CENTROS DE PROCESSAMENTO DE DADOS

2020/2021

Miguel Lopes[1], Iuri Carrasqueiro[2], João Tendeiro[3]

[1] 2222397@my.ipleiria.pt, Engenharia Informática [Diurno]

[2] 2222059@my.ipleiria.pt, Engenharia Informática [Diurno]

[3] 2222047@my.ipleiria.pt, Engenharia Informática [Diurno]

Resumo. Este trabalho laboratorial foi desenvolvido no âmbito da unidade curricular de Centros de Processamento de Dados, com o principal objetivo de planear, desenhar, implementar, configurar e documentar uma topologia de rede empresarial interligada à Internet através de vários ISPs. A solução proposta abrangeu a configuração de três datacenters, visando assegurar alta disponibilidade e eficiente balanceamento de carga para diversos serviços críticos como HTTP, DNS e FTP. Implementámos várias tecnologias e estratégias, incluindo clusters de alta disponibilidade para serviços web e DNS no Datacenter 1, um servidor Windows configurado tanto para NAS quanto para Remote Desktop no Datacenter 2, e soluções avançadas de backups e monitorização integrada no Datacenter 3. Através do uso de NAT, conseguimos um balanceamento de carga eficaz, garantindo uma distribuição uniforme das solicitações de rede entre os servidores disponíveis. Os resultados alcançados demonstraram que a infraestrutura projetada não só cumpre os requisitos de conectividade, segurança e resiliência, mas também otimiza a gestão de recursos e o desempenho das aplicações. Este projeto permitiu aplicar na prática os conhecimentos teóricos e práticos adquiridos, destacando a importância do planeamento cuidadoso e da implementação técnica precisa no contexto de redes empresariais complexas.

Palavras-chave: Datacenter, disponibilidade, balanceamento, backups, monitorização.

1. Introdução

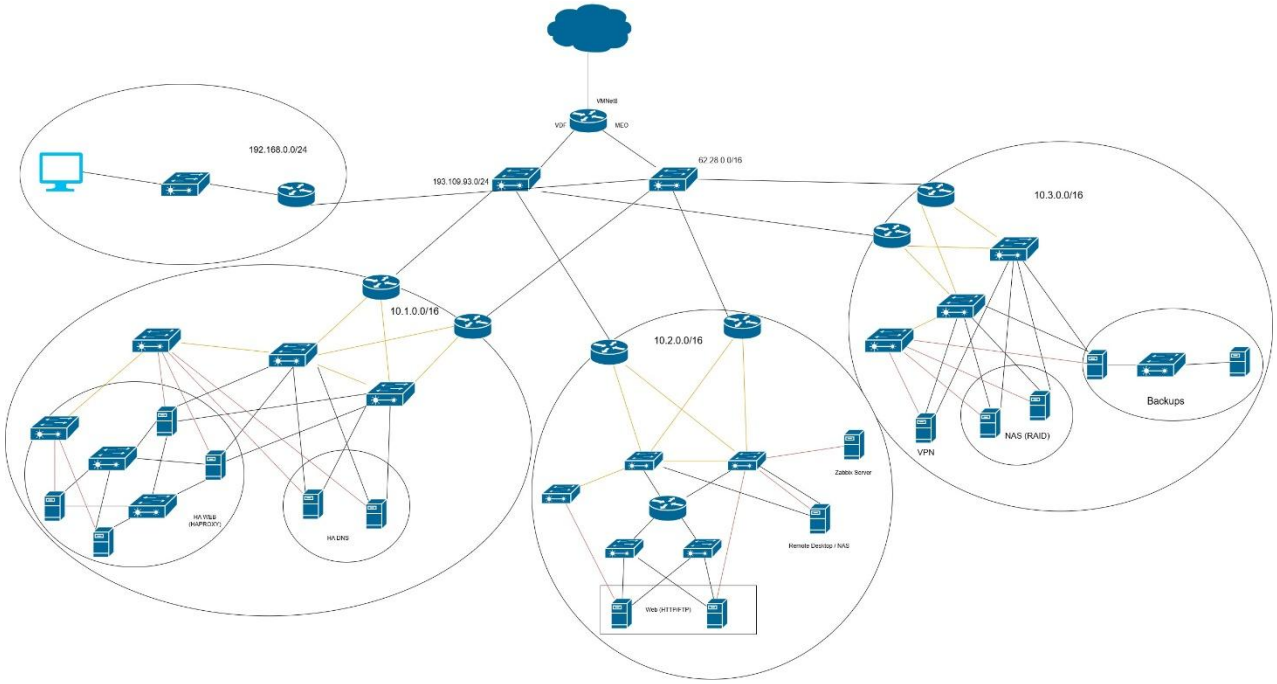
Este trabalho laboratorial tem como objetivo principal planear, desenhar, implementar, configurar e documentar uma topologia de rede empresarial interligada à Internet através de múltiplos provedores de serviços de Internet (ISPs). O foco do projeto é explorar e aplicar os conhecimentos adquiridos na unidade curricular de Centros de Processamento de Dados (CPD).

A infraestrutura proposta inclui três datacenters interligados, conectados à Internet via dois ISPs distintos (Meo e Vodafone), garantindo resiliência, alta disponibilidade e balanceamento de carga. Estes datacenters atendem tanto clientes particulares quanto empresas, fornecendo serviços de acesso remoto, alojamento de dados e soluções escaláveis e redundantes. Para garantir a qualidade e continuidade dos serviços, foram implementadas diversas tecnologias e práticas, tais como:

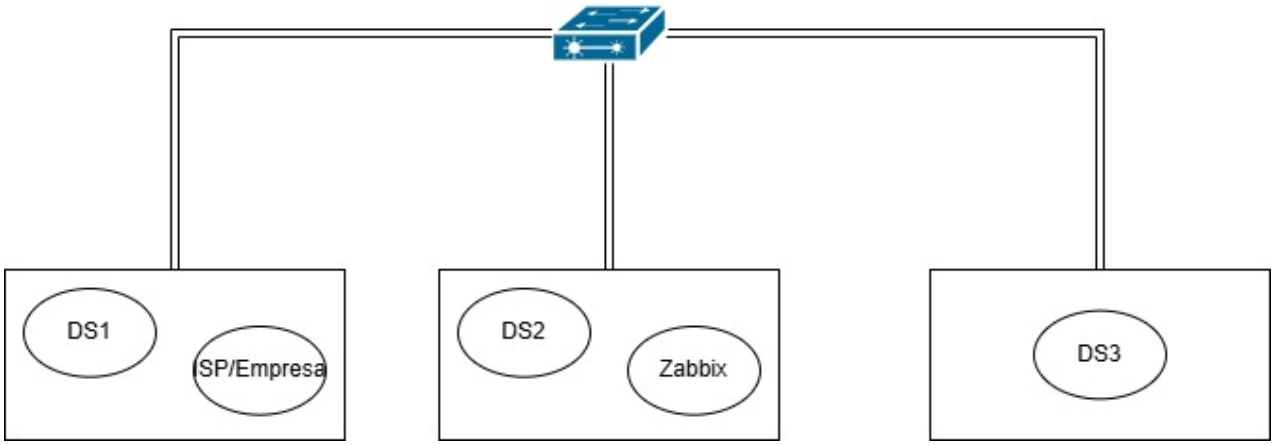
- **Soluções distribuídas de acesso remoto a serviços e ficheiros:** Utilizando tecnologias como VPN para acesso seguro e NAS para centralizar e proteger os dados.
- **Balanceamento de carga e alta disponibilidade:** Implementados em sistemas Linux, com suporte para IP virtual e mecanismos de failover.
- **Encaminhamento avançado:** Configurações otimizadas de encaminhamento para assegurar o desempenho das conexões entre os datacenters e a comunicação externa.

O **GNS3** foi utilizado como ferramenta principal para simular a rede, complementada com equipamentos físicos no laboratório.
Este documento está organizado para detalhar as decisões técnicas e operacionais tomadas ao longo do trabalho, abordando desde os conceitos e ferramentas utilizados até a configuração prática dos serviços e a validação da solução proposta.

1.1 Diagrama Lógico



1.2 Diagrama Físico

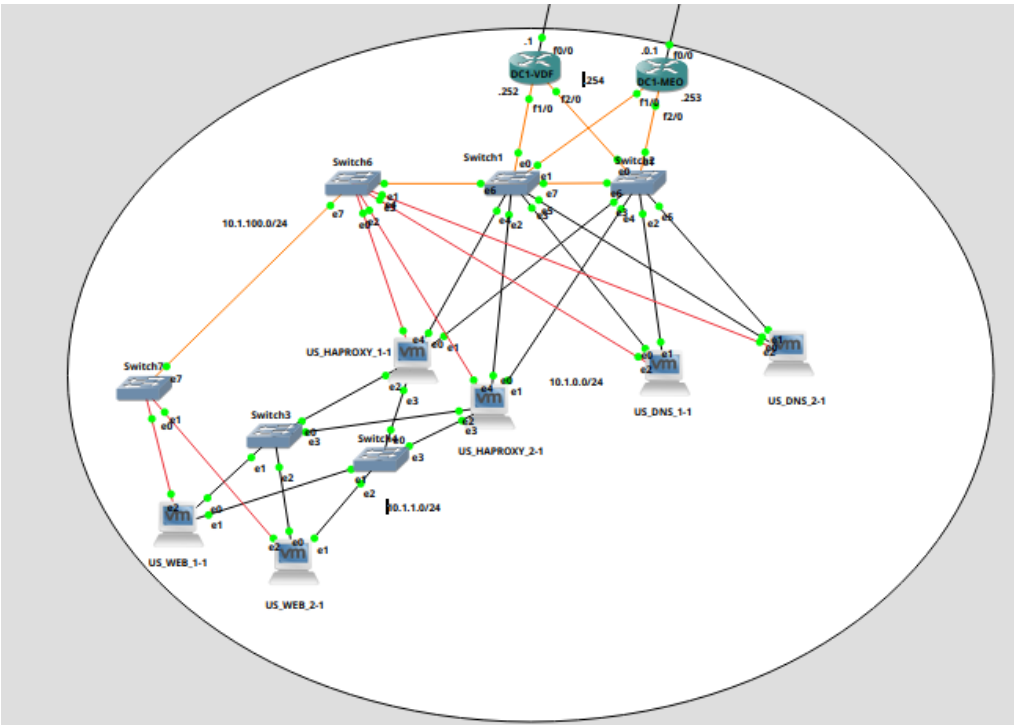


2. Solução proposta

Em cada um dos Datacenters foram configurados dois routers de acesso aos ISPs, um para cada ISP. Esses routers possuem duas interfaces para a ligação ao Datacenter como failover, utilizando a funcionalidade integrated routing and bridging para esse propósito. Entre ambos os routers, é utilizado o protocolo HSRP com o gateway da rede do Datacenter.

A comunicação entre os Datacenters é feita com túneis GRE, configurado de modo que caso um dos routers principais dos datacenters vá abaixo, todos os Datacenters começam a comunicar através dos routers secundários, sendo o router principal o router conectado ao ISP Meo e o secundário o router conectado ao ISP Vodafone.

I. Datacenter 1



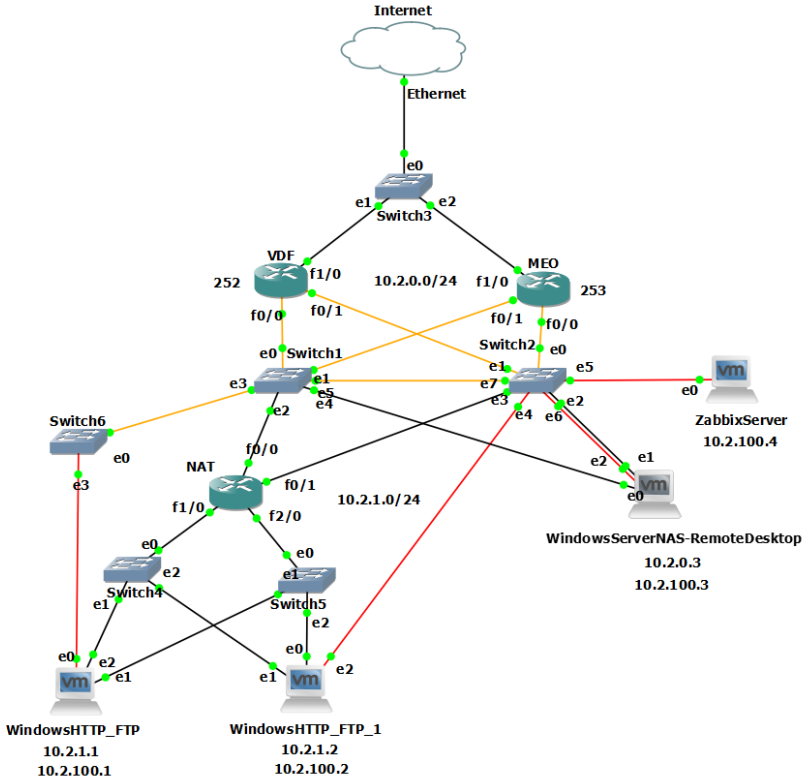
Este Data Center inclui dois clusters de alta disponibilidade para os serviços de Web (HTTP) e DNS. O serviço Web utiliza o servidor aplicacional Nginx, para disponibilizar as páginas Web, configurado em dois servidores Linux. Estes dois servidores são balanceados através de um balanceador de carga que, neste caso, o HAProxy.
O serviço HAProxy está configurado em duas máquinas diferentes, como cluster, sendo este disponibilizado através do serviço HeartBeat.

O serviço DNS, disponibilizado através do servidor aplicacional Bind9, resolve o domínio e subdomínios da rede. Este serviço está configurado em dois servidores Linux, configurado em modo Master-Slave, para uma sincronização das configurações entre estes. Os servidores utilizam como cluster de alta disponibilidade o serviço KeepAlived.

Como o acesso à Internet é feito através de dois ISPs, ou seja, o Data Center possui dois IPs públicos, foi necessário fazer configurações adicionais ao serviço de DNS para suportar esta vertente, uma vez que, o acesso da Internet ao Datacenter pode ser feito através de dois ISPs diferentes, o que obriga a que os endereços IPs devolvidos correspondem ao endereço IP público utilizado. Para isto, foram criadas duas instâncias do Bind9, onde cada uma das instâncias resolve o domínio e subdomínios da rede, mas devolvendo IPs diferentes. Uma instância devolve o IP público do ISP MEO e a outra instância devolve o IP público do ISP Vodafone. Assim, os clientes tendo configurado como servidor de DNS os dois IPs públicos do Datacenter, o serviço devolve sempre o IP para qual foi feito o pedido DNS, permitindo também que, no caso de falha de um dos routers do Datacenter, toda a comunicação seja feita através do outro router, ou seja, através do outro IP público.

Por fim, para permitir que os serviços Web disponibilizados pelos outros Datacenters funcionem em caso de falha de algum router, ambas as instâncias resolvem todos os subdomínios, devolvendo o IPs públicos deste Data Center. Com isso, todos os pedidos HTTP são feitos para este Data Center, onde são direcionados, utilizando o endereço IP privado dos servidores dos outros Data Centers, através de um reverse proxy. Este reverse proxy, disponibilizado através do servidor aplicacional Nginx, foi configurado nas máquinas que fornecem o serviço HAProxy, utilizando também a segurança de falha oferecida pelo HeartBeat.

II. Datacenter 2

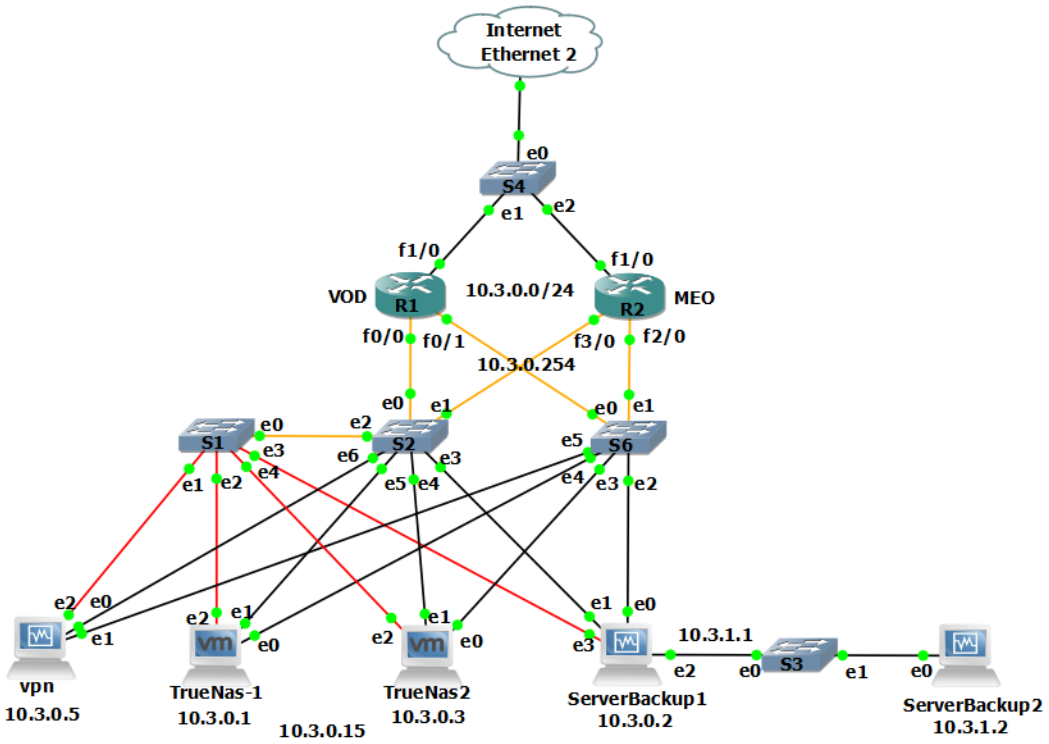


No "Datacenter 2", implementámos várias soluções fundamentais para a otimização da nossa infraestrutura de TI. Instalámos um servidor Windows Server que funciona simultaneamente como NAS e como plataforma de trabalho remoto através do Remote Desktop, oferecendo flexibilidade e acesso seguro aos nossos recursos. Este servidor permite o acesso à NAS pelo caminho de rede \\10.2.0.3\NAS_share e ao ambiente de Remote Desktop através do IP 10.2.0.3.

Configurámos também um cluster de servidores Web que suportam os protocolos HTTP e FTP, utilizando o IIS do Windows Server para uma gestão eficiente. O servidor Web está configurado para ser acedido através do endereço cpdijm.pt ou diretamente pelo IP 10.2.1.100. Os pedidos são distribuídos através de NAT entre o Server 1 e Server 2, assegurando um balanceamento de carga eficiente.

Adicionalmente, como um extra ao projeto, implementámos um servidor Linux equipado com o Zabbix, especificamente configurado para monitorizar continuamente todos os dispositivos na VLAN 100 dos nossos Datacenters. Esta implementação assegura uma vigilância constante sobre esta segmentação particular da nossa rede, garantindo a identificação precoce de qualquer anomalia e mantendo a máxima eficiência e segurança do ambiente monitorizado.

III. Datacenter 3



Foram implementadas soluções que permitem acesso remoto seguro dos clientes à NAS, sincronização de dados entre servidores, alta disponibilidade, e backup automatizado, conforme especificado.

Configuração da Nas:

-Foi utilizada a tecnologia ZFS com uma configuração RAID-Z1 em uma pool de armazenamento composta por três discos de 20GB cada. Essa configuração oferece redundância de dados, garantindo que o sistema continue funcional mesmo em caso de falha de um único disco, além de fornecer verificação contínua de integridade e correção automática de erros, protegendo os dados contra corrupção silenciosa.

-A tecnologia ZFS com uma configuração RAID-Z1 em uma pool de armazenamento composta por três discos de 20GB cada, garantindo redundância de dados e proteção contra falhas de um único disco.

- A sincronização entre dois servidores True NAS foi implementada usando o "rsync task" configurado com tarefas programadas, a partir de sincronização dos dados diariamente por meio de tarefas push (enviar) e pull (receber) configuradas no True Nas 2. Estas ligações são feitas por módulos ssh de chave publica.

-A alta disponibilidade, para garantir que o serviço continue disponível mesmo que um dos servidores fique indisponível, foi configurado um IP virtual (10.3.0.15) utilizando um mecanismo de Link Aggregation. Esse IP alterna entre os dois servidores NAS, garantindo que o serviço continue disponível mesmo que um dos servidores fique indisponível.

-Foi configurado uma pasta partilhada utilizando o protocolo Samba, garantindo que os clientes possam aceder os dados remotamente após conectarem-se à VPN.

Configuração da VPN:

-Para permitir acesso remoto seguro à NAS pelos clientes externos, foi configurado o serviço WireGuard devido ao seu desempenho elevado e gerenciamento simplificado.

-O servidor VPN foi configurado com a gama de IPs 10.8.0.0/24, sendo 10.8.0.1 atribuído ao servidor.

-O acesso externo ao servidor VPN foi configurado por meio de port forwarding nos routers dos provedores Vodafone e MEO no Datacenter 3: configurado para encaminhar conexões na porta 51820 do IP público para o IP interno do servidor VPN (10.3.0.5).

-Foi configurado no servidor WireGuard que os clientes externos terão acesso exclusivamente às seguintes redes internas 10.3.0.0/24, 10.2.0.0/24, 10.1.0.0/24, garantindo que somente o tráfego para essas redes será aceite via VPN.

Configuração de Backup Centralizado:

-O software BackupPC foi configurado no Servidor Backup 1 para gerenciar backups centralizados, garantindo alta eficiência no armazenamento por meio de duplicação de dados. O BackupPC foi configurado para utilizar o protocolo rsync em conjunto com comunicação via SSH autenticada por chaves públicas, assegurando uma transferência segura e confiável entre o servidor e os hosts de destino. Além disso, foram ajustados parâmetros de compressão e agendamento automático de backups incrementais e completos, otimizando o desempenho e minimizando o impacto na rede durante as operações de backup.

-Para os servidores Windows, o backup foi realizado a partir de uma pasta partilhada via Samba e cobian backup configurado para serem realizados diariamente backups incrementais.

-Foi criada uma sub-rede isolada entre os servidores Backup 1 e Backup 2 para proteger os backups secundários do acesso pela rede principal. Sendo estes feitos a partir de um script para fazer backup das pastas onde estão a ser guardados os backups do servidor de backups 1. São feitas a partir de rsync e sessão ssh utilizando chaves de autenticação.

3. Plano de endereçamento

Como rede pública, foram utilizados dois ISPs diferentes, o ISP MEO e o ISP Vodafone. Para a rede de cada operador foram utilizadas gamas de endereço IP reais de cada operador, ou seja, 62.28.0.0/16 para a rede da MEO e 193.109.93.0/24 para a rede da Vodafone. Para a rede dos Datacenters, foram utilizadas as gamas 10.X.0.0/16, sendo o X o número do Datacenter. Dentro de cada um, a sub-rede 10.X.0.0/24 foi utilizada como sub-rede principal, com a sub-rede 10.X.1.0/24 para redes secundárias. Por fim, a sub-rede 10.x.100.0/24, utilizada na VLAN 100, foi utilizada como rede de gestão e monitorização.

4. Desenvolvimento

Foi desenvolvido um script no Servidor Backups 2 com o objetivo de garantir uma cópia adicional dos dados mais importantes do cenário em uma rede segura. Esse script utiliza o rsync em conjunto com sessões SSH autenticadas por chave pública para aceder às pastas onde os backups estão a ser armazenados no Servidor Backups 1. Após a transferência, o script cria uma pasta no Servidor Backups 2 para armazenar a cópia dos dados. Para automatizar esse processo, o script foi configurado no cron, sendo executado diariamente às 1h05.

No Datacenter 1, nos servidores do serviço DNS, foram desenvolvidos scripts de execução das duas instâncias do serviço Bind9 e serviços para a execução desses scripts, para o início automático das instâncias ao iniciar os servidores.

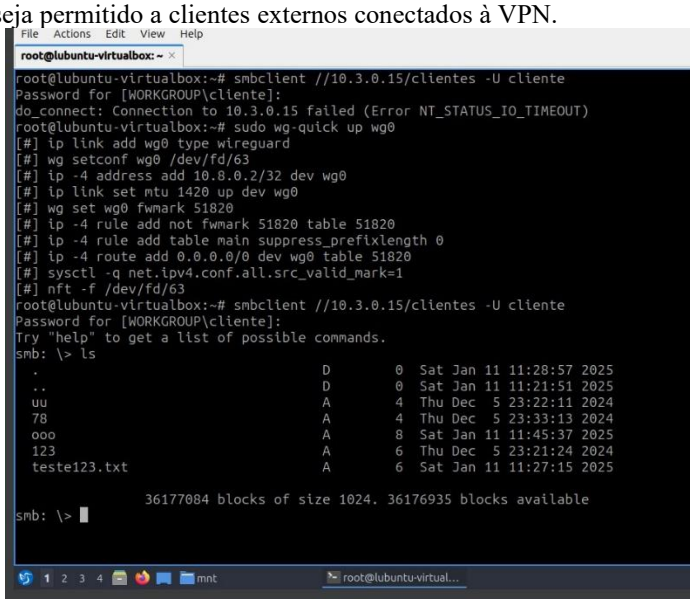
5. Atividade(s) extra

A atividade extra selecionada para o nosso projeto foi a implementação de uma solução de monitorização integrada, destinada a supervisionar todos os datacenters de forma contínua. A solução escolhida para esta tarefa foi o Zabbix. A explicação da instalação e implementação está no relatório em anexo.

6. Testes e resultados

- Acesso Remoto a Pasta Partilhada via Samba

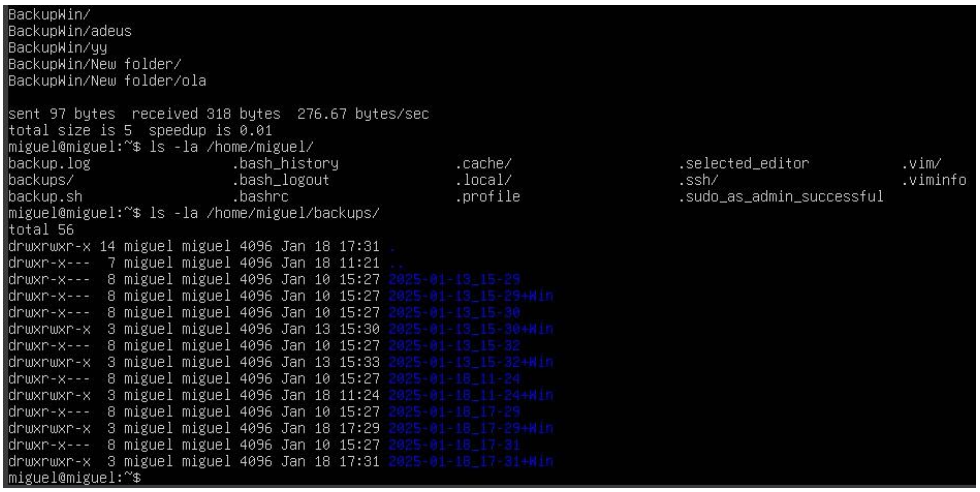
Objetivo:
Validar a segurança e a funcionalidade do acesso remoto às pastas partilhadas configuradas no servidor TrueNAS, garantindo que o acesso seja permitido a clientes externos conectados à VPN.



Análise: O acesso inicialmente foi corretamente negado, reforçando que a pasta partilhada não é acessível para clientes externos fora da rede interna protegida. Após a conexão com a VPN, o cliente conseguiu aceder a pasta partilhada sem problemas garantindo o correto funcionamento da VPN. O comando `smbclient` listou corretamente o conteúdo da pasta, confirmando que o acesso foi autenticado e permitido.

- Script do Servidor Backups 2

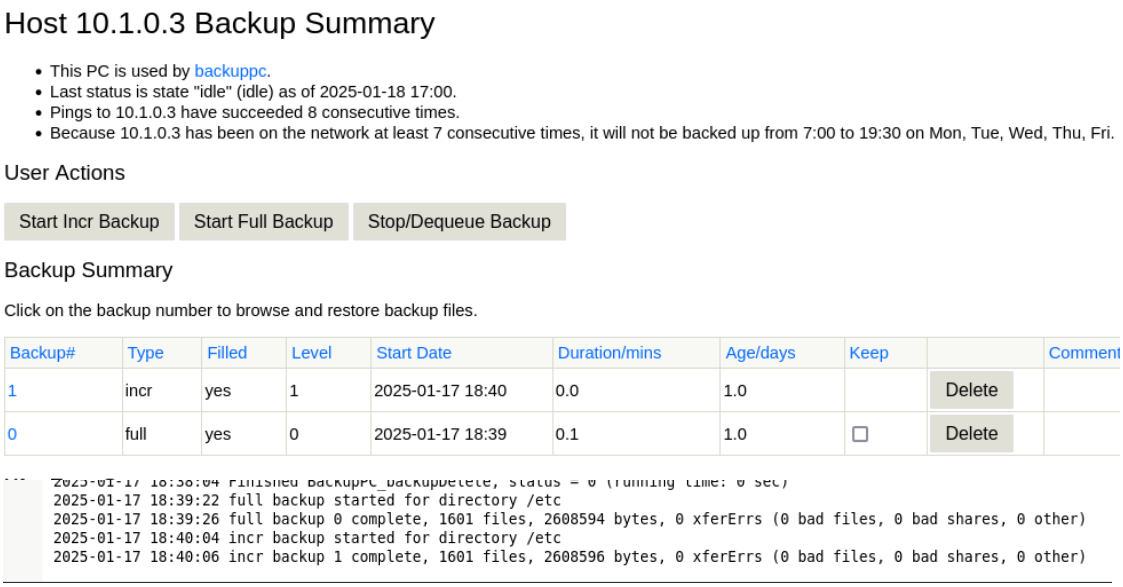
Objetivo: O objetivo deste teste é verificar o funcionamento do script backups.sh, garantindo que ele consiga acessar corretamente os backups armazenados no Servidor Backups 1 e criar, no Servidor Backups 2, novas pastas organizadas contendo os dados do Cobian e do BackupPC.



Análise: O script está a funcionar conforme o esperado, executando as tarefas de forma precisa e eficiente. Ele consegue acessar, através de rsync e SSH, todos os ficheiros armazenados nas pastas de backup do Servidor Backups 1. Além disso, realiza a separação dos dados em duas pastas distintas no Servidor Backups 2, uma destinada aos backups realizados pelo Cobian e outra para os gerados pelo BackupPC.

- Backuppc incremental e completo para Servidor no Dataset 1

Objetivo: Verificar o funcionamento do **BackupPC** para realizar backups de servidores no mesmo datacenter e em outros datacenters. Neste teste, foi avaliado especificamente o backup do servidor **10.1.0.3** localizado no **Datacenter 1**, com foco na pasta **/etc**.



Host 10.1.0.3 Backup Summary

- This PC is used by backuppc.
- Last status is state "idle" (idle) as of 2025-01-18 17:00.
- Pings to 10.1.0.3 have succeeded 8 consecutive times.
- Because 10.1.0.3 has been on the network at least 7 consecutive times, it will not be backed up from 7:00 to 19:30 on Mon, Tue, Wed, Thu, Fri.

User Actions

Start Incr Backup | Start Full Backup | Stop/Dequeue Backup

Backup Summary

Click on the backup number to browse and restore backup files.

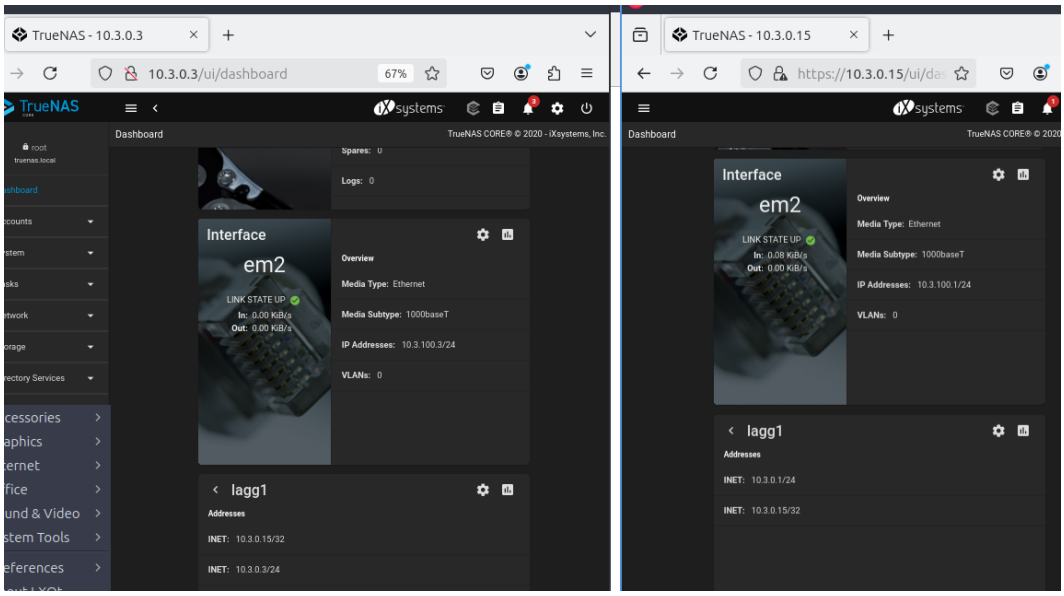
Backup#	Type	Filled	Level	Start Date	Duration/mins	Age/days	Keep		Comment
1	incr	yes	1	2025-01-17 18:40	0.0	1.0		Delete	
0	full	yes	0	2025-01-17 18:39	0.1	1.0	☐	Delete	

```
2025-01-17 18:38:04 Finished BackupPC_backupDelete, status = 0 (running time: 0 sec)
2025-01-17 18:39:22 full backup started for directory /etc
2025-01-17 18:39:26 full backup 0 complete, 1601 files, 2608594 bytes, 0 xferErrs (0 bad files, 0 bad shares, 0 other)
2025-01-17 18:40:04 incr backup started for directory /etc
2025-01-17 18:40:06 incr backup 1 complete, 1601 files, 2608596 bytes, 0 xferErrs (0 bad files, 0 bad shares, 0 other)
```

Análise: Com base na imagem acima, podemos confirmar que o BackupPC executou dois backups da pasta /etc do servidor 10.1.0.3: um backup completo e um backup incremental. Ambos os processos foram bem-sucedidos, indicando que a configuração do BackupPC e a comunicação entre o servidor de backup e o servidor remoto estão corretas.

- True NAS Link agragation

Objetivo: Acesso as true nas uma pelo link partilhado e outra pelo link normal. Sendo a com o link partilhado a primeira a ser ligada. Somente muda caso esta for abaixo.



Análise: Foi possível verificar que o acesso através do Link Aggregation foi realizado com sucesso, garantindo que o serviço permaneça disponível. Em caso de falha no servidor principal, o IP virtual é automaticamente transferido para o servidor secundário, assegurando a continuidade do acesso.

- VPN PEERS

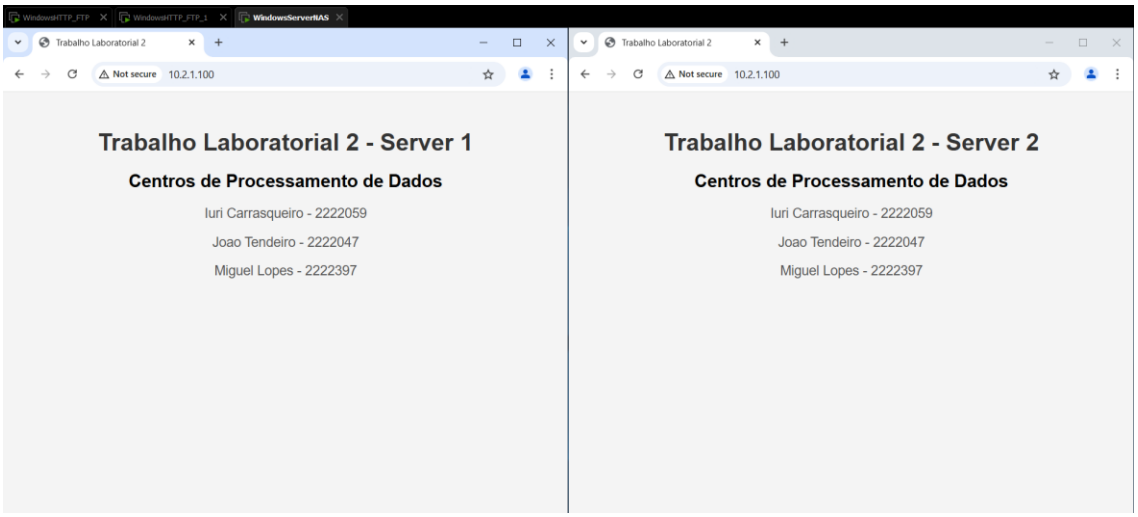
Objetivo: Verificação do acesso a vpn por um cliente externo.

```
miguel@miguel:~$ sudo more /etc/wireguard/wg0.conf
[sudo] password for miguel:
[Interface]
Address = 10.8.0.1/24
SaveConfig = true
PostUp = iptables -A FORWARD -i %1 -j ACCEPT
PostUp = iptables -A FORWARD -o %1 -j ACCEPT
PostUp = iptables -t nat -A POSTROUTING -o bond0 -j MASQUERADE
PostDown = iptables -D FORWARD -i %1 -j ACCEPT
PostDown = iptables -D FORWARD -o %1 -j ACCEPT
PostDown = iptables -t nat -D POSTROUTING -o bond0 -j MASQUERADE
ListenPort = 51820
PrivateKey = OOhIaWtloJ2aWwEedJgJer+XVa/VCy96nQs+yrmW0mo=

[Peer]
PublicKey = AuQ4jimpEs1y/B6Cm5UwC5UAiJp2Knc3EwQQnPB2dFQ=

[Peer]
PublicKey = AuQ4jimpEs1y/B6Cm5UwC5UAiJp2knc3EwQQnPB2dFQ=
AllowedIPs = 10.8.0.2/32
Endpoint = 10.3.2.2:42912

[Peer]
PublicKey = uqA6Dkue8ObRfOwN1NRrzBferiNJiM9NuYgy+ERZOG8=
AllowedIPs = 10.8.0.3/32
Endpoint = 193.109.93.100:34958
miguel@miguel:~$
```

Análise: Com a imagem acima podemos observar os peers criados para cada cliente e de onde veem.

- Acesso Web ao Cluster do Datacenter 2

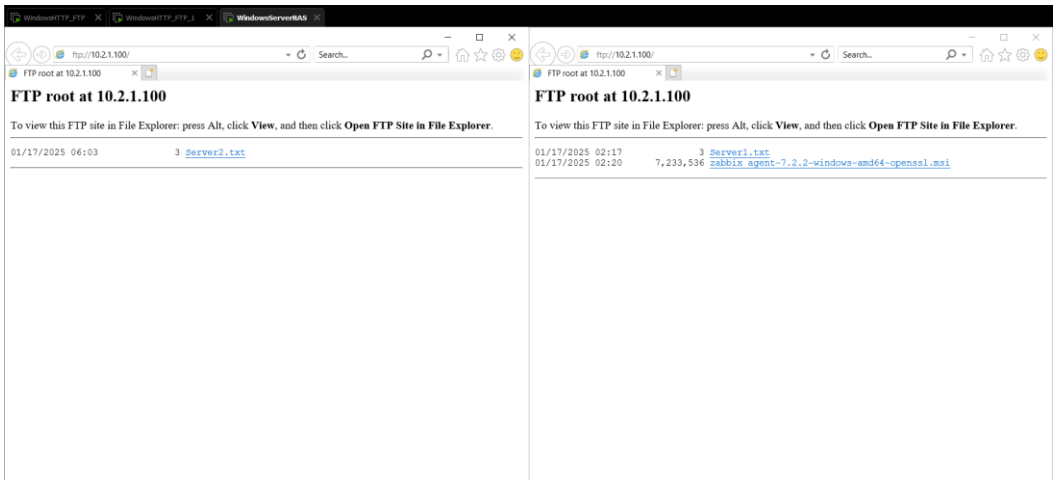
Objetivo: verificar a eficácia do sistema de balanceamento de carga NAT implementado, garantindo que as requisições ao mesmo endereço IP público fossem distribuídas de forma uniforme entre os dois servidores, Server 1 e Server 2.



Análise: Como se pode ver na imagem ao aceder ao mesmo endereço IP público, os resultados foram alternados entre o Server 1 e o Server 2. Este comportamento indica que o balanceamento através de NAT está a funcionar.

- Acesso FTP ao Cluster do Datacenter 2

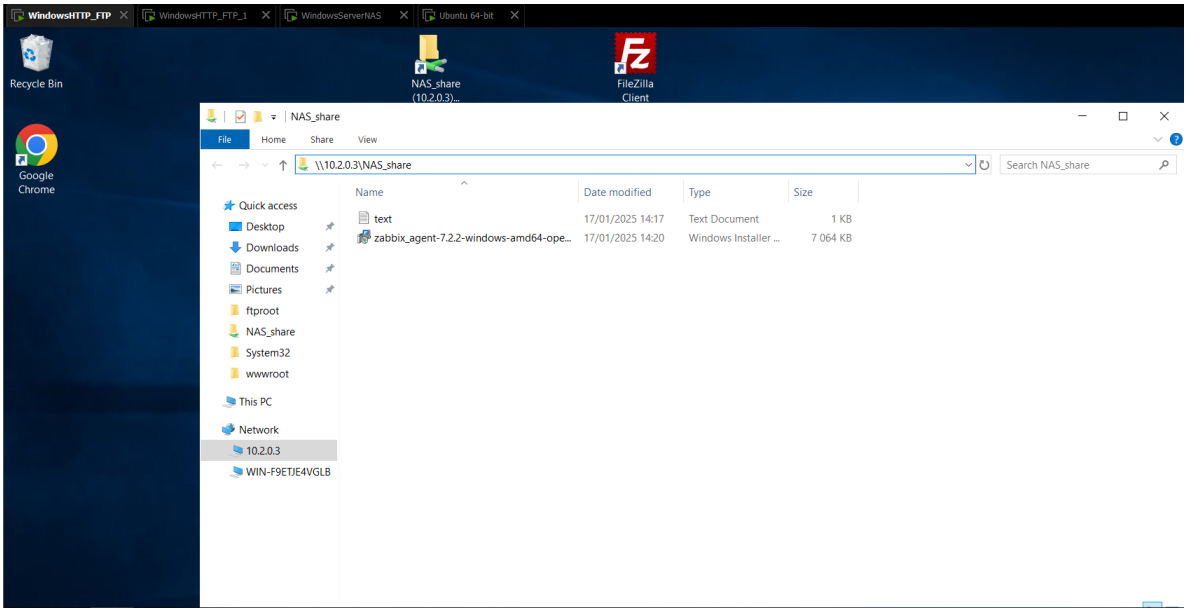
Objetivo: validar a configuração de balanceamento de carga NAT para o serviço FTP, garantindo que as conexões FTP ao mesmo endereço IP público fossem distribuídas de forma uniforme entre os dois servidores, Server 1 e Server 2.



Análise: Como se pode ver na imagem ao aceder ao mesmo endereço IP público, os resultados foram alternados entre o Server 1 e o Server 2. Este comportamento indica que o balanceamento através de NAT está a funcionar.

- Pasta partilhada do Datacenter 2

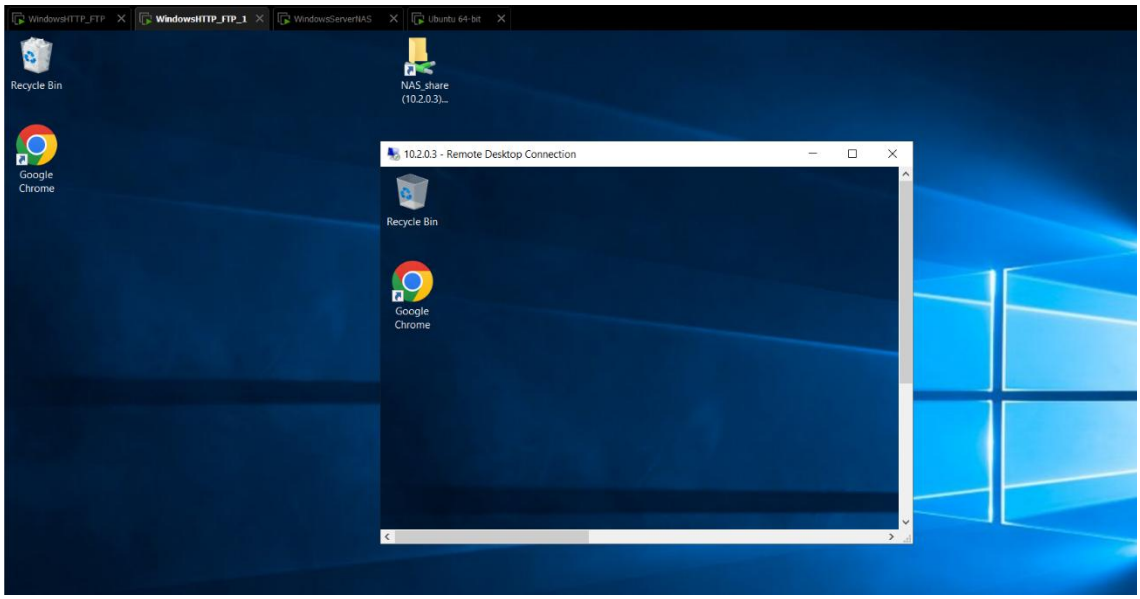
Objetivo: verificar a acessibilidade e funcionalidade da pasta partilhada NAS, configurada no endereço IP 10.2.0.3. O teste procurou confirmar que os arquivos e recursos partilhados estão acessíveis a partir de diferentes máquinas na rede, garantindo a eficiência na partilha de recursos.



Análise: O teste confirmou que a pasta NAS_share no servidor com IP 10.2.0.3 está corretamente configurada e acessível a partir de máquinas cliente na rede.

- Remote desktop do Datacenter 2

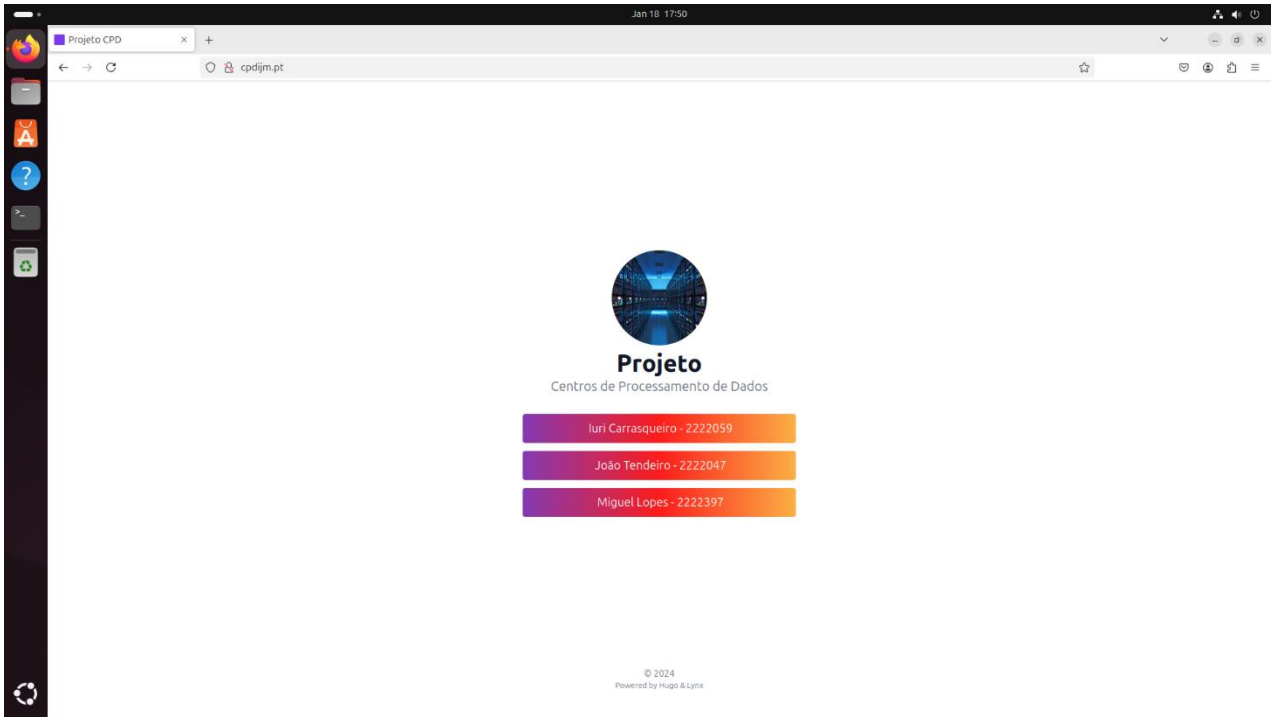
Objetivo: avaliar a funcionalidade e eficácia da conexão Remote Desktop para o IP 10.2.0.3. Procurou-se confirmar que é possível aceder e operar a máquina remota de forma eficaz a partir de outra estação de trabalho,

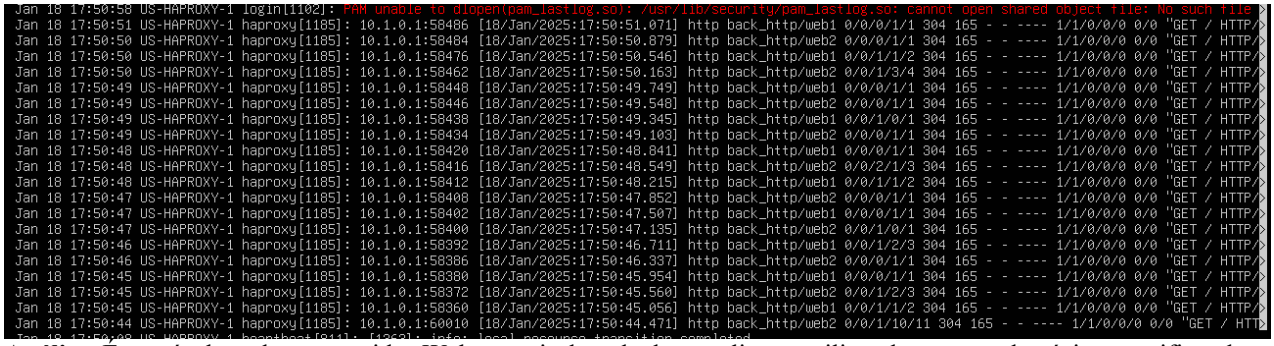


Análise: A imagem mostra a interface do cliente Remote Desktop com a conexão estabelecida ao servidor 10.2.0.3.

- Acesso Web ao Cluster do Datacenter 1

Objetivo: avaliar o acesso ao servidor web do Datacenter 1 e verificar o balanceamento de carga feito pelo HAProxy

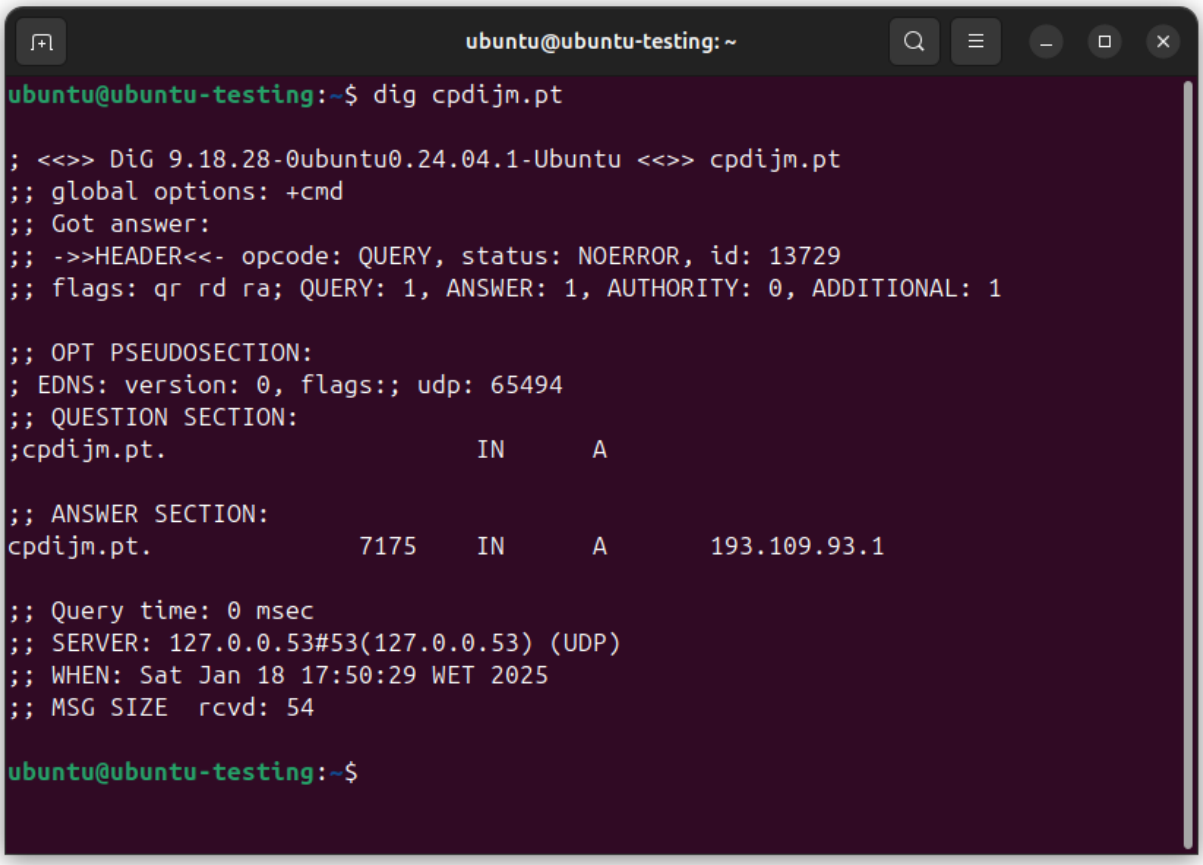




Análise: É possível aceder ao servidor Web a partir da rede de um cliente, utilizando o nosso domínio e, verificando o cluster HAProxy, podemos ver que a comunicação é balanceada através dos dois servidores Web.

- Acesso ao servidor DNS

Objetivo: Acesso ao servidor DNS a partir da rede de um cliente.



Análise: Utilizando a ferramenta dig, podemos verificar que a resolução de nomes do servidor de DNS, onde este devolve o IP público do Datacenter na rede do ISP Vodafone, uma vez que este é o único ponto de acesso ao Datacenter na realização deste teste.

7. Conclusões

Este trabalho laboratorial permitiu alcançar os objetivos estabelecidos, implementando uma topologia de rede empresarial robusta e eficiente. Durante o desenvolvimento do projeto, foram realizadas diversas configurações e testes que garantiram o funcionamento correto da infraestrutura, com ênfase na alta disponibilidade, balanceamento de carga e acesso remoto seguro.

Propostas de melhoria

-Otimização do Balanceamento de Carga:

Embora o balanceamento de carga entre os ISPs tenha sido implementado com sucesso, a adoção de protocolos de encaminhamento dinâmico, como o BGP, poderia oferecer uma maior flexibilidade e resiliência, especialmente em ambientes com múltiplos ISPs e redes mais complexas.

- Implementação de Serviços de Segurança

A inclusão de firewalls para a proteção e filtragem de tráfego, tanto na camada de rede quanto nas camadas de aplicação, seria uma melhoria importante para garantir a segurança da infraestrutura. Além disso, a implementação de sistemas de deteção e prevenção de intrusões.

Em resumo, o trabalho foi bem-sucedido em demonstrar e validar uma infraestrutura de rede empresarial resiliente e de alta disponibilidade, sendo os nossos objetivos para este trabalho alcançados. Embora os testes tenham sido concluídos com sucesso, a evolução contínua da infraestrutura proposta, aliada à implementação de melhorias sugeridas, pode levar a um sistema ainda mais robusto e escalável.