

Relatório de Estágio

José Pedro Albuquerque

Curso Técnico Superior Profissional em
Cibersegurança

set | 2023

GUARDA
POLI
TÉCNICO



POLI TÉCNICO GUARDA

Escola Superior de Tecnologia e Gestão

IMPLEMENTAÇÃO DE UMA INFRAESTRUTURA DE REDE

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

José Pedro Albuquerque
Setembro 2023

POLI TÉCNICO GUARDA

Escola Superior de Tecnologia e Gestão

IMPLEMENTAÇÃO DE UMA INFRAESTRUTURA DE REDE

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

Professor(a) Orientador(a): Fernando Melo Rodrigues

Professor(a) Coorientador(a): Pedro Manuel Pinto Teixeira

José Pedro Albuquerque

Setembro 2023

Agradecimentos

Prestes a concluir o meu percurso académico, não posso deixar de expressar a minha sincera gratidão a todos aqueles que me apoiaram e motivaram.

Começo por agradecer à instituição em si, mais concretamente, à Escola Superior de Tecnologia e Gestão, que me acolheu durante os dois anos e facultou todos os meios necessários para a realização do meu CTeSP.

Gostaria de agradecer ao Professor Engenheiro Fernando Melo Rodrigues por ter aceitado o meu convite para ser meu orientador e disponibilizar-se prontamente a aconselhar-me e esclarecer-me qualquer dúvida ao longo deste período.

Um agradecimento é dirigido ao Professor Engenheiro Pedro Pinto, por todo o apoio, ajuda, e simpatia ao longo deste período de estágio.

Por fim, mas não menos importante, agradeço a toda a minha família, em especial à minha avó, pelo esforço e apoio incondicional.

Um agradecimento aos colegas de estágio, João e Micael pela simpatia e disponibilidade.

Ficha de Identificação

Aluno

Nome: José Pedro Albuquerque

Número: 1705863

CTeSP: 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: Especialista

Docente Orientador de Estágio

Nome: Fernando Melo Rodrigues

Email: fmr@ipg.pt

Função: Professor Adjunto

Grau Académico: Especialista

Resumo

A Cibersegurança é um aspeto crucial de qualquer organização e é necessário ter uma abordagem abrangente para identificar quaisquer lacunas ou preocupações. Esta é uma necessidade cada vez mais importante para as empresas, que precisam atualizar as suas infraestruturas e aprimorar os sistemas de acordo com as necessidades do negócio. O conceito de *Separation of Concerns* é fundamental para garantir a segurança dos dados e informações, separando as diferentes áreas e responsabilidades dentro da empresa. Como tal, para garantir a segurança dos dados e informações, é fundamental que as empresas apliquem políticas de segurança, eduquem os colaboradores e monitorizem as redes sociais a procura de informações confidenciais.

Durante o meu estágio, tive a oportunidade de propor e implementar diversas soluções para os mais diversos serviços, a fim de escolher as mais adequadas às necessidades da instituição, alguns exemplos dessas soluções são: o Proxmox (Um Hypervisor); PowerDNS (Servidor de DNS). Utilizando o Proxmox instalei e configurei um cluster com três servidores para suportar todos os serviços atuais, aqueles que foram implementados / reimplementados por mim, e serviços futuros.

Foi também instalado e configurado um servidor para backups de todas as VMs e containers hospedados nesses mesmos servidores.

Abstract

Cybersecurity is a crucial aspect of any organization and it is necessary to have a comprehensive approach to identify any gaps or concerns. This is an increasingly important need for companies, which need to upgrade their infrastructures and improve systems according to business needs. The concept of Separation of Concerns is fundamental to ensure the security of data and information, separating the different areas and responsibilities within the company. As such, to ensure the security of data and information, it is critical that companies enforce security policies, educate employees, and monitor social networks for sensitive information.

During my internship, I had the opportunity to propose and implement several solutions for the most diverse services, in order to choose the most appropriate to the needs of the institution, some examples of these solutions are: Proxmox (A Hypervisor); PowerDNS (DNS Server). Using Proxmox I installed and configured a cluster with 3 servers to support all current services, those that were implemented / reimplemented by me, and future services.

A server has also been installed and configured for backups of all VMs and containers hosted on those same servers.

Índice

Introdução.....	1
1.1 Motivação.....	1
1.2 Caraterização sumária da instituição	1
1.3 Objetivos	2
1.4 Estrutura do documento	3
Resultados Esperados	4
Tecnologias	5
3.1 Proxmox.....	5
3.2 PowerDNS.....	6
3.3 Docker.....	6
3.4 Nginx	7
3.5 Zabbix.....	7
3.6 Grafana.....	8
3.7 InfluxDB.....	9
Tarefas Realizadas	10
4.1 Preparação dos servidores físicos para a instalação do Proxmox.....	11
4.2 Criação e configuração do cluster	12
4.3 Criação das máquinas virtuais e containers para alojar os serviços	13
4.3.1 Instalação e configuração do DNS Externo (PowerDNS).....	14
4.3.2 Instalação e configuração do Proxy Reverso (NGINX).....	16
4.3.3 Instalação da solução Zabbix	21
4.3.4 Instalação da solução Grafana	23
4.3.5 Instalação da solução InfluxDB	24
4.4 Criação de dashboards no Grafana para a monitorização da rede e do cluster.....	25
4.5 Realização de documentos relativos ao inventário de ativos.....	27
4.6 Manutenção de bastidores	28
Conclusões	30
5.1 Trabalho Futuro.....	30
Bibliografia	32
Anexos	33
Anexo A.....	33

Glossário de Abreviaturas

CTs	Containers
DDoS	Distributed denial of service
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of service
ESTG	Escola Superior de Tecnologia de Gestão
FTP	File Transfer Protocol
GPG	GNU Privacy Guard
HTTP	Hypertext Transfer Protocol
IoT	Internet of things
KVM	Kernel-based Virtual Machine
LXC	Linux Containers
RHEL	Red Hat Enterprise Linux
RPM	Red Hat Package Manager
SELinux	Security-Enhanced Linux
SO	Sistema operativo
SSH	Secure Shell Protocol
SSL	Secure Sockets Layer
UPS's	Uninterruptible Power Supply
VLANs	Virtual local area networks
VMs	Virtual Machines

Capítulo 1

Introdução

1.1 Motivação

A motivação para desenvolver o projeto em questão, surge da importância que a segurança da informação tem nas nossas vidas. Sendo cada vez mais importante assegurar nas mais diversas entidades mecanismos que permitam mitigar e neutralizar possíveis ameaças, que coloquem em causa a integridade da informação a esta pertencente.

Para além deste ponto anteriormente referido, a maior motivação é sem dúvida, a possibilidade de contribuir tanto para a instituição na qual me insiro, bem como para um esforço tido ao longo dos anos a fim de assegurar um ciberespaço nacional seguro.

1.2 Caracterização 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.

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 na ESTG do 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 do IPG 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 na ESTG, localizando-se no campus do Politécnico da Guarda, na Avenida Dr. Francisco Sá Carneiro, nº50, 6300-559, Guarda.

1.3 Objetivos

O objetivo de propor e implementar várias soluções, incluindo a configuração de um cluster Proxmox e a melhoria dos serviços, durante o estágio foi: analisar a infraestrutura atual, identificar áreas de melhoria e abordar a necessidade urgente de melhorar esses mesmos. Os serviços existentes careciam de manutenção e apresentavam diversas vulnerabilidades que poderiam prejudicar a instituição.

Através dessa análise e a implementação de soluções como o Proxmox, o objetivo foi alcançar o seguinte:

- Melhorar a disponibilidade dos serviços
O cluster garante alta disponibilidade migrando automaticamente máquinas virtuais (VMs) ou containers (CTs) para outro nó em caso de falha do servidor, diminuindo assim o tempo de inatividade e garantindo a disponibilidade contínua do serviço.
- Reforçar a segurança
Ao abordar as vulnerabilidades nos serviços existentes, as soluções implementadas visaram melhorar a maturidade global de segurança da instituição.
- Otimizar o desempenho
A configuração do cluster e outras soluções implementadas visam melhorar o desempenho dos serviços, distribuindo a carga de trabalho em vários servidores e utilizando recursos de forma eficiente.

- Permitir escalabilidade:
A configuração do cluster e a adição de novos serviços fornecem uma infraestrutura escalável que pode acomodar o crescimento e a expansão futuros dos serviços da instituição.

O foco não foi apenas em melhorias imediatas, mas também em estabelecer as bases para uma infraestrutura robusta e resiliente que possa suportar as necessidades da instituição a longo prazo

1.4 Estrutura do documento

O presente documento está organizado em cinco capítulos, descrevendo em pormenor todo o trabalho realizado ao longo do estágio, bem como as razões subjacentes às decisões que tiveram de ser tomadas.

- **Capítulo 1 - Introdução:** Apresenta o contexto e os objetivos do projeto.
- **Capítulo 2 - Resultados Esperados:** Descreve os resultados esperados relativos ao trabalho realizado ao longo do estágio.
- **Capítulo 3 - Tecnologias:** Como o nome do capítulo sugere, este capítulo descreve as tecnologias usadas ao longo do trabalho, abordando também um pouco sobre as vantagens e desvantagens das mesmas
- **Capítulo 4 - Tarefas Realizadas:** Apresenta as tarefas realizadas ao longo do estágio.
- **Capítulo 5 - Conclusões:** Apresenta as conclusões do projeto, os objetivos alcançados, bem como sugestões para trabalhos futuros.

Capítulo 2

Resultados Esperados

Com base no contexto fornecido, podemos inferir alguns resultados esperados das soluções propostas e implementadas durante o estágio:

- **Melhoria da eficiência dos serviços**

A implementação de soluções como o Proxmox e o PowerDNS visa melhorar a eficiência e qualidade dos diversos serviços oferecidos pela instituição. O Proxmox permite a instalação e configuração de um cluster com vários servidores, o que pode resultar em um desempenho aprimorado e maior confiabilidade dos serviços.

- **Gestão centralizada**

O uso do Proxmox permite a gestão centralizada de máquinas virtuais e containers. A interface gráfica do Proxmox oferece uma maneira fácil de gerir VMs, CTs, armazenamento e clusters. Essa capacidade de gestão centralizada simplifica a administração e monitorização da infraestrutura da instituição.

- **Backup e recuperação em caso de desastres**

Como parte da implementação, prevê-se a instalação e configuração de um servidor específico para fazer backup de todas as VMs e CTs hospedados nos servidores. Isso garante que os dados estejam protegidos e possam ser restaurados em caso de problemas ou desastres.

- **Escalabilidade e preparação para o futuro:**

A criação de um cluster usando o Proxmox permite escalabilidade e suporte a serviços futuros. O mesmo facilita a migração de VMs e CTs entre hosts físicos, implementação rápida de serviços em todo o cluster, como firewall e alta disponibilidade. Isso garante que a infraestrutura da instituição possa se adaptar e crescer conforme necessário.

Em resumo, os resultados esperados das soluções propostas e implementadas durante o estágio incluem a melhoria da eficiência dos serviços, a gestão centralizada, o backup e recuperação em caso de desastres, e a escalabilidade para futuras necessidades. Esses resultados contribuem para a eficácia e confiabilidade geral da infraestrutura informática da instituição.

Capítulo 3

Tecnologias

Durante o meu estágio, foram utilizadas diversas tecnologias e soluções para chegar ao objetivo de melhorar os serviços da instituição. Neste capítulo vou introduzir e abordar essas mesmas tecnologias e soluções.

3.1 Proxmox

O Proxmox é uma plataforma *open source* de virtualização baseada numa distribuição Linux (Debian) que oferece diversas vantagens e recursos para a criação e gestão de máquinas virtuais. É compatível com duas tecnologias principais de virtualização: KVM e LXC.

O KVM (Kernel-based Virtual Machine) é um módulo de virtualização gratuito e *open source* disponível no kernel Linux que permite ao kernel funcionar como um hipervisor, permitindo que uma máquina execute vários ambientes virtuais isolados chamados de guests ou máquinas virtuais.

Relativamente ao KVM, o LXC é um método de virtualização a nível do sistema operativo que permite executar vários sistemas Linux isolados em uma só máquina usando um único kernel Linux. É uma plataforma *open source* que promete facilidade de uso e uma experiência intuitiva e moderna, o objetivo do LXC é criar um ambiente que se aproxime o mais possível de uma instalação Linux padrão sem a necessidade de um kernel separado.

As principais vantagens do Proxmox VE em relação a outros softwares de virtualização são:

- **O custo-benefício;**
- **A integração com KVM e LXC;**
- **O ambiente completo de virtualização;**
- **A estabilidade e segurança, além da flexibilidade e escalabilidade.**

Essas vantagens tornam o Proxmox VE uma opção atraente para empresas e utilizadores que desejam implementar uma solução de virtualização eficiente e econômica.

O KVM oferece isolamento completo e desempenho próximo ao nativo, enquanto o LXC proporciona eficiência de recursos e inicialização rápida.

3.2 PowerDNS

O PowerDNS é um software de servidor DNS, escrito em C++, que é utilizado para alojar nomes de domínio. O mesmo é altamente escalável e flexível, permitindo oferecer um serviço de DNS autoritativo de alto desempenho para os utilizadores de um determinado domínio. O PowerDNS é conhecido pela sua implementação de DNSSEC, que é um conjunto de extensões para o protocolo DNS que aumenta a segurança, autenticidade e integridade dos processos de resolução de domínios.

Algumas vantagens e desvantagens do PowerDNS em relação a outros softwares incluem:

Vantagens:

- **Desempenho;**
- **Escalabilidade;**
- **Implementação;**
- **Segurança.**

Desvantagens:

- **Complexidade**, o mesmo pode ser mais complexo de configurar e usar do que outros softwares de DNS;
- **Custo**, embora seja um software de código aberto, a empresa que o desenvolve também oferece uma versão comercial com recursos adicionais.

Embora possa ser mais complexo de configurar e usar do que outros softwares de DNS, o mesmo é amplamente utilizado por pequenas e grandes empresas em todo o mundo.

3.3 Docker

O Docker é uma plataforma de *containerization* open source que permite a criação, execução, gestão e distribuição de software em ambientes independentes e isolados, chamados de containers.

Algumas das vantagens do uso do Docker incluem:

- **Eficiência de recursos;**
- **Portabilidade;**
- **Facilidade de uso;**
- **Escalabilidade e arquitetura de micro serviços.**

O Docker é uma ferramenta valiosa para programadores e administradores de sistemas. O mesmo permite que o software seja separado da infraestrutura, facilitando a entrega rápida de um ou mais serviços e é amplamente utilizado no mundo.

3.4 Nginx

O Nginx é um software para servidor web de código aberto que também pode ser usado como um proxy reverso. Um proxy reverso é um tipo de servidor proxy que fica atrás da firewall numa rede privada e direciona pedidos de clientes para o servidor apropriado. O Nginx é amplamente utilizado como um proxy reverso, permitindo aumentar a segurança e o desempenho dos sites.

Algumas das vantagens do uso do Nginx como um proxy reverso incluem:

- **Segurança e anonimato:** Ao interceptar pedidos destinados aos servidores, um proxy reverso protege a identidade do servidor e atua como uma defesa adicional contra ataques, como DDoS e DoS;
- **Desempenho:** O Nginx pode melhorar o desempenho, a confiabilidade e a escalabilidade dos sites. Ao ser configurado para otimizar conteúdos o Nginx comprime os formatos configurados para melhorar o tempo de carregamento de uma página web a um cliente;
- **Flexibilidade:** O Nginx pode ser configurado para atender a várias necessidades, incluindo balanceamento de carga, cache, SSL offloading e muito mais.

O Nginx é usado por sites de alto volume de tráfego, como Dropbox, Netflix, entre outros. Pois oferece todos os benefícios de um proxy reverso. É simples de implementar e proporciona ao utilizador uma forma fácil de implementar segurança contra ataques a servidores web, é altamente escalável e pode lidar com um grande número de ligações simultâneas. Em comparação com outros softwares de servidor web como o Apache, o Nginx é conhecido por ser mais leve e rápido

3.5 Zabbix

O Zabbix é uma ferramenta *open source* de monitorização que pode ser utilizada para monitorar toda a infraestrutura de rede e aplicações de uma empresa

Algumas vantagens do Zabbix incluem:

- **Facilidade de manipulação:** O Zabbix possui uma interface amigável e fácil de usar, o que agiliza o trabalho diário;
- **Alertas em tempo real:** A ferramenta permite enviar alertas de problemas por email e possui diversas outras integrações de alertas, possibilitando uma resposta rápida a eventos críticos;
- **Gráficos personalizáveis:** O Zabbix oferece a possibilidade de personalizar os gráficos permitindo uma visualização mais clara e adaptada às necessidades da empresa;

- **Monitorização abrangente:** O Zabbix é capaz de monitorar diversos aspetos da infraestrutura, como servidores, redes, bases de dados, aplicações e além disso possui diversos templates oficiais e da comunidade que garantem o suporte a diversos outros sistemas.

No entanto, também existem algumas desvantagens associadas ao uso do Zabbix:

- **Curva de aprendizagem;**
- **Configuração inicial complexa.**

Além das vantagens e desvantagens é uma ferramenta amplamente usada e possui uma comunidade ativa de utilizadores e programadores, o que garante suporte e atualizações frequentes.

3.6 Grafana

O Grafana é uma plataforma de visualização e análise de dados que permite a construção de dashboards com indicadores customizados.

Algumas vantagens do Grafana incluem:

- **Flexibilidade:** O Grafana é altamente personalizável e pode ser integrado a diversas fontes de dados, como base de dados e outras ferramentas;
- **Visualização de dados em tempo real:** A ferramenta permite a visualização de dados em tempo real, o que facilita a tomada de decisões rápidas;
- **Interface intuitiva:** O Grafana possui uma interface amigável e fácil de usar, o que agiliza o trabalho diário.

No entanto, também existem algumas desvantagens associadas ao uso do Grafana:

- **Curva de aprendizagem;**
- **Limitações na versão gratuita.**

Uma das integrações possíveis no Grafana é o Zabbix utilizando o plugin Zabbix para Grafana, que permite a visualização de dados do Zabbix em dashboards do Grafana. Esta integração pode ser útil para empresas que já utilizam o Zabbix como ferramenta de monitorização e desejam visualizar os dados em dashboards personalizados no Grafana.

3.7 InfluxDB

O InfluxDB é uma base de dados não relacional de código aberto, projetada para armazenar e consultar grandes volumes de dados de séries temporais, como dados de sensores e métricas de desempenho.

Algumas vantagens do InfluxDB incluem:

- **Alta performance:** O InfluxDB é otimizado para consultas de séries temporais e pode lidar com grandes volumes de dados com facilidade;
- **Escalabilidade:** O InfluxDB é projetado para ser altamente escalável, permitindo a distribuição dos dados em vários servidores para lidar com grandes volumes de dados e cargas de trabalho;
- **Flexibilidade:** O InfluxDB suporta uma variedade de linguagens de consulta, incluindo SQL-like e flux, uma linguagem de consulta específica para séries temporais.

Algumas desvantagens do InfluxDB incluem:

- **Limitações de armazenamento:** O InfluxDB é projetado para armazenar dados de séries temporais e pode não ser a melhor escolha para outros tipos de dados;
- **Grande curva de aprendizagem:** O InfluxDB tem uma curva de aprendizagem lenta, especialmente se não estiver familiarizado com base de dados de séries temporais.

Além disso, o InfluxDB é frequentemente usado em conjunto com outras ferramentas de análise de dados, como o Grafana, para visualização de dados. É também usado em IoT para armazenar e analisar dados de sensores.

Capítulo 4

Tarefas Realizadas

Neste Capítulo, vão ser descritas as tarefas realizadas, até ao término do estágio curricular.

1. Preparação dos servidores físicos para a instalação do Proxmox;
2. Criação e configuração do cluster;
3. Criação das máquinas virtuais e containers para alojar os serviços;
4. Criação de dashboards no Grafana para a monitorização da rede e do cluster;
5. Realização de documentos relativos ao inventário de ativos;
6. Manutenção de bastidores;

4.1 Preparação dos servidores físicos para a instalação do Proxmox

Após terminada a tarefa referida no ponto anterior, procedi a escolha e preparação dos 3 servidores físicos destinados ao Cluster Proxmox. Nesta fase foi atualizada toda a firmware relativa aos componentes dos servidores, configurado os discos do sistema como RAID 1 e efetuada a instalação do Proxmox, tal como se ilustra nas figuras 3 e 4.

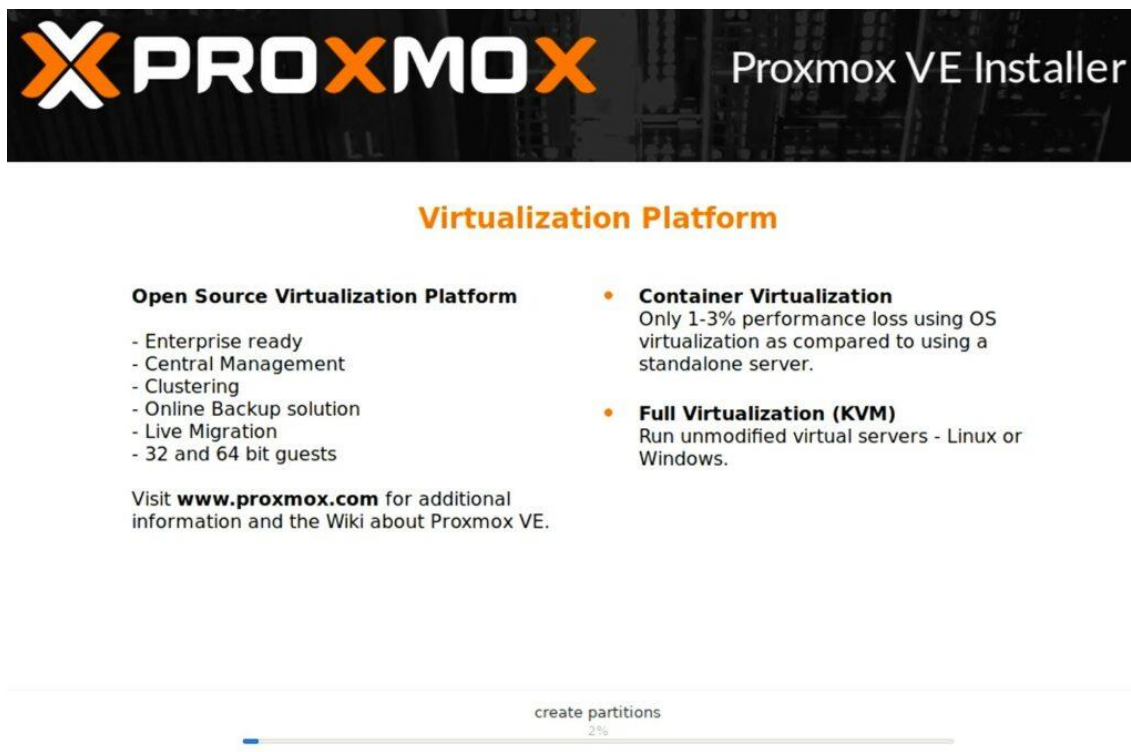


Figura 3 – Instalação do Proxmox

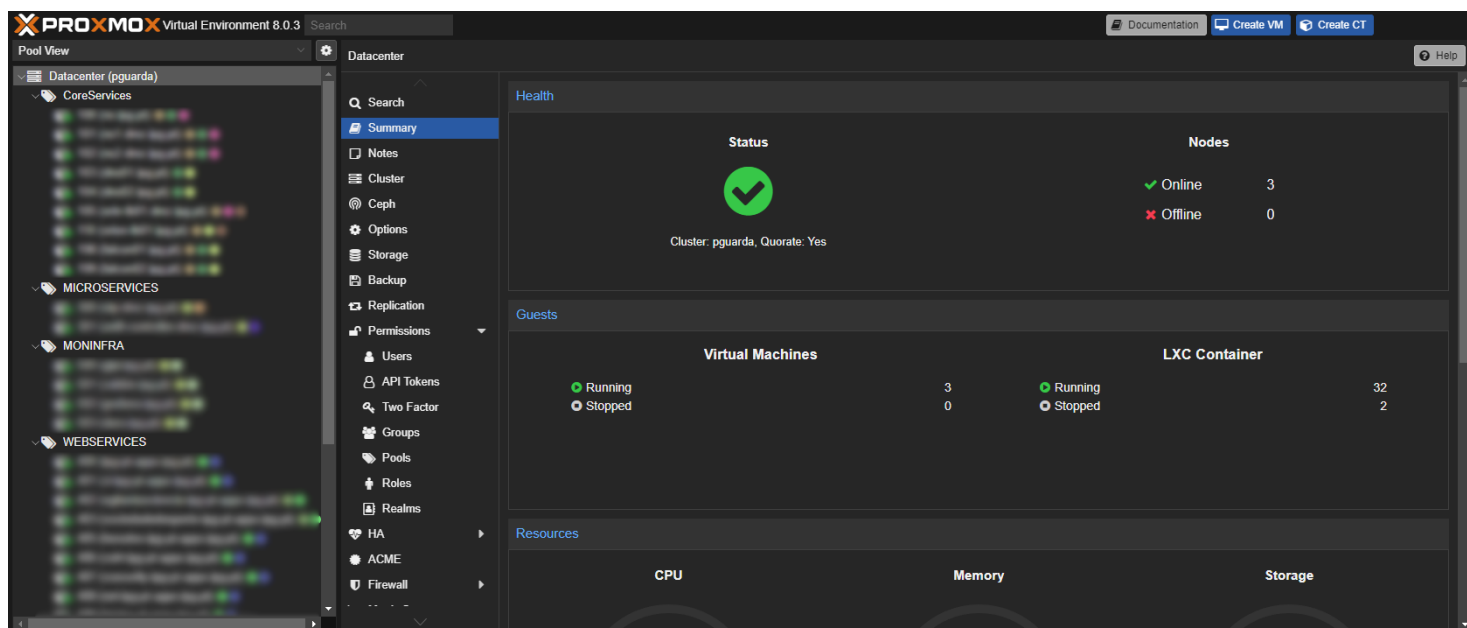


Figura 4 – Cluster Proxmox
Politécnico Guarda

Na Figura 3 pode ver-se um passo da instalação da plataforma Proxmox. Enquanto que na Figura 4 pode ver-se a instalação concluída e configurada, bem como todos os serviços atualmente em produção. De referir que esta foi distorcida por questões de segurança.

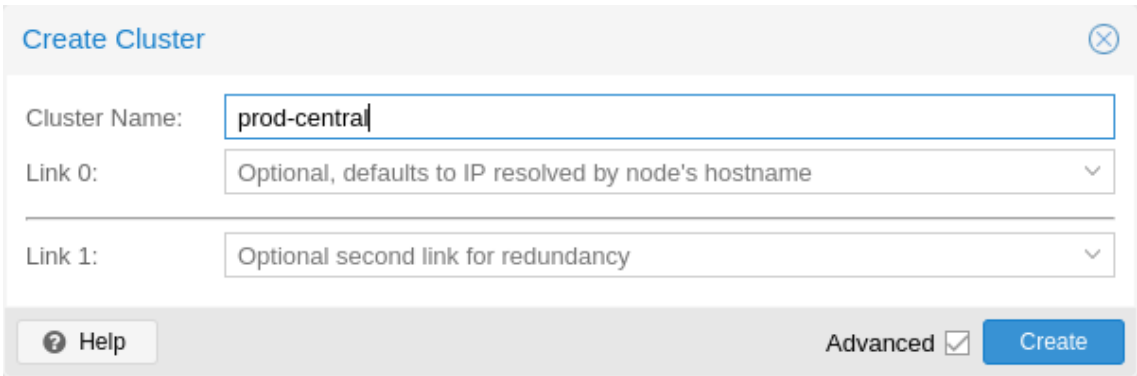
4.2 Criação e configuração do cluster

Depois da instalação, foi criado o cluster de acordo com as recomendações da equipa responsável pelo Proxmox, das quais se destacam as seguintes:

- Mínimo 3 servidores;
- Rede dedicada as migrações entre servidores das máquinas hospedadas (VMs / CTs);
- Rede dedicada a sincronização entre os servidores do cluster;
- Realização de backups usando a solução Proxmox Backup Server.

Antes de criar o cluster, procedi a configuração idêntica dos servidores, a nível de rede e armazenamento e só de seguida continuei o processo.

Para isso acedi a interface web do primeiro servidor e procedi a criação do cluster, ver figura 5



The screenshot shows the 'Create Cluster' form in the Proxmox web interface. The 'Cluster Name' field contains 'prod-central'. The 'Link 0' dropdown menu is set to 'Optional, defaults to IP resolved by node's hostname'. The 'Link 1' dropdown menu is set to 'Optional second link for redundancy'. At the bottom of the form, there is a 'Help' button, an 'Advanced' checkbox which is checked, and a blue 'Create' button.

Figura 5 – Criar Cluster

No parâmetro **Link 0** foi selecionada a rede dedicada a sincronização entre os servidores do cluster.

De seguida acedi a interface dos restantes servidores e juntei os mesmos a este cluster, tal como se pode ver na Figura 6

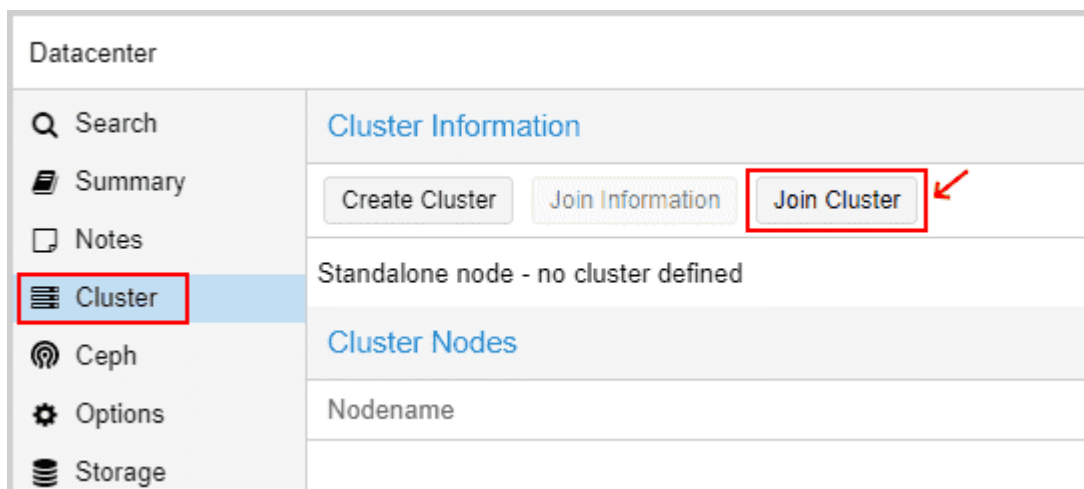


Figura 6 – Juntar servidor ao cluster

4.3 Criação das máquinas virtuais e containers para alojar os serviços

Foram criadas e preparadas as máquinas virtuais e containers necessários para alojar a nova infraestrutura proposta e implementada por mim, bem como os sites web já existentes.

Como referido no capítulo 3, algumas das soluções implementadas são:

- **PowerDNS** para servidor de nomes autoritativo responsável pelas zonas: ipg.pt e politecnicoguarda.pt;
- **Nginx** para proxy reverso, responsável pela coordenação do tráfego aos sites corretos, garantido no processo uma ligação estável e segura, aplicando os últimos padrões no que toca a implementação de servidores web e cabeçalhos HTTP de segurança;
- **Zabbix** para monitorização dos equipamentos ativos;
- **Grafana** para visualização dos dados previamente obtidos pelo Zabbix;
- **InfluxDB** para armazenar os dados gerados pelo Cluster Proxmox para serem visualizados no Grafana.

Para o processo de instalação das soluções anteriormente referidas foi criado um template recorrendo a distribuição Rocky Linux, sendo esta uma das mais viáveis e aconselhada a nível empresarial por a mesma ser derivada do RHEL e estar assente em ser open-source e suportada pela comunidade, proporcionando estabilidade sólida com atualizações regulares e um ciclo de vida de suporte de 10 anos, tudo sem nenhum custo.

4.3.1 Instalação e configuração do DNS Externo (PowerDNS)

Primeiramente temos de colocar o SELinux em modo permissivo, para tal executamos o seguinte comando e alteramos a linha **SELINUX** para **SELINUX=permissive**:

```
nano /etc/sysconfig/selinux
```

De seguida adicionamos o repositório **Stable** do **PowerDNS** ao sistema, para tal executamos os seguintes comandos:

```
curl -o /etc/yum.repos.d/powerdns-auth-48.repo  
https://repo.powerdns.com/repo-files/el-auth-47.repo  
dnf update
```

Após estes passos procedemos a instalação do serviço PowerDNS com suporte a MySQL.

```
dnf install pdns pdns-backend-mysql bind-utils -y
```

```
dnf install mariadb-server mariadb  
systemctl enable --now mariadb
```

```
mysql_secure_installation
```

Posteriormente, procedemos a criação da base de dados a ser usada pelo serviço.

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

```
CREATE DATABASE <nomedb>;  
GRANT ALL ON <nomedb>.* TO '<utilizador>'@'localhost'  
IDENTIFIED BY 'Password$egur4';
```

```
nano /etc/my.cnf.d/mariadb-server.cnf
```

Em seguida, alteramos o DNS usado pelo sistema, para tal recorreremos aos seguintes comandos.

Desassociar o ficheiro usado pelo sistema.

```
unlink /etc/resolv.conf
```

Colocar **DNS=none** no perfil de rede.

```
nano /etc/NetworkManager/system-connections/enp1s0.nmconnection
```

Reiniciar o gestor de rede.

```
systemctl restart NetworkManager
```

Editar o ficheiro e colocar o/os nameservers pretendidos, Ex: 1.1.1.2.

```
nano /etc/resolv.conf
```

Realizada a configuração verificamos a conectividade e resolução de nomes através do seguinte comando.

```
ping cloudflare.com
```

Após o passo anterior bem-sucedido, importamos o esquema da base de dados.

```
mysql -u pdns -p pdnsdb < /usr/share/doc/pdns-backend-mysql/schema.mysql.sql
```

De seguida realizamos uma copia do ficheiro de configuração, de modo a usar a mesma como base na nova configuração.

```
mv /etc/pdns/pdns.conf /etc/pdns/pdns.conf.bak  
nano /etc/pdns/pdns.conf
```

Realizada a configuração anterior, necessitamos de adicionar a firewall do sistema o porto usado pelo serviço de DNS, nomeadamente o 53, através dos seguintes comandos.

```
firewall-cmd --add-service=dns --permanent  
firewall-cmd --reload
```

Após adicionarmos o porto anteriormente referido, podemos iniciar a configuração do PowerDNS na máquina que vai ter o cargo de **Master** (Primário) e nas máquinas que vão ter o cargo **Slave** (Secundário).

Feito isso basta em cada máquina **Slave** executar o seguinte comando na base de dados, substituindo <ip master> pelo Endereço IP da máquina **Master** e <fqdn> pelo hostname completo da máquina **Slave** em questão, Ex: ns01.empresa.pt.

```
insert into supermasters values ('<ip master>',  
'<fqdn>', 'admin');
```

```
reboot
```

4.3.2 Instalação e configuração do Proxy Reverso (NGINX)

A instalação do NGINX é muito simples, sendo apenas necessário efetuar os seguintes comandos.

```
sudo dnf update
```

```
sudo dnf install nginx
```

```
sudo systemctl enable nginx
```

Realizada esta etapa, procedemos a configuração do NGINX como pretendido, para isso acedemos ao diretório onde ficam armazenadas as configurações e aplicamos as alterações necessárias.

```
cd /etc/nginx
```

De modo a colocarmos o Nginx a operar como reverse proxy no seguinte nome: site1.empresa.pt é necessário efetuar as seguintes configurações

```
nano security.conf
```

```
# Cabeçalhos de segurança
add_header X-XSS-Protection "1; mode=block" always;
add_header X-Content-Type-Options "nosniff" always;
add_header Referrer-Policy "no-referrer-when-downgrade"
always;
add_header Content-Security-Policy "default-src 'self' http:
https: ws: wss: data: blob: 'unsafe-inline'; frame-ancestors
'self';" always;
add_header Permissions-Policy "interest-cohort=()" always;
add_header Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload" always;

# . well-known
location ~ /\.(?!well-known) {
    deny all;
}
```

```
nano /general.conf
```

```
# favicon.ico
location = /favicon.ico {
    log_not_found off;
}
# robots.txt
location = /robots.txt {
    log_not_found off;
}
# gzip
gzip                on;
gzip_vary           on;
gzip_proxied       any;
gzip_comp_level    6;

gzip_types text/plain text/css text/xml application/json
           application/javascript application/rss+xml
           application/atom+xml image/svg+xml;
```

```
nano proxy.conf
```

```
proxy_http_version 1.1;
proxy_cache_bypass $http_upgrade;

# Proxy SSL
proxy_ssl_server_name          on;

# Proxy headers
proxy_set_header Upgrade $http_upgrade;
proxy_set_header Connection $connection_upgrade;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header Forwarded $proxy_add_forwarded;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header X-Forwarded-Proto $scheme;
proxy_set_header X-Forwarded-Host $host;
proxy_set_header X-Forwarded-Port $server_port;

# Proxy timeouts
proxy_connect_timeout          60s;
proxy_send_timeout             60s;
proxy_read_timeout             60s;
```

```
nano conf.d/site1.empresa.pt.conf
```

```
server {
    listen 1.1.1.1:80;
    server_name site1.empresa.pt;
    return 301 https://site1.empresa.pt$request_uri;
}
server {
    listen 1.1.1.1:443 ssl http2;
    server_name site1.empresa.pt;
    # SSL
    ssl_certificate /etc/nginx/ssl/site1.empresa.pt.crt;
    ssl_certificate_key /etc/nginx/ssl/site1.empresa.pt.key;
    # Headers
    include security.conf;
    # Logging
    access_log /var/log/nginx/access-site1.log combined
buffer=512k flush=1m;
    error_log /var/log/nginx/error-site1.log warn;
    # Reverse proxy
    location / {
        proxy_pass http://app1.intra.empresa.pt;
        proxy_set_header Host $host;
        include proxy.conf;
    }
    # Configuração adicional
    include general.conf;
}
```

Posteriormente a configuração, temos o NGINX a operar como reverse proxy para uma aplicação da empresa com bases bem definidas e regendo-se pelas boas praticas.

Para verificar se as alterações foram efetuadas com sucesso, recorreremos ao seguinte comando, que em caso contrário apresenta os erros existentes na configuração.

```
sudo nginx -t
```

Feito isso e se o resultado do comando anterior for “OK” podemos iniciar o serviço usando o seguinte comando

```
sudo systemctl start nginx
```

Além do comando referido anteriormente, o seguinte comando também pode nos ajudar a perceber o que poderá ter falhado ao iniciar o serviço.

```
sudo systemctl status nginx
```

4.3.3 Instalação da solução **Zabbix**

Para a instalação do Zabbix, recorreremos ao comando e repositório abaixo mencionado.

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

Posteriormente é necessário realizar a instalação das dependências necessárias, para tal utilizamos o seguinte comando.

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

Instaladas as dependências, procedemos a criação da base de dados e utilizador.

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

```
create database zabbix character set utf8mb4 collate  
utf8mb4_bin;
```

```
create user zabbix@localhost identified by 'password';
```

```
grant all privileges on zabbix.* to zabbix@localhost;
```

```
set global log_bin_trust_function_creators = 1;
```

```
quit;
```

Criada a base de dados e respetivo utilizador, procedemos a importação do esquema e dados iniciais.

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

Em seguida realizamos a desativação da opção `log_bin_trust_function_creators` na base de dados.

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

```
set global log_bin_trust_function_creators = 0;
```

```
quit;
```

De modo a reforçar a segurança da nossa instalação editamos o ficheiro `/etc/zabbix/zabbix_server.conf` e efetuamos as alterações necessárias, entre elas, o campo `DBPassword`, onde colocamos a password definida para o utilizador `zabbix` na Base de dados.

```
DBPassword=password
```

Já no diretório `/etc/nginx/conf.d/zabbix.conf` e efetuamos as alterações necessárias, entre elas, o campo `listen` e `server_name`, que corresponde ao IP/Porta de escuta do servidor web e ao nome do servidor

```
listen 8080;  
server_name zabbix.empresa.pt;
```

De seguida, iniciamos o serviço e se todos os passos tiverem sido devidamente executados, será iniciado.

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

Após a conclusão destes passos podemos abrir o nosso navegador e aceder a interface web de gestão do zabbix, através do IP da máquina ou o nome definido anteriormente no campo `server_name`.

4.3.4 Instalação da solução **Grafana**

Para instalação do Grafana recorreremos ao seguinte repositório RPM de modo a descarregar a solução e procedemos a importação da chave GPG.

```
wget -q -O gpg.key https://rpm.grafana.com/gpg.key  
sudo rpm --import gpg.key
```

Posteriormente criamos um ficheiro `/etc/yum.repos.d/grafana.repo` com o seguinte conteúdo.

```
[grafana]  
name=grafana  
baseurl=https://rpm.grafana.com  
repo_gpgcheck=1  
enabled=1  
gpgcheck=1  
gpgkey=https://rpm.grafana.com/gpg.key  
sslverify=1  
sslcacert=/etc/pki/tls/certs/ca-bundle.crt  
exclude=*beta*
```

Após descarregada realizamos a instalação do Grafana, através do seguinte comando.


```
sudo dnf install grafana-enterprise
```

4.3.5 Instalação da solução **InfluxDB**

Para a instalação do InfluxDB, esta acaba por ser bastante prática e rápida.

Como tal, é necessário adicionar o repositório do InfluxDB ao sistema criando o ficheiro `/etc/yum.repos.d/influxdata.repo` com o seguinte conteúdo

```
[influxdata]
name = InfluxData Repository - Stable
baseurl =
https://repos.influxdata.com/stable/$basearch/main
enabled = 1
gpgcheck = 1
gpgkey = https://repos.influxdata.com/influxdata-
archive_compat.key
```

Posteriormente proceder então a instalação da solução.

```
sudo dnf install influxdb2
```

4.4 Criação de dashboards no Grafana para a monitorização da rede e do cluster

Após a instalação e configuração do Zabbix, foram adicionados switches e equipamentos a monitorar ao mesmo. De seguida foi instalada e configurada a solução Grafana, que permite visualizar diversos tipos de dados obtidos de várias integrações que a mesma possui, entre elas, o Zabbix e o InfluxDB.

Foram criados dashboards uteis para a equipa do Centro de Informática, permitindo assim obter uma visão geral de toda a infraestrutura em tempo real, tal como se ilustra na figura 7, onde podemos ver o dashboard da rede com os dados obtidos pelo Zabbix e na figura 8 o dashboard relativamente ao cluster com os dados obtidos pelo InfluxDB

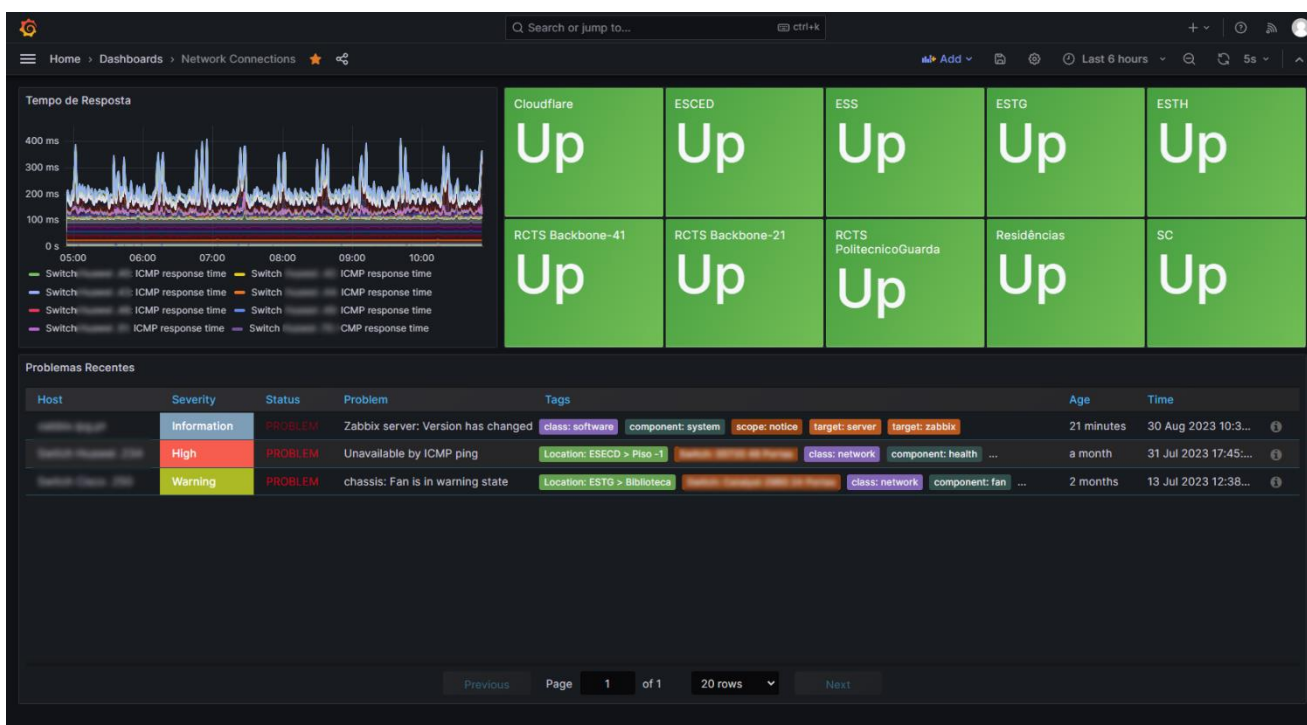


Figura 7 – Dashboard da Rede (Dados provenientes do Zabbix)

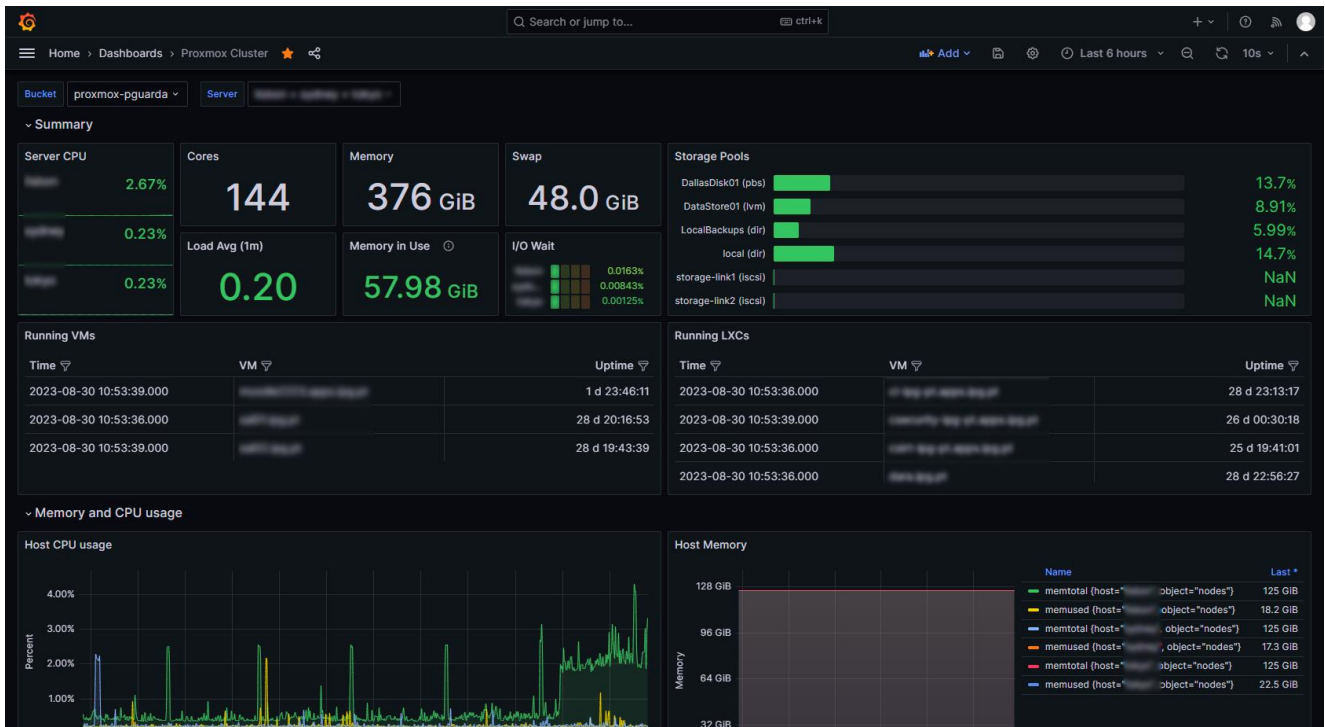


Figura 8 – Dashboard do Cluster (Dados provenientes do InfluxDB)

4.5 Realização de documentos relativos ao inventário de ativos

Em paralelo à instalação dos serviços foi realizada a devida documentação dos mesmos, a fim de facilitar a futura identificação, manutenção e eventuais alterações. O documento encontra-se dividido em diversas secções como: IP Público, ID, IP Privado, IP Storage, Nome, Descrição, Tipo, SO, Serviços, VLANs, Localização, Ativo.

No **Anexo A** consta uma imagem demonstrativa dessa mesma lista, a mesma conta com mais de 36 registos detalhando a informação dos ativos desta nova infraestrutura do Politécnico da Guarda.

4.6 Manutenção de bastidores

Durante as primeiras semanas do estágio foi elaborada uma listagem de bastidores a efetuar manutenção, essa manutenção consistiu na:

- Limpeza dos bastidores;
- Troca de equipamentos ativos (Switchs, UPS's);
- Troca dos patch cords (Cabos de Ethernet que fazem a ligação do equipamento ativo, os Switchs, ao passivo, os Patch panels).

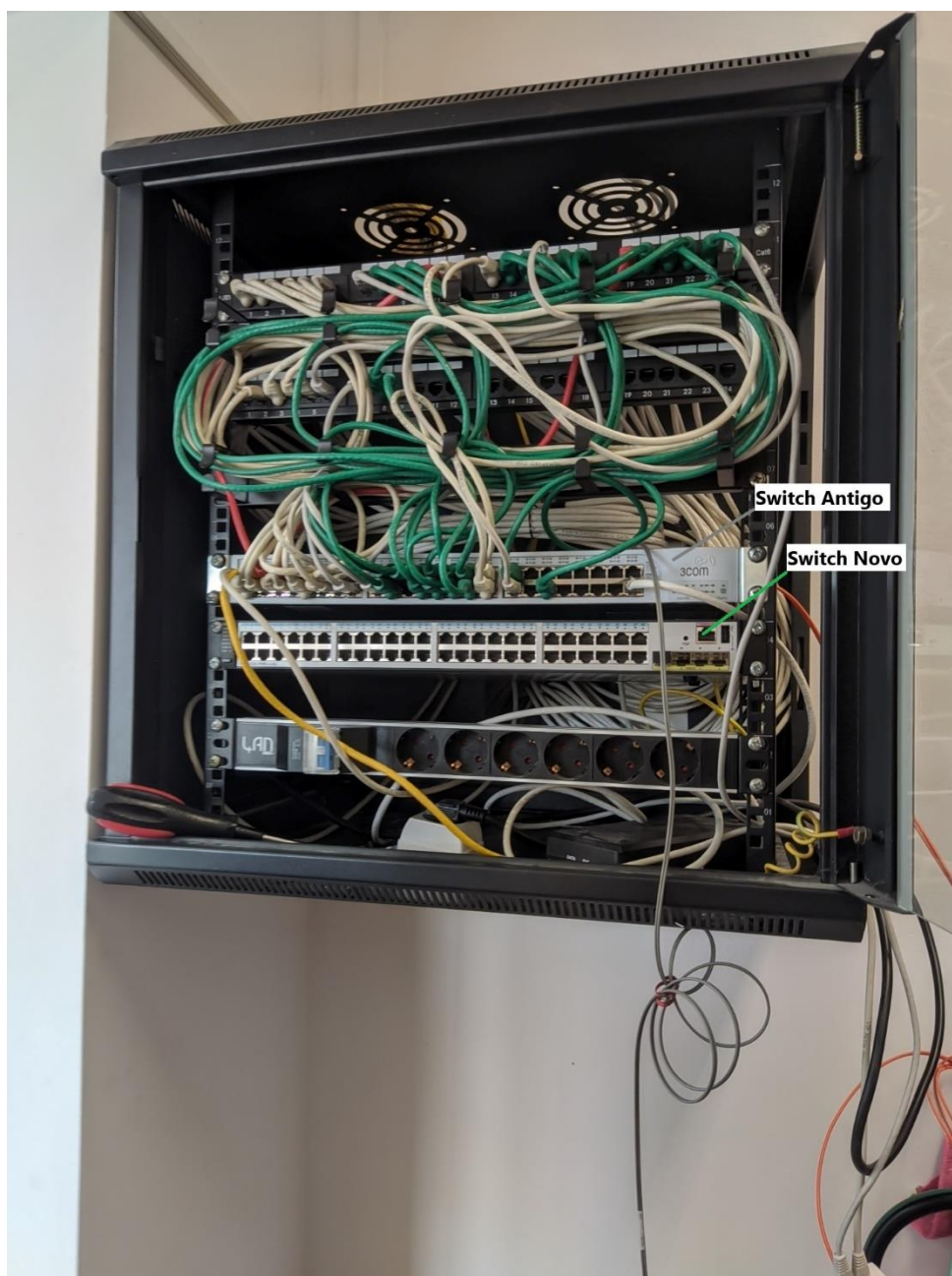


Figura 1 – Bastidor Escola Superior de Saúde (Antes)



Figura 2 - Bastidor Escola Superior de Saúde (Depois)

Capítulo 5

Conclusões

O mundo tecnológico tem-se transformado a um ritmo vertiginoso, onde se verificam milhares de ataques informáticos que ganham forma a cada segundo, como tal, seria de tremenda negligência afirmar que os serviços e sistemas atualmente disponíveis se encontram totalmente seguros. Desta forma, é imperativo que qualquer organização tenha como ação prioritária o amadurecimento nesta problemática, que é a Cibersegurança.

O presente relatório faz referência ao percurso realizado na Unidade Curricular Estágio para obtenção do diploma de técnico(a) superior profissional em Cibersegurança, no Centro de Informática do Politécnico da Guarda. O principal objetivo deste foi melhorar a infraestrutura da instituição tendo em conta a enorme importância dos seguintes pontos:

- **Melhoria da disponibilidade dos serviços;**
- **Reforço da segurança;**
- **Otimização do desempenho;**
- **Escalabilidade.**

5.1 Trabalho Futuro

O trabalho futuro é migrar, implementar/reimplementar os restantes serviços existentes e necessários para o bom funcionamento da instituição para esta nova infraestrutura no intuito de uniformizar e ir de encontro com os últimos standards e boas práticas de segurança.

Não deixando de parte, um ponto muito importante a se fazer na instituição em questão é aplicar políticas de segurança e conformidade, atualmente as existentes não tem “força”, O que quero dizer com isto é por exemplo:

O projeto X pretende ter uma máquina com acesso SSH, HTTP, FTP, o mesmo acaba quase que sempre cedido, não há um controlo e verificação prévia, tem de ser feitas as seguintes perguntas: O porque, o que, para quando, uma análise técnica aos serviços que vão estar a correr, e uma análise de risco por parte da equipa do Centro De Informática.

Se este mesmo comportamento for permitido pode trazer problemas futuros a instituição pois X serviço pode ser alvo de ataque e ser comprometido, e com isso poder escalar o acesso a outros sistemas da instituição

Bibliografia

(2023). Obtido de Proxmox: <https://www.proxmox.com/en/>

(2023). Obtido de PowerDNS: <https://www.powerdns.com/>

(2023). Obtido de Docker: <https://www.docker.com/>

(2023). Obtido de NGINX: <https://www.nginx.com/>

(2023). Obtido de Zabbix: <https://www.zabbix.com/>

(2023). Obtido de Grafana: <https://grafana.com/>

(2023). Obtido de InfluxDB: <https://www.influxdata.com/>

Anexos

Anexo A

POLI TÉCNICO GUARDA | CENTRO DE INFORMÁTICA

IP Público	ID	IP Privado	IP Storage	Nome	Descrição
N/A	N/A		N/A		Switch de Gestão
N/A	N/A		N/A		Interface de Gestão
N/A	N/A				Proxmox Cluster Node 1
N/A	N/A		N/A		Interface de Gestão
N/A	N/A				Proxmox Cluster Node 2
N/A	N/A		N/A		Interface de Gestão
N/A	N/A				Proxmox Cluster Node 3
N/A	100		N/A		NS Externo Master (Web UI)
	101		N/A		NS Externo Primário
	102		N/A		NS Externo Secundário
N/A	103		N/A		DNS Interno Primário
N/A	104		N/A		DNS Interno Secundário
N/A	105		N/A		Proxy Reverso Externo Primário
N/A	106		N/A		Proxy Reverso Externo Secundário
N/A	N/A		N/A		VIP Proxy Reverso Externo

Tipo	SO	Serviços	VLANs	Localização	Ativo
Switch				DataCenter	Sim
Servidor		iBMC		DataCenter	Sim
Servidor	Proxmox 8	Hypervisor		DataCenter	Sim
Servidor		iBMC		DataCenter	Sim
Servidor	Proxmox 8	Hypervisor		DataCenter	Sim
Servidor		iBMC		DataCenter	Sim
Servidor	Proxmox 8	Hypervisor		DataCenter	Sim
Container	RockyLinux 9	PowerDNS		DataCenter /	Sim
Container	RockyLinux 9	PowerDNS		DataCenter /	Sim
Container	RockyLinux 9	PowerDNS		DataCenter /	Sim
Container	RockyLinux 9	DNS		DataCenter /	Sim
Container	RockyLinux 9	DNS		DataCenter /	Sim
Container	RockyLinux 9	Nginx		DataCenter /	Sim
Container	RockyLinux 9	Nginx		DataCenter /	Não
Virtual IP				DataCenter	Não