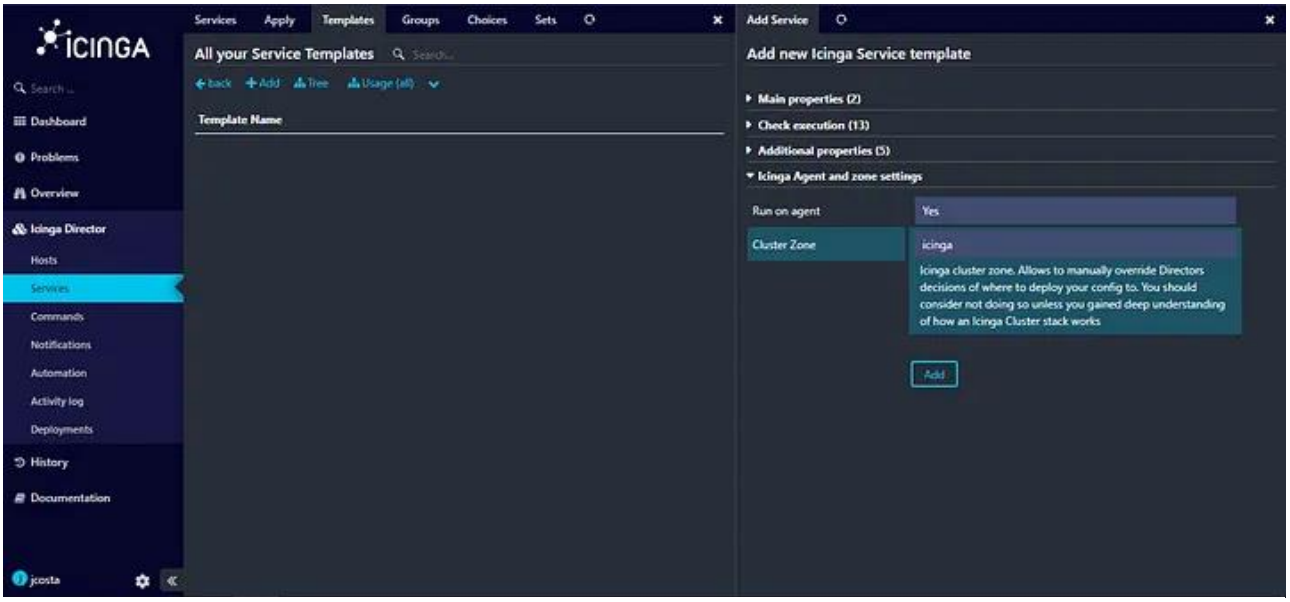


*Figura 22 - Run on Agent*

Agora como está indicado na figura 23 vamos então adicionar os serviços ao nosso host para isso vamos aceder á página “Single Services” e depois “Add”.

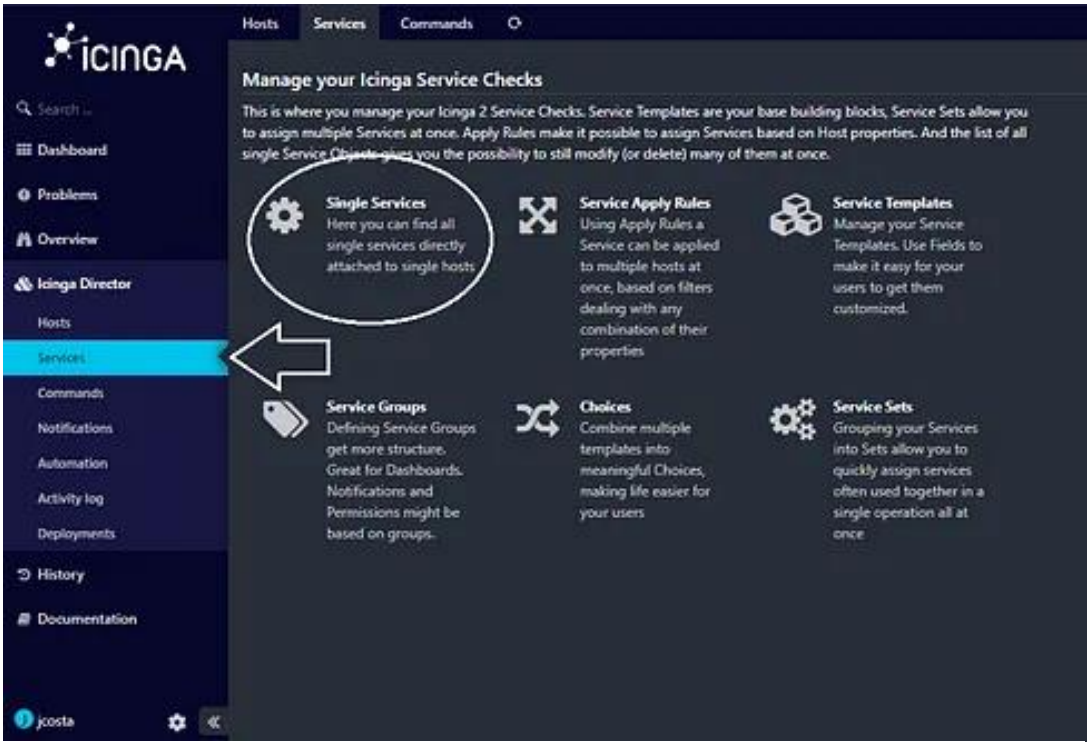


*Figura 23 - Adição de Serviços ao Host*

Como exemplo iremos adicionar o serviço que monitoriza os discos do sistema, o mesmo tem o nome de “disk-windows”. Iremos definir o nome do serviço, a *template* criada anteriormente, o *host* desejado, e o comando que neste caso é o “disk-windows”, e por fim “Add” tal como é feito na figura 24.

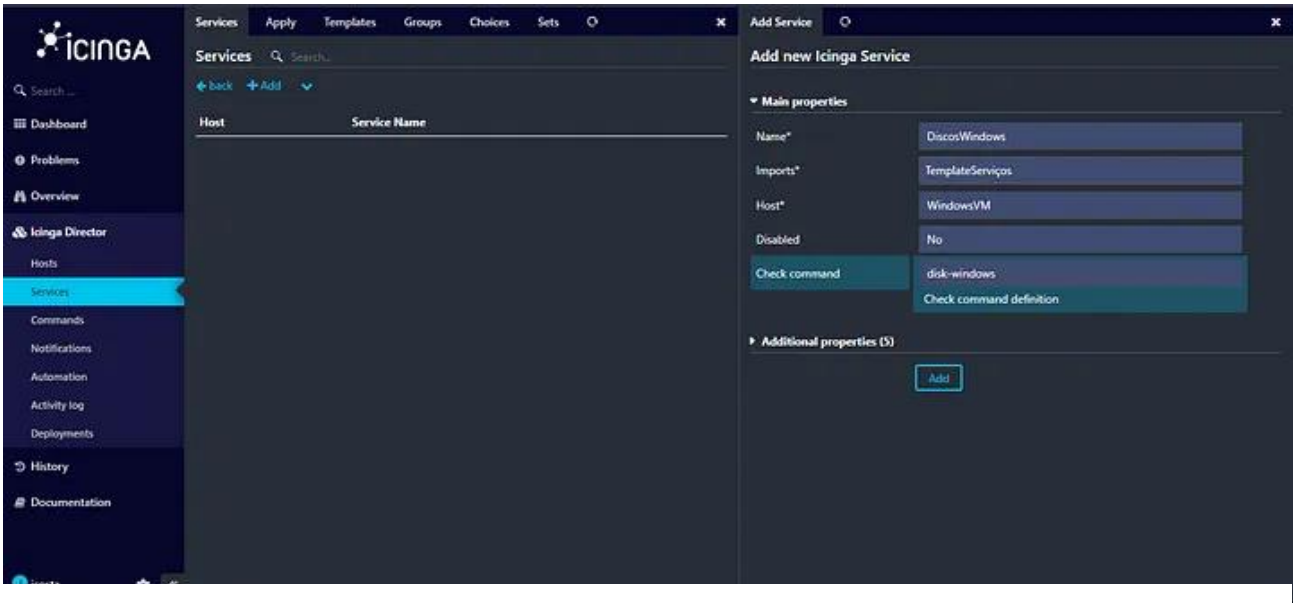


*Figura 24 - Serviço a monitorizar*

E por fim após termos feito *deploy* de todas as alterações podemos finalmente monitorizar os discos do windows. Só precisamos de nos deslocar nas definições de "overview" e depois "services" e estará disponível o serviço que adicionamos anteriormente. Podemos ver na figura 25 os valores do disco C:\ da máquina.

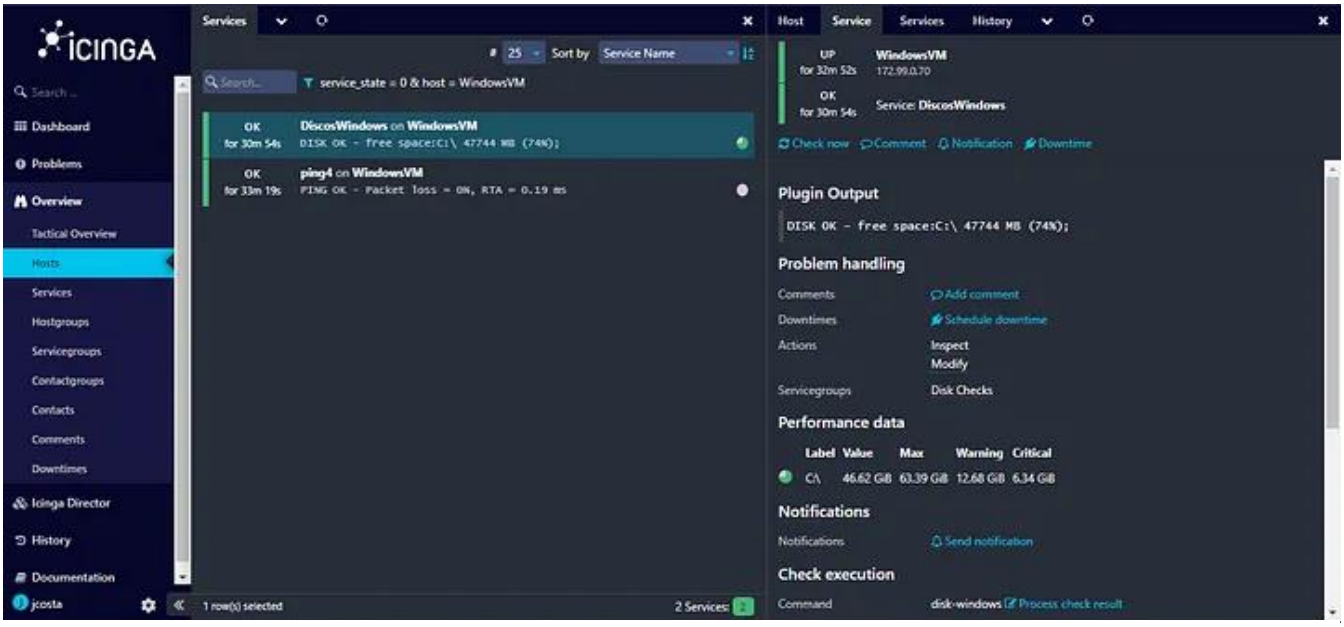


*Figura 25 - Monitorização dos Discos*

## 5.2 Zabbix

Para iniciar a instalação do Zabbix no Rocky Linux é necessário instalar o repositório do mesmo para isso vamos utilizar os seguintes comandos:

```
rpm -Uvh https://repo.zabbix.com/zabbix/6.4/rhel/9/x86_64/zabbix-release-6.4-1.el9.noarch.rpm
dnf clean all
```

Vamos agora instalar o Zabbix *server*, *frontend*, *agent* através deste comando:

```
dnf install zabbix-server-mysql zabbix-web-mysql zabbix-nginx-conf zabbix-sql-scrIPts zabbix-selinux-policy zabbix-agent
```

Após a instalação ter sido terminada vamos agora criar uma base de dados para o Zabbix:

```
mysql -u root -p
password
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```

Vamos agora importar o esquema inicial e os dados da base de dados:

```
zcat /usr/share/zabbix-sql-scrIPts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
```

Irá ser pedida a password criada anteriormente para o utilizador “zabbix”. Iremos agora desativar o “log_bin_trust_function_creators” através dos comandos:

```
mysql -uroot -p
'password'
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;
```

Vamos editar o ficheiro /etc/zabbix/zabbix_server.conf onde vamos colocar a password definida na BD:

```
DBPassword="password"
```

Agora vamos editar também o ficheiro /etc/nginx/conf.d/zabbix.conf onde vamos colocar a porta que vai ser utilizada pelo zabbix e o nome do servidor:

```
listen 8080;
server_name example.com
```

Vamos agora reiniciar os processos do agente e do servidor e colocá-los no arranque para iniciarem sempre que o servidor é ligado:

```
systemctl restart zabbix-server zabbix-agent nginx php-fpm
systemctl enable zabbix-server zabbix-agent nginx php-fpm
```

Como podemos ver na figura 26 é possível aceder á interface web do zabbix através do IP do mesmo, junto da sua porta configurada anteriormente e proceder á configuração inicial do zabbix.

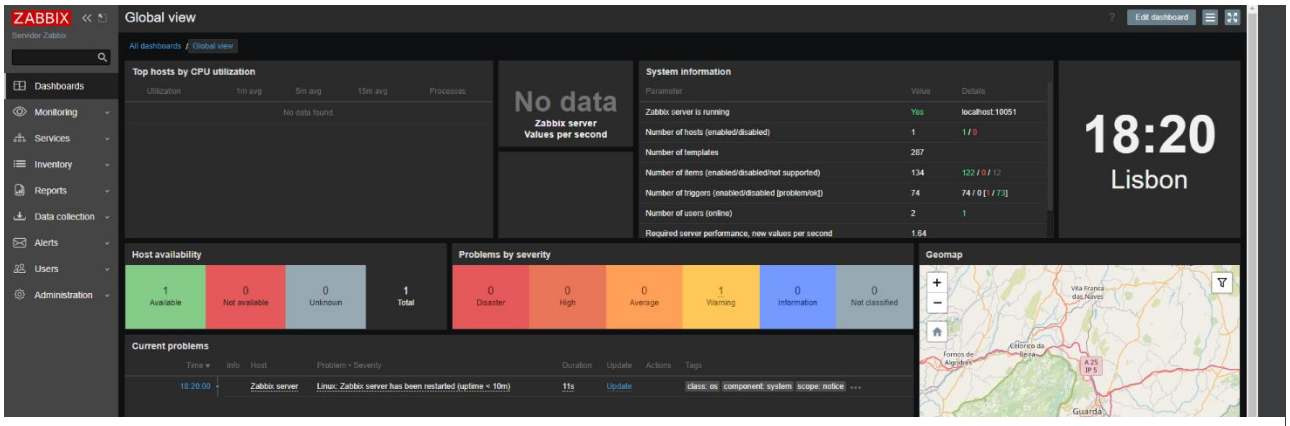


*Figura 26 - Interface Web do Zabbix*

### 5.2.1 Como configurar o agente do Zabbix num ambiente Windows

Para configurar o agente do zabbix num ambiente Windows vamos descarregar o *setup* no website oficial do zabbix. Após o *setup* estar descarregado vamos agora iniciar o mesmo.

1º Passo: Para dar início á instalação do agente vamos pressionar o botão "Next".

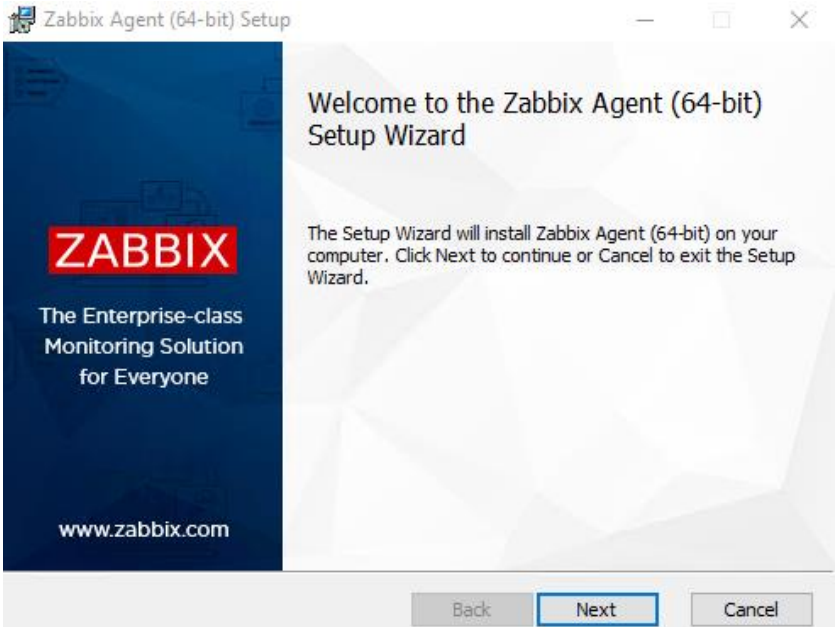


*Figura 27 - Inicio do Setup do Agente do Zabbix*

2º Passo: Vamos agora aceitar os termos da licença e clicar em "Next".


*Figura 28 - Termos do Agente do Zabbix*

3º Passo: Aqui irá ficar tudo por omissão pois queremos que todas as funcionalidades sejam instaladas tal como na figura 29.

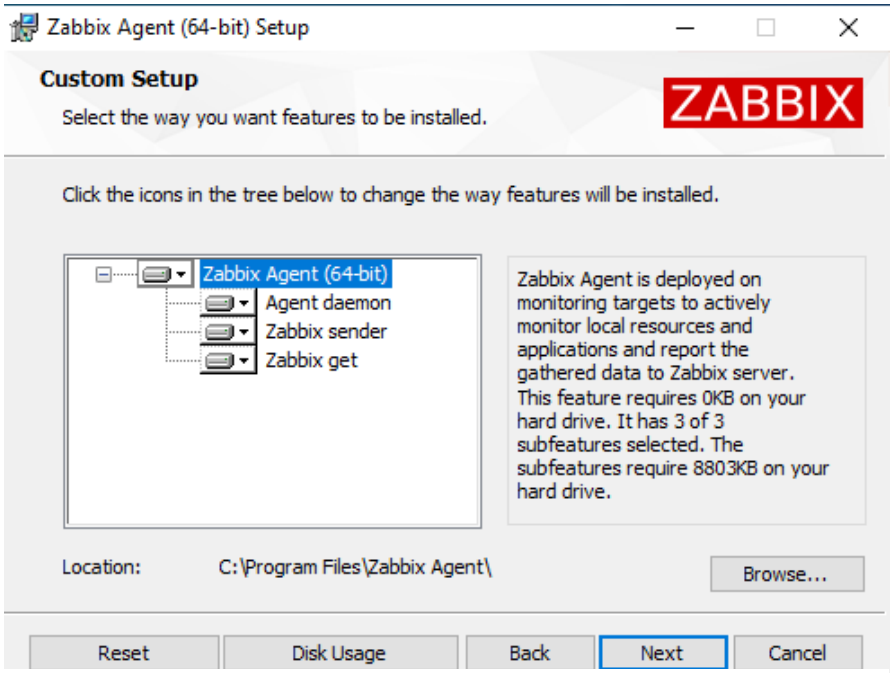


*Figura 29 - Funcionalidades do Agente do Zabbix*

4º Passo: Agora vamos definir qual será o nome da máquina onde o agente vai ficar em execução, vamos também definir o IP da máquina onde o Zabbix está instalado com a devida porta e vamos ativar também o "PSK" para uma maior segurança.

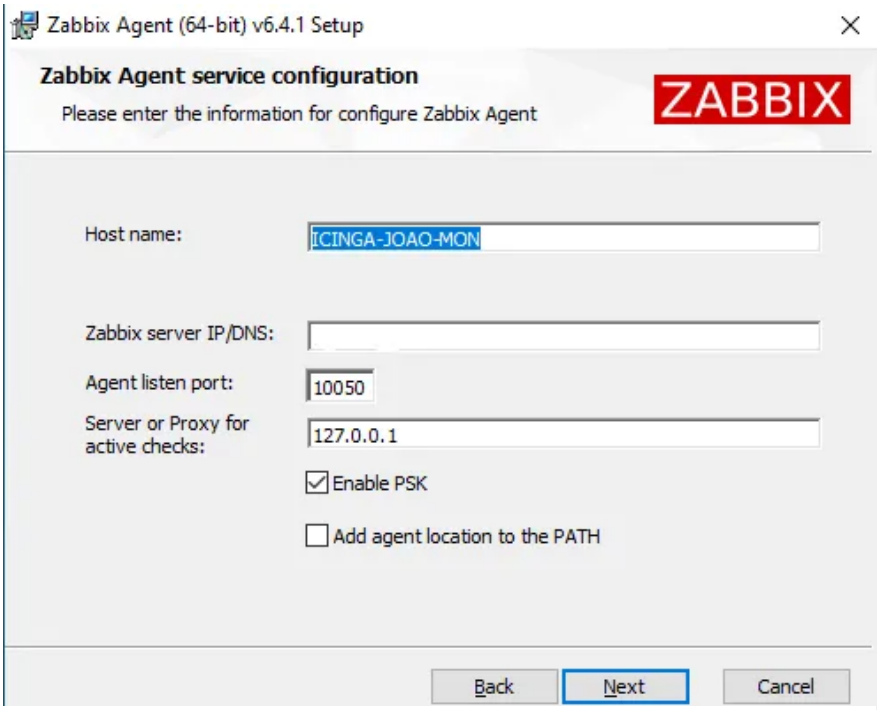


*Figura 30 - Configuração do Agente*

5º Passo: Vamos agora inserir a nossa chave "PSK" gerada com a devida identidade.

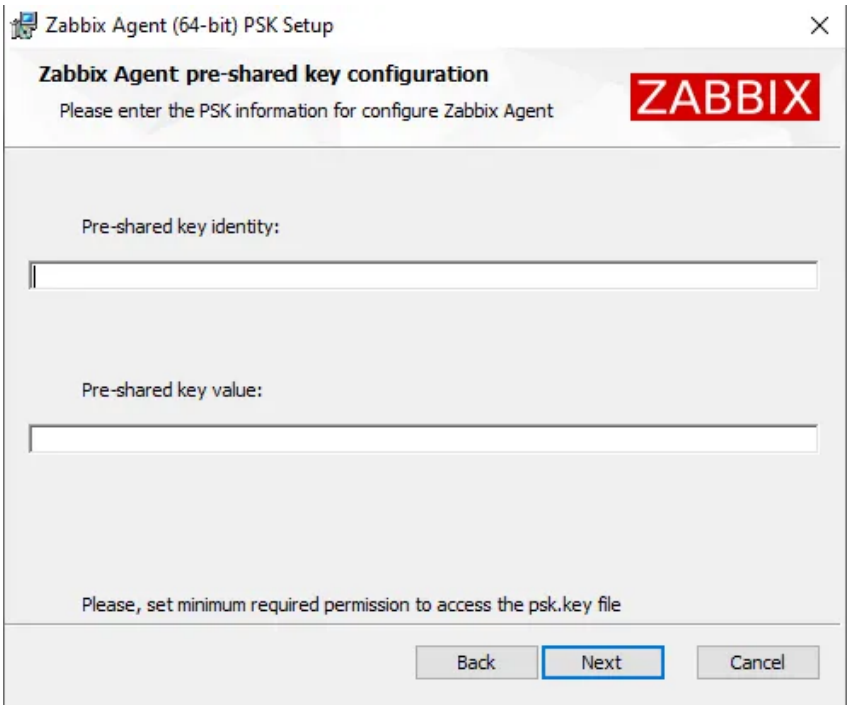


*Figura 31 - Chave PSK do Agente*

6º Passo: Agora por fim é só pressionarmos "Install" e o setup irá finalizar como podemos ver na figura 32, agora só falta adicionar o host no Zabbix para ser monitorizado.

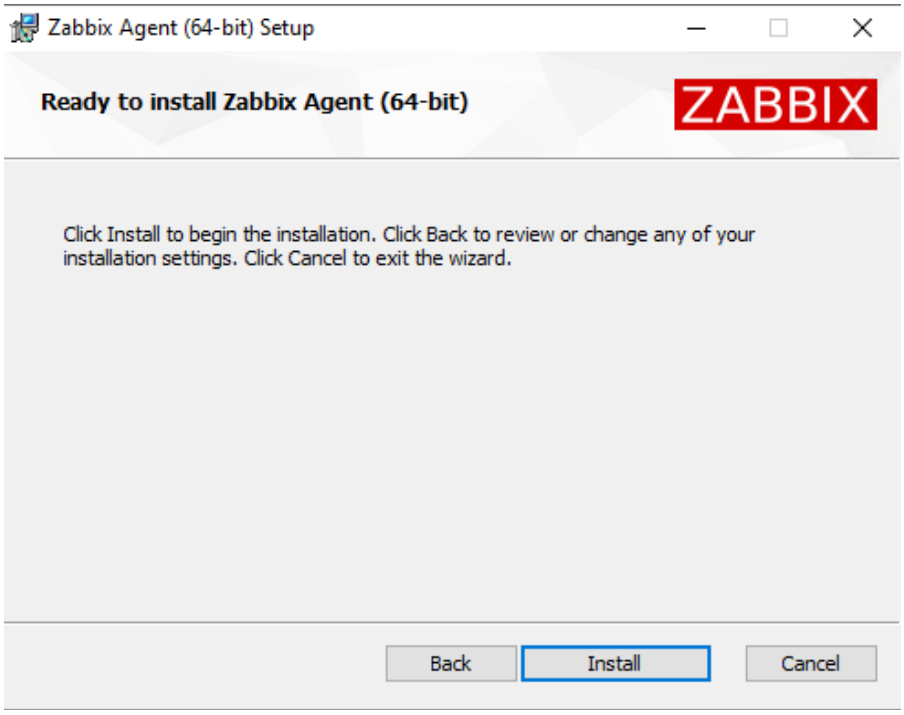


*Figura 32 - Fim do setup do agente*

### 5.2.2 Como adicionar Hosts Windows no Zabbix

Para adicionarmos o nosso primeiro *Host* de um Windows Server vamos seguir os seguintes passos:

1º Passo: Primeiramente vamos entrar na secção dos "Hosts" localizada na Dropdown "Data Collection".

2º Passo: Logo após realizar o passo anterior vamos pressionar o botão "Create Host".

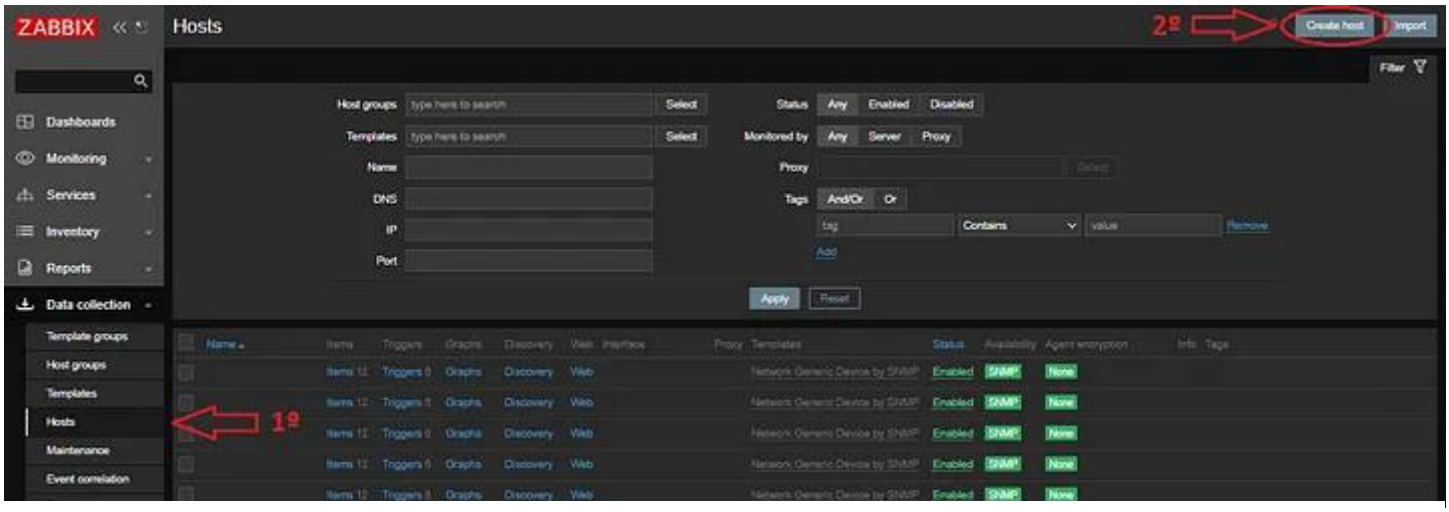


*Figura 33 - Criação de um novo host no Zabbix*

3º Passo: Vamos agora definir o nome do nosso primeiro *Host*, e logo de seguida vamos adicionar a *template* que pretendemos no botão "Select" neste caso vai ser "Windows by Zabbix agent" pois trata-se de uma máquina Windows com um agente.

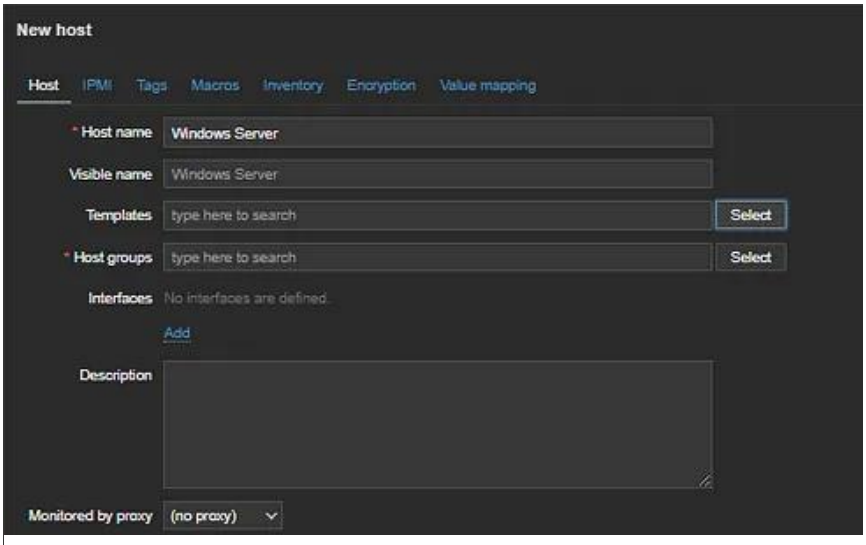


*Figura 34 - Configuração da Template do Host*

4º Passo: Na parte das interfaces vamos selecionar "Agent" e de seguida vamos inserir o IP da nossa máquina a ser monitorizada com a sua devida porta como é mostrado na figura 35.

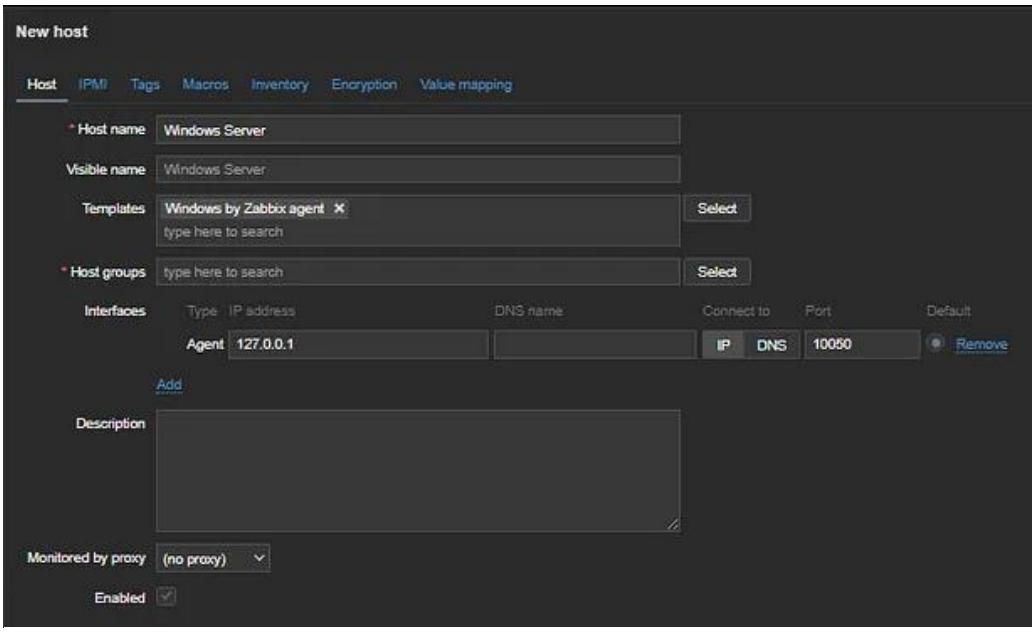


*Figura 35 - Configuração do IP do Host*

5º Passo: Por fim na janela "Encryption" vamos selecionar a opção de encriptação "PSK" e selecionar a opção "PSK", finalmente podemos adicionar a nossa identidade PSK inserida no agente tal como a sua chave "PSK", pressionamos "Add" e temos o nosso *Host* adicionado com sucesso.

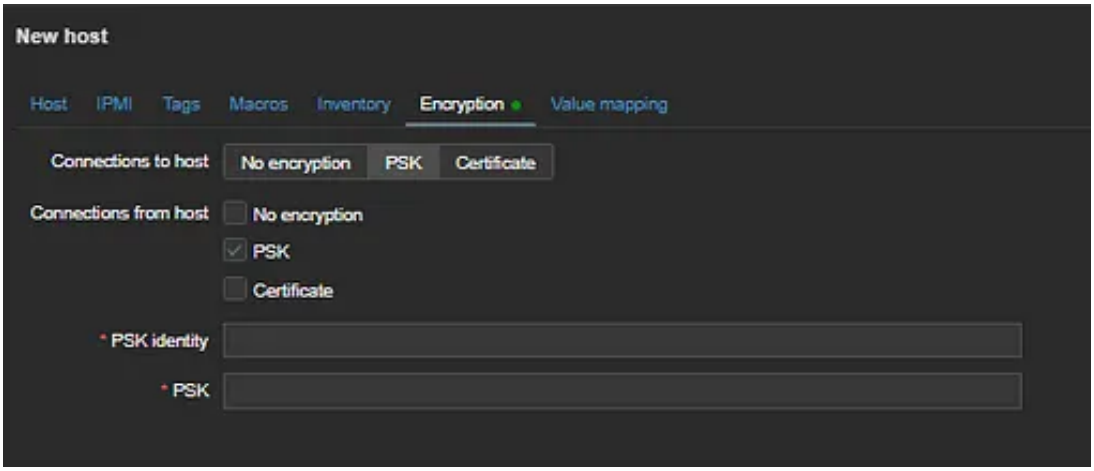


*Figura 36 - Chave PSK do Host*

### 5.2.3 Templates do Zabbix

As *templates* disponíveis no Zabbix são conjuntos predefinidos de objetos de monitorização, como itens, *triggers* e gráficos. Elas servem como modelos reutilizáveis para configurar e monitorizar dispositivos, sistemas e aplicativos. Com as *templates*, os administradores podem importar facilmente as configurações necessárias, economizando tempo e esforço na criação manual. Estas *templates* abrangem uma ampla variedade de áreas e são mantidas pela comunidade Zabbix. Isso permite que os utilizadores compartilhem e aproveitem o conhecimento coletivo para monitorizar diferentes sistemas de forma eficiente. Existe uma infinidade de *templates*, precisamos apenas de procurar a que se adequa melhor ao equipamento que pretendemos monitorizar. Podemos ver na figura 37 algumas das *templates* que o Zabbix possui. Resumindo, as *Templates* do Zabbix simplificam o processo de monitorização, agilizando a configuração e oferecendo um repositório abrangente de modelos prontos para uso.

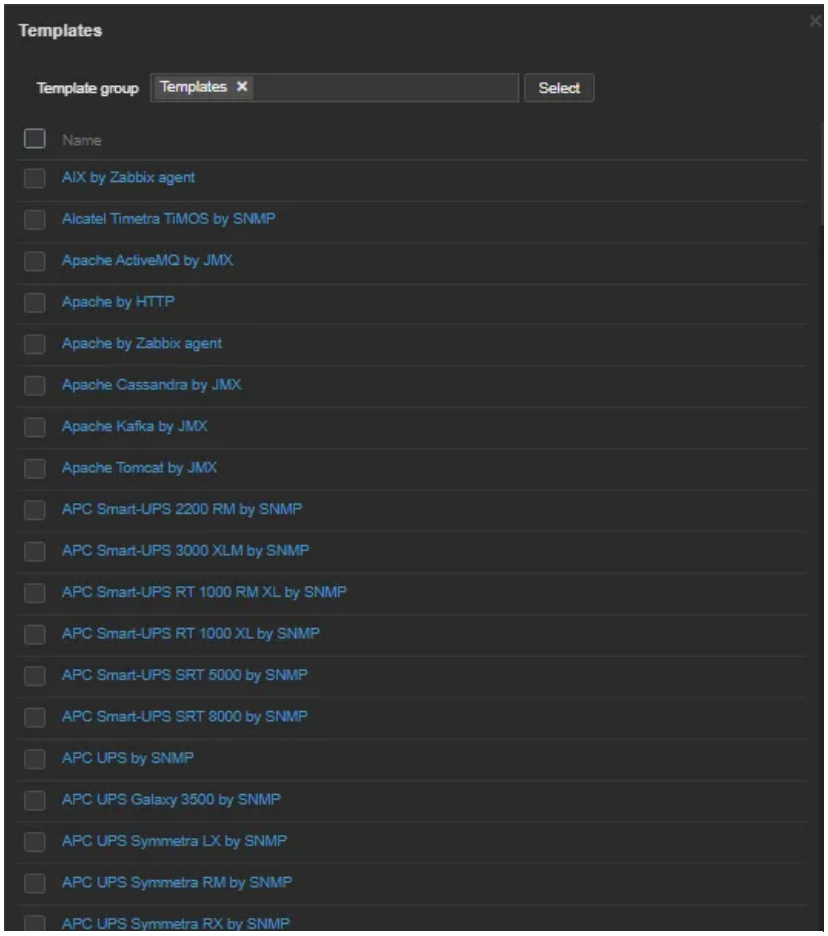


*Figura 37 - Diferentes Templates Do Zabbix*

### 5.2.4 Alertas via E-mail no Zabbix

Primeiramente para ativarmos os alertas via E-mail é necessário ter um utilizador criado. Após termos criado o utilizador podemos ver na imagem seguinte a janela "Media" onde vamos definir o E-mail desse mesmo utilizador

1º Passo: Vamos entrar nas definições do utilizador pretendido e definir o E-mail do mesmo. Para isso entramos na janela "Media" desse utilizador como podemos ver na figura 38.

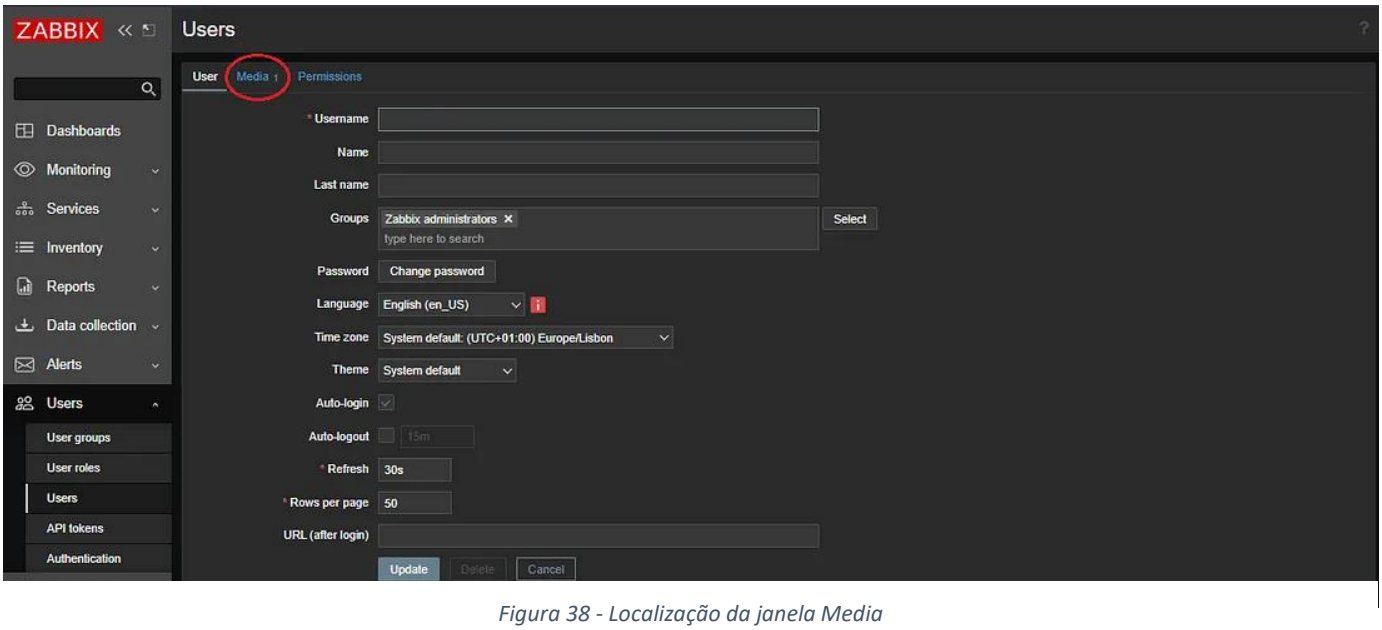


*Figura 38 - Localização da janela Media*

2º Passo: Dentro da janela "Media" clicamos agora em "Add" para adicionarmos o E-mail tal como na figura 39.

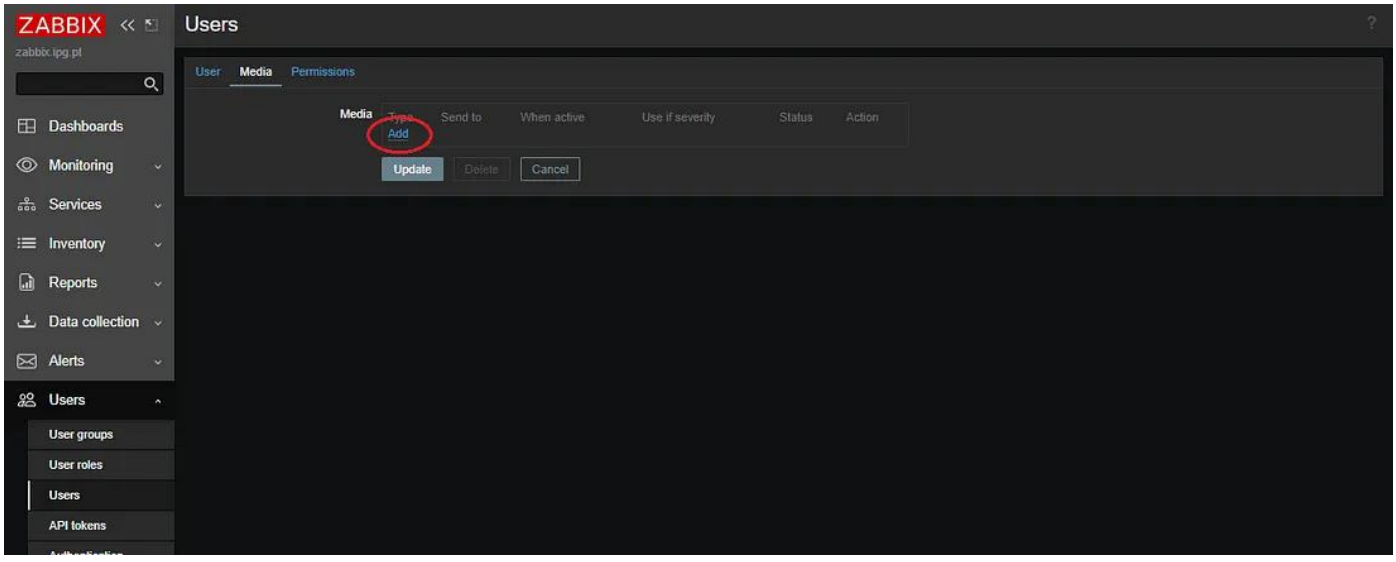


*Figura 39 – Localização do botão para adicionar media ao utilizador*

3º Passo: Adiciona-se o E-mail pretendido na caixa de texto. Podemos também selecionar a severidade dos e-mails que pretendemos receber nesse mesmo E-mail.

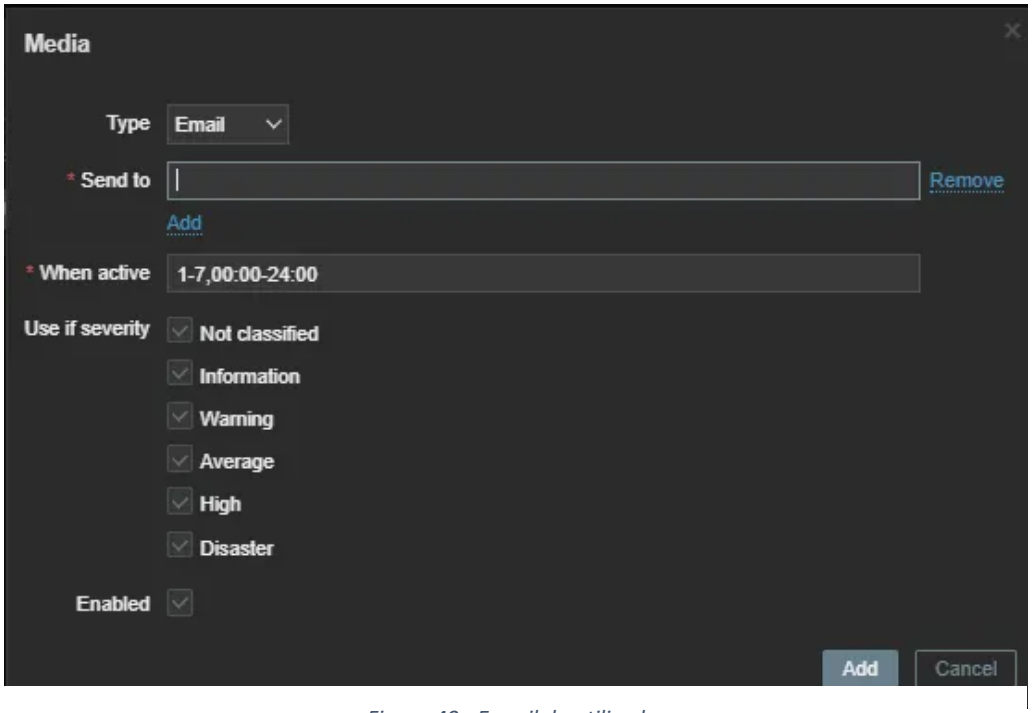


*Figura 40 - E-mail do utilizador*

4º Passo: Agora na secção "Administration" em "Media Types" vamos colocar no "Type" a opção Email, vamos definir o servidor SMTP do Gmail com a devida porta o email que vamos utilizar para enviar todos os emails e selecionar o tipo de mensagem enviada.

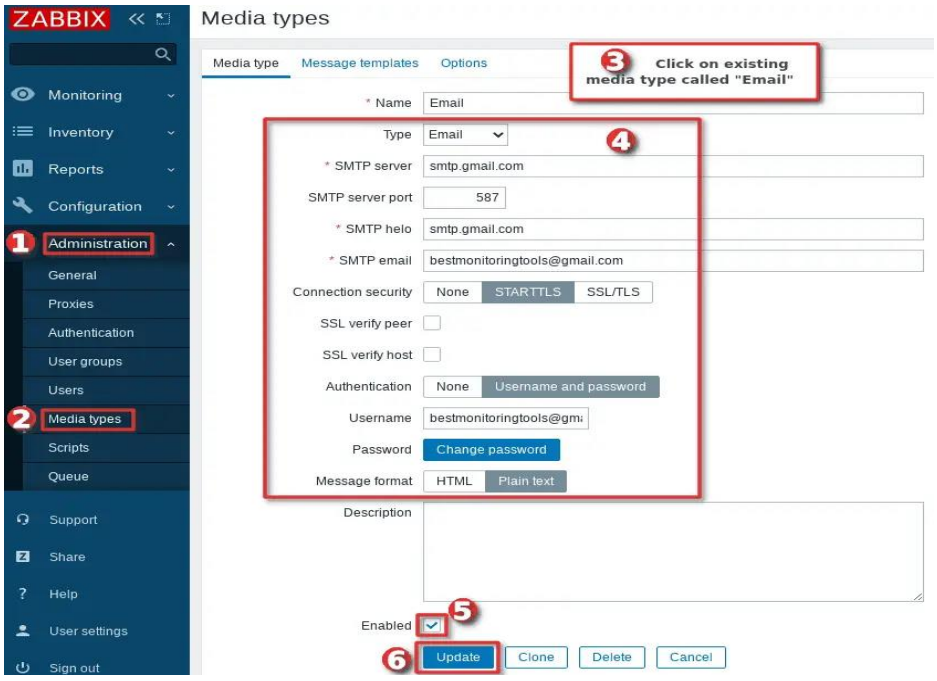


*Figura 41 - Criação da Media Type*

*Fonte: https://bestmonitoringtools.com/zabbix-alerts-setup-zabbix-email-notifications-escalations/*

5º Passo: Por fim na secção “Configuration” em “Actions” vamos colocar enable na opção do ponto 4, para que sejam emitidos Emails, para todos os *users* do zabbix declarados como Administradores tal como é indicado na figura 42.

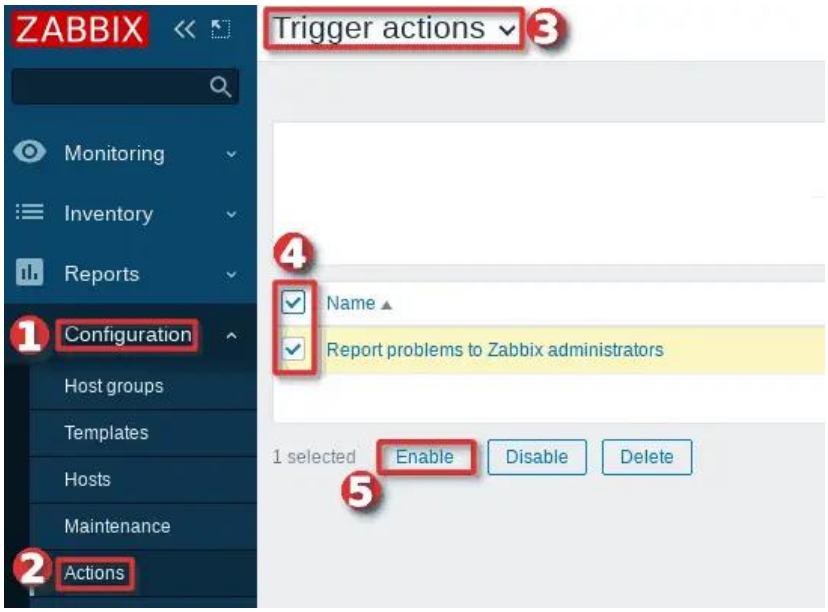


*Figura 42 - Enable na Ação das Notificações*

*Fonte: https://bestmonitoringtools.com/zabbix-alerts-setup-zabbix-email-notifications-escalations/*

### 5.2.5 Criação de gráficos

No zabbix é possível também criar o nosso próprio *dashboard* e personalizá-lo com diversos *widgets*, tais como relógios, um painel de problemas que ocorreram ou estão a decorrer, entre muitos outros. Um *widget* muito relevante são os gráficos pois permitem-nos fazer uma análise objetiva de um certo objeto de um host como por exemplo a percentagem de utilização do processador de um certo *host*.

Isso permite-nos saber se o mesmo está com valores anómalos e se assim estiver, leva-nos a uma intervenção imediata. É possível ver um exemplo de um gráfico na figura 43 onde é analisada a utilização do CPU do servidor zabbix

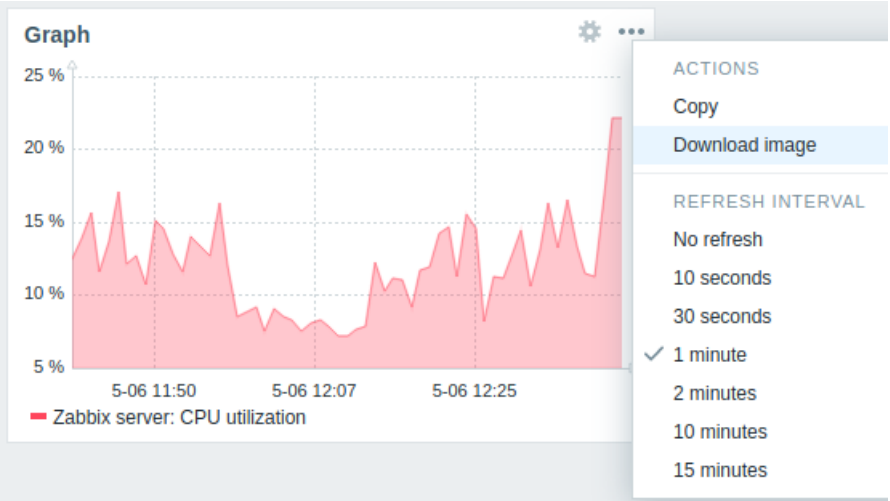


*Figura 43 - Gráfico da utilização do CPU*

*Fonte: https://www.zabbix.com/documentation/current/en/manual/web_interface/frontend_sections/dashboards/widgets/graph*

# 6 Atualização de Firmwares

Participei na atualização de Firmwares de dispositivos da rede, tais como, switches e VoIP's garantindo que eles estivessem atualizados com as versões mais recentes, o que é fundamental para manter a segurança e o desempenho. Para realizar este processo utilizei o **Tftpd64** uma ferramenta de software de administração útil para redes pequenas, que não apresenta grandes problemas, utiliza poucos recursos do sistema, possui uma interface simples e é gratuita. É uma ferramenta que atualiza a firmware do equipamento através do protocolo **TFTP** (Trivial File Transfer Protocol). Foi usado um portátil como servidor de **TFTP** onde estava essa ferramenta instalada. Para estabelecer uma comunicação entre o servidor e o dispositivo, foi atribuído um IP a ambos na mesma rede enquanto estes estavam ligados através de um cabo Ethernet, como podemos ver na figura 44 e 45. Na figura 46 podemos ver o VoIP a ser atualizado através da ferramenta mencionada anteriormente.


*Figura 44 - Configuração do IP do VoIP*

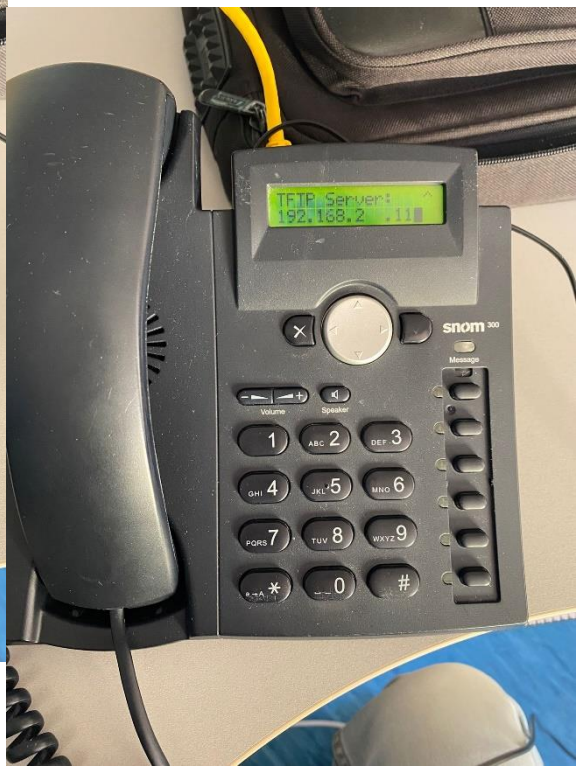


*Figura 45 - Configuração do IP do servidor TFPT (portátil)*

Na figura 46 podemos ver a imagem da firmware a ser carregada pelo VoIP e na figura 47 a mesma a ser atualizada.


*Figura 47 - Imagem da firmware a ser carregada*

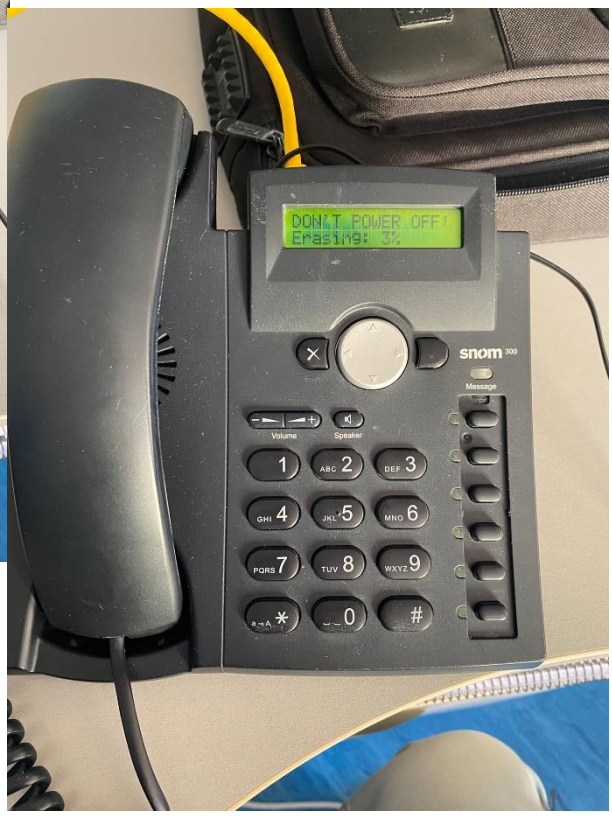


*Figura 46 - Firmware a ser atualizada*

# 7 Outras operações realizadas

Durante o meu período de estágio foram também realizadas outras operações, mas não menos importantes, que incluíram:

- **Atualização de equipamentos:** No meu período de estágio foram trocados certos equipamentos para equipamentos mais recentes, tais como, *switches* e VoIP's.
- **Atualização de Fibras Ópticas:** Também participei na atualização das fibras ópticas de certos equipamentos, substituindo as fibras antigas por versões mais recentes e eficientes, melhorando significativamente a capacidade de transmissão de dados e a confiabilidade da rede.
- **Suporte a colaboradores e alunos:** Foi dado um certo apoio técnico aos colaboradores e alunos do Instituto em diferentes ocasiões, tais como, problemas de rede em gabinetes, problemas com a plataforma de gestão documental, problemas com dispositivos das salas de aula, problemas com os telefones VoIP's etc...
- **Preparação de eventos:** Foi dado apoio na preparação do evento CSECURITY23, o maior evento de cibersegurança do interior, tanto na parte técnica como na parte de divulgação.
- **Resolução de Problemas da Rede:** Tive a oportunidade de solucionar problemas de rede, identificando e corrigindo certos problemas de conexão.
- **Gestão de ativos:** Tive também a oportunidade de trabalhar com a plataforma GPLI, um gestor de ativos, para atualizar os dados existentes e adicionar certos ativos em falta.
- **Organização do local de trabalho:** Nos primeiros dias de estágio foram feitas diversas organizações e arrumações do local de trabalho.

# 8 Conclusão

## 8.1 Dificuldades Sentidas

Durante o período do estágio, enfrentei algumas dificuldades que, apesar de desafiadoras, representaram oportunidades valiosas de aprendizagem e crescimento profissional. Estas dificuldades incluíram:

- **Dificuldade de Instalação de soluções:** Uma solução que senti que foi bastante desafiadora de utilizar foi o Icinga, pois a mesmo tinha uma instalação muito complexa, utilizava muitas bases de dados, e ao seguir o seu guia de instalação oficial não obtive sucesso.
- **Dificuldade de compreensão:** Certas vezes durante o período de estágio senti uma dificuldade de compreensão em relação a certas situações do mundo de TI que para mim eram novas e eu ainda não tinha experienciado, porém a equipa com que me encontrava explicava tudo de uma forma compreensível e atenciosa.
- **Problemas Técnicos Complexos:** Lidar com problemas técnicos complexos, como interrupções na rede, falhas de hardware e questões de segurança, representou um desafio constante.

## 8.2 Conclusão Final

Ao longo deste período de estágio, tive a oportunidade de aprofundar o meu conhecimento na monitorização da rede, ao investigar e comparar duas soluções distintas: Icinga e Zabbix. Esta experiência proporcionou uma visão valiosa das complexidades envolvidas na gestão eficaz da rede de uma infraestrutura. Através da análise detalhada das características, vantagens e desvantagens de ambas as soluções, pude perceber que não existe uma abordagem única para a monitorização de redes que se aplique universalmente a todos os cenários. Em vez disso, a escolha entre o Icinga e o Zabbix deve ser orientada pelos requisitos específicos de uma organização, a sua infraestrutura de rede existente e os seus objetivos de negócios. Além disso, durante o estágio, pude desenvolver as minhas habilidades técnicas ao trabalhar com ferramentas e tecnologias relacionadas à monitorização da rede, o que considero extremamente valioso para a minha carreira na área da tecnologia da informação. Por fim, a experiência deste estágio proporcionou-me uma compreensão mais profunda da importância da monitorização da rede como uma ferramenta essencial para garantir a eficiência operacional, a segurança e o desempenho de uma infraestrutura de TI. Estou confiante de que as habilidades adquiridas ao longo deste estágio serão fundamentais para a minha contribuição futura em projetos relacionados à gestão de redes.

Agradeço mais uma vez a todos os membros do Centro de Informática do Politécnico da Guarda pela oportunidade de aprendizagem e pelo apoio contínuo durante este estágio. Estou ansioso para continuar a aprimorar as minhas habilidades e conhecimentos nesta área e em áreas semelhantes e contribuir para o sucesso da organização em futuros desafios tecnológicos. Este estágio foi uma experiência valiosa e enriquecedora que fortaleceu a minha paixão pela área de tecnologia da informação.

# 9 Referências

(2022). Obtido de PolitecnicoGuarda: https://politecnicoguarda.pt/sobrenos/o-politecnico-da-guarda/

*Gráficos Zabbix*. (s.d.). Obtido de zabbix: https://www.zabbix.com/documentation/current/en/manual/web_interface/frontend_sections/dashboards/widgets/graph

*Instalação Icinga*. (s.d.). Obtido de tecmint: https://www.tecmint.com/install-icinga2-monitoring-debian/

*Instalação MariaDB*. (s.d.). Obtido de tecmint: https://www.tecmint.com/install-mariadb-database-in-debian-10/

*Instalação Zabbix*. (s.d.). Obtido de zabbix: https://www.zabbix.com/download?zabbix=6.4&os_distribution=rocky_linux&os_version=9&components=server_frontend_agent&db=mysql&ws=nginx

MariaDB Foundation. (06 de junho de 2022). *MariaDB*. Obtido de https://mariadb.org/: https://mariadb.org/

*Notificações Zabbix*. (s.d.). Obtido de https://bestmonitoringtools.com/zabbix-alerts-setup-zabbix-email-notifications-escalations/