

# CENTROS DE PROCESSAMENTO DE DADOS

2020/2021

Daniel Valverde<sup>1</sup>, David Guilherme<sup>2</sup>, Gonalo Vicente<sup>3</sup>

<sup>1</sup> [2181831@my.ipleiria.pt](mailto:2181831@my.ipleiria.pt), Engenharia Informtica, Diurno

<sup>2</sup> [2171629@my.ipleiria.pt](mailto:2171629@my.ipleiria.pt), Engenharia Informtica, Diurno

<sup>3</sup> [2172131@my.ipleiria.pt](mailto:2172131@my.ipleiria.pt), Engenharia Informtica, Diurno

**Resumo:** O presente documento descreve os trabalhos desenvolvidos no mbito da unidade curricular Centros de Processamento de Dados pertence  licenciatura em Engenharia Informtica e descreve a configurao e administrao trs *Datacenters* configurados em trs mquinas distintas e uma rede a simular clientes numa outra mquina.

Para este trabalho foi utilizado o software GNS3 e VirtualBox, para a implementao de todos os cenrios. Os datacenter's esto interligados via dois ISP's (MEO e Vodafone) simulados por uma VPN disponibilizada pelos docentes, e existem ligaes dedicadas que permitem a comunicao direta entre Datacenters.

**Palavras-chave:** Datacenter, Virtualizao, Cloud, VPN, GNS3, VirtualBox, ISP.

## 1. Introduo inicial

Este projeto insere-se no mbito da unidade curricular Centro de Processamento de Dados e tem como finalidade descrever a soluo implementada para resolver o problema da empresa “CPD Hosting”. Foram traados objetivos com base nos que so referidos no enunciado, sendo estes:

- Endereamento e encaminhamento dinmico em IPv4;
- Instalao e configurao de servios fundamentais da rede de uma empresa, tais como DNS, HTTP, FTP e SMTP;
- Solues integrada de backups nos datacenters;
- Soluo de NAS com acesso remoto a filesystems;
- Solues de alta disponibilidade e balanceamento de carga nas camadas de rede e de aplicao;
- Aes de troubleshooting.

Para a soluo do problema foram seguidos os pressupostos ditados no enunciado, sendo estes:

- Todos os servios devero ter garantia de alta disponibilidade e sistemas de backup remotos de baixa complexidade de administrao. Todo o trfego dever ser balanceado da melhor forma possvel pelos trs datacenters;
- Os ISP podero ser implementados por apenas um router + um switch;
- O “Datacenter 1” dever ter um cluster de alta disponibilidade para o servio Web (HTTP);
- O “Datacenter 1” dever ter um cluster de alta disponibilidade para o servio de DNS;
- O “Datacenter 2” dever ter um servidor em Windows Server que funcione como NAS e como mquina de trabalho remoto (Remote Desktop);
- O “Datacenter 2” ter igualmente um cluster de servidores Web (HTTP e FTP), sendo os pedidos balanceados atravs de NAT;
- Os clientes devero ter acesso remoto a uma NAS existente no “Datacenter 3”, atravs de uma rede privada (VPN). A NAS est configurada com RAID, devendo assegurar mirror dos dados e sincronismo entre servidores; No “Datacenter 3” est configurada uma soluo de backups centralizados, que automatiza as operaes de backup dos servidores de todos os datacenters.

Considerando os objetivos traçados e os pressupostos pedidos, realizou-se um desenho de rede representativo do esquema de rede de cada um dos datacenters. A solução desenhada conta com quatro ambientes virtuais: três destes destinados a Datacenter's e um ambiente dedicado à simulação de clientes.

No Datacenter 1, disponibilizaram-se serviços HTTP, DNS, DHCP e NTP. Foram utilizadas duas máquinas para implementar um cluster de alta disponibilidade HTTP, e outras duas máquinas para implementar um cluster de alta disponibilidade com os serviços de DNS, DHCP e NTP. O Datacenter 1 conta também com uma máquina Windows destinada à manutenção e administração dos serviços.

No Datacenter 2, estão disponibilizados os serviços HTTP, FTP, NAS e Remote Desktop. Para o serviço HTTP foi implementado um cluster de alta disponibilidade com duas máquina e com recurso ao serviço HaProxy, serviço este que também foi configurado em um cluster com recurso ao heartbeat. Para o serviço FTP foi implementado um cluster de alta disponibilidade com duas máquinas e com recurso ao heartbeat. O Datacenter 2 conta também com um Windows Server que contém um serviço de NAS, que pode ser acedido pelos clientes, e também está disponível como máquina de ambiente trabalho remoto.

No Datacenter 3, está implementada uma solução que centraliza os backups de todos os datacenter's, para este propósito foram disponibilizadas duas máquinas, existe uma máquina dedicada a realizar os backups de todos os servidores dos datacenter's, e uma outra máquina que faz o backups dos dados presentes na máquina principal de backup's oferecendo assim uma solução de backup's à prova de ransomwares. Neste datacenter está também implementado um serviço de NAS em cluster implementado com o sistema operativo TrueNas configurada com RAID que assegura o mirror de dados e sincronismo entre servidores, de onde os clientes tem acesso através de servidor VPN também presente neste datacenter. A VPN foi implementada com recurso a uma máquina ubuntu e à framework OpenVpn que permite configurar servidores de vpn privados.

A nível de endereçamento de rede foram atribuídas as seguintes gamas de ip's por cada datacenter:

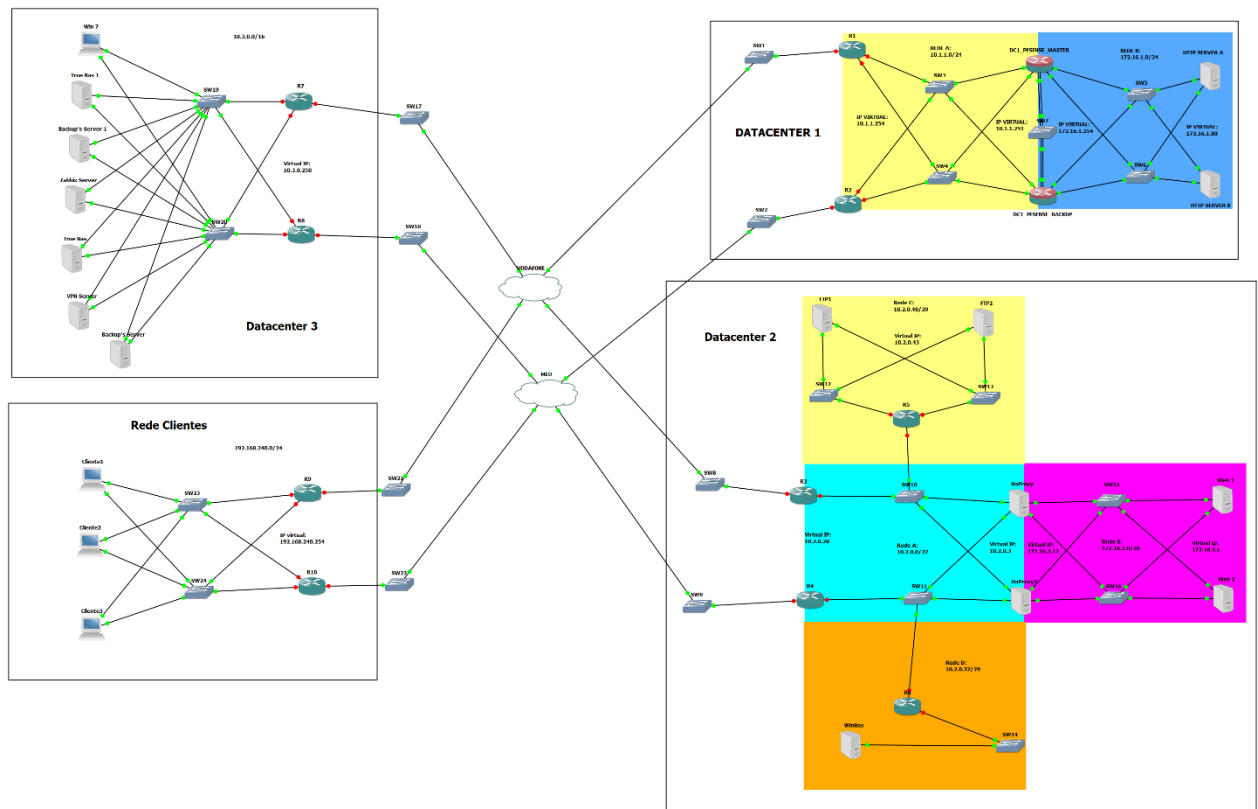
- 10.1.0.0/16 e 172.16.1.0/24 - Datacenter 1;
- 10.2.0.0/16 e 172.16.2.0/24 - Datacenter 2;
- 10.3.0.0/16 - Datacenter 3;

Sendo que o sub-endereçamento de cada datacenter ficou ao critério de cada administrador dos respectivos datacenter's.

Para o cenário simulador dos clientes utilizou-se uma unica gama de ip's: 192.168.240.0/24.

De seguida apresenta-se o diagrama geral da solução e posteriormente é apresentada a implementação dos serviços em cada datacenter.

## 2. Solução implementada



**Figura 1 - Cenário completo final implementado**

Na figura 1 é possível observar o cenário implementando sendo que cada datacenter corresponde aos ambientes virtuais implementados em máquinas físicas.

Estes ambientes virtuais serão interligados por meio de dois ISP's distintos: MEO e VODAFONE (simulados com router + switch). A comunicação entre cenários está assegurada através de uma VPN disponibilizada pelos docentes, e por encaminhamento via tuneis GRE.

No Datacenter 1 são disponibilizados serviços como: HTTP, DHCP, DNS e NTP. Estão assegurados dois Cluster's de Alta Disponibilidade, redundância e Load Balancing por intermédio das duas máquinas pfSense.

No Datacenter 2 são disponibilizados os seguintes serviços: HTTP, FTP, NAS e Remote Desktop. O Windows Server garante a funcionalidade de Remote Desktop e NAS para os clientes.

No Datacenter 3 são disponibilizados os serviços de: NAS, Backup's e Monitorização de Rede (máquina Zabbix). Está garantida uma VPN OpenVpn (máquina Vpn Server) para permitir o acesso através de rede privada aos servidores de NAS. É neste Datacenter que serão garantidos Backup's centralizados de todos os Datacenters.

No ambiente virtual dos clientes estão presentes máquinas a simular clientes para os vários serviços disponibilizados.

### 3 - Datacenter 1

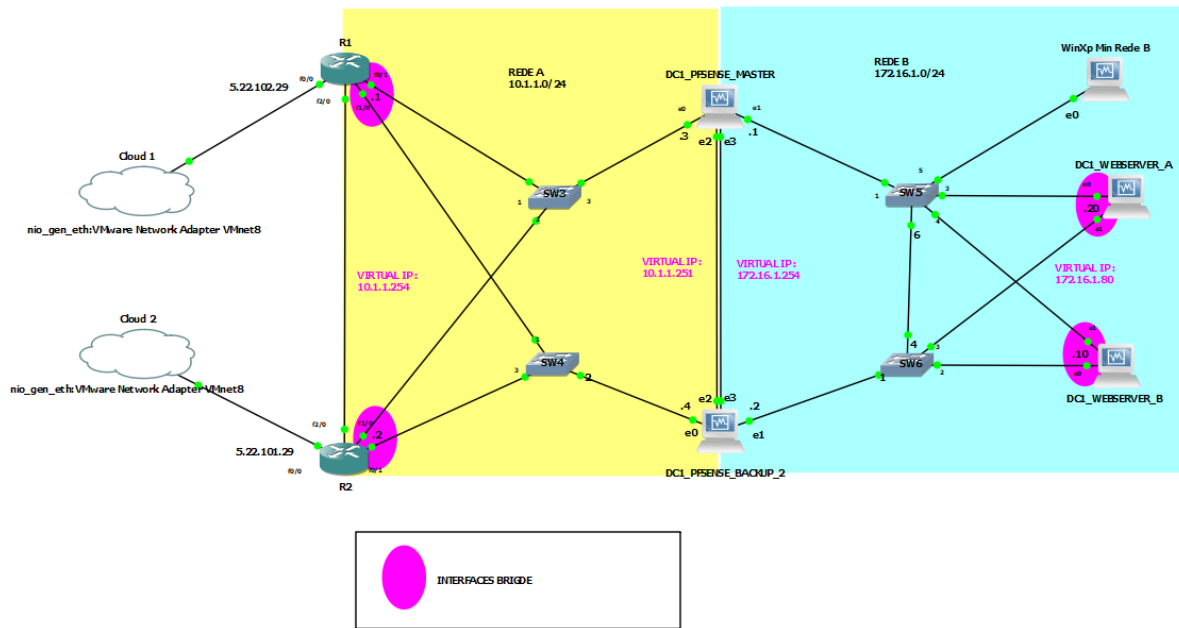


Figura 2 - Cenário Datacenter 1

No Datacenter 1 encontram-se presentes os serviços HTTP, DNS, DHCP e NTP, sendo que o serviço HTTP está implementado como um cluster de alta disponibilidade com recurso a dois servidores Ubuntu, e os restantes serviços estão também implementados em um cluster de alta disponibilidade, com recurso a duas máquinas Pfsense.

Para além dos serviços implementados todos os dispositivos de rede estão configurados e conectados de forma a oferecerem soluções de redundância e balanceamento de carga.

De seguida é apresentada a abordagem de implementação a cada um dos serviços referidos.

#### 3.1 – Cluster de Alta Disponibilidade para o Serviço HTTP

Este cluster foi implementado com duas máquinas (dc1\_webserver\_a e dc1\_webserver\_b), com o Ubuntu Server 14.04 e com recurso ao heartbeat. Por defeito a máquina DC1\_WEBSERVER\_A é a máquina principal onde o serviço deverá estar ativo através do IP virtual 172.16.1.80, caso esta máquina falhe, o heartbeat irá atribuir o IP virtual à máquina DC1\_WEBSERVER\_B e desta forma o serviço ficará ativo na máquina secundária através do mesmo IP (172.16.1.80), até que a máquina principal volte à normalidade. Para o serviço HTTP foi utilizado o servidor apache2 em cada uma das máquinas, com configurações iguais.

A nível de redundância de rede, cada servidor tem configurada uma interface virtual bridge que agrega duas interfaces interligadas cada uma a switch's de rede distintos, permitindo assim que o tráfego possa ser balanceado pelas duas interfaces físicas. Na figura 2 pode-se observar a interface bridge do servidor DC1\_WEBSERVER\_A bem como o IP virtual que lhe está atribuído.

```
# This file describes the network interface
# and how to activate them. For more
#
# The loopback network interface
auto lo
iface lo inet loopback
#
# The primary network interface
#auto eth2
#iface eth2 inet dhcp
auto br0
iface br0 inet static
address 172.16.1.20
netmask 255.255.255.0
gateway 172.16.1.254
dns-nameserver 172.16.1.254
bridge_ports eth0 eth1
bridge_stp on
bridge_maxwait 0
```

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 state UP group default qlen 1000
    link/ether 08:00:27:20:0c:73 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master br0 state UP group default qlen 1000
    link/ether 08:00:27:cf:84:a1 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a00:27ff:fe2f:84a1/64 scope link
        valid_lft forever preferred_lft forever
4: eth2: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 08:00:27:c2:32:06 brd ff:ff:ff:ff:ff:ff
5: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    inet 172.16.1.20/24 brd 172.16.1.255 scope global br0
        valid_lft forever preferred_lft forever
    inet 172.16.1.80/24 brd 172.16.1.255 scope global secondary br0:0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe20:c73/64 scope link
        valid_lft forever preferred_lft forever
```

```

GNU nano 2.2.6                               File: /etc/ha.d/haresources
dc1webservera 172.16.1.80/24/br0 apache2

```

Figura 4 - Configuração do Ip virtual

### 3.2 - Cluster de Alta Disponibilidade para o serviço DNS, DHCP e NTP

O cluster de alta disponibilidade para o serviço DNS, DHCP e NTP foi implementado com recurso a duas máquinas pfsense. A pfsense é um sistema operativo baseado em FreeBSD e é um software de firewall e roteamento, que permite também configurar serviços como DNS, DHCP, NTP, VPN, etc.

A pfsense permite o funcionamento em cluster através de um recurso próprio denominado de “High Availability Sync”. Este recurso permite que as pfsenses sincronizem as suas configurações constantemente e desta forma garantir um serviço de alta disponibilidade. Para que isto seja possível as duas máquinas precisam de estar diretamente ligadas para que aconteça a sincronização quase instantânea das configurações, para isto ser possível foi configurado um link com recurso a um link aggregation em FailOver entre as duas pfsense’s, dedicado à sincronização entre ambas.

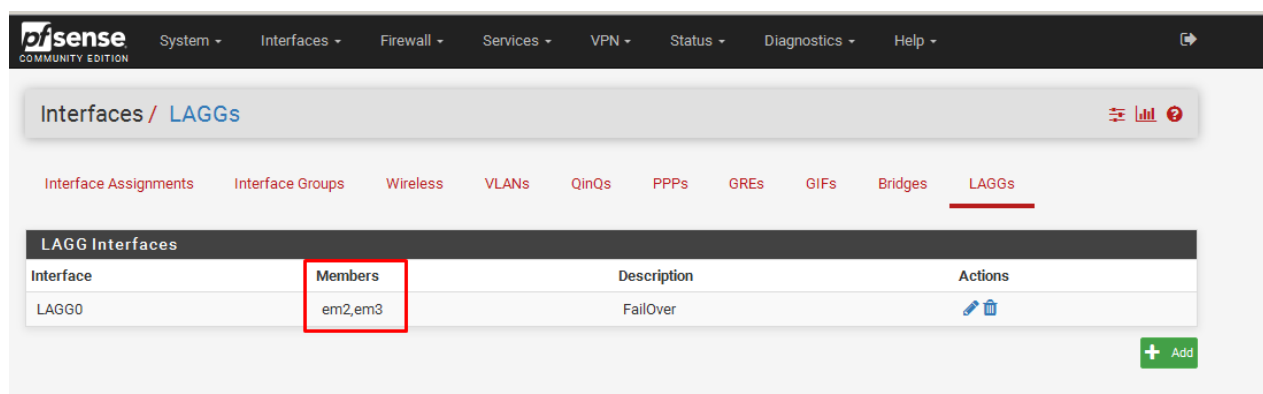


Figura 5 - Configuração do Link Agregation Pfsense

De forma a configurar as duas pfsense’s como um cluster de alta disponibilidade, para além do serviço “High Availability Sync” foram também configurados IP’s virtuais em modo CARP (failover), que permitem que o acesso aos serviços presentes na pfsense sejam sempre acedidos seja qual for a máquina pfsense que está de “pé”. A máquina pfsense\_Master tem por defeito os IP’s virtuais atribuídos e caso esta máquina falhe, os ip’s ficam ativos na máquina pfsense\_Backup mantendo os serviços acessíveis através do mesmo ip.

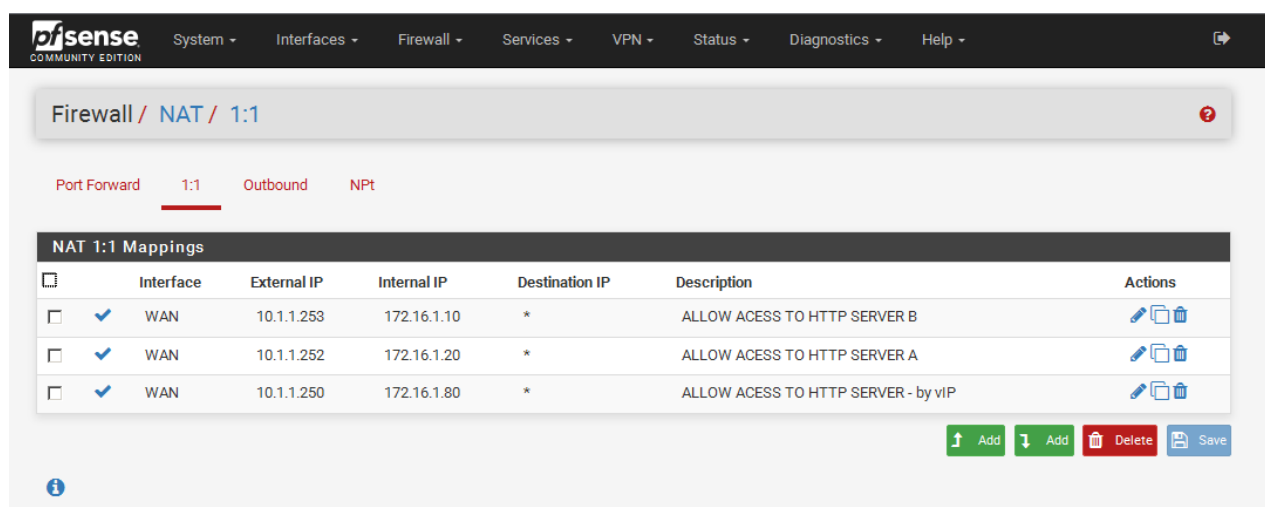
CARP Status		
CARP Interface	IP Address	Status
WAN@1	10.1.1.250	MASTER
LAN@2	172.16.1.254	MASTER
WAN@3	10.1.1.252	MASTER
WAN@4	10.1.1.253	MASTER
WAN@5	10.1.1.251	MASTER

Figura 6 - IP's virtuais

Na figura 7 é possível verificar os ip's virtuais configurados, existem 5 ip's virtuais com finalidades distintas.

- 10.1.1.250 – Ip virtual mapeado por NAT para acesso ao cluster HTTP;
- 172.16.1.254 – Ip virtual para acesso ao serviço DHCP da interface LAN;
- 10.1.1.252 – Ip virtual mapeado por NAT para acesso ao servidor HTTP\_A (utilizado pelo servidor de backups do dc3);
- 10.1.1.253 – Ip virtual mapeado por NAT para acesso ao servidor HTTP\_B (utilizado pelo servidor de backups do dc3);
- 10.1.1.251 – Ip virtual para acesso ao serviço DNS e NTP através da interface WAN;

Foi configurado o balanceamento por NAT para acesso aos servidores através do ip's virtuais configurados para o efeito. Este é um procedimento mandatório, pois a pfsense funciona como um router firewall que protege o acesso à rede dos servidores através de redes externas.



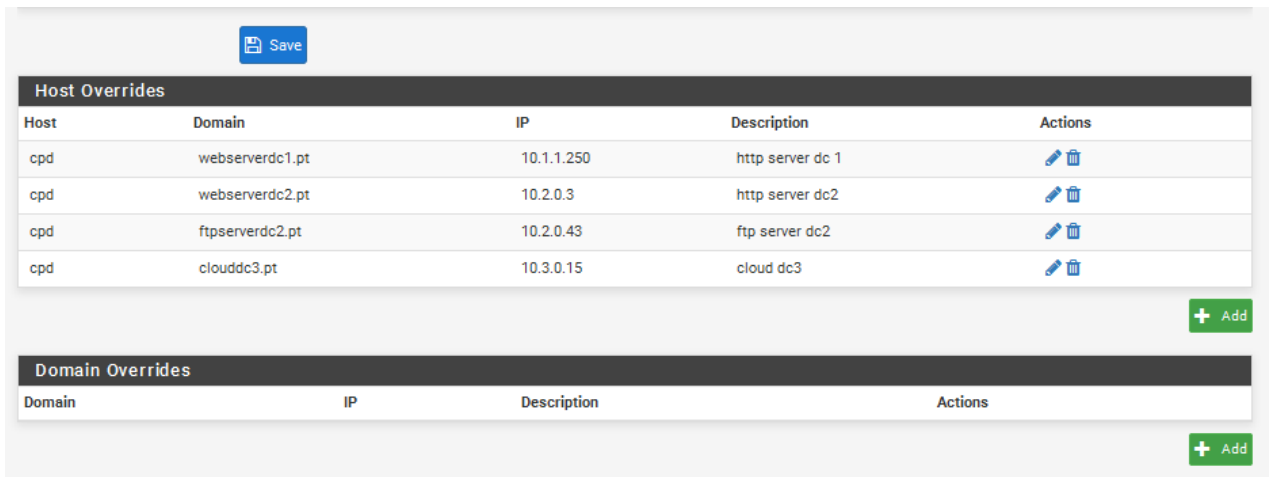
NAT 1:1 Mappings						
	Interface	External IP	Internal IP	Destination IP	Description	Actions
<input type="checkbox"/>	✓ WAN	10.1.1.253	172.16.1.10	*	ALLOW ACCESS TO HTTP SERVER B	
<input type="checkbox"/>	✓ WAN	10.1.1.252	172.16.1.20	*	ALLOW ACCESS TO HTTP SERVER A	
<input type="checkbox"/>	✓ WAN	10.1.1.250	172.16.1.80	*	ALLOW ACCESS TO HTTP SERVER - by VIP	

Figura 7 - Mapeamentos nat configurados









O serviço DNS foi implementado com o recurso ao serviço “DNS fowarder”, que funciona como um servidor que redireciona os pedidos para um servidor de DNS remoto, que neste caso foi utilizado o servidor de DNS da google 8.8.8.8, contudo é possível configurar entradas de DNS que sobrepõem possíveis entradas que possam existir no servidor remote. Desta forma é possível atribuir domínios para os serviços presentes nos datacenter's desenvolvidos e também bloquear o acesso a alguns recursos caso isso seja necessário.

O serviço de DHCP está implementado na rede interna do Datacenter 1 (172.16.1.0/24) e é através da máquina WinXp que pode ser testar visto que esta máquina não é responsável por assumir um serviço. A pool de endereços a atribuir dinamicamente é a seguinte: 172.16.1.115 até 172.16.1.190. Por intermédio do DHCP, são passados dois

endereços de servidores DNS, dois endereços de servidores NTP, o IP a atribuir à máquina que se liga (compreendido na pool) e o endereço de gateway definido para a rede (172.16.1.254 – IP Virtual da pfSense).



The screenshot displays the pfSense DNS server configuration page. At the top left is a blue 'Save' button. Below it is the 'Host Overrides' section, which contains a table with the following data:

Host	Domain	IP	Description	Actions
cpd	webserverdc1.pt	10.1.1.250	http server dc 1	 
cpd	webserverdc2.pt	10.2.0.3	http server dc2	 
cpd	ftpserverdc2.pt	10.2.0.43	ftp server dc2	 
cpd	clouddc3.pt	10.3.0.15	cloud dc3	 

Below the Host Overrides table is a green '+ Add' button. Underneath is the 'Domain Overrides' section, which has a table with the following structure:

Domain	IP	Description	Actions
--------	----	-------------	---------

Below the Domain Overrides table is another green '+ Add' button.

Figura 8 - Domínios configurados DNS server

### 3.3 – Configuração de backup's remotos

Para salvar as configurações dos servidores web configurados, os servidores enviam Backup's das configurações para o servidor de backup's implementado no Datacenter 3. A implementação foi realizada através de um script (figura 3) que foi configurado para executar de forma automática através do crontab (figura 11).

No crontab foram configuradas instruções que centralizam os dados a fazer backup numa única pasta (/Pasta Backups) e instruções para executar o script (backupTOTAL.sh) localizado na pasta /home/\$user dos servidores.

O script desenvolvido está responsável por criar um ficheiro comprimido (.tgz) com todos os dados que estão contidos na pasta onde são centralizados os dados, e enviar esse ficheiro para o servidor de backup's remoto implementado no Datacenter 3 (10.3.0.10) através de ssh. Para isto ser possível foram configuradas chaves ssh em cada máquina e foram partilhadas com a máquina de backup's remotos de forma a que a conexão ssh possa ser executada automaticamente, sem a introdução de palavras-passe. Nas figuras seguintes é possível visualizar o conteúdo do script desenvolvido bem como o ficheiro crontab que contém as instruções de execução e sincronização de dados.

```
#!/bin/bash
#####
#
# Backup de ficheiros.
#
#####
# Pastas e Ficheiros para fazer Backup (Separedo por espaços).
backup_files="/PastaBackup"
#Destinos do Backup
dest2="/BCK_local"
# Nome para o ficheiro de Backup.
daySemana=$(date +%A)
dayDia=$(date +%F)
dayHoras=$(date +%R)
hostname=$(hostname -s)
fileName="TOTAL-$hostname-$daySemana-$dayDia_$dayHoras.tar.gz"
# MENSAGEM: Inicio de Backup.
echo "A INICIAR: Backup de: $backup_files"
#date
#echo
logger -i -s -p info -t 'Backup' "Inicio do Backup!"
#Criação do Ficheiro TAR e envio por SSH para outra máquina.
tar -cvpz $backup_files | ssh ubuntu@10.3.0.10 "(cat > /home/ubuntu/Backups/HttpServer/$fileName.tar.gz)"
#Criação do Ficheiro TAR para Armazenamento Externo.
tar -czvf $dest2/$fileName $backup_files
# MANSAGEM: Fim de Backup.
#echo
#echo "Backup terminado com sucesso"
#echo "Realizado a:"
#date
logger -i -s -p info -t 'Backup' "Backup executado com sucesso!"
```

Figura 9 - Script utilizado para a os backups remotos

```
GNU nano 2.2.6 File: /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab`
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron !& ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron !& ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron !& ( cd / && run-parts --report /etc/cron.monthly )
#
0,15,30,45 * * * * ubuntu /home/ubuntu/backupTOTAL.sh
14,29,44,59 * * * * root rsync -zarvh /home/ubuntu /PastaBackup
14,29,44,59 * * * * root rsync -zarvh /etc/ha.d /PastaBackup
14,29,44,59 * * * * root rsync -zarvh /etc/network /PastaBackup
14,29,44,59 * * * * root rsync -zarvh /var/www/html /PastaBackup
```

Figura 10 - Crontab dos servidores Web

Para efectuar os backup's das máquinas pfSense foi utilizado um processo similar. Os backups são também efectuados através de ssh, contudo é a máquina remota que tem o papel de se ligar via ssh automaticamente e copiar os ficheiros de configuração. Para isto ser possível foi gerada uma chave ssh na máquina remota e esta foi adicionada nas máquinas pfSense para que estas permitam a conexão sem palavra passe (figura 5). Através da interface gráfica pfSense efectuaram-se os seguintes passos : System -> User Management -> edit user admin -> authorized ssh keys.

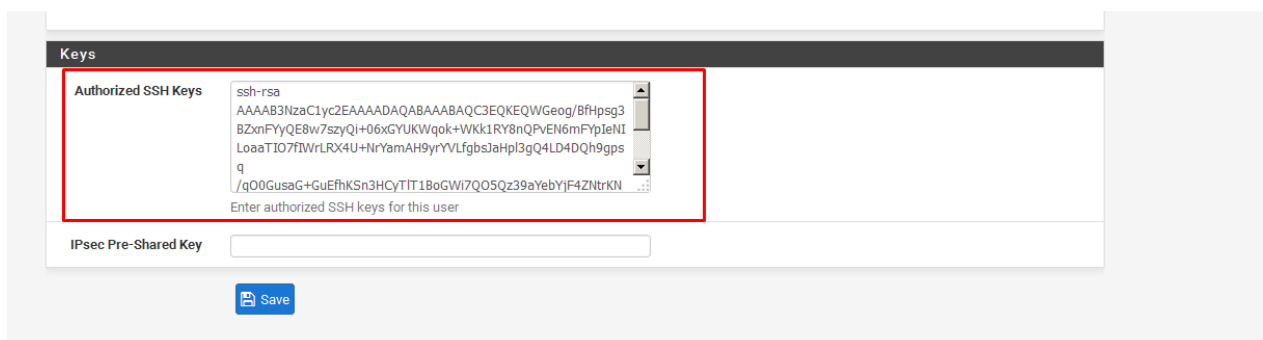


Figura 11 - Chave ssh autorizada na PfSense



Na maquina de backup's do datacenter 3 foi adicionada uma intrução no crontab que executa o seguinte commando “ssh admin@10.1.1.4 cat /cf/conf/config.xml > /backups/backup.xml”, sendo que as configurações da pfsense ficam presentes no ficheiro “backups.xml” e é possível recuperar o estado das pfsense através desse mesmo ficheiro.

### 3.4 – Configuração de redundância, balanceamento de carga na camada de rede, e comunicação entre datacenters.

Os Router's de entrada no Datacenter estão configurados com 3 tuneis GRE (figura 15) que permitem a conexão direta com os restantes Datacenters e cenário de clientes. A comunicação entre cenários é assegurada desta forma.

A nível de redundância de rede balanceamento de carga, ambos os routers estão configurados com interfaces Bridge e IP'S virtuais de forma a garantir que todas as máquinas presentes no cenário obtenham sempre um *gateway* disponível através do IP virtual 10.1.1.254. Nas figuras 4, 5 e 6 é possível visualizar as configurações efetuadas nos routers entrada do *DataCenter*. Na figura 6 é possível ver as configurações dos tuneis configurados, estes conseguem assegurar a comunicação entre cenários, através da VPN disponibilizada pelos docentes para a realização do projeto.

```
Bridge Group 1 is running the IEEE compatible Spanning Tree protocol
    Port 5 (FastEthernet0/1) of bridge group 1 is forwarding
    Port 6 (FastEthernet1/0) of bridge group 1 is forwarding
R1#
```

Figura 12 - Verificação configuração bridge

```
R1#sh standby brief
          P indicates configured to preempt.
Interface Grp Pri P State Active Standby Virtual IP
BV1       1   90  P Active local  10.1.1.2  10.1.1.254
R1#
```

Figura 13 - Verificação de configuração virtual IP

```
interface Tunnel1
ip address 11.11.11.6 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 5.22.102.29
tunnel destination 5.22.111.29
!
interface Tunnel2
ip address 11.11.11.13 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 5.22.102.29
tunnel destination 5.22.102.30
!
interface Tunnel3
ip address 11.11.11.22 255.255.255.252
ip mtu 1400
ip tcp adjust-mss 1360
tunnel source 5.22.102.29
tunnel destination 5.22.102.40
!
```

Figura 14 - Configurações dos tuneis para comunicação entre cenários

## 4. Datacenter 2

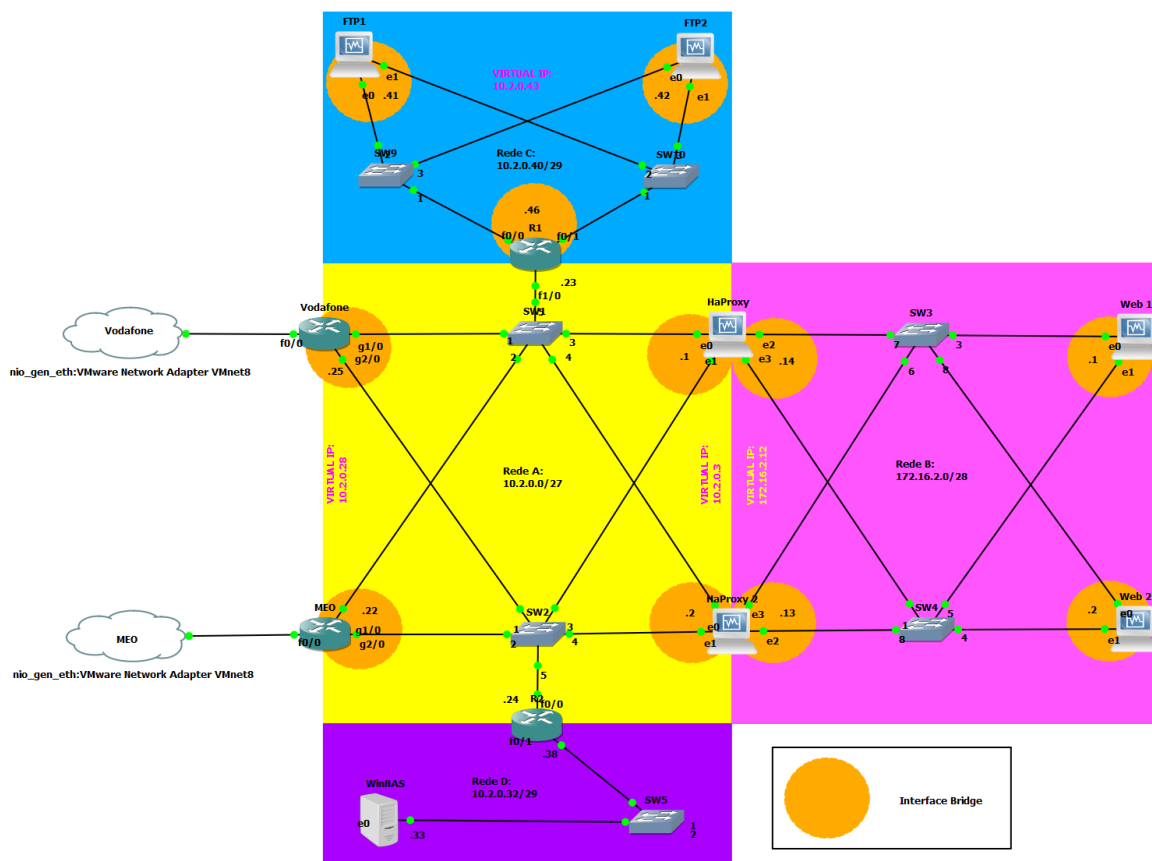


Figura 15 - Cenário Datacenter 2

Este Datacenter é composto por vários servidores, e são eles:

- Windows Server, um servidor com a função de NAS e ambiente de trabalho remoto;
- Ubuntu Server's, dois com servidores WEB, dois com os serviços Haproxy e Heartbeat, e dois com servidores FTP e o serviço Heartbeat.

Os pedidos HTTP feitos a este Datacenter são balanceados pelo Haproxy, os routers principais do Datacenter enviam o pedido para os HAproxy's no porto 80 os quais vão fazer o balanceamento e enviar esse pedido para um dos servidores WEB.

Os servidores FTP estão inseridos noutra cluster de alta disponibilidade, onde o balanceamento é feito pelo Heartbeat.

Os servidores estão a fazer backups locais, e a enviar Backups para o servidor de backups do Datacenter 3.

### 4.1 – Soluções de alta disponibilidades e redundância

Foram configurados três clusters de alta disponibilidade, dois nos servidores Haproxy's, outro nos servidores FTP, o que vai garantir que qualquer pedido HTTP seja sempre respondido visto que se o servidor principal falhar o segundo toma o seu lugar, o mesmo acontece para os servidores FTP, estas soluções foram configuradas usando o serviço Heartbeat, onde tivemos de dar a conhecer cada servidor do cluster, definir qual deles iria ser o servidor principal e definir um IP virtual, o IP do cluster.

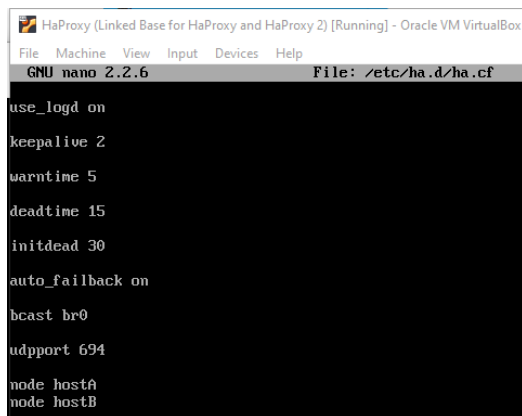


Figura 16 - Ficheiro /etc/ha.d/ha.cf referente ao Heartbeat

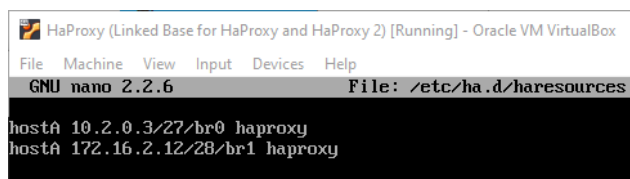


Figura 17 - Ficheiro /etc/ha.d/haresources referente ao Heartbeat

Quanto à redundância, nos servidores WEB, FTP e Haproxy configuramos uma interface bridge, e a estas estão associadas duas interfaces existentes, por exemplo, eth0 e eth1. Desta forma conseguimos assegurar que se um dos cabos switches ou routers falhar o outro estará lá para o substituir sem comprometer o serviço.

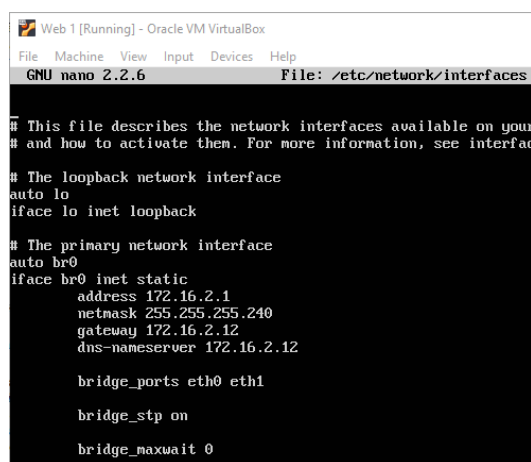


Figura 18 - Interface bridge no servidor WEB1

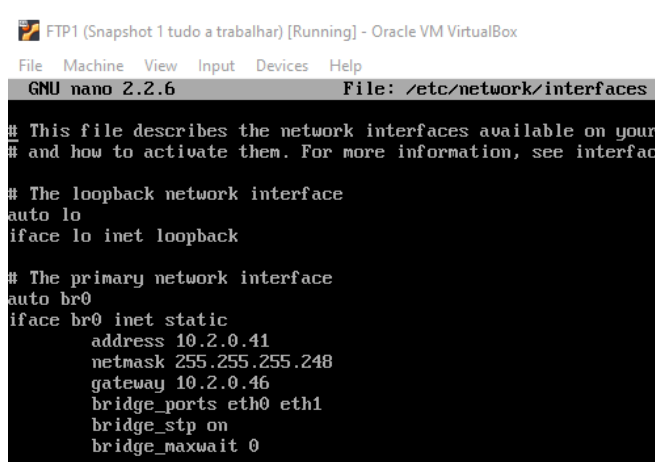


Figura 19 - Interface bridge no servidor FTP1

## 4.2 Windows server como NAS e Remote Desktop

A NAS no windows server foi criada através da criação de pastas partilhadas, com o propósito de cada cliente ter a sua pasta e criamos utilizadores para os respetivos clientes.

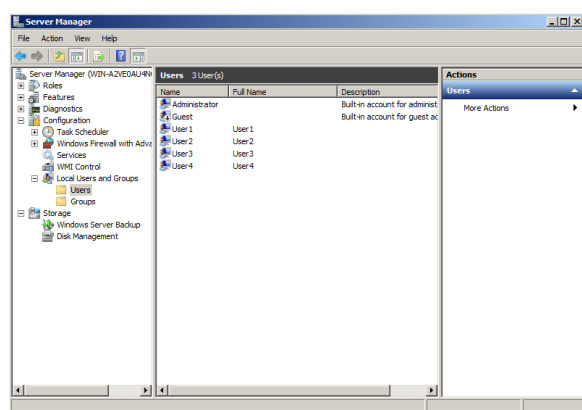


Figura 20 - Criação de utilizadores

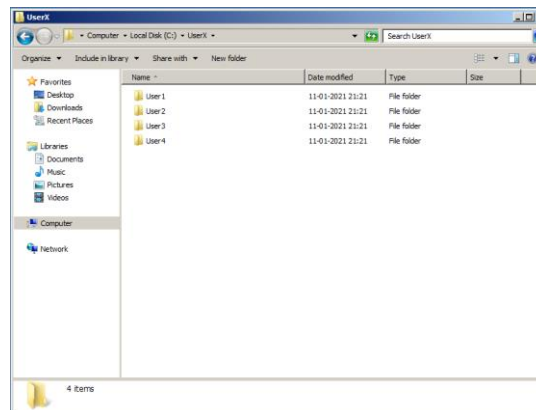


Figura 21 - Criação das pastas dos utilizadores

No caso do Remote Desktop, foi necessário permitir conexões remotas para esta máquina, somente quem terá acesso será o administrador, pois visto ser um servidor que poderá conter dados sensíveis de utilizadores não fazia sentido os utilizadores terem acesso ao servidor pois dessa forma poderiam aceder a todos os dados, por isso achamos mais correto só o administrador ter acesso ao servidor.

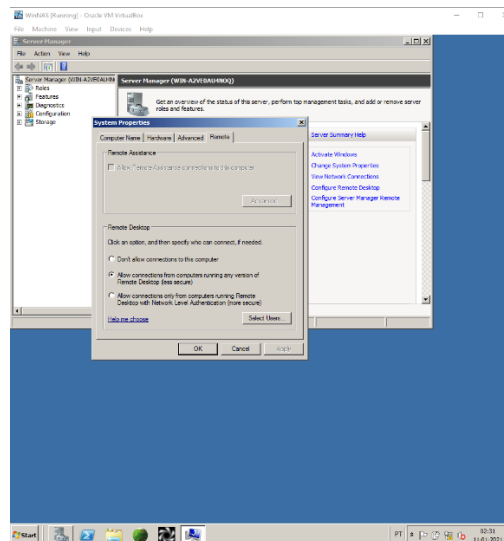


Figura 22 - Permitir o remote desktop

### 4.3 - Configuração Backups Remotos

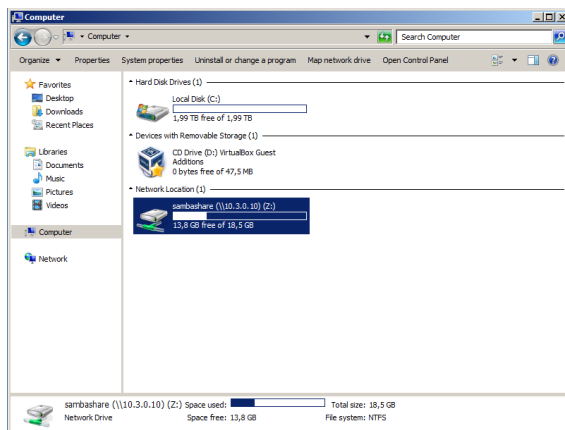
Para garantir a redundância e segurança de todos dados críticos e configurações dos servidores, todos os servidores enviam Backup's para um servidor alojado no Datacenter 3. Para os servidores com o sistema operativo Ubuntu Server são feitos Backups através de um Script e configurações no ficheiro crontab.

No crontab (Figura 10) existem dois tipos de instruções distintas: um conjunto de linhas que centraliza todas as pastas e ficheiros numa única pasta (/PastaBackup) que são executadas ao minuto 14, 29, 44 e 59 de todas as horas de todos os dias e uma linha que executa o Script "backupTotal.sh" (Figura 9) no minuto 0, 15, 30 e 45 de todas as horas de todos os dias.

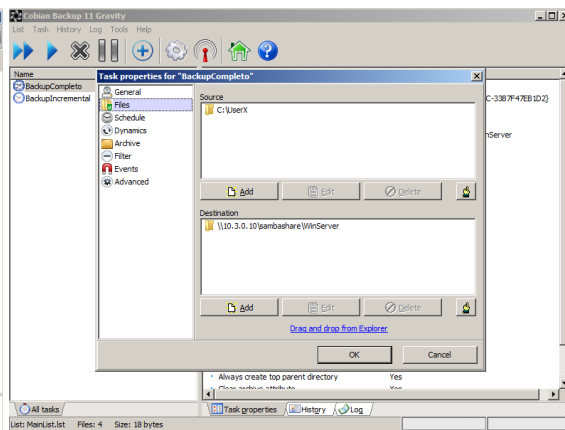
O Script é responsável por fazer um .zip da pasta onde está contida a informação a realizar Backup (/PastaBackup), guardar localmente e enviar, via SSH, para a pasta "Backups" localizada na máquina responsável por centralizar todos os Backup's do projeto. Por sua vez, cada máquina tem uma pasta com o seu nome dentro da pasta "Backups" para melhor controlo dos dados. Para possibilitar o envio dos Backup's via SSH, em cada máquina foi gerada uma chave e esta foi partilhada com o servidor de Backup's através dos seguintes comandos: "ssh-keygen -t rsa" e "ssh-copy-id ubuntu@10.3.0.10".

Nos servidores FTP foi instalado o serviço unison que nos permite fazer a sincronização de ficheiros entre ambos os servidores, com o auxílio de um cronjob os servidores estão a sincronizar a pasta /home/ubuntu/Files de dois em dois minutos para garantir que na falha do servidor principal os dados estão garantidos no servidor secundario.

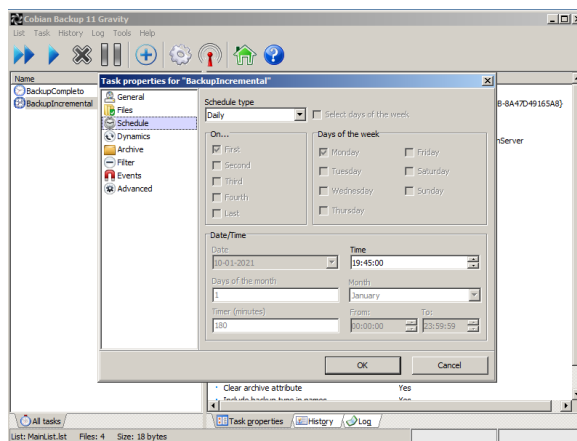
No Windows Sever utilizamos o software Cobian Backup 11 Gravity e fizemos o mapeamento de unidade rede para a pasta onde irão ficar os Backups desta máquina. No software Cobian Backup 11 Gravity, criámos 2 tarefas, uma para um backup incremental e outra para um backup completo, onde definimos o que vamos enviar, para onde e quando, neste caso definimos que o backup completo será feito semanalmente às 19h45, o backup incremental será feito há mesma hora mas diariamente.



**Figura 23 - Unidade de rede do Datacenter 3**



**Figura 24 - Directorias de backup**



**Figura 25 - Agendamento de backups**

## 5. Datacenter 3

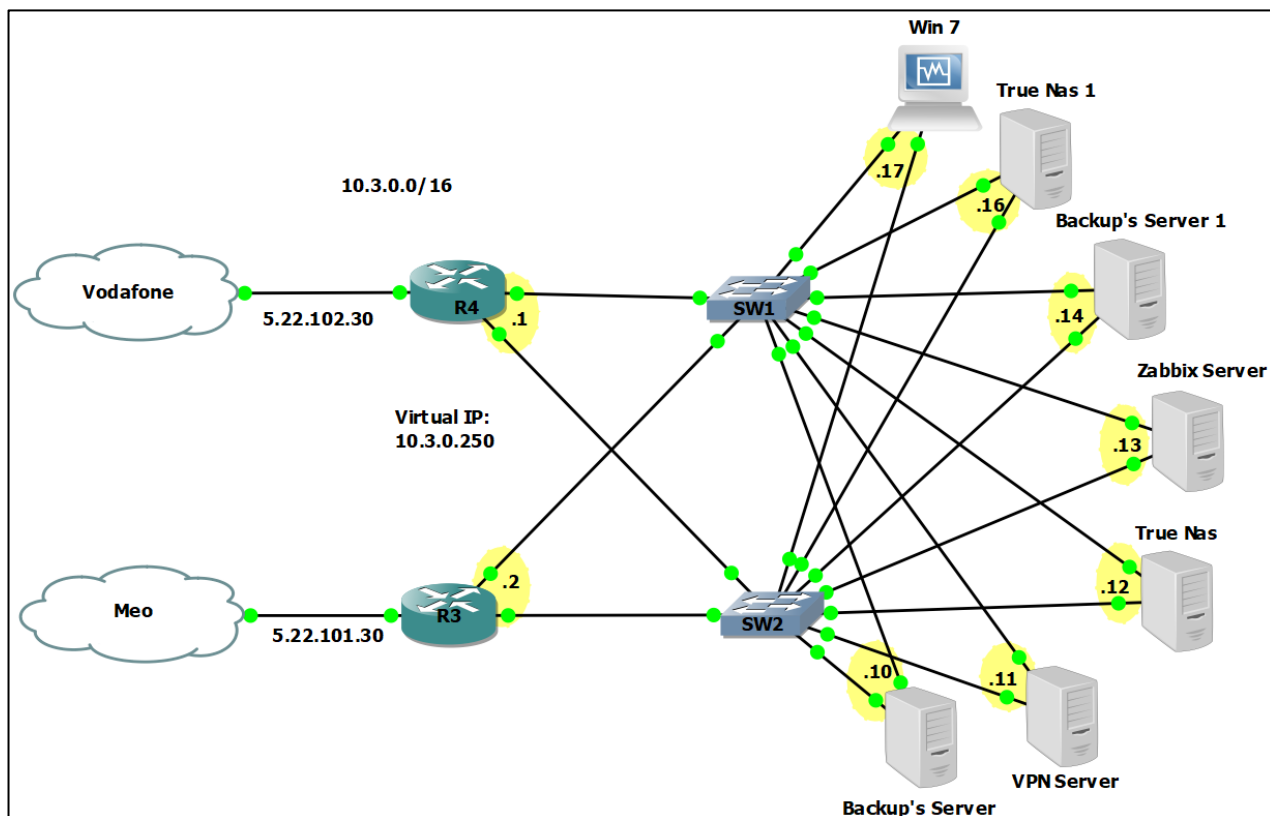


Figura 26 - Diagrama do Datacenter 3

No Datacenter 3, encontra-se disponibilizada a solução de NAS, que permite aos clientes alojar os seus dados num servidor que, além de fazer mirror dos dados, encontra-se em sincronização com outro servidor, utilizando para tal o sistema operativo True Nas. Através deste sistema operativo, existe também disponível uma cloud para todos os clientes.

Através do sistema operativo Ubuntu Server, encontram-se configurados dois servidores de Backups. Para o Backup's Server são enviados todos os backup's de todos os servidores existentes no Datacenter 1, 2 e 3, bem como dos clientes. Depois, o Backup Server envia todos esses backup's para um Backup's Server 1.

Existe também um servidor de VPN que permite aos clientes aceder ao NAS, sendo para tal usado o sistema operativo Ubuntu Server.

De forma a monitorizar todos os equipamentos dos diferentes Datacenter's, encontra-se instalado o Zabbix, que monitoriza diversas informações sobre os equipamentos configurados, como por exemplo, o consumo de RAM, CPU ou se se encontram ativos.

▼ NAS	0	0	0	ONLINE	
▼ MIRROR	0	0	0	ONLINE	⋮
ada2p2	0	0	0	ONLINE	⋮
ada1p2	0	0	0	ONLINE	⋮

Figura 27 - Raid em Mirror

### 5.1 - Solução de backups

Tal como referido anteriormente, o nosso cenário dispõem de um serviço de backups centralizado. Assim, todos os equipamentos presentes na rede dos clients e nas diversas redes dos diferentes Datacenters presentes na nossa

solução enviam um backup para o servidor Backup's Server. Após receber os backups das diferentes máquinas, este servidor envia para um outro servidor (Backup's Server 1), de forma a garantir que os dados se encontram salvaguardados no caso de acontecer algum problema ao mesmo.

Também já foi referido, que os clientes iriam ter acesso a uma NAS, de forma a alojar os seus dados. Sendo assim, e numa forma de garantir a redundancia dos dados, além deste servidor se encontrar configurado com mirror dos dados, existe uma sincronização com o servidor True Nas 1, para onde diariamente é enviada uma cópia dos dados dos clientes.

De forma a automatizar os backups, nas máquinas com o sistema operativo Windows, foi utilizado o software Cobian que permite agendar diversos tipos de Backups. No nosso caso, encontra-se configurado um Backup do tipo full que é executado uma vez por semana, e todos os restantes dias é executado um backup do tipo incremental. Assim, o ficheiro gerado, é enviado através do mapeamento de uma pasta que se encontra no servidor Backup's Server.

Para automatizar os backups, nas máquinas com o sistema operativo Linux, recorreu-se a um procedimento semelhante, porém resolvemos utilizar um script bash (Figura 9). Foi configurada uma entrada na crontab que, utilizando o comando rsync, de forma a centralizar numa unica pasta todas as pastas que se pretende fazer backup. Uma outra entrada foi configurada na crontab, para que o script seja executado com uma periodicidade de 15 minutos. Este script é responsável por fazer um zip da pasta que contém todas as pastas que se pretendem salvaguardar e enviar para um outro servidor através de SSH. Porém, para que o script ficasse automático, como se pretendia, foi necessário proceder a uma autenticação assimétrica, usando chaves assimétricas. Para tal, basta executar dois comandos ("ssh-keygen -t rsa" e "ssh-copy-id hostname@IP"), onde os campos hostname e IP serão substituídos pelo hostname e pelo endereço IP do servidor para o qual se pretende enviar a informação.

```
0,15,30,45 * * * * ubuntu /home/ubuntu/backupTOTAL.sh
14,29,44,59 * * * * root rsync -zarvh /home/ubuntu /PastaBackup
14,29,44,59 * * * * root rsync -zarvh /etc/netplan
14,29,44,59 * * * * root rsync -zarvh /etc/zabbix
```

Figura 28 - Ficheiro crontab do servidor Backup's

```
./Cliente1:
Desktop 2021-01-10 20:36:24 (Full).7z

./Cliente2:
Desktop 2021-01-10 20:34:51 (Full).7z

./Cliente3:
Desktop 2021-01-10 19:21:08 (Full).7z
Desktop 2021-01-10 19:30:15 (Full).7z
Desktop 2021-01-10 20:26:21 (Full).7z
Desktop 2021-01-10 20:31:56 (Incremental).7z

./FTP1:
TOTAL-FTP1-Monday-00:00.tgz.tar.gz TOTAL-FTP1-Sunday-17:58.tgz.tar.gz
TOTAL-FTP1-Monday-01:00.tgz.tar.gz TOTAL-FTP1-Sunday-18:30.tgz.tar.gz
TOTAL-FTP1-Monday-01:15.tgz.tar.gz TOTAL-FTP1-Sunday-18:45.tgz.tar.gz
TOTAL-FTP1-Monday-01:30.tgz.tar.gz TOTAL-FTP1-Sunday-19:00.tgz.tar.gz
TOTAL-FTP1-Monday-15:00.tgz.tar.gz TOTAL-FTP1-Sunday-19:45.tgz.tar.gz
TOTAL-FTP1-Monday-15:15.tgz.tar.gz TOTAL-FTP1-Sunday-20:00.tgz.tar.gz
TOTAL-FTP1-Monday-22:15.tgz.tar.gz TOTAL-FTP1-Sunday-21:45.tgz.tar.gz
TOTAL-FTP1-Monday-22:30.tgz.tar.gz TOTAL-FTP1-Sunday-23:30.tgz.tar.gz
TOTAL-FTP1-Monday-22:45.tgz.tar.gz TOTAL-FTP1-Sunday-23:45.tgz.tar.gz

./FTP2:
TOTAL-FTP2-Monday-01:00.tgz.tar.gz TOTAL-FTP2-Sunday-19:15.tgz.tar.gz
TOTAL-FTP2-Monday-01:15.tgz.tar.gz TOTAL-FTP2-Sunday-19:45.tgz.tar.gz
TOTAL-FTP2-Monday-01:30.tgz.tar.gz TOTAL-FTP2-Sunday-20:00.tgz.tar.gz
TOTAL-FTP2-Sunday-18:09.tgz.tar.gz TOTAL-FTP2-Sunday-21:45.tgz.tar.gz
TOTAL-FTP2-Sunday-19:00.tgz.tar.gz

./HttpServer:
TOTAL-dclwebservera-Monday-00:45.tgz.tar.gz
TOTAL-dclwebservera-Monday-15:00.tgz.tar.gz
TOTAL-dclwebservera-Monday-15:15.tgz.tar.gz
TOTAL-dclwebservera-Monday-22:15.tgz.tar.gz
TOTAL-dclwebservera-Monday-22:30.tgz.tar.gz
TOTAL-dclwebservera-Monday-22:45.tgz.tar.gz
TOTAL-dclwebservera-Sunday-18:07.tgz.tar.gz
TOTAL-dclwebservera-Sunday-18:08.tgz.tar.gz
TOTAL-dclwebservera-Sunday-18:30.tgz.tar.gz
TOTAL-dclwebservera-Sunday-18:45.tgz.tar.gz
TOTAL-dclwebservera-Sunday-19:00.tgz.tar.gz
TOTAL-dclwebservera-Sunday-19:15.tgz.tar.gz
```

Figura 29 - Backups organizados por servidor

## 5.2 - Máquina de administração

Como é possível visualizar no cenário do projeto, existe uma máquina Windows 7 no Datacenter 3. Esta máquina tem como principal função gerir, através da interface web, os dois servidores com o sistema operativo True Nas existentes, bem como o sistema de cloud Next Cloud que se encontra no servidor True Nas. Uma outra função para esta máquina, é monitorizar, através do software Zabbix o estado de todo o cenário. Existe também, no servidor Backup's Server a possibilidade de fazer algumas configurações através de um cliente Web, mais propriamente o Webmin.

Caso exista algum problema em algum servidor, esta máquina está preparada para aceder através de SSH a todos os servidores que se encontram no Datacenter 3.

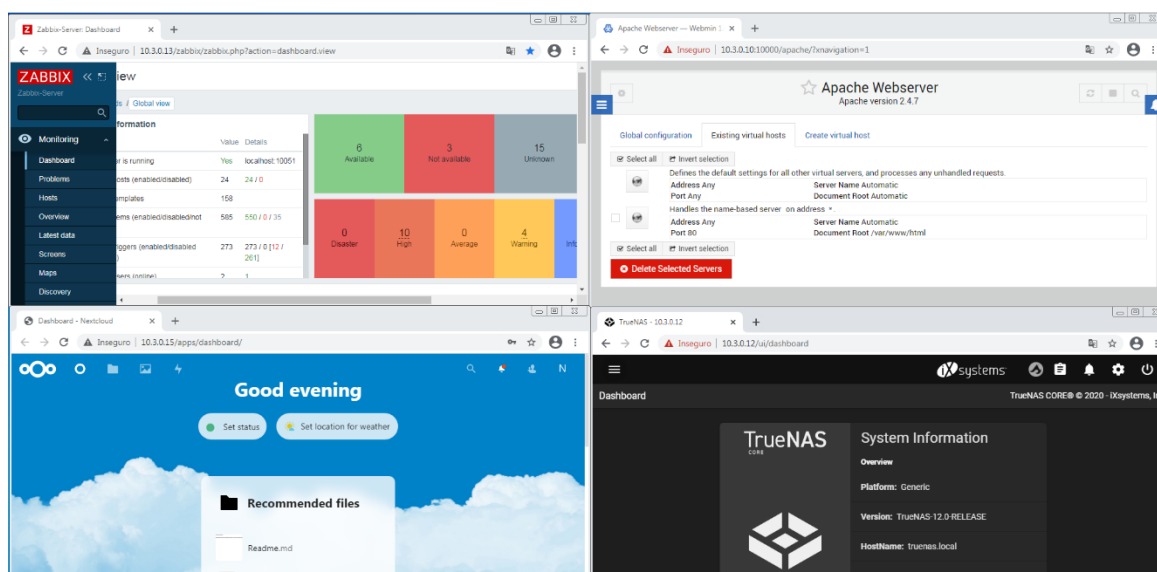


Figura 30 - Computador de Administração

## 5.3 - Solução de VPN

Um dos pressupostos do projeto era a existência de uma VPN a que fosse possível os clientes ligarem-se de forma a aceder ao NAS, porém, devido às limitações resultantes da pandemia da Covid-19 e à necessidade de recorrer a uma VPN para interligar os 3 Datacenters, existiu alguns problemas nas tentativas de utilizar o port forwarding. Assim, foi configurado um tunel GRE entre os os 3 Datacenters e a rede dos clientes e assim não existe a necessidade de uma VPN OpenVPN, porém, apesar de desnecessário, esta VPN encontra-se completamente funcional.

## 5.4 - Solução de monitorização

De forma a monitorizar os diferentes Datacenters foi utilizado o serviço Zabbix, que se encontra alojado num servidor Ubuntu, no datacenter 3. Este serviço permite monitorizar dispositivos nos diversos Datacenters, como routers e servidores.

Para que seja possível receber informações sobre os diversos servidores, encontra-se configurado o zabbix-agent em todas as máquinas linux bem como na pfSense. Assim, o zabbix-agent envia informações relativas ao consumo de RAM ou CPU, bem como o estado em que se encontra.

Nos routers, no servidor de DNS e em máquinas Windows, é utilizado o ICMP para verificar o estado do equipamento.



Depois de adicionar os equipamentos ao Zabbix, é possível criar um mapa, semelhante ao do cenário GNS, onde aparece a informação sobre o estado destes. Existe um relatório adicional, onde se encontra descrito este processo com uma maior precisão.

### 5.5 - Acesso dos clientes à NAS

No Datacenter 3, existe uma NAS configurada através do sistema operativo True Nas. Para tal, foi criada uma pasta pessoal para cada utilizador e uma pasta pública acessível para todos os clientes, requerendo apenas a autenticação para controlar caso seja um utilizador válido.

Pools								
NAS <span>ONLINE</span> <span>7.73 GiB (8%) Used   86.72 GiB Free</span>								
Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
▼ NAS	FILESYSTEM	7.73 GiB	86.72 GiB	lz4	1.90	false	OFF	
▼ locage	FILESYSTEM	7.60 GiB	86.72 GiB	lz4	1.87	false	OFF	
> download	FILESYSTEM	660.06 MiB	86.72 GiB	lz4	1.00	false	OFF	
images	FILESYSTEM	95.00 KiB	86.72 GiB	lz4	1.00	false	OFF	
> jails	FILESYSTEM	4.53 GiB	86.72 GiB	lz4	1.93	false	OFF	
log	FILESYSTEM	100.00 KiB	86.72 GiB	lz4	1.19	false	OFF	
> releases	FILESYSTEM	2.42 GiB	86.72 GiB	lz4	2.02	false	OFF	
templates	FILESYSTEM	95.00 KiB	86.72 GiB	lz4	1.00	false	OFF	
Publico	FILESYSTEM	84.13 MiB	86.72 GiB	Inherits (lz4)	1.01	false	OFF	

Figura 31 - Diretorias presentes na NAS

## 6. Cenário virtual dos clientes

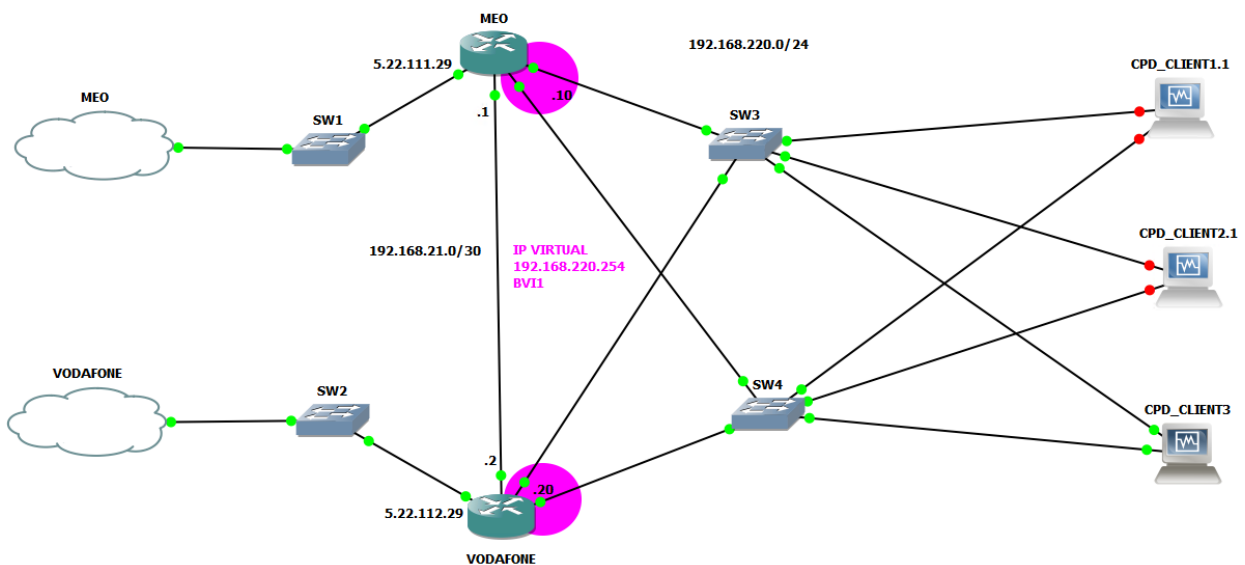


Figura 32 - Cenário virtual dos clientes

O cenário dos clientes é composto por dois routers que simulam o acesso aos dois ISP'S (MEO e VODAFONE), e por três máquinas virtuais com o Windows 7 que simulam os clientes que acedem aos serviços implementados nos datacenter's. O cenário utiliza apenas uma rede: 192.168.220.0/24.

## 6.1 - Funcionalidades disponíveis aos clientes

Os clientes conseguem aceder aos seguintes serviços:

- Acesso Remoto ao WinServer do Datacenter2 (Remote Desktop);
- Acesso Remoto a NAS do Datacenter 2 e Datacenter 3;
- Acesso a servidores WEB e FTP.

## 6.2 - Acesso Remoto ao Windows Server do Datacenter2

O acesso ao servidor Windows Server pode ser efectuado a partir de qualquer máquina cliente que opere uma distribuição Windows, e basta aceder ao software já embutido no Windows “Ligação de ambiente trabalho remoto” onde irá ser solicitado o IP do servidor.

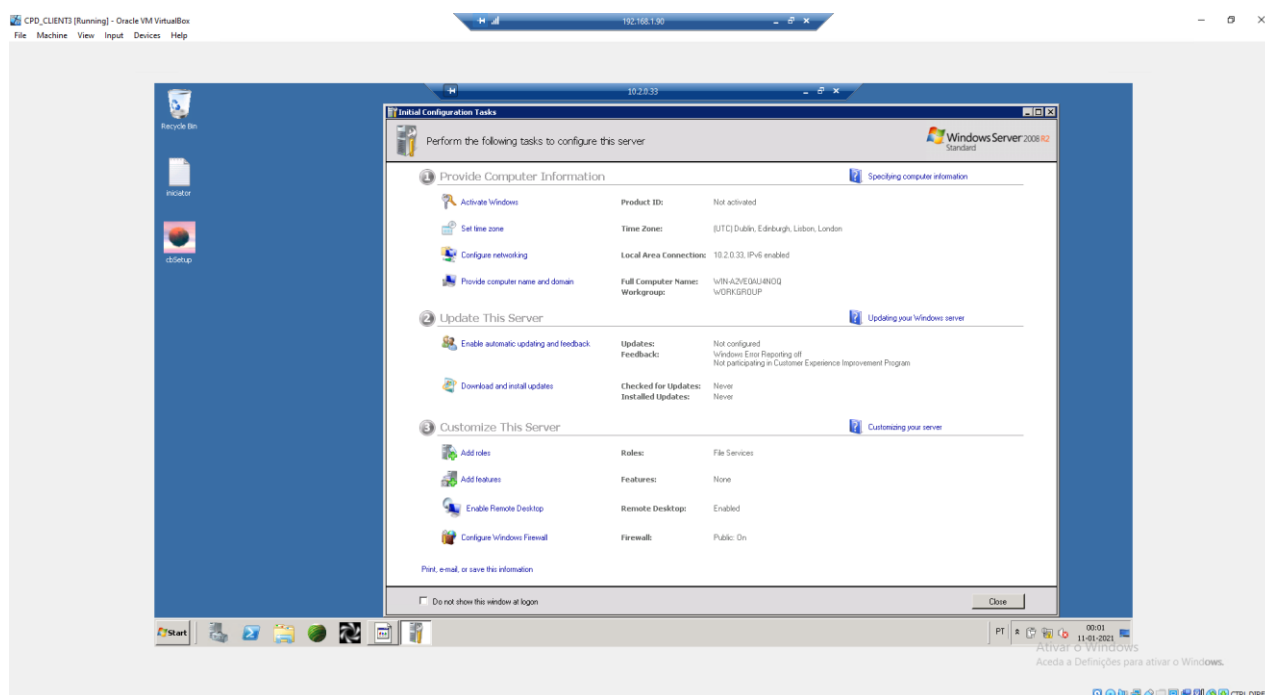


Figura 33 - Teste de Acesso remoto

## 6.3 – Acesso remoto à NAS

O acesso às NAS configuradas nos Datacenter 2 e 3 é efectuado através do explorador do windows utilizando a funcionalidade de mapear unidades de rede, através desta funcionalidade basta inserir o ip remoto e as credenciais de acesso.

Para a ligação à NAS presente no Datacenter 3 foi configura uma VPN que permite a conexão à rede privada do DC3 e por sua vez à NAS.

## 6.3 – Acesso a servidores Web e FTP

Para acesso a estes serviços os utilizadores apenas precisam de aceder aos domínios criados no servidor de DNS do DC1 através de uma aplicação que suporte a conexão a estes serviços (browser, filezilla, etc.). Os domínios disponíveis são:

- cpd.webserverdc1.pt;
- cpd.webserverdc2.pt;

- cpd.ftpservdc2.pt;

## 7 – Atividades extra

Perante as proposta que foram apresentadas, na nossa rede foram implementadas duas atividades extras, sendo estas:

- Implementar no “Datacenter 3” uma solução de monitorização integrada (sem ser o Nagios), designadamente da infraestrutura, da rede e dos seus serviços, que monitorize o estado de todos os datacenters;
  - Para esta opção a solução utilizada foi o Zabbix;
- Implementar uma solução de alta disponibilidade e/ou balanceamento de carga com clusters de servidores que não tenha sido abordada nas aulas;
  - Para esta opção a solução utilizada foi o *PfSense*;

## 8 - Testes e resultados

### 8.1 – Datacenter 1

#### 8.1.1 – Teste do serviço HTTP e DNS



Figura 34 - Website do Datacenter 1 acedido através do dominio

### 8.2 – Datacenter 2

## 8.2.1 – Teste do serviço HTTP



Figura 35 - Website do Datacenter 2

## 8.2.1 – Teste serviço FTP

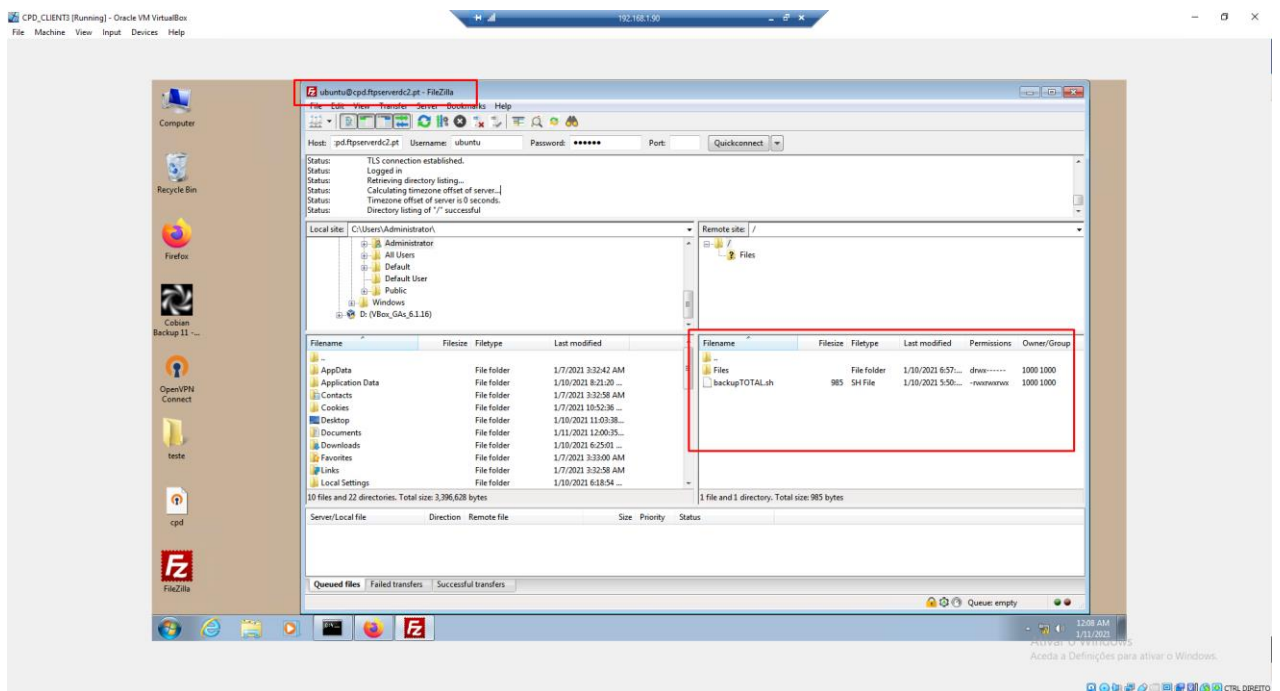


Figura 36 - Acesso ao servidor FTP DC2

### 8.2.3 – Teste ao serviço Remote Desktop

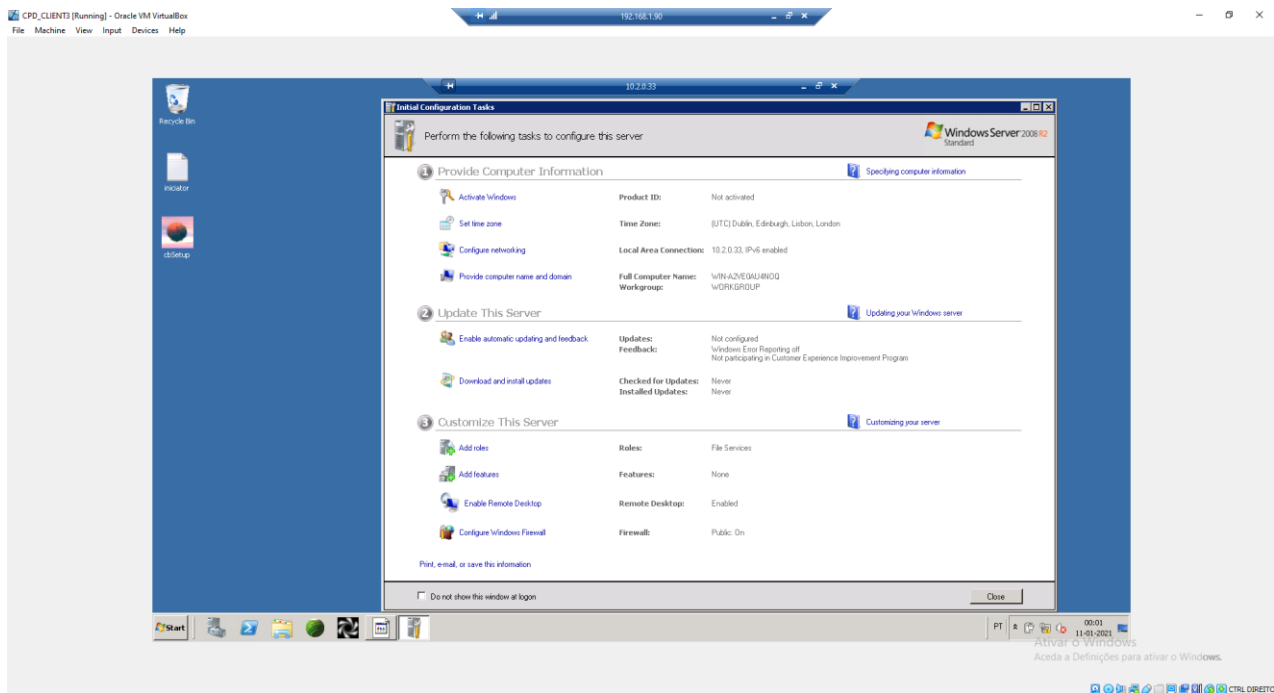


Figura 37 - Teste ao serviço Remote Desktop do Windows Server do DC2

### 8.2.3 - Teste de acesso à NAS

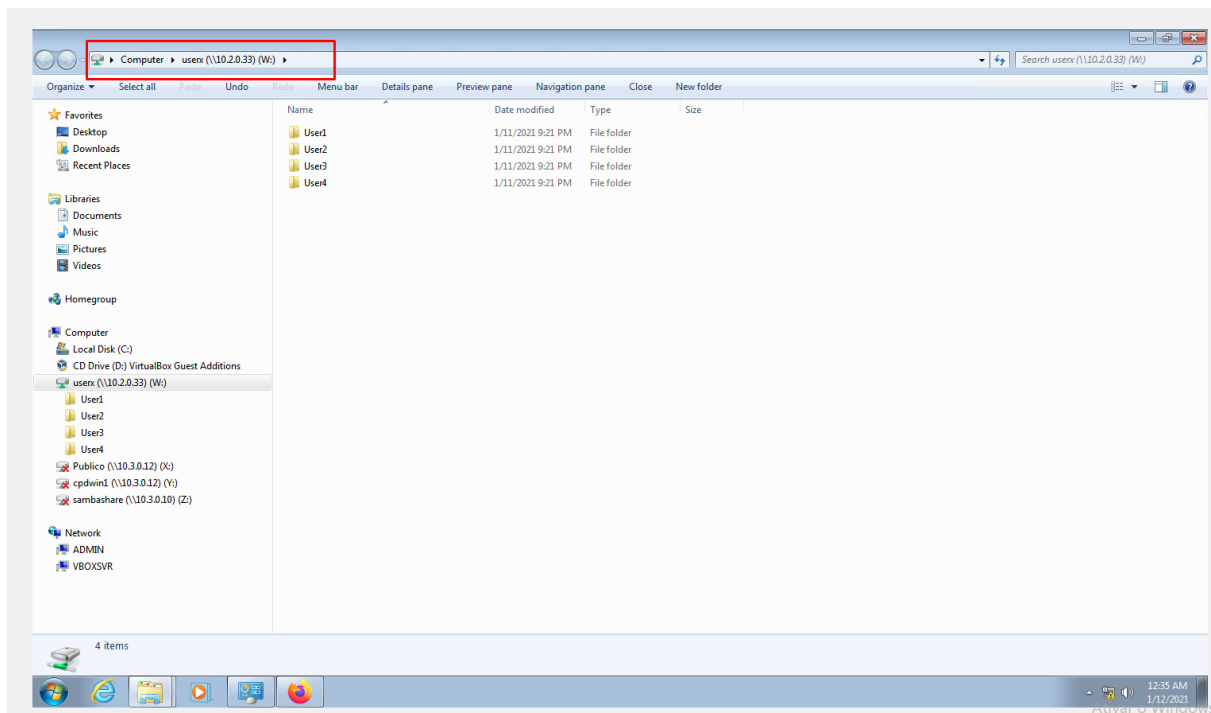


Figura 38 - Acesso à NAS do DC2

## 8.3 Datacenter 3

### 8.3.1 – Acesso à cloud

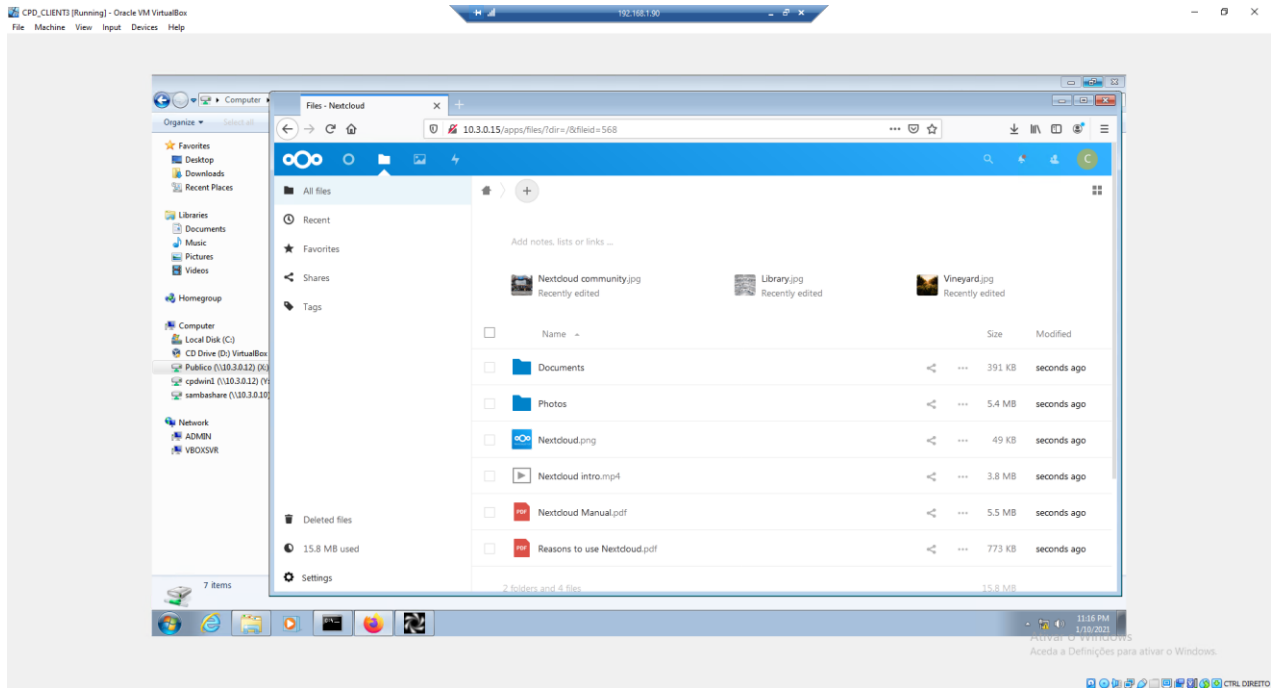


Figura 39 - Acesso à cloud do DC3

### 8.3.1 – Acesso à NAS

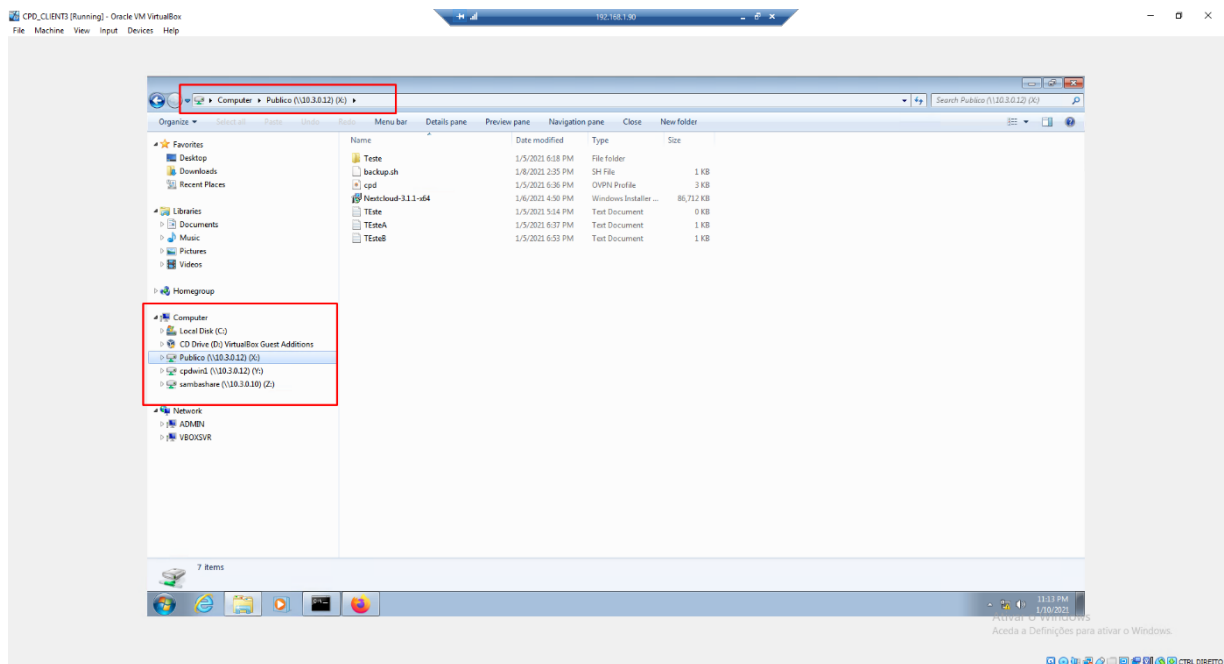


Figura 40 - Acesso à NAS DC3

### 8.3.2 - Acesso à VPN

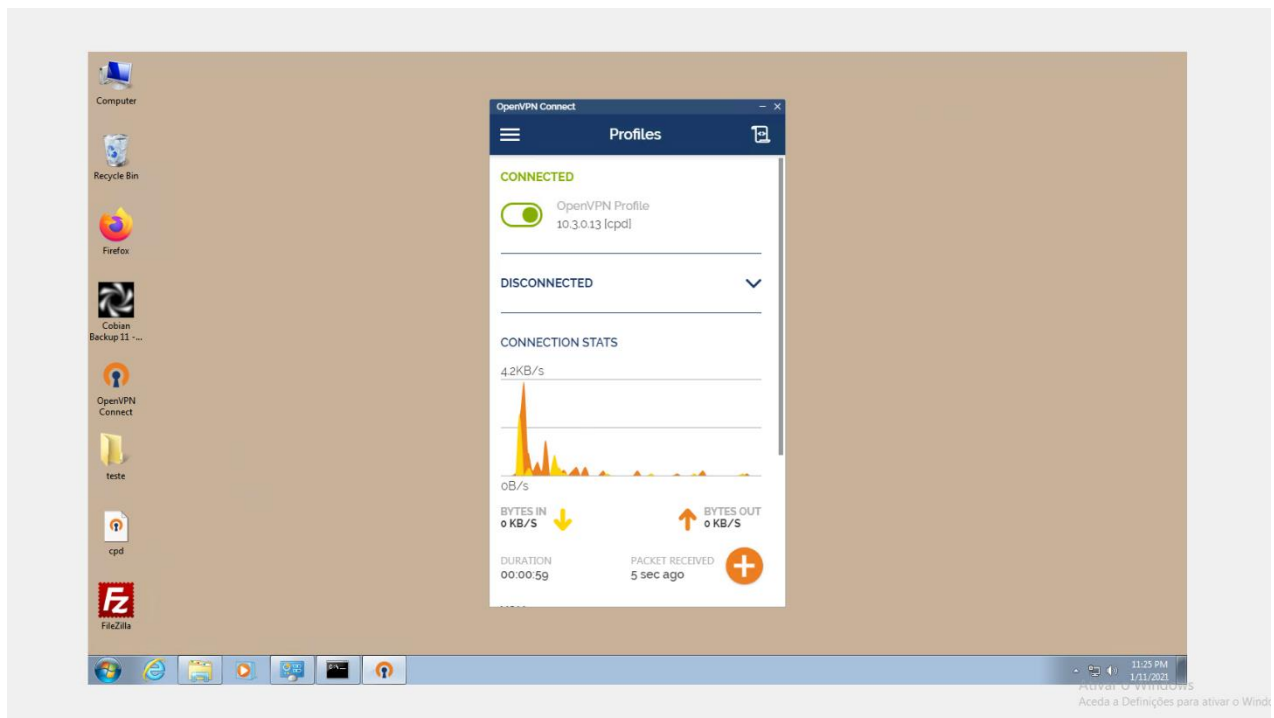


Figura 41 - Acesso à VPN

8.3.4 - Monitorização Zabbix

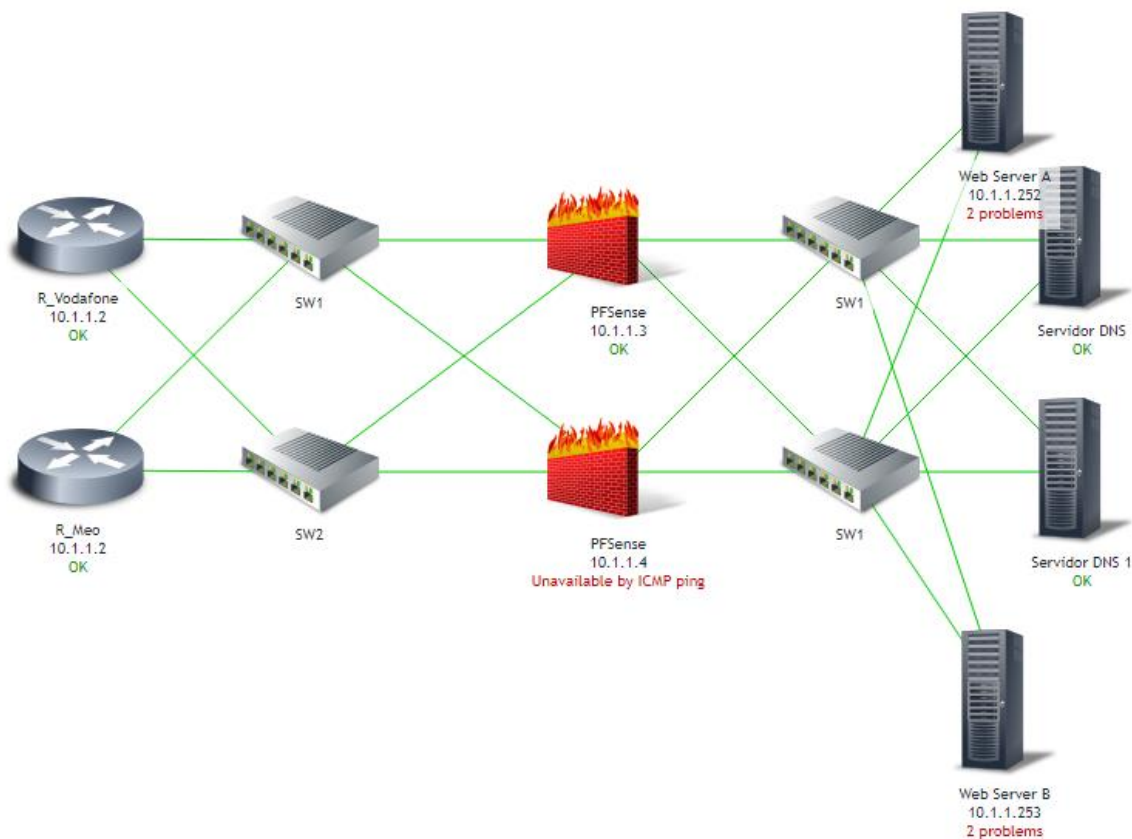


Figura 42 - Cenário DC1 - ZABBIX

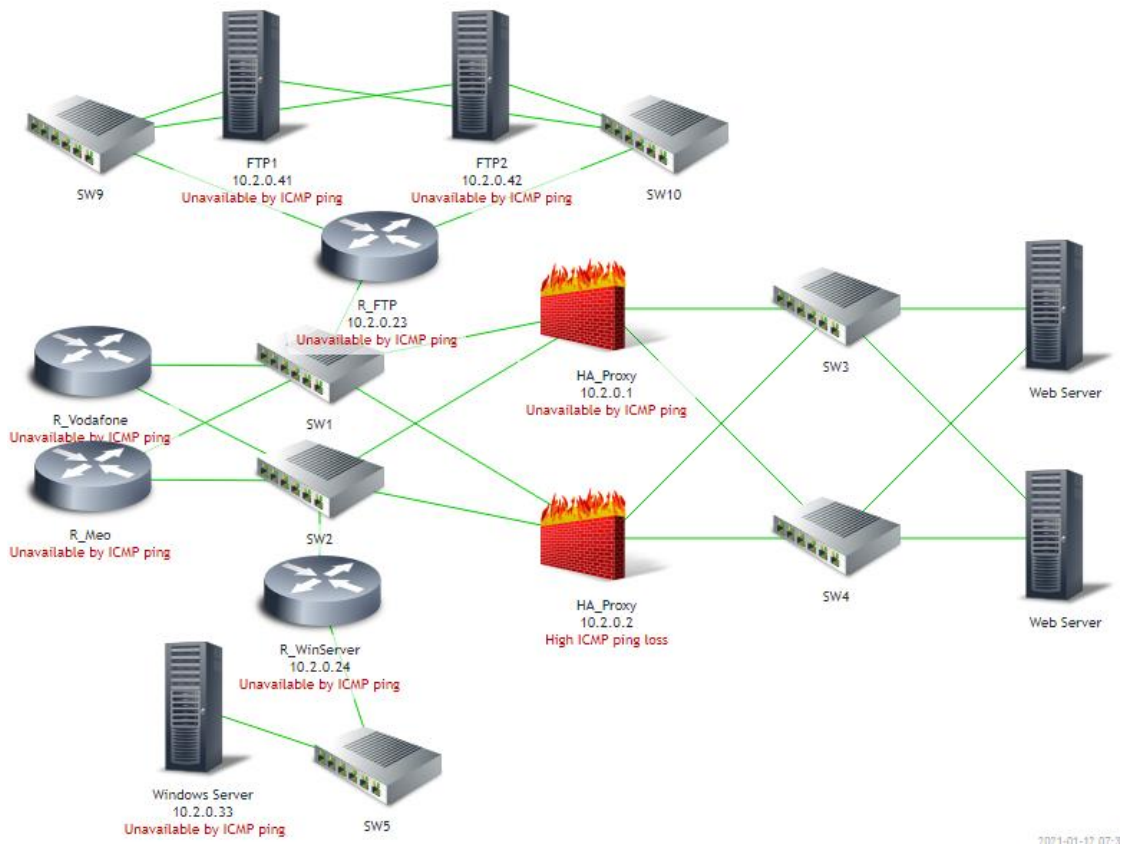


Figura 43 - Cenário DC2 - Zabbix



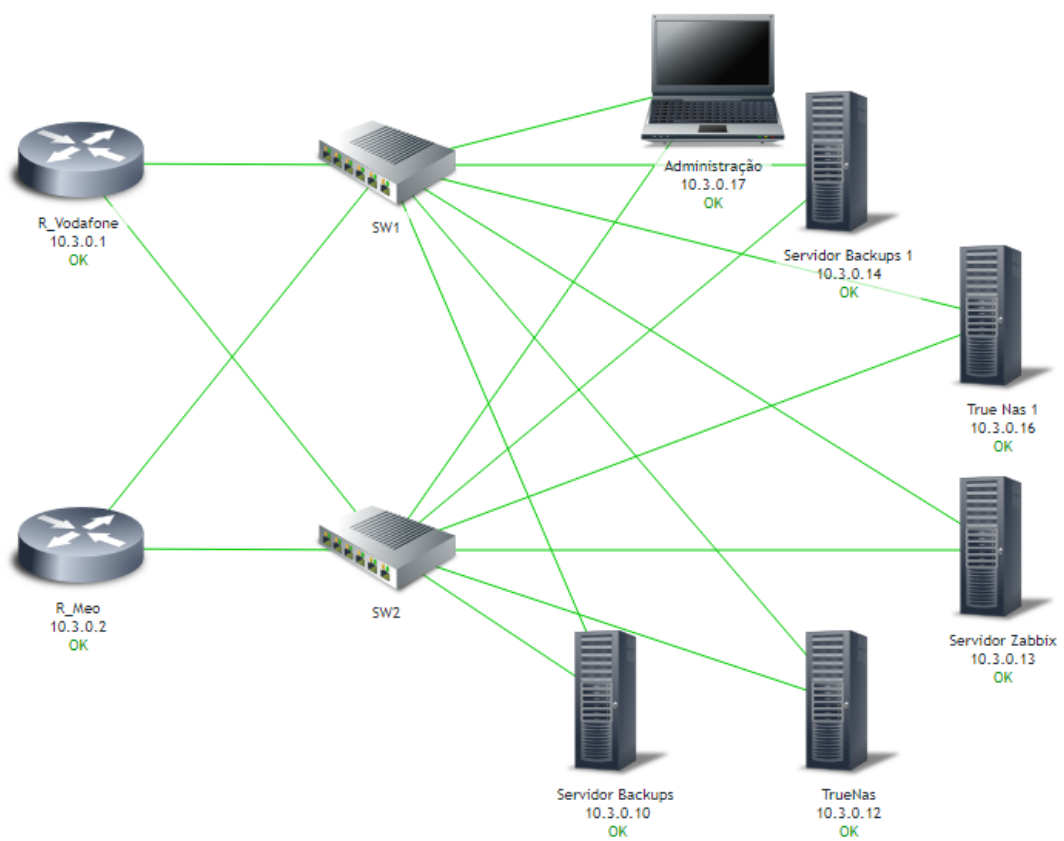


Figura 44 - Cenário DC3 ZABBIX

## 9 – Conclusão

Depois do projeto todo implementado, podemos garantir que cumprimos praticamente todos os critérios solicitados para a resolução do problema da empresa “CPDHosting”, cumprindo assim com os objetivos propostos.

Porém, temos noção que em todos os Datacenters existe sempre espaço para melhorias, como por exemplo:

- A Alta Disponibilidade e Redundância, poderia ser mais aprofundada.
- O sistema de backups foi implementado de forma meramente exemplificativa, poderia ser bastante mais aprofundado e detalhado.
- Poderia ter sido implementado a sincronização com ambientes remotos (presentes na internet).
- A configuração dos tuneis dedicados poderia ter sido mais segura.
- O balanceamento por NAT poderia ter sido implementado.
- Adicionar RAID1 em todos os servidores para obter desta forma redundancia de informação.

É de notar que devido á pandemia e aos escassos recursos não nos foi possível fazer a interligação do cenário virtualizado no GNS3 com equipamentos ALU-SAR 7705.

## 10 - Bibliografia

- [1] R. K. Sr, “How to Setup Bridge Networking with KVM on Ubuntu 20.04,” *How to get your VMs seen by your home network.*, 14 maio 2020.
- [2] “How to set up a Linux VPN server (Beginner's Guide),” [Online]. Available: <https://averagelinuxuser.com/linux-vpn-server/>.
- [3] “How To Backup Your FreeNAS 11.3 Using ZFS Replication,” 4 5 2020. [Online]. Available: [www.youtube.com](http://www.youtube.com).
- [4] J. Wallen, “How to synchronize Ubuntu server directories with Unison,” 5 Maio 2020. [Online]. Available: [www.techrepublic.com](http://www.techrepublic.com). [Acedido em 10 Janeiro 2021].
- [5] “Zabbix Monitor Windows using Agent,” [Online]. Available: <https://techexpert.tips/>.
- [6] Regina, “[Ubuntu] How to set up an FTP server on Ubuntu 14.04 or 16.04,” 12 2018. [Online]. Available: <https://community.time4vps.com/>.
- [7] Netgate, “Using the AutoConfigBackup Service,” Netgate Docs, [Online]. Available: <https://docs.netgate.com/pfsense/en/latest/backup/autoconfigbackup.html>. [Acedido em 2021 01 10].
- [8] Cisco, “Understanding Bridge Virtual Interface (BVI) and Bridge Domain Interface (BDI),” Cisco, 2016 10 9. [Online]. Available: <https://www.cisco.com/c/en/us/support/docs/lan-switching/integrated-routing-bridging-irb/200650-Understanding-Bridge-Virtual-Interface.html>.
- [9] A. Bytes, “pfSense SSH Key Authentication,” 2017 01 11. [Online]. Available: <https://www.bytesizedalex.com/pfsense-ssh-key-authentication/>.
- [10] Netgate, “Port Forward and 1:1 NAT Interaction,” Netgate Docs, [Online]. Available: <https://pfsense-docs.readthedocs.io/en/latest/nat/port-forward-and-1-1-nat-interaction.html>.
- [11] Netgate, “NTP Server Configuration,” [Online]. Available: <https://docs.netgate.com/pfsense/en/latest/services/ntpd/server.html>.
- [12] Cisco, “Configuring GRE Tunnel Over Cable,” [Online]. Available: <https://www.cisco.com/c/en/us/support/docs/broadband-cable/cable-modems/12084-gre-tunnel-over-cable.html>.