

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS E INFORMÁTICA
Bacharelado em Sistemas de Informação

Camila Fernanda da Silva, Francisco Matos, Gabriela Scarabelli Bahia, Henrique Lima,
Nathalia Souto, Wallace Sousa

**PROJETO INFRAESTRUTURA DE REDE
ONG: QUATRO PATAS**

Belo Horizonte
2024

1 INTRODUÇÃO

A missão da Quatro Patas Solidárias é de extrema importância, pois visa proporcionar cuidado e proteção aos cachorros que se encontram em situações de abandono ou vulnerabilidade. Ao oferecer serviços como resgate, castração, vacinação, adoção, hospedagem, educação e conscientização sobre a causa animal, a organização não apenas ajuda os animais diretamente, mas também trabalha para promover uma mudança de mentalidade e comportamento em relação aos direitos dos animais.

A participação de voluntários, doações e parcerias é fundamental para o funcionamento e sustentabilidade da ONG. Através desses recursos, a Quatro Patas Solidárias pode ampliar seu alcance e oferecer um suporte mais abrangente aos cachorros necessitados, bem como educar a comunidade sobre a importância do tratamento ético e humanitário aos animais.

A crença de que os cachorros são seres sencientes que merecem amor, respeito e dignidade reflete o compromisso da organização em defender os direitos dos animais e garantir que recebam o cuidado e o tratamento adequados. Essa visão orienta todas as atividades e iniciativas da Quatro Patas Solidárias, impulsionando seu trabalho em prol do bem-estar animal.

A estrutura da Quatro Patas Solidárias compreende uma matriz estrategicamente situada na região central de Belo Horizonte, juntamente com três filiais distribuídas em pontos-chave da região metropolitana. Essas filiais estão localizadas em Nova Lima, Contagem e na região da Pampulha, também em Belo Horizonte.

2 SERVIÇOS

Uma ong que cuida de cachorros precisa de tecnologias que facilitem a sua gestão, comunicação, divulgação e operação. Algumas dessas tecnologias são:

- Site: Apresenta a ong para o público e permite o acesso aos seus serviços e informações.
- Serviço de hospedagem para a aplicação.
- Serviço FTP
- Banco de dados: Possibilita o salvamento de contato de parceiros.
- Software de gestão: Auxilia na administração da ong e gera relatórios e indicadores.
- Software de comunicação: Possibilita a interação entre os membros da ong e os demais envolvidos na causa animal.
- Aplicativo mobile: Disponibiliza as principais funcionalidades do site da ong em uma versão mobile.

3 INFRAESTRUTURA

Uma ong que cuida de cachorros precisa de uma infraestrutura que garanta a conectividade, a segurança, o desempenho e a disponibilidade dos seus serviços e dados. Algumas das características dessa infraestrutura são:

- Site hospedado no AWS: Oferece diversos serviços de computação em nuvem, como hospedagem, armazenamento, processamento, segurança, etc.
- Uso de DHCP dentro das unidades para novas conexões: Atribui automaticamente um endereço IP a cada dispositivo que se conecta à rede da ong.
- Servidores com endereço de IP devidamente configurados.
- Pontos de acessos WI FI - APs.
- Um roteador em cada uma das unidades para prover a comunicação da rede WAN.
- Pontos de acesso: Interliga diferentes redes e suporta protocolos de rede, segurança, qualidade de serviço, frequências e padrões de Wi-Fi.
- Roteador: Um roteador em cada unidade para fazer a ligação e comunicação da rede WAN das localidades.
- Firewall: Garante a segurança dos dados trafegados na rede como uma barreira a invasões de ataques virtuais.
- Switch: Permite a comunicação e tráfego de dados entre os elementos conectados na rede.
- VPN: Permite a conexão segura e remota entre os dispositivos dos membros da ong.

4 TOPOLOGIA

A escolha da topologia do tipo anel para conectar a matriz e as três filiais da Quatro Patas Solidárias foi motivada por diversas razões:

- Eficiência na comunicação: Em uma topologia de anel, cada nó (ou filial, no caso da ONG) está conectado diretamente aos nós adjacentes, criando um caminho de comunicação direto e eficiente entre todos os pontos da rede. Isso pode facilitar a troca de informações, coordenação de atividades e tomada de decisões entre a matriz e as filiais.

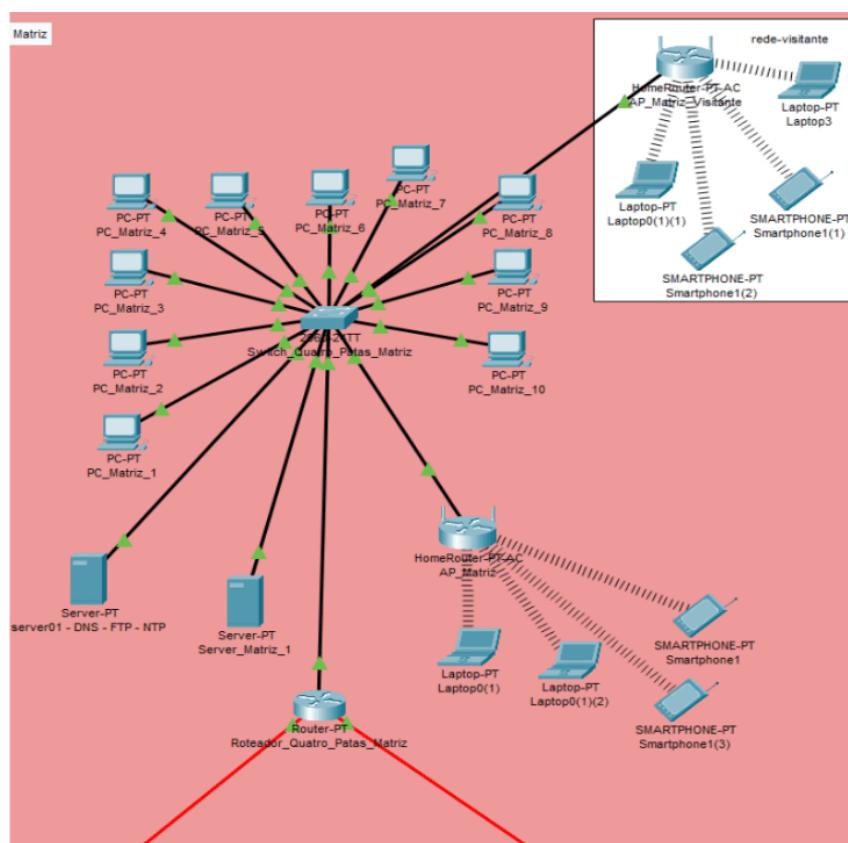
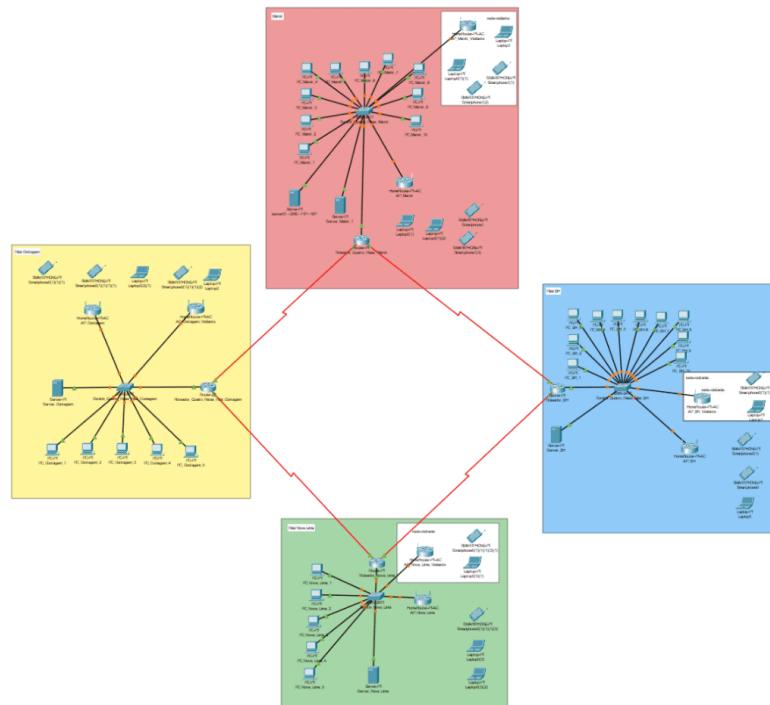
- Redundância e tolerância a falhas: Na topologia de anel, se um dos nós (ou filiais) falhar, a comunicação pode ser roteada através de um caminho alternativo na direção oposta, garantindo que a rede permaneça operacional. Isso proporciona uma maior redundância e tolerância a falhas, o que é importante em um contexto onde a continuidade das operações é crucial.

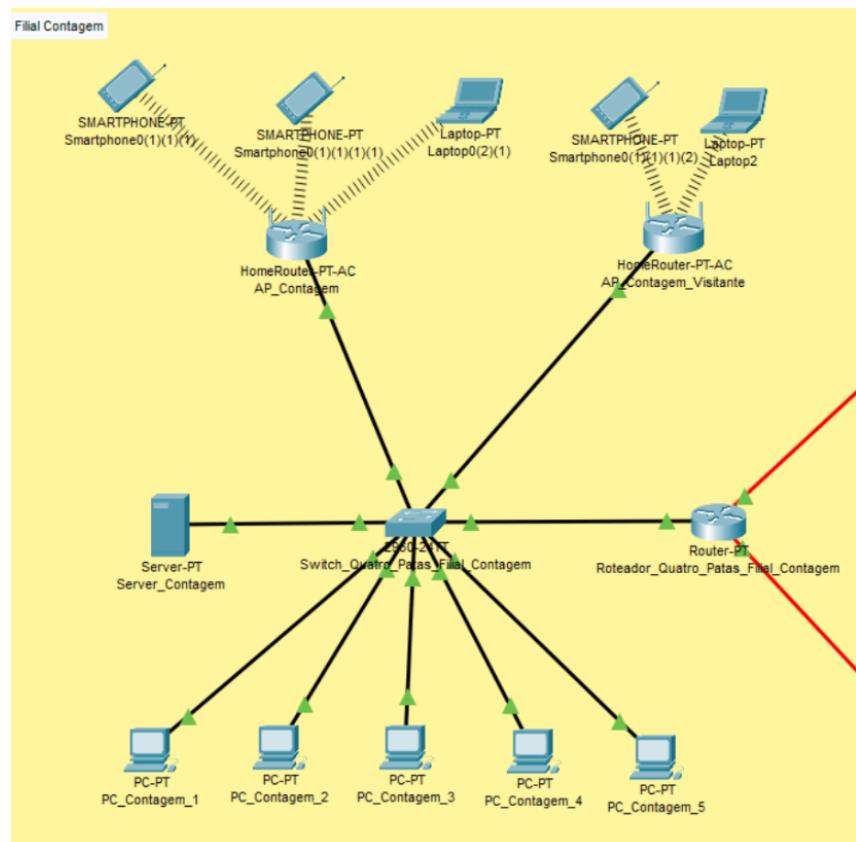
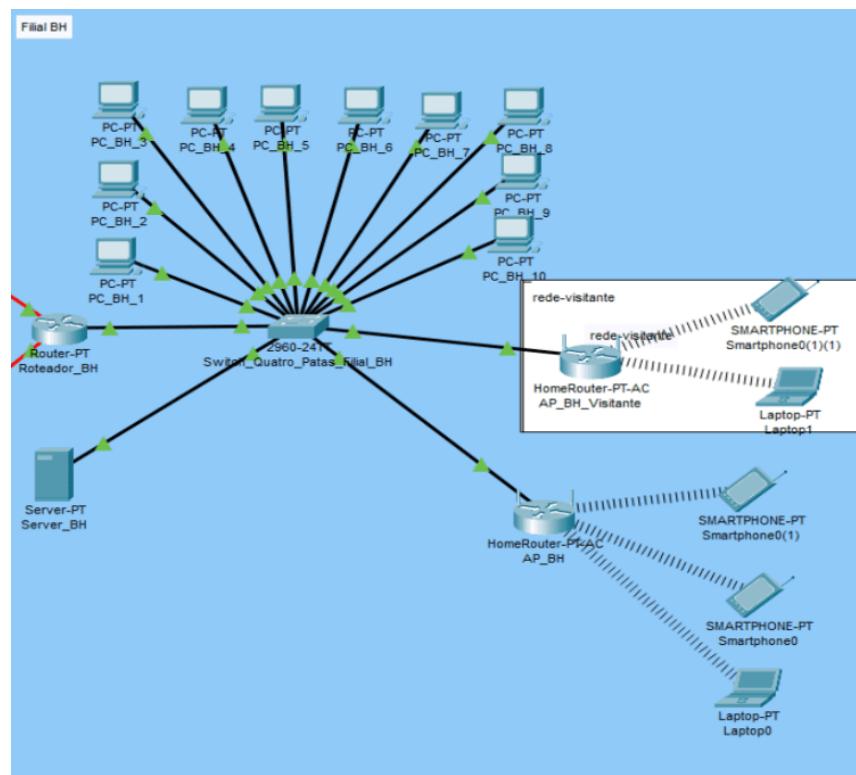
- Facilidade de expansão: A topologia de anel é facilmente escalável. Novas filiais podem ser adicionadas à rede simplesmente conectando-as ao anel existente, sem a necessidade de reconfiguração significativa da infraestrutura de comunicação. Isso permite que a organização cresça e se adapte às necessidades em constante evolução, mantendo uma estrutura de rede coesa e eficiente.

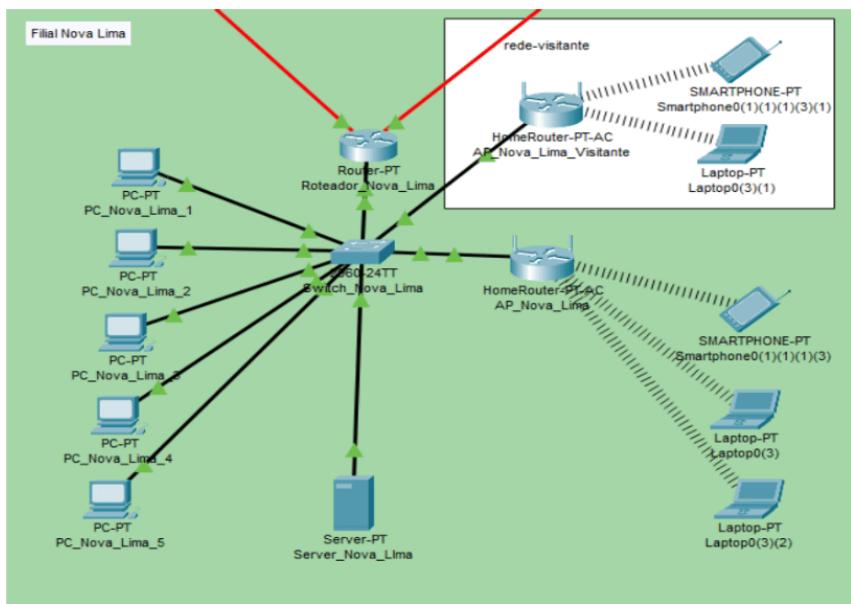
- Simplicidade e custo-efetividade: A topologia de anel é relativamente simples de configurar e manter, o que pode resultar em custos mais baixos de implantação e manutenção da rede. Isso é especialmente importante para uma organização sem fins lucrativos, onde recursos financeiros podem ser limitados.

Em resumo, a escolha da topologia de anel para conectar a matriz e as filiais da Quatro Patas Solidárias pode proporcionar eficiência na comunicação, redundância e tolerância a falhas, facilidade de expansão e simplicidade operacional, contribuindo para o sucesso e a eficácia das operações da organização.

5 PROTÓTIPO







6 AMBIENTES DE IMPLANTAÇÃO

6.1 Criação do AD:

O servidor AD foi estabelecido na nuvem da Amazon utilizando o Directory Service. O processo começou com a criação de uma instância EC2 e, em seguida, essa instância foi vinculada ao Directory Service da Amazon com todas as configurações realizadas de maneira adequada.

AD Directory Service Ativo:

The screenshot shows the AWS Directory Service console in the 'Active Directory' section. A single directory named 'adquatropatas.org' is listed. The details show it's a Microsoft AD Standard directory with the ID 'd-9067fe795f'. The status is 'Ativo' (Active).

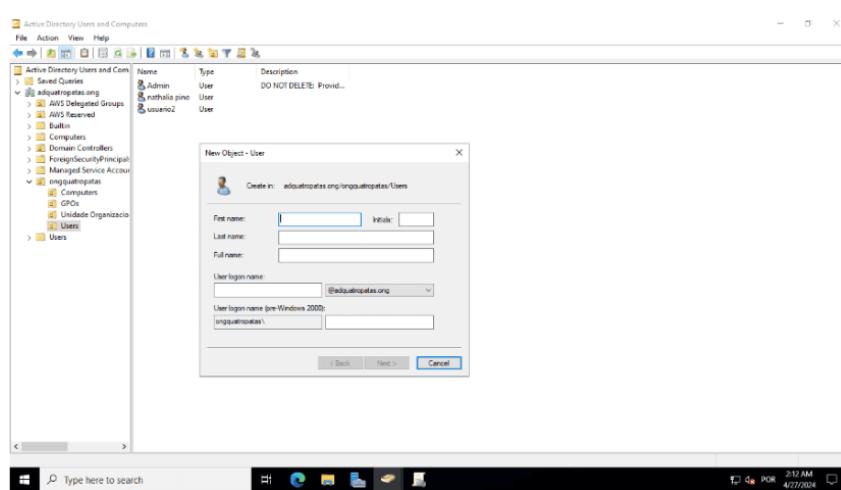
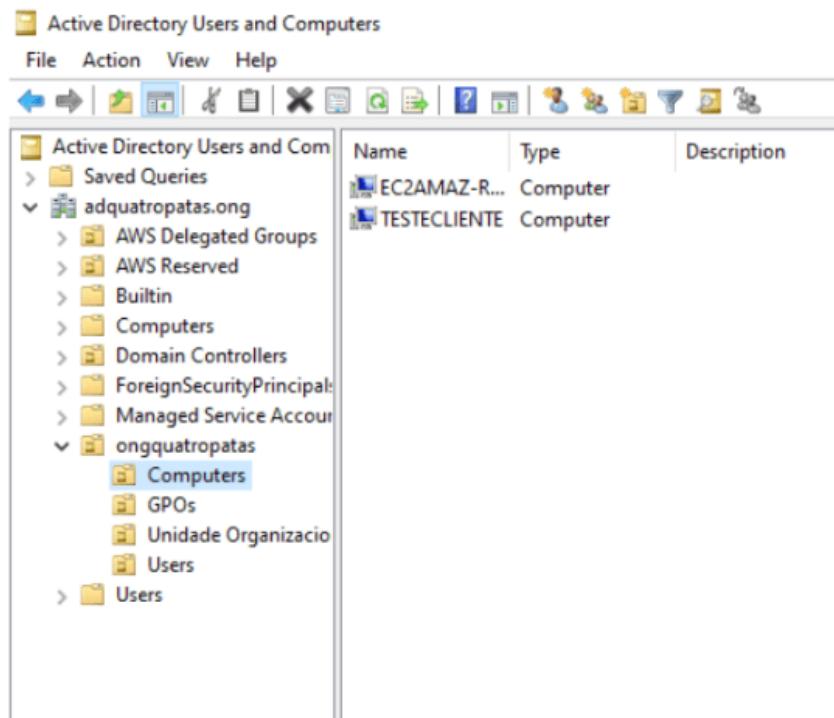
This screenshot provides more detailed information about the 'd-9067fe795f' directory. It lists the type as Microsoft AD, edition as Standard, and operational system version as Windows Server 2019. It also shows the DNS name as 'adquatropatas.org' and the EC2 instance used for administration.

This screenshot shows the network configuration for the directory. It lists the VPC as 'vpc-09c35e0638cc2ef05' and the subnet ranges as 'subnet-0290a757ffbf023b' and 'subnet-0dd6e451ae01de32c'. The status is 'Ativo' (Active) with the last update on 'quarta-feira, 17 de abril de 2024'.

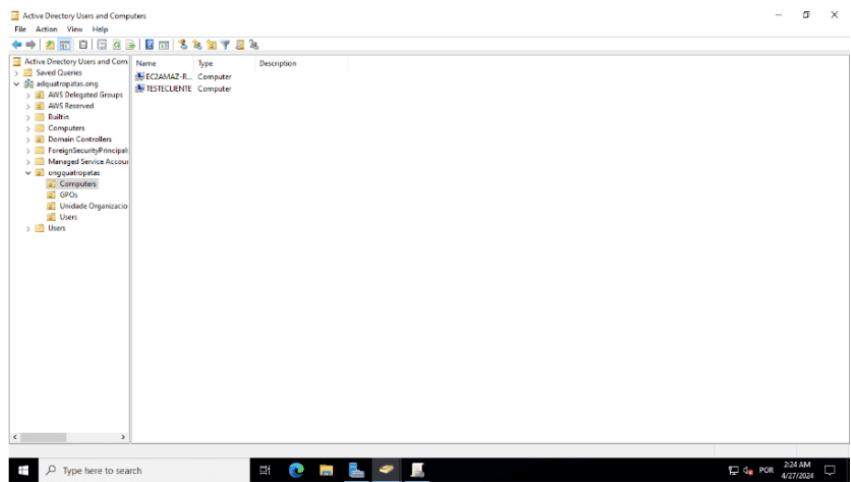
Dentro do servidor AD e após a configuração inicial do servidor Active Directory (AD) ter sido concluída com êxito, foi feita a criação de usuários, definição de senhas e implementação de Políticas de Grupo (GPOs).

Também foi criada uma máquina cliente de teste. Esta máquina cliente foi ingressada ao domínio do AD e estabelecida com o objetivo de realizar testes abrangentes para garantir que todas as configurações estejam funcionando conforme o esperado.

Serviço AD:



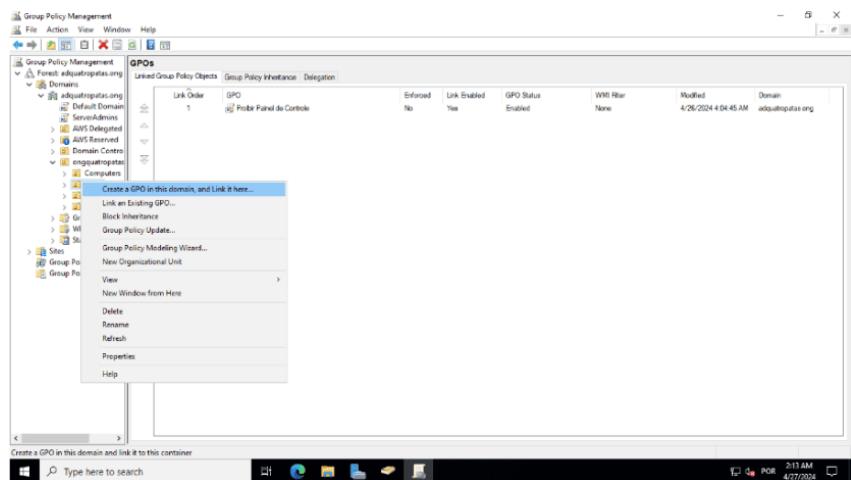
Criação de usuários:



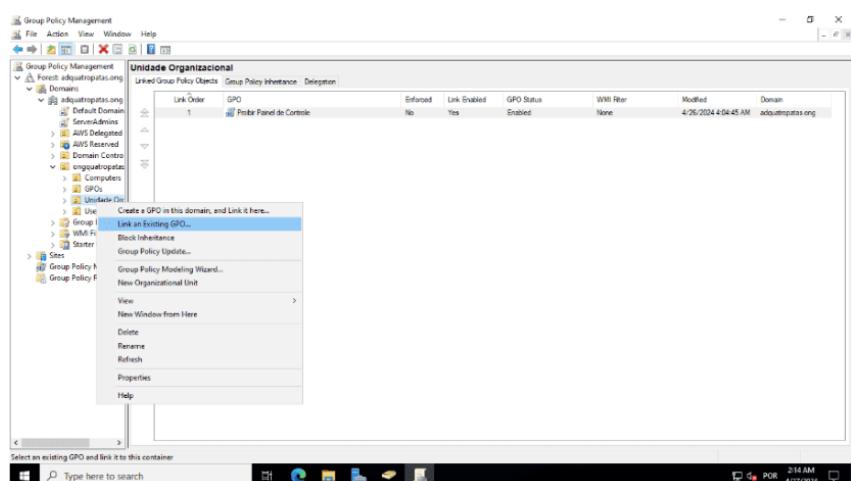
Definindo (criando) GPOs:

Dentro do Console de Gerenciamento de Política de Grupo (GPMC) foi criada uma nova GPO.

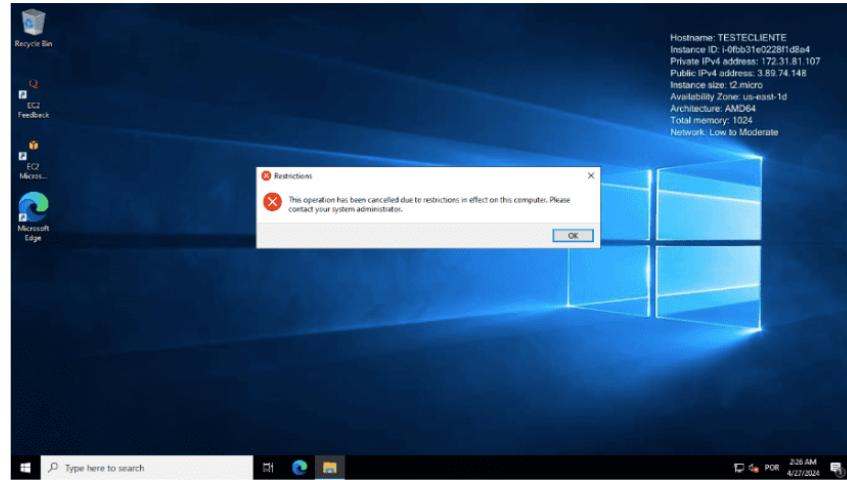
Para fins de organização, uma unidade dedicada foi estabelecida apenas para as novas GPOs.



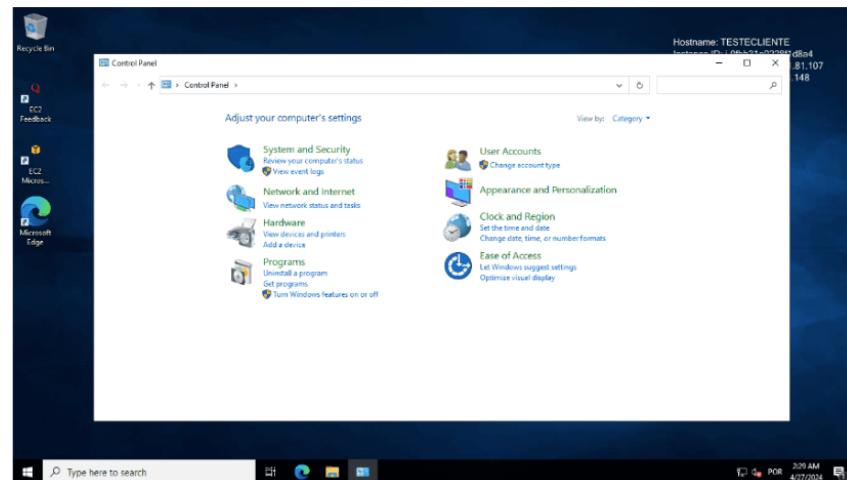
Em seguida, essa GPO foi vinculada a uma unidade organizacional. A política em questão criada, refere-se à proibição de acesso ao Painel de Controle, e foi vinculada a uma unidade organizacional que inclui o usuário 1.



TESTANDO: Ao acessar a máquina teste/cliente com as credenciais do usuário 1 (após fazer o login com sua senha previamente cadastrada), percebe-se que ele não consegue acessar o Painel de Controle.



Porém, ao conectar com usuário 2 (outro usuário de teste), o mesmo, consegue acessar normalmente o painel de controle, pois não está vinculado a esta política:



Dados gerais:

ongquatropatas\Admin
ongquatropatas\nathalia
ongquatropatas\usuario1
ongquatropatas\usuario2
IP público AD: 34.233.0.194

6.2 DNS:

Os DNS foram feitos na nuvem através do Route 53:

DNS do site:

Nome do registro: "ongquatropatas.com- Este é o nome do domínio para o qual foi configurado o registro.

Tipo de registro: "A- Este é o tipo de registro que roteia o tráfego para um endereço IPv4, adequado para direcionar o tráfego do domínio para o servidor onde o site está hospedado.

Valor: O endereço IP do servidor onde o site está hospedado. Isso indica aos resoluvedores DNS para onde direcionar o tráfego quando alguém acessa "ongquatropatas.com".

TTL (Time to Live): valor padrão.

Política de retorno: "roteamento simples", significa que o tráfego será roteado diretamente para o endereço IP especificado no registro A.

Testando registro:

Conforme mostrado: nenhum erro na configuração.

6.3 Servidor FTP:

O servidor foi implementado em uma máquina virtual no serviço EC2 da AWS, rodando uma distribuição ubuntu.

O serviço usado para implementar o FTP foi o VSFTPD:

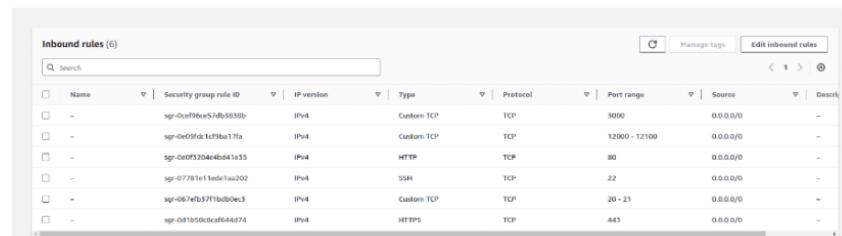
```
ubuntu@ip-172-31-81-176:~$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2024-04-25 16:28:59 UTC; 4min 41s ago
       PID: 447 (vsftpd)
      Tasks: 3 (limit: 1121)
     Memory: 2.4M
        CPU: 121ms
       CGroup: /system.slice/vsftpd.service
               └─ 447 /usr/sbin/vsftpd /etc/vsftpd.conf
                  ├─ 1717 /usr/sbin/vsftpd /etc/vsftpd.conf
                  ├─ 1718 /usr/sbin/vsftpd /etc/vsftpd.conf
                  └─ 1719 /usr/sbin/vsftpd /etc/vsftpd.conf

Apr 25 16:28:59 ip-172-31-81-176 systemd[1]: Starting vsftpd FTP server...
Apr 25 16:28:59 ip-172-31-81-176 systemd[1]: Started vsftpd FTP server.
ubuntu@ip-172-31-81-176:~$
```

E as configurações do servidor foram colocadas no arquivo vsftpd.conf (/home/ubuntu/etc/), lá foi especificado o caminho para o arquivo com a lista de usuários que tem acesso ao servidor assim como o caminho para o diretório base dos arquivos do servidor e as devidas permissões de escrita:

```
GNU nano 0.2
#chroot_local_user=YES
#chroot_list_enable=YES
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncFTP" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# Customization
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty. Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
#
# Uncomment this to indicate that vsftpd uses a utf8 filesystem.
utf8_filesystem=YES
#
userlist_deny=NO
userlist_file=/etc/vsftpd/user_list
tcp_wrappers=NO
#
# Shared path
#
local_root=/home/aluno/dados
chroot_local_user=YES
allow_writeable_chroot=YES
write_enable=YES
```

Na máquina virtual foram configuradas as portas de acesso ao servidor, sendo na faixa 20-21 e 12000-12100, ambas foram liberadas tanto na AWS como na instância da VM em si:



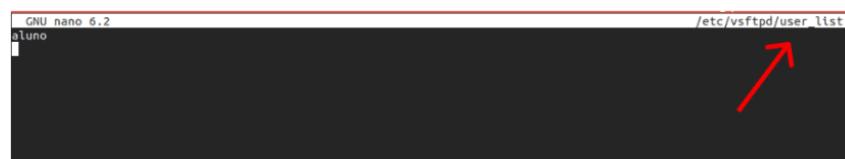
```
ubuntu@ip-172-31-81-176:~$ sudo ufw status
Status: active

To                         Action      From
--                         --          --
20:21/tcp                  ALLOW       Anywhere
12000:12100/tcp             ALLOW       Anywhere
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443                        ALLOW       Anywhere
8080/tcp                  ALLOW       Anywhere
3000/tcp                  ALLOW       Anywhere
20:21/tcp (v6)              ALLOW       Anywhere (v6)
12000:12100/tcp (v6)        ALLOW       Anywhere (v6)
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
443 (v6)                  ALLOW       Anywhere (v6)
8080/tcp (v6)              ALLOW       Anywhere (v6)
3000/tcp (v6)              ALLOW       Anywhere (v6)

ubuntu@ip-172-31-81-176:~$
```

O usuário que foi criado e que recebeu acesso ao servidor foi o usuário aluno, e seu nome foi colocado no arquivo de lista de usuário que possuem acesso ao servidor (`/etc/vsftpd/user_list`):

```
ubuntu@ip-172-31-81-176:~$ cut -d: -f1 /etc/passwd
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
lrc
gnats
nobody
systemd-network
systemd-resolve
messagebus
systemd-timesync
syslog
_apt
tss
uuid
tcpdump
sshd
pollinate
landscape
fwupd-refresh
ec2-instance-connect
_chrony
ubuntu
lxd
ftp
aluno ←
postgres
ubuntu@ip-172-31-81-176:~$
```

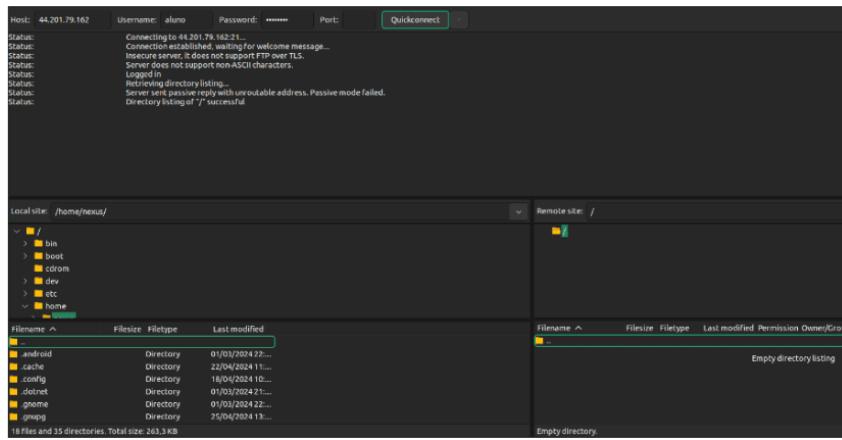


```
GNU nano 6.2
aluno
```

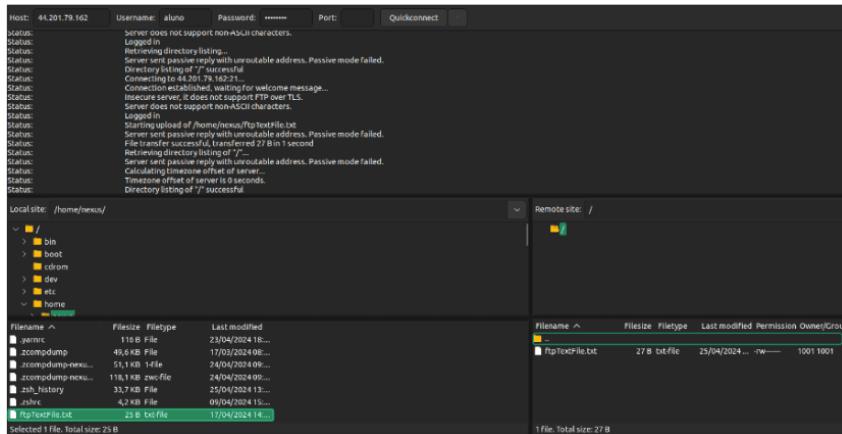
Por motivos de teste todos os arquivos do diretório base do servidor foram excluídos (`/home/aluno/dados/`):

```
ubuntu@ip-172-31-81-176:/home/aluno/dados$ ls
ubuntu@ip-172-31-81-176:/home/aluno/dados$
```

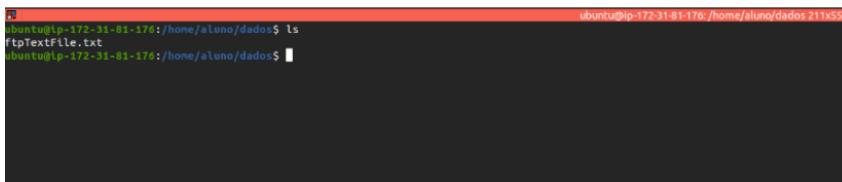
E o acesso ao servidor foi feito por um cliente FTP, nesse caso o Filezilla, utilizando o ip publico da máquina virtual como host e o username e senha do usuário para fazer o acesso:



Logo sem seguida um arquivo de teste foi adicionado ao servidor, o arquivo ftpTextFile.txt e estava localizado na raiz da minha máquina física:



E em seguida os arquivos do servidor foram listados mostrando que a transferência do arquivo ftpTextFile.txt foi feita com sucesso e o arquivo já está armazenado dentro do servidor FTP.



6.4 Servidor HTTP

O servidor de HTTP foi implementado em uma máquina virtual pelo serviço EC2 da AWS, rodando uma distribuição ubuntu.

O serviço usado para implementar o servidor foi o Apache:

```

ubuntu@ip-172-31-81-176:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2024-04-25 21:07:42 UTC; 7min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Process: 1183 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 1187 (apache2)
   Tasks: 55 (limit: 1121)
  Memory: 8.4M
    CPU: 118ms
   CGroup: /system.slice/apache2.service
           └─1187 /usr/sbin/apache2 -k start
             ├─1188 /usr/sbin/apache2 -k start
             ├─1189 /usr/sbin/apache2 -k start
             └─1190 /usr/sbin/apache2 -k start

Apr 25 21:07:42 ip-172-31-81-176 systemd[1]: Starting The Apache HTTP Server...
Apr 25 21:07:42 ip-172-31-81-176 systemd[1]: Started The Apache HTTP Server.
ubuntu@ip-172-31-81-176:~$ 

```

As portas de acesso ao servidor foram liberadas na AWS e na máquina virtual sendo elas:

- Porta 80: HTTP;
- Porta 443: HTTPS;
- Porta 3000: Servidor NodeJS Express da aplicação web.

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sgr-0ef96e575db5353	5000	TCP	0.0.0.0/0	launch-wizard-2	-
-	sgr-0cf9fc1chba1fa	12000 - 12100	TCP	0.0.0.0/0	launch-wizard-2	-
-	sgr-0ef320c6c6bed1fe15	80	TCP	0.0.0.0/0	launch-wizard-2	-
-	sgr-07f81e11ode1aa202	22	TCP	0.0.0.0/0	launch-wizard-2	-
-	sgr-067ffaf371fb0e0e3	20 - 21	TCP	0.0.0.0/0	launch-wizard-2	-
-	sgr-0db50dcuf644d74	443	TCP	0.0.0.0/0	launch-wizard-2	-

```

ubuntu@ip-172-31-81-176:~$ sudo ufw status
Status: active

To                         Action      From
--                         ----      ---
20:21/tcp                  ALLOW      Anywhere
12000:12100/tcp            ALLOW      Anywhere
22/tcp                     ALLOW      Anywhere
80/tcp                     ALLOW      Anywhere
443                        ALLOW      Anywhere
8080/tcp                  ALLOW      Anywhere
3000/tcp                  ALLOW      Anywhere
20:21/tcp (v6)             ALLOW      Anywhere (v6)
12000:12100/tcp (v6)       ALLOW      Anywhere (v6)
22/tcp (v6)                ALLOW      Anywhere (v6)
80/tcp (v6)                ALLOW      Anywhere (v6)
443 (v6)                  ALLOW      Anywhere (v6)
8080/tcp (v6)              ALLOW      Anywhere (v6)
3000/tcp (v6)              ALLOW      Anywhere (v6)

ubuntu@ip-172-31-81-176:~$ 

```

No arquivo 000-default.conf, que possui as configurações do servidor padrão do apache (/etc/apache2/sites-enabled/) foi configurada uma proxy com o ip público da máquina virtual e a porta 3000 que estará rodando a aplicação:

```

GNU nano 6.2                               /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    ProxyRequests Off
    ProxyPreserveHost On
    ProxyVia Full
    <Proxy *>
        Require all granted
    </Proxy>
    ProxyPass / http://3.82.243.238:3000/
    ProxyPassReverse / http://3.82.243.238:3000/
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

```

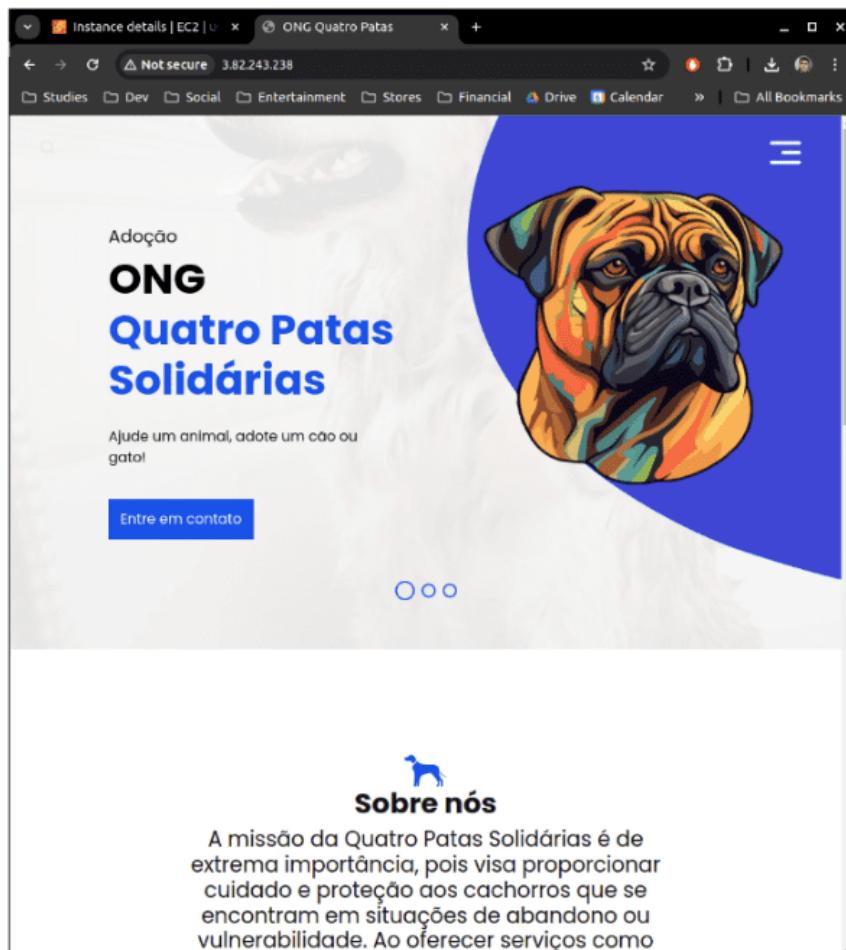
Em seguida o servidor foi iniciado utilizando o NodeJS com a biblioteca Express, que estara apontado para a porta 3000:

```

ubuntu@ip-172-31-81-176:/var/www/html$ ls
app.js  config  models  node_modules  package-lock.json  package.json  public  routes
ubuntu@ip-172-31-81-176:/var/www/html$ sudo /home/ubuntu/.nvm/versions/node/v16.20.2/bin/node app.js
Executing (default): SELECT table_name FROM information_schema.tables WHERE table_schema = 'public' AND table_name = 'animais'
Executing (default): SELECT i.relname AS name, ix.indisprimary AS primary, ix.indisunique AS unique, ix.indkey AS indkey, array_agg(a.attname) AS column_indexes, array_agg(a.attname) AS column_names, pg_get_indexdef(ix.indexrelid) AS definition FROM pg_class t, pg_class i, pg_index ix, pg_attribute a WHERE t.oid = ix.indexrelid AND i.oid = ix.indexrelid AND a.attrelid = t.oid AND t.relknd = 'r' AND t.relname = 'animais'
' GROUP BY i.relname, ix.indexrelid, ix.indisprimary, ix.indisunique, ix.indkey ORDER BY i.relname;
Sucesso
Servidor rodando na porta 3000

```

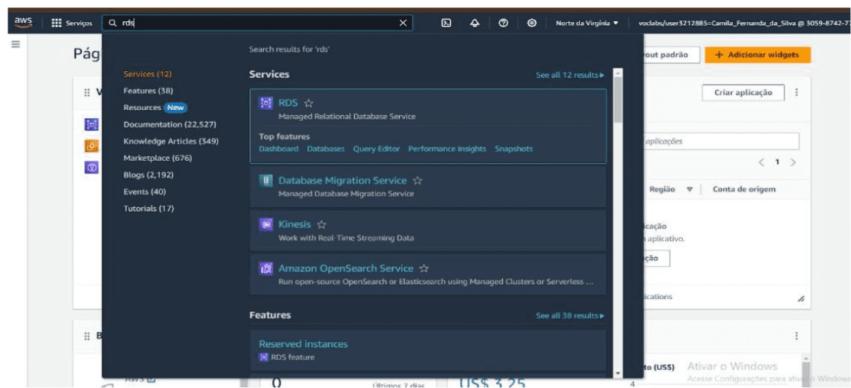
E ao acessar o ip público da máquina virtual na porta 3000 podemos visualizar a aplicação rodando:



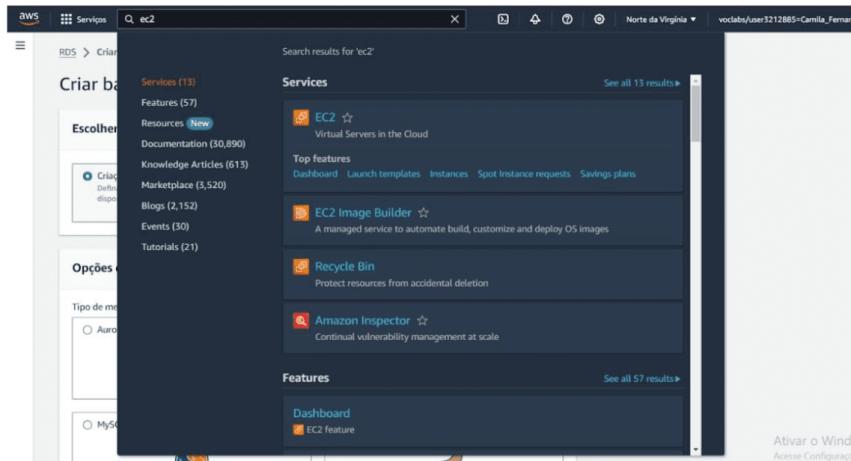
6.5 Criação do Banco de Dados

Para a criação do banco de dados:

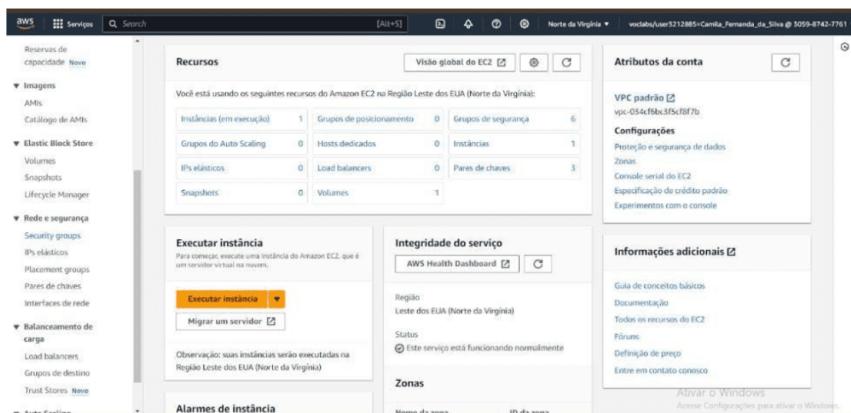
Pesquisou-se por RDS e clicou-se em serviço. RDS é o serviço de banco relacional na AWS;



Antes de se criar o banco, é necessário a criação de um Security Group. O security group é criado na aba de serviços EC2;



Após clicar em EC2, navegue até security group no canto inferior esquerdo;



Posteriormente, ao clicar em security group, clique em criar grupo de segurança;

Grupos de segurança (6) Informações					
	Name	ID do grupo de segurança	Nome do grupo de segurança	ID da VPC	Descrição
	-	sg-03d57cb08b11775e	launch-wizard-4	vpc-034cf6bc3f5cf8f7b	Launch-wiz
	-	sg-0eaab35af4bbab0	launch-wizard-2	vpc-034cf6bc3f5cf8f7b	Launch-wiz
	-	sg-07565b5b9a8678516	launch-wizard-5	vpc-034cf6bc3f5cf8f7b	Launch-wiz
	-	sg-0e079f64dd069c56	Launch-wizard-1	vpc-034cf6bc3f5cf8f7b	Launch-wiz
	-	sg-0783e5a6172e78449	default	vpc-034cf6bc3f5cf8f7b	default VPC

Para criar o grupo de segurança, preencha as informações do formulário;

Um grupo de segurança atua como um firewall virtual para sua instância para controlar o tráfego de entrada e saída. Para criar um novo grupo de segurança, preencha os campos abaixo.

Detalhes básicos
Nome do grupo de segurança <input type="text" value="banco-dos-pintinhos"/>
O nome não pode ser editado após a criação.
Descrição Informações <input type="text" value="acesso ao rds do segundo banco"/>
VPC Informações <input type="text" value="vpc-034cf6bc3f5cf8f7b"/>
Regras de entrada Informações
Este grupo de segurança não tem regras de entrada.
<input type="button" value="Adicionar regra"/>
Regras de saída Informações
<input type="button" value="Ativar o Windows"/>

Adicione uma regra de entrada, escolhendo o banco que vai usar, e quem pode acessá-lo. Feito isso, clique em criar grupo no canto inferior direito;

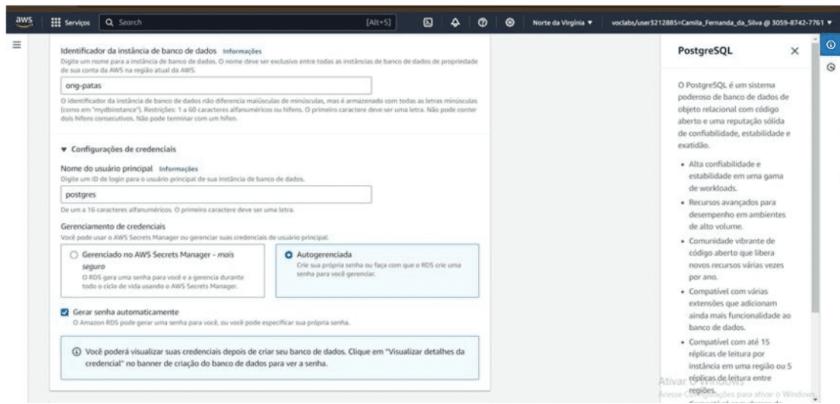
VPC Informações vpc-034cf6bc3f5cf8f7b
Regras de entrada Informações
Tipo <input type="text" value="PostgreSQL"/> Protocolo <input type="text" value="TCP"/> Intervalo de portas <input type="text" value="5432"/> Origem <input type="text" value="Qual..."/> Descrição - opcional <input type="text"/>
<input type="button" value="Excluir"/> <input type="button" value="0.0.0.0 X"/>
<input type="button" value="Adicionar regra"/>
As regras com a origem 0.0.0.0 ou ::/0 permitem que todos os endereços IP acessem a instância. Recomendamos configurar as regras de grupo de segurança para permitir o acesso apenas de endereços IP conhecidos.
Regras de saída Informações
Tipo <input type="text" value="informações"/> Protocolo <input type="text" value="informações"/> Intervalo de portas <input type="text" value="informações"/> Destino <input type="text" value="informações"/> Descrição - opcional <input type="text"/> Ativar o Windows

Procure novamente por RDS em service e clique em banco de dados no canto esquerdo superior e em seguida em criar banco de dados;

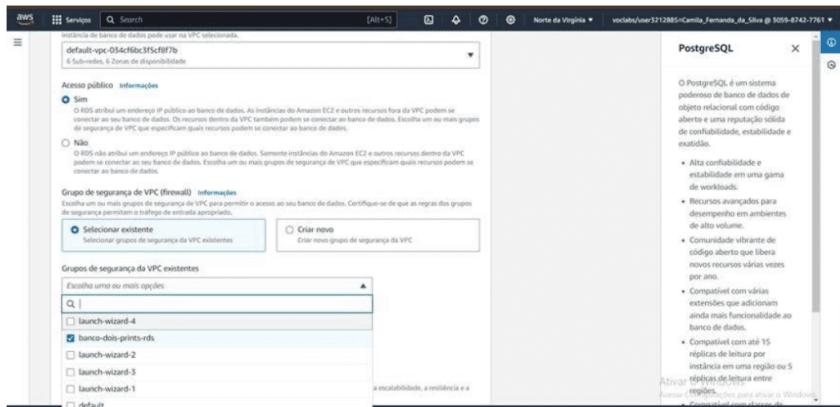
Clique em criar banco padrão;

Escolha o tipo de db a ser utilizado;

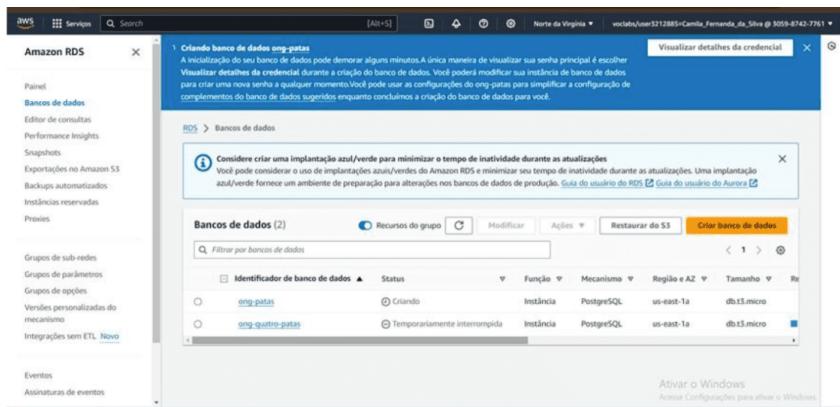
Dê um nome ao banco e marque a opção gerar senha automaticamente;



Marque a opção acesso ao público, selecione o grupo de segurança criado e clique em criar banco no final da página;

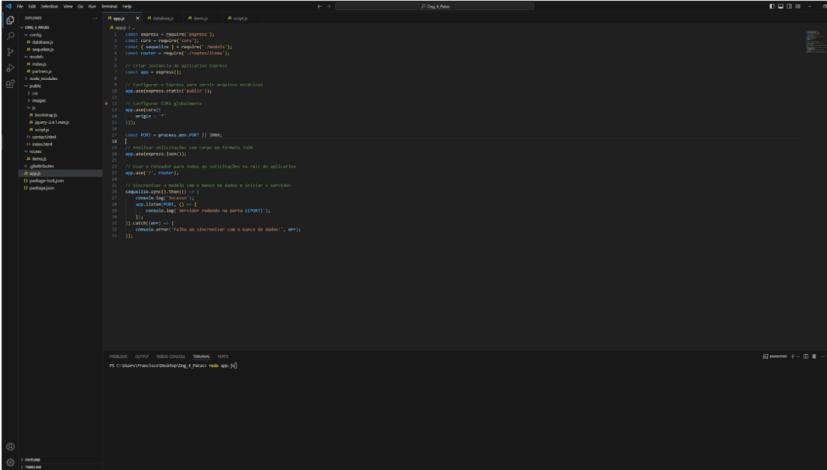


Banco criado.



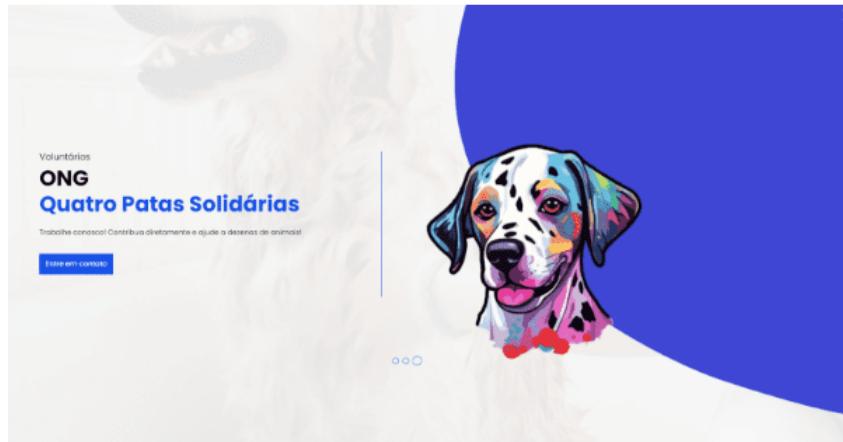
6.6 Aplicação

A aplicação foi criada em node, utilizando express e back-end simples.



```
PS C:\Users\thiago\browsing\Node.js> node app.js
```

O front-end foi feito utilizando javascript com jquery e bootstrap, priorizando recursividade e simplicidade de uso seja mobile ou desktop.



 [Gobba.it](#)

Sobre nós
A missão da Quatro Patas Solidárias é de extrema importância, pois visa proporcionar cuidado e proteção aos cachorros que se encontram em situações de abandono ou vulnerabilidade. Ao oferecer serviços como resgate, castração, vacinação, odontologia, hospitalização, educação e conscientização para o cuidado animal, a organização não apenas ajuda os animais diferentes, mas também trabalha para promover mudanças de mentalidade e comportamento em relação aos direitos dos animais.



 Entre em contato

Visita uma ou mais unidades, adota ou ajuda animais saudáveis, basta preencher o formulário

1083



Entre em contato

Visite uma de nossas unidades, adote ou ajude animais conosco, basta preencher o formulário abaixo!

Quatro Patas Solidárias

Trabalhe conosco! Contribua diretamente e ajude a dezenas de animais!

[Entre em contato](#)

O back-end do código foi feito de maneira a já se conectar com o banco criado na AWS

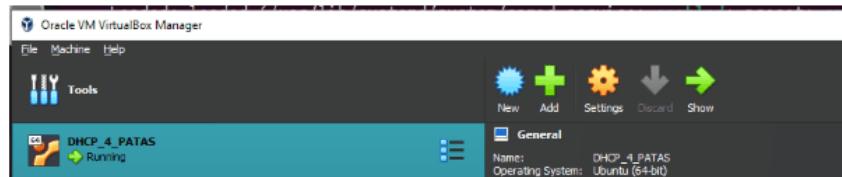
```

module.exports = {
  dialect: 'postgres',
  username: 'postgres',
  password: 'RcJoosonevjs0tXxFiQ',
  host: 'ong-quatro-patas.cyafqex6p0ng.us-east-1.rds.amazonaws.com',
  port: 5432,
  database: 'postgres',
  dialectOptions: {
    ssl: {
      require: true,
      rejectUnauthorized: false
    }
  }
};

```

6.7 Servidor DHCP

O servidor foi implementado em uma máquina virtual local no serviço VirtualBox da Oracle, rodando uma distribuição ubuntu.



Após a VM criada e rodando, eu rodei e configurei o ubuntu da máquina.

Instalando o servidor de dhcp:

```
ubuntu@ip-172-31-31-168: ~
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sun Apr 28 09:54:55 2024 from 190.52.73.230
ubuntu@ip-172-31-31-168:~$ sudo apt install isc-dhcp-server
```

Acessando dados da máquina através do ifconfig.

```
ubuntu@ip-172-31-31-168: ~
Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sun Apr 28 09:47:52 2024 from 190.52.73.230
ubuntu@ip-172-31-31-168:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 172.31.31.168 netmask 255.255.240.0 broadcast 172.31.31.255
        inet6 fe80::8ff:ffff%enp0s3 brd ff:ff:ff:ff:ff:ff scopeid 0x20<link>
            ether 0a:ff:f0:47:3b:3f txqueuelen 1000 (Ethernet)
            RX packets 28844 bytes 32902768 (32.9 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 7853 bytes 912557 (912.5 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 272 bytes 29688 (29.6 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 272 bytes 29688 (29.6 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
ubuntu@ip-172-31-31-168:~$
```

Configurando com o nano o servidor DHCP com os dados do ifconfig.

```
esx ubuntu@ip-172-31-31-168: ~
GNU nano 7.2                               /etc/dhcp/dhcpd.conf
# configuration file instead of this file.
#
# option definitions common to all supported networks...
#
# Configurações globais
default-lease-time 600;
max-lease-time 7200;
authoritative;

# Definição da sub-rede e configurações para a interface eth0
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.100 192.168.1.200;
    option routers 192.168.1.1;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
    option domain-name "ong-4-patas";
    interface en0;
}

# The ddns-updates-style parameter controls whether or not the server will

^G Help          ^O Write Out   ^W Where Is   ^K Cut           ^T Execute      ^C Location    M-U Undo
^X Exit          ^R Read File   ^Y Replace    ^U Paste         ^J Justify     ^V Go To Line  M-B Redo
                                         ^P Paste       ^L Location   ^A Set Mark
                                         ^M Copy
```

Iniciando o servidor pela primeira vez.

Configurando para que o servidor DHCP fosse ligado na inicialização da máquina.

```
ubuntu@ip-172-31-31-168:~  
3 updates can be applied immediately.  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
last login: Sun Apr 28 09:47:52 2024 from 190.52.73.230  
ubuntu@ip-172-31-31-168:~$ ifconfig  
enX0: flags=4163UP,BROADCAST,RUNNING,MULTICAST mtu 9001  
    inet 172.31.31.168 brd 172.31.31.255 netmask 255.255.240.0 broadcast 172.31.31.255  
        inet6 fe80::8ff:fffffe47:3b3f brd fe80::ff:fffffe47:3b3f prefixlen 64 scopeid 0x20<link>  
        ether 0a:ff:ff:04:47:3b brd 0xffffffffffffffff</ether>  
        RX packets 28844 bytes 32982768 (32.9 MB)  
        RX errors 0 dropped 0 overruns 0 frame 0  
        TX packets 7853 bytes 912557 (912.5 KB)  
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73UP,LOOPBACK,RUNNING mtu 65536  
    inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0  
        inet6 ::1 brd ::1 prefixlen 128 scopeid 0x10<host>  
        loop txqueuelen 1000 <local loopback>  
        RX packets 272 bytes 296888 (29.6 KB)  
        RX errors 0 dropped 0 overruns 0 frame 0  
        TX packets 272 bytes 296888 (29.6 KB)  
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
ubuntu@ip-172-31-31-168:~$ sudo nano /etc/dhcp/dhcpd.conf  
ubuntu@ip-172-31-31-168:~$ sudo systemctl enable isc-dhcp-server
```

Verificando status para constatar que o servidor está funcionando corretamente.

```

Select ubuntu@ip-172-31-31-168: ~
loop txqueuelen 1000 (Local Loopback)
RX packets 272 bytes 29688 (29.6 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 272 bytes 29688 (29.6 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ubuntu@ip-172-31-31-168:~$ sudo nano /etc/dhcp/dhcpd.conf
ubuntu@ip-172-31-31-168:~$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset: enabled)
     Active: active (running) since Sun 2024-04-28 09:30:29 UTC; 26min ago
       Docs: man:dhcpd(8)
   Main PID: 2666 (dhcpd)
      Tasks: 1 (limit: 1130)
        Memory: 3.8M (peak: 4.0M)
         CPU: 10ms
        Group: /system.slice/isc-dhcp-server.service
           └─2666 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf

Apr 28 09:30:29 ip-172-31-31-168 dhcpd[2666]: PID file: /run/dhcp-server/dhcpd.pid
Apr 28 09:30:29 ip-172-31-31-168 dhcpd[2666]: Wrote 0 leases to leases file
Apr 28 09:30:29 ip-172-31-31-168 dhcpd[2666]: Listening on LPF/enx0/0a:ff:f0:47:3b:3f/192.168.1.0/24
Apr 28 09:30:29 ip-172-31-31-168 dhcpd[2666]: Sending on  LPF/enx0/0a:ff:f0:47:3b:3f/192.168.1.0/24
Apr 28 09:30:29 ip-172-31-31-168 dhcpd[2666]: Sending on  Socket/fallback/fallback-net
Apr 28 09:30:29 ip-172-31-31-168 dhcpd[2666]: Sending on  LPF/enx0/0a:ff:f0:47:3b:3f/192.168.1.0/24
Apr 28 09:30:29 ip-172-31-31-168 dhcpd[2666]: Sending on  Socket/fallback/fallback-net
Apr 28 09:30:29 ip-172-31-31-168 dhcpd[2666]: Server starting service.
Apr 28 09:43:26 ip-172-31-31-168 dhcpd[2666]: DHCPREQUEST for 172.31.31.168 from 0a:ff:f0:47:3b:3f via enx0: unknown le
lines 1-21/21 (END)

```

6.8 Software de comunicação e Serviço de e-mail

6.8.1 servidor Windows

NOME: Win_SignalR

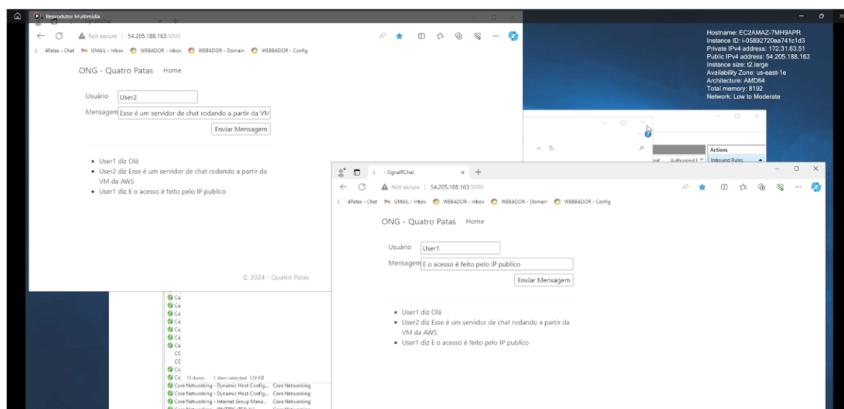
ID: i-05892720aa741c1d3

IPv4 PUBLICO: 54.205.188.163

ACESSO: ec2-54-205-188-163.compute-1.amazonaws.com

Administrator

O-EgffNmRyfa@lU=xHgzft8ZmPR2ukb?



6.8.2 Servidor Linux

NOME: Servidor_Email

ID: i-09f2c3ecdafb39adf

IPv4: 34.239.192.85

ACESSO: ssh -i "PostFix.pem" ubuntu@ec2-34-239-192-85.compute-1.amazonaws.com
ubuntu

—BEGIN RSA PRIVATE KEY—

MIIEpQIBAAKCAQEA8UCtIKXKEZVBLc8Rg9KBSoKjLHykRzTUJCNeaLyl7YY4YkEA
IDI9DUMbEPisslc of U8xvgoBz3RTh0DLod3vigawCEWyCnegj/834bjF1Sm2L90r3JIZ+ZMDW8oM/
aQ2fbtylRAK1D1WcCTG1C61zsXSAK7UH8CJ447tnrus4PWweKC6OgEA5P/wAfx0c QsyYoPjwZH
37exUC6t9FxXNgSWcC6uy2pw91ji0B/68TEgKwIDAQABoIBAQDnci3liUfvUGpE YUgjWBs-
zeVrDvhv4OCVhOhFDl9/znHWRRV0hz4SkqYFY6cj8GwO8G/LTp1QPS0Er G61/76PznfDZLsvcoC

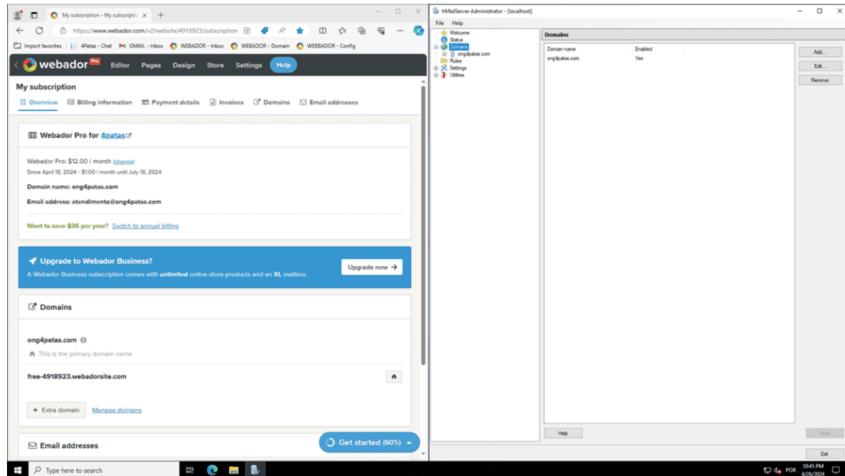
7CG7hO8DxGf9ZQDes7/GrjDe81tvmV5LHc5NjljEtZSTJbDVTSD393yw6WjHcPiX pcJ1VgbizCz8lzl
 iLDd04LtQhm6rq+TBM8ZzPS1tHUBBnuYSFZ2F1+IKdS7Xot/a4S0xNRgGe5uzOtV OVy0PzRxAc
 Pkh1joas6wfss8q56UWTQcJUUZfkCg7C8BqUXqZ3Rza0ajs6lCoOAoqKvwnNxDnj6 NnOqtB-
 GinfoFFCSdJrl76s00A39k3mn/NbmUwxUApLJ6euxHBksXcppDAoGBAPKq x8jQfvx0DKXnNrLQ
 kI6+vfrhj0hhpHi8GOfZEQkvvLQF/1U+jnJru3eocvsJo0iOdrLPoIfEP7VoQLb BoRGamL-
 NiNbsq+/3eg2COTV0Fa59u54hVZT4hc5AoGBAOcYO/vH2p+HoUsekan+ CJmDFIWQ9lPmroefQ
 oCpCVr9oxycqMNufETIujnglrWTen3mSGSdl9SOeOTvwqJ2mZKc/sbCqbhKbEKnG po3gWlMTxni
 s3wmGDn0htwwRjZrM2J4ut+YDrWSURKrsguvWI6/3yve7WGrzo1ANv/QJ78AzsHJ cyu5L7pjiNW
 XZkr8p/JAoGANeXJLWw5N8ovzwks3a4RqHQNI4RIADmPxkZSAMWArWVMVWQkb28z
 24oDs0NUlzATVd3BgcsIRUbT6fSpbfcpbcB5orpY/T9TUJEOGU0pZTbfHJ4MXH/H W7B3Q9Kbt5

—END RSA PRIVATE KEY—

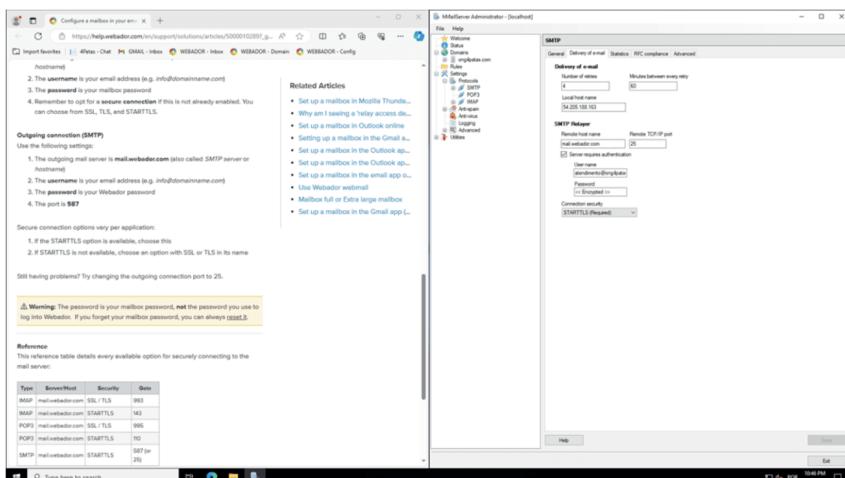
FALHA NO SERVIÇO DE EMAIL

Foram feitas duas tentativas de implantar um servidor de e-mail utilizando VM's na AWS.

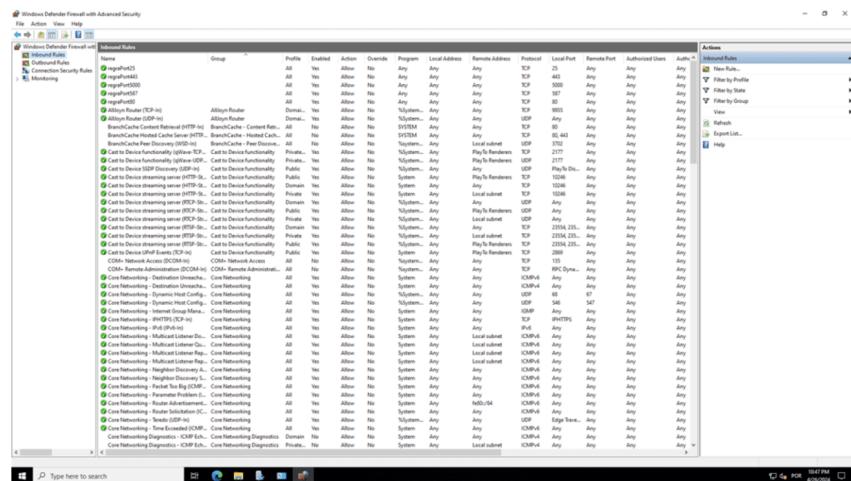
Na primeira tentativa foi utilizando o WINDOWS SERVER e o software HMAIL-SERVER, para a configuração desse servidor foi adquirido um domínio próprio pelo site WEBADOR.



Para a configuração inicial deste servidor foi utilizada a documentação do HMAILSER-VER disponível em: 'https://www.hmailserver.com/documentation/latest/?page=reference_account' também foi utilizada a documentação do WEBADOR disponível em: '<https://help.webador.com/en/>



Além disso foi feito uma configuração adicional no FIREWALL do WINDOWS SERVER para garantir que as portas [25, 80, 443, 587] permitissem todos os acessos e também foi feito essa mesma configuração de porta no grupo de segurança da VM dentro da AWS.



Regras de entrada (8)	Name	ID da regra do grupo...	Versão de IP	Tipo	Protocolo	Intervalo de portas	Origem	Descrição
	sgr-0623237ebe0eaef1	IMAP	IPv4	TCP	143	0.0.0.0/0	-	
	sgr-07a696a71515...	Todo o tráfego	IPv4	Tudo	Todo	0.0.0.0/0	-	
	sgr-03f3f99a1fb828e	HTTP	IPv4	TCP	443	0.0.0.0/0	-	
	sgr-0f0f9afab566e2040	SMTP	IPv4	TCP	25	0.0.0.0/0	-	
	sgr-0e5f919427e765d...	TCP personalizado	IPv4	TCP	587	0.0.0.0/0	-	
	sgr-06b57a6059aa7727	HTTP	IPv4	TCP	80	0.0.0.0/0	-	
	sgr-063702627f5792bd	RDP	IPv4	TCP	3389	0.0.0.0/0	-	
	sgr-06ad940b51ad9b...	TCP personalizado	IPv4	TCP	5000	0.0.0.0/0	-	

Os testes realizados pelo HMAILSERVER não tiveram sucesso, pois é possível acessar o e-mail pela web através do WEBADOR e assim foi comprovado que os envios não chegaram ao servidor, também esse software tem um controle de acesso e envio e o mesmo mostra que não está havendo nenhuma comunicação.

Então foi concluído que mesmo tendo a configuração recomendada algum fator desconhecido impediou a conexão.

A segunda tentativa foi utilizando o LINUX e o software POSTFIX, para a configuração desse servidor foi criado um e-mail gratuito no GMAIL que deveria fazer a ponte com o domínio adquirido no WEBADOR.

Por se tratar de um SO de linha de comando, segue os passos que foram feito:

LINKS DE REFERÊNCIA

https://www.postfix.org/BASIC_CONFIGURATION_README.html

https://www.postfix.org/SMTYPD_ACCESS_README.html

<https://rtcamp.com/tutorials/linux/ubuntu-postfix-gmail-smtp/>

<https://www.youtube.com/watch?v=XbxjYt4bWnw&t=763>

PREPARAÇÃO DO AMBIENTE

1. sudo apt-get update
2. sudo passwd ubuntu > 12345

INSTALAÇÃO DOS SOFTWARES

3. sudo apt-get install postfix mailutils libsasl2-2 ca-certificates libsasl2-modules
4. 'Internet Site' na instalação do POSTFIX
5. 'System mail name' > 'mail.ong4patas.com'

CONFIGURAÇÃO DO POSTFIX

6. sudo vim /etc/postfix/main.cf
7. relayhost = [smtp.gmail.com]:587
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_use_tls = yes

CREDENCIAIS DO GMAIL

8. sudo vim /etc/postfix/sasl_passwd
9. [smtp.gmail.com]:587 ong4PatasEixo5@gmail.com:abcd@1234

PERMISSÕES E CERTIFICADOS

10. sudo chmod 400 /etc/postfix/sasl_passwd
11. sudo postmap /etc/postfix/sasl_passwd
12. sudo /etc/init.d/postfix reload

TESTE

13. echo "Teste de envio1. mail -s \"Olá\"atendimento@ong4patas.com
14. echo "Teste de envio2. mail -s \"Olá\"ong4PatasEixo5@gmail.com

Não houve nenhum erro informado na execução desses comandos, porém quando os testes são feitos de enviar as mensagens, as mesmas não são recebidas no GMAIL. A configuração de segurança dessa VM é do mesmo grupo que foi configurado no WINDOWS SERVER, permitindo acesso livre a todo tipo de conexão.

```
Copyright (C) Microsoft Corporation. Todos os direitos reservados.

Instale o PowerShell mais recente para obter novos recursos e aprimoramentos! https://aka.ms/PSWindows

PS C:\Users\Wallace Sousa\Downloads\VM LINUX> ssh -i "PostFix.pem" ubuntu@ec2-34-239-192-85.compute-1.amazonaws.com
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1080-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Fri Apr 26 23:02:14 UTC 2024

System load: 0.0          Processes:           120
Usage of /: 27.6% of 6.71GB  Users logged in:      0
Memory usage: 2%          IPv4 address for enX0: 172.31.52.205
Swap usage:  0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

You have new mail.

Last login: Fri Apr 26 23:02:16 2024 from 201.17.210.126
ubuntu@ip-172-31-52-205:~$ |
```

```

ubuntu@ip-172-31-52-205:~$ PS C:\Users\Wallace Sousa\Downloads\VM LINUX> ssh -i "PostFix.pem" ubuntu@ec2-34-239-192-85.compute-1.amazonaws.com
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1008-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Fri Apr 26 23:07:23 UTC 2024

System load: 0.0 Processes: 128
Usage of /: 27.6% of 6.71GB Users logged in: 0
Memory usage: 2% IPv4 address for enX0: 172.31.52.205
Swap usage: 0%

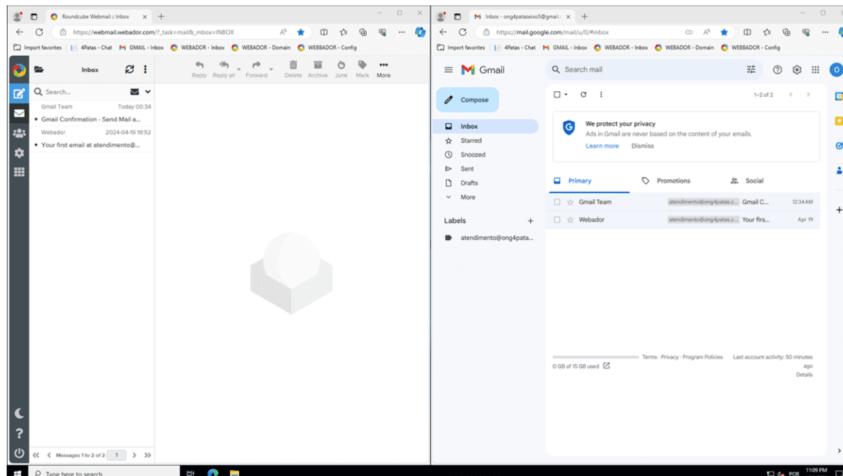
Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

You have new mail.

Last login: Fri Apr 26 23:06:13 2024 from 201.17.210.126
ubuntu@ip-172-31-52-205:~$ sudo vim /etc/postfix/main.cf
ubuntu@ip-172-31-52-205:~$ echo "Teste de envio1." | mail -s "Olá" atendimento@ong4patas.com
ubuntu@ip-172-31-52-205:~$ echo "Teste de envio2." | mail -s "Olá" ong4PatasEixos@gmail.com
ubuntu@ip-172-31-52-205:~$
```



Então foi concluído que mesmo tendo a configuração recomendada algum fator desconhecido impediu a conexão.

6.9 Servidor de aplicação .NET

O servidor utilizou a implementação do Apache para disponibilizar os serviços aos usuários.

Foi realizada a instalação do .Net Runtime no sistema operacional do ubuntu e a configuração do serviço no Apache seguindo as instruções disponibilizadas no site oficial da microsoft disponibilizado para acesso ao final desta sessão.

- Instale o .NET Runtime com os seguintes comandos:

```
sudo apt-get update && sudo apt-get install -y aspnetcore-runtime-7.0
```

```
ubuntu@ip-172-31-20-3:~$ sudo apt-get update && sudo apt-get install -y aspnetcore-runtime-7.0
```

- Instale as dependências:

```
sudo apt install zlib1g
```

```
ubuntu@ip-172-31-20-3:~$ sudo apt install zlib1g |
```

- Verifique se a versão instalada é a desejada
dotnet –version

```
ubuntu@ip-172-31-81-176:~$ dotnet --version  
8.0.103
```

4. Configure o apache:

- Vá ate o diretorio que contenha as configurações
cd /etc/apache2/sites-available

```
ubuntu@ip-172-31-20-3:~$ cd /etc/apache2/sites-available
```

- Crie um arquivo de configurações e escreva-as de acordo com a aplicação desejada
sudo vim NETCORE.conf

```
ubuntu@ip-172-31-20-3:/etc/apache2/sites-available$ sudo vim NETCORE.conf
```

```
<VirtualHost *:*>  
    RequestHeader set "X-Forwarded-Proto" expr=%{REQUEST_SCHEME}s  
</VirtualHost>  
  
<VirtualHost *:80>  
    ProxyPreserveHost On  
    ProxyPass / http://127.0.0.1:5000/  
    ProxyPassReverse / http://127.0.0.1:5000/  
    ServerName www.example.com  
    ServerAlias *.example.com  
    ErrorLog ${APACHE_LOG_DIR}/helloapp-error.log  
    CustomLog ${APACHE_LOG_DIR}/helloapp-access.log common  
</VirtualHost>
```

- Salve o arquivo e verifique se o syntax está correto
sudo apachectl configtest

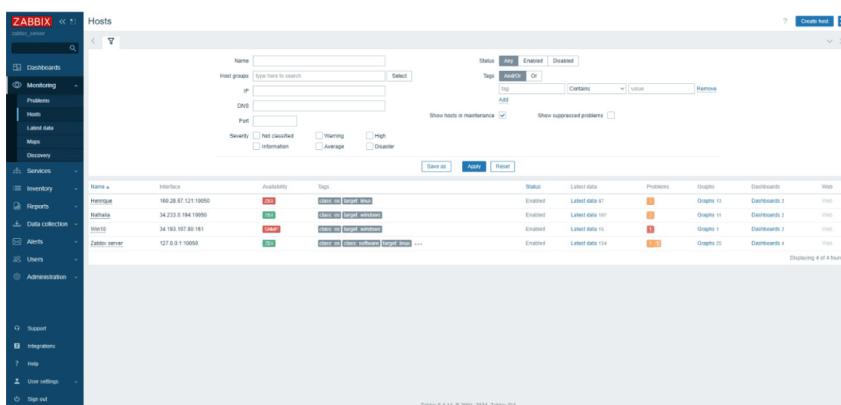
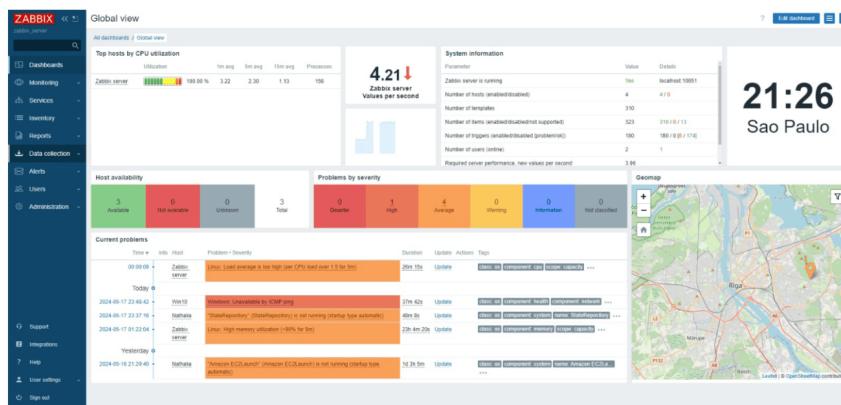
```
ubuntu@ip-172-31-81-176:~$ sudo apachectl configtest  
Syntax OK
```

- Reinic peace o apache
sudo systemctl restart httpd
sudo systemctl enable httpd

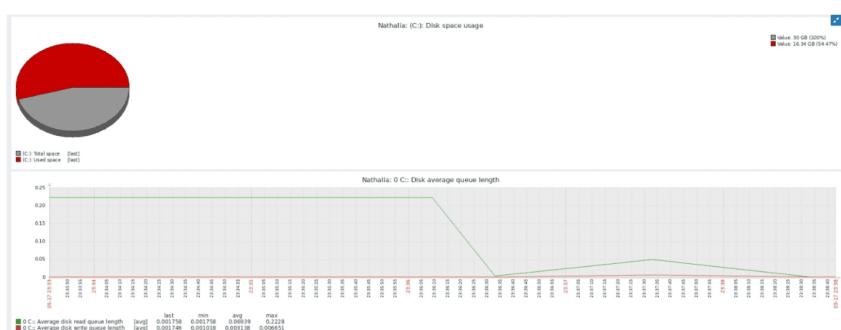
7 MONITORAMENTO DE SERVIÇOS COM O ZABBIX

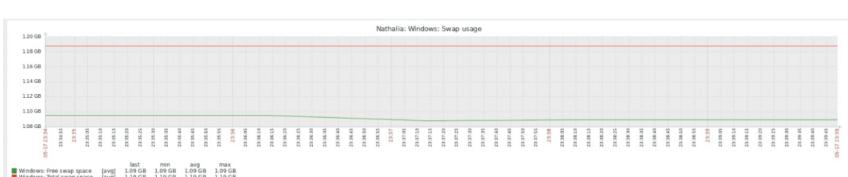
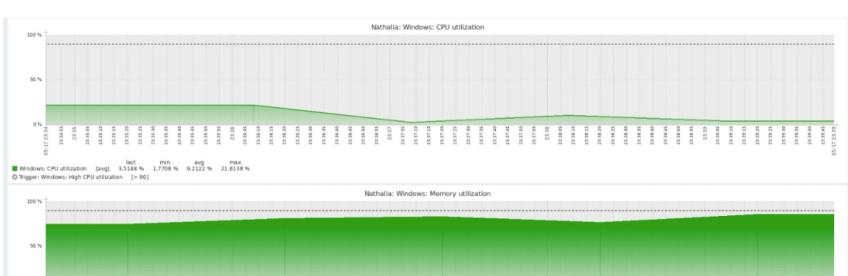
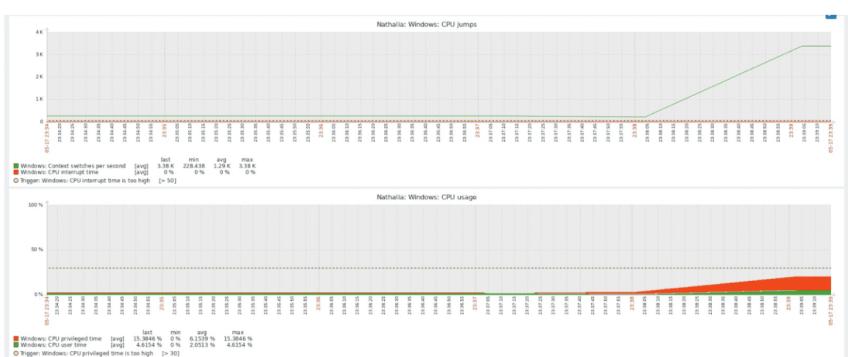
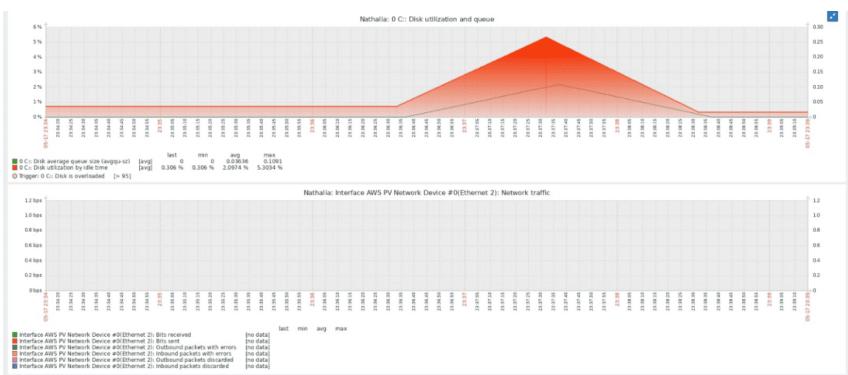
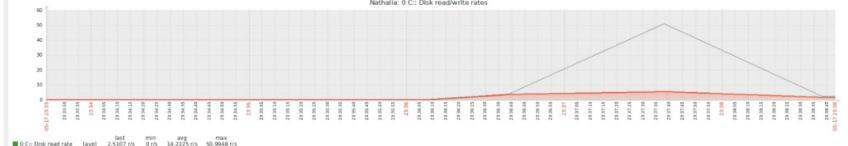
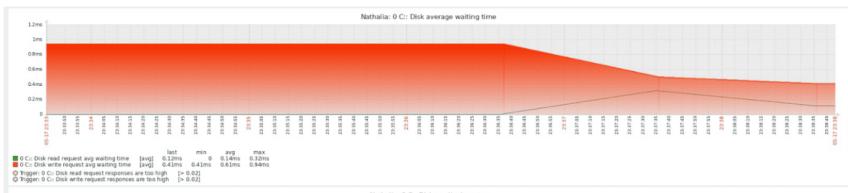
Neste relatório é apresentado gráficos do desempenho e monitoramento dos servidores utilizando o Zabbix. O Zabbix permite monitorar vários aspectos críticos do servidores, como uso de CPU, memória, disponibilidade de serviços e outros parâmetros essenciais.

7.1 Servidores Cloud:

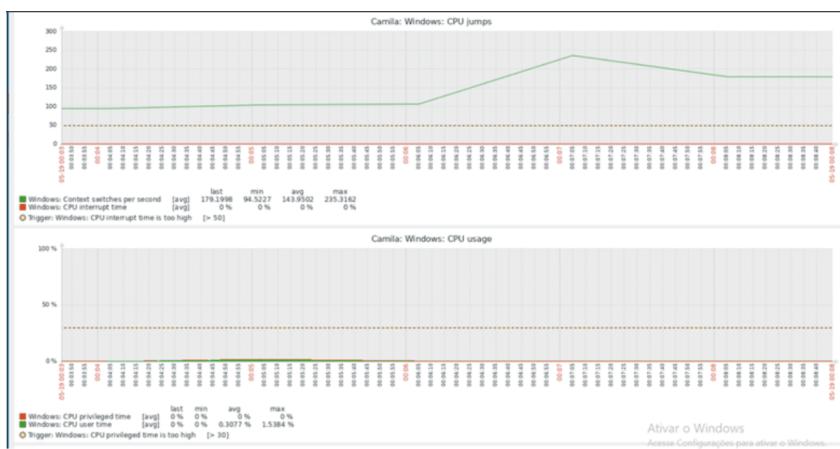
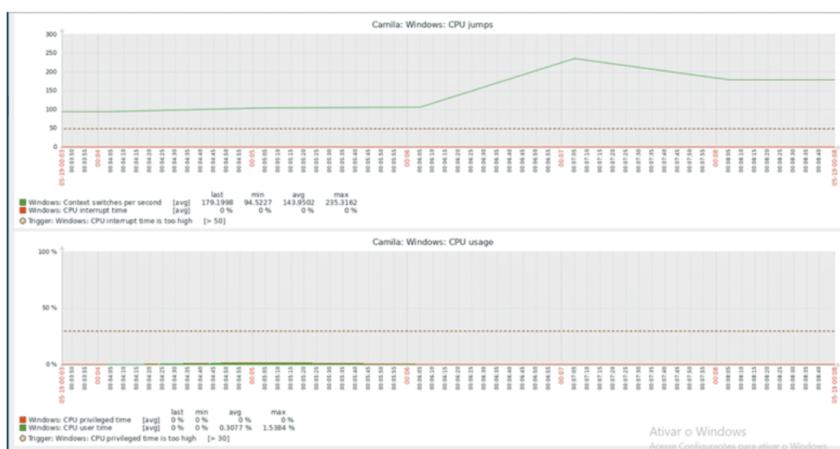
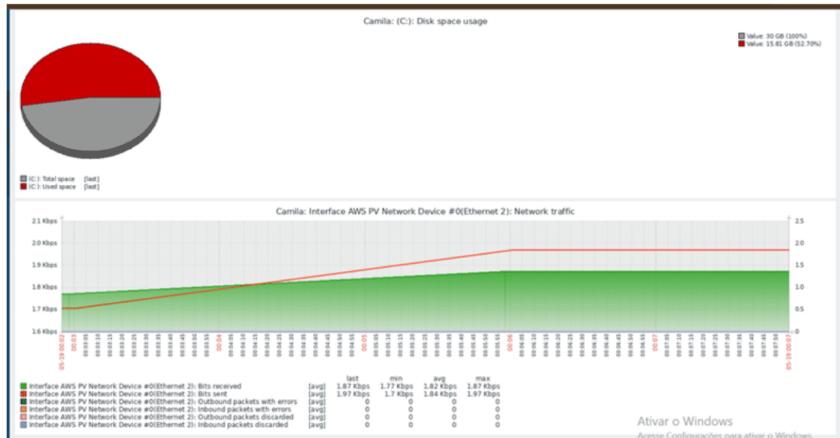


7.2 Servidor AD:

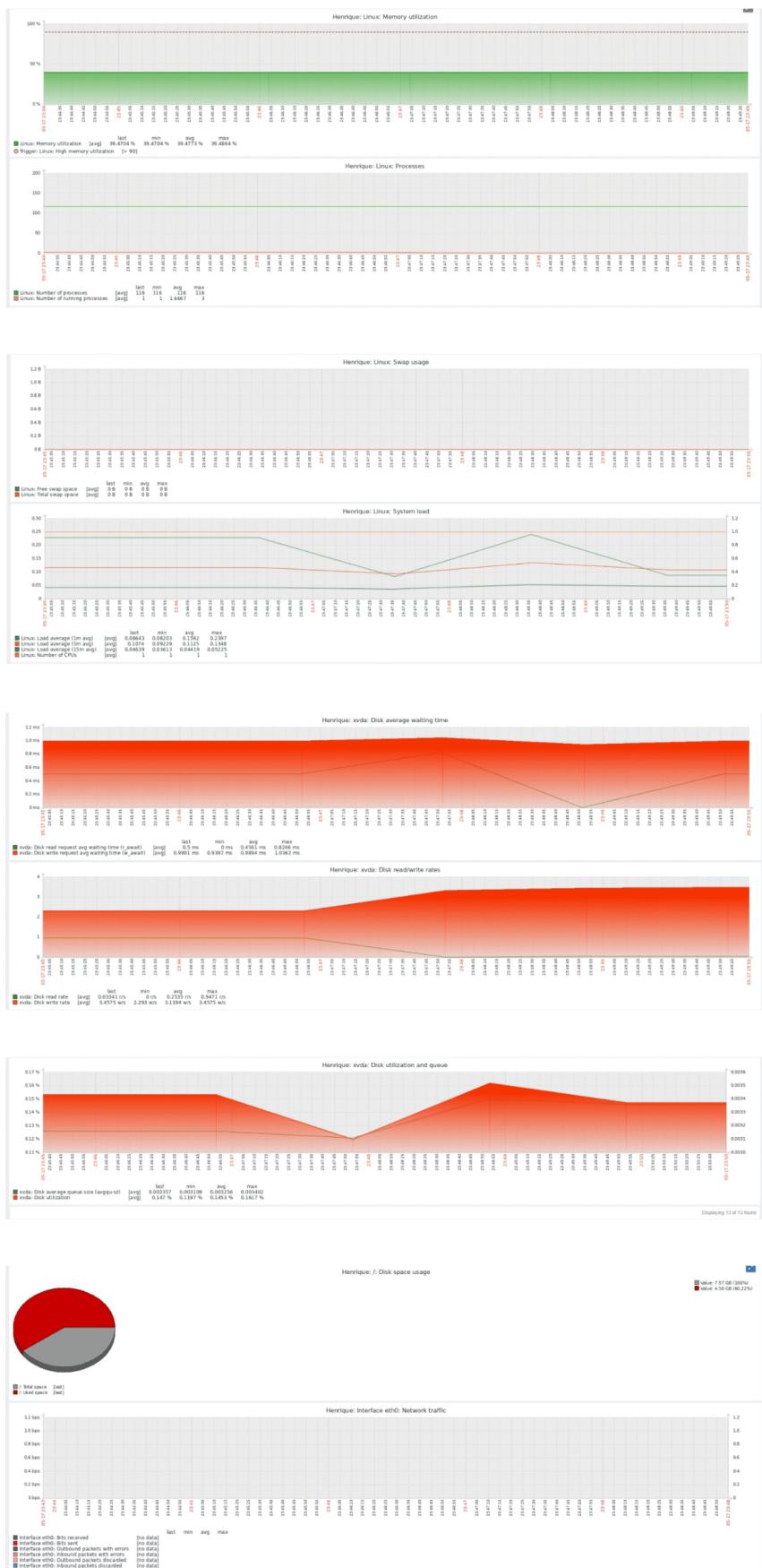


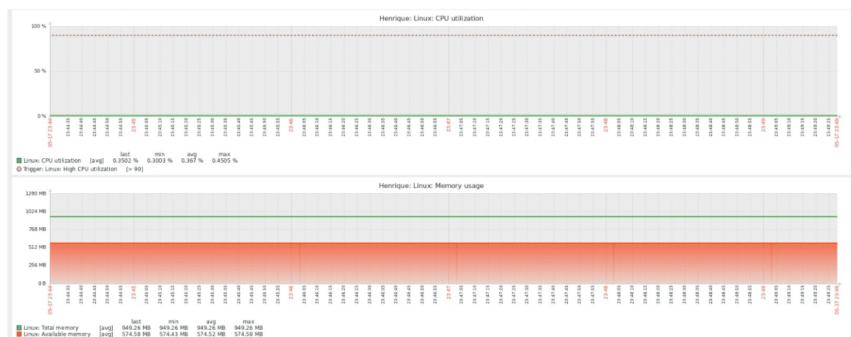
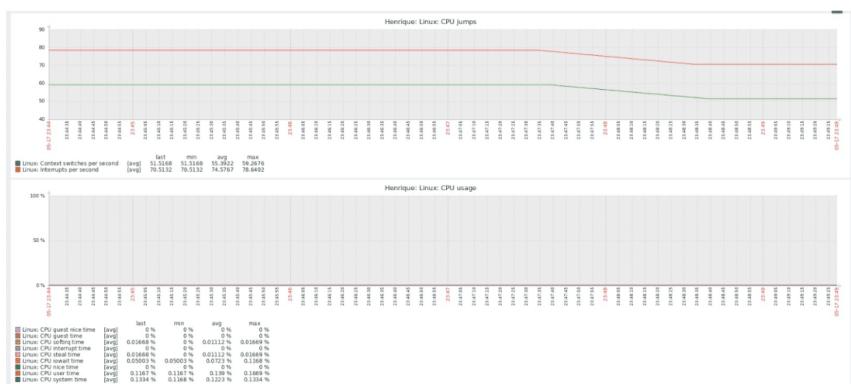


7.3 Servidor Banco de Dados

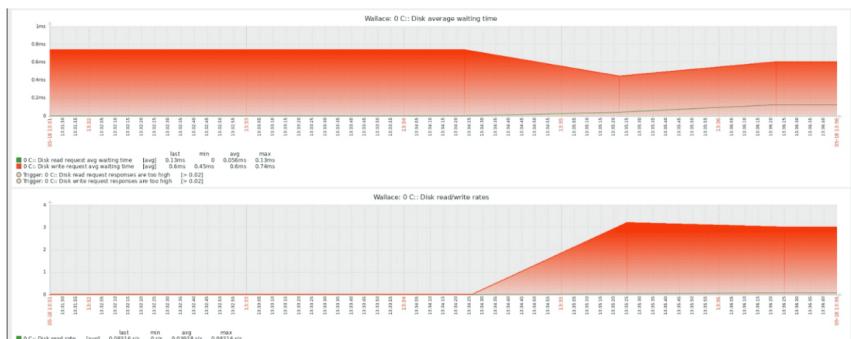
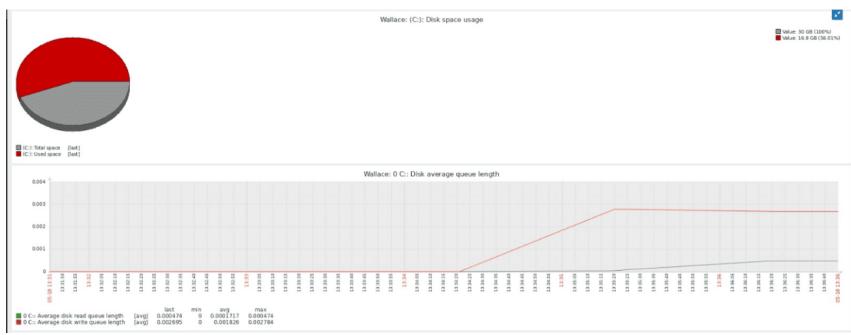


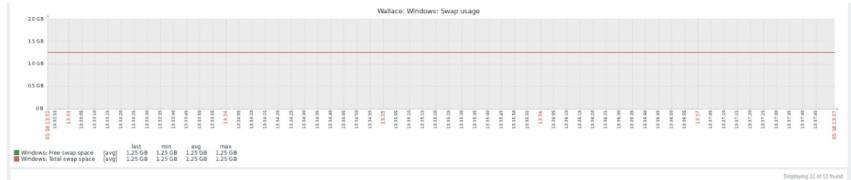
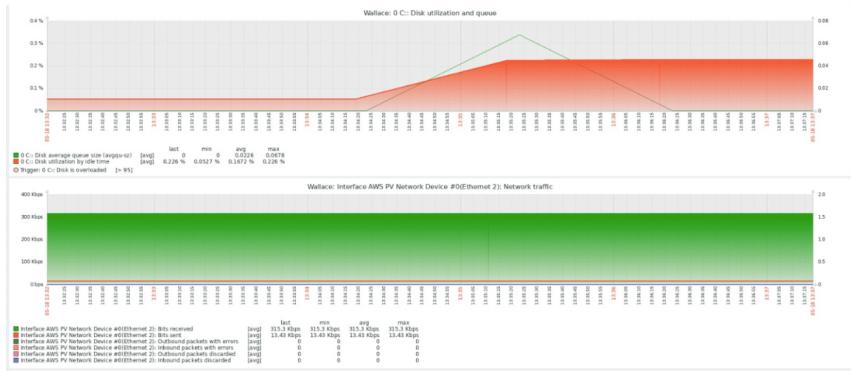
7.4 Servidor Web, FTP e de Aplicação:





7.5 Servidor de Comunicação (Chat)



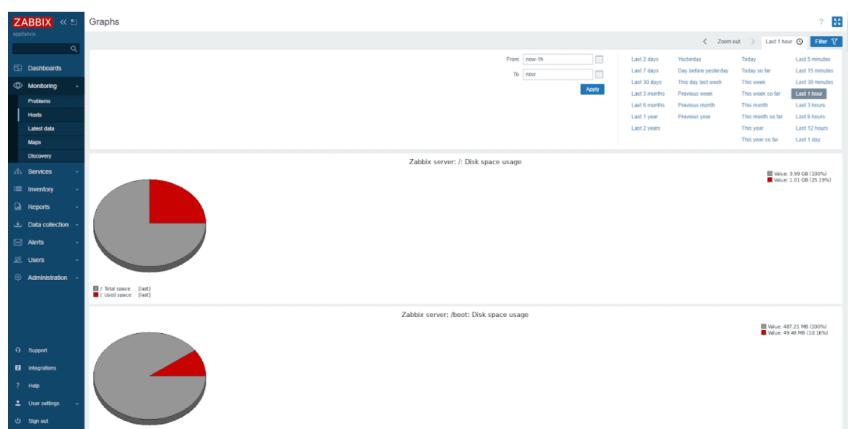


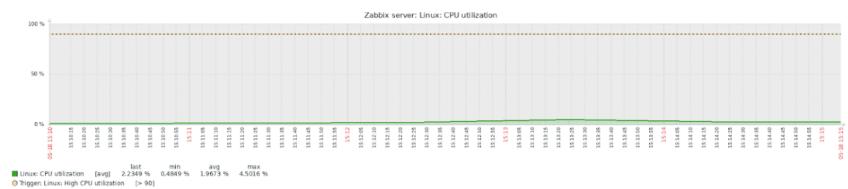
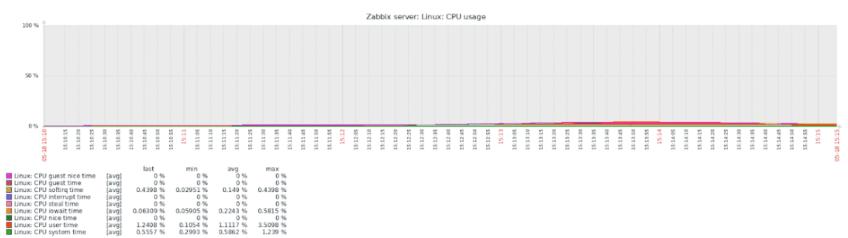
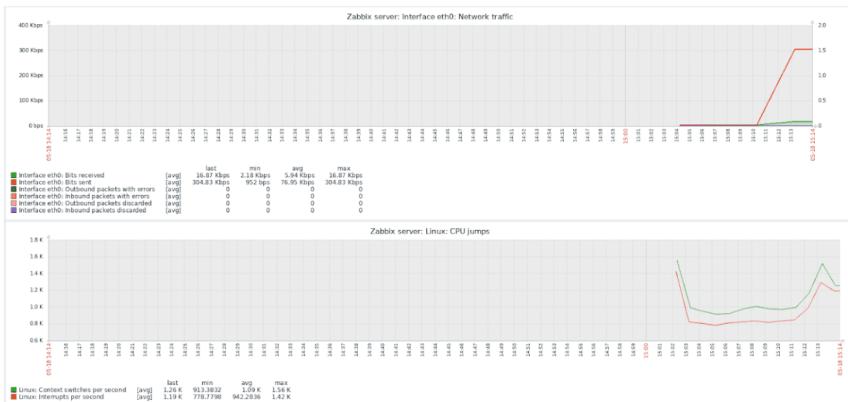
7.6 Servidor Zabbix Local

The screenshot shows the Zabbix Global view dashboard. It includes:

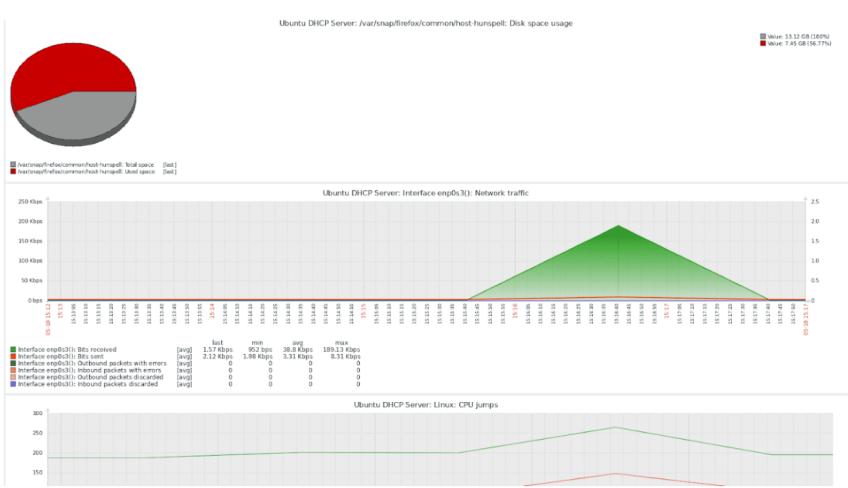
- System information:** Shows Zabbix server is running, last check (seconds) at 1051, and various statistics like number of hosts (210), items (210), triggers (116), and problems (116).
- Host availability:** A chart showing 1 Available, 0 Not available, 0 Unknown, and 1 Total.
- Problems by severity:** A chart showing 0 Critical, 0 High, 0 Average, 2 Warning, 0 Information, and 0 Not classified.
- Current problems:** A table listing two problems:
 - Ubuntu DHCP Server: Linux: Ubuntu DHCP Server has been registered (active > 30m) - Last update: 2024-01-27 12:27:30, Status: Enabled, Actions: 12
 - Zabbix server: Zabbix server has been registered (active > 10d) - Last update: 2024-01-27 12:27:30, Status: Enabled, Actions: 12
- Geemap:** A map of São Paulo showing monitoring points.

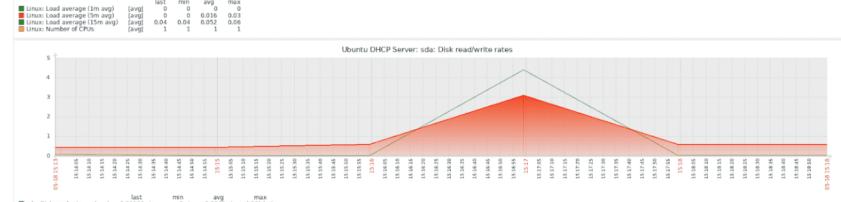
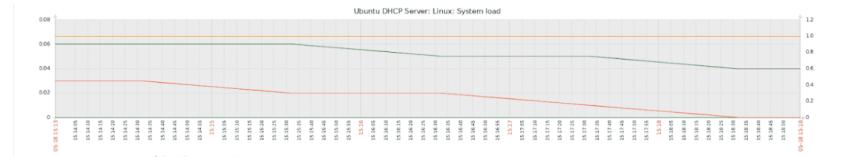
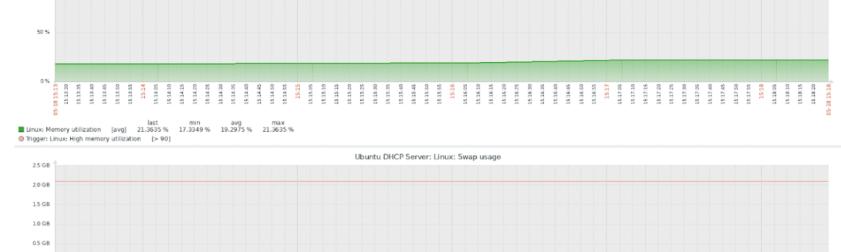
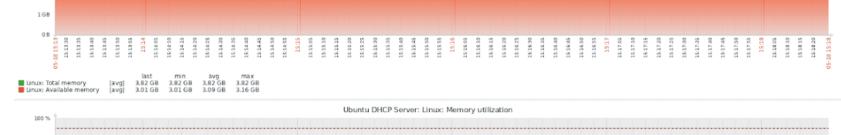
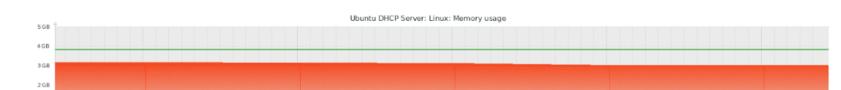
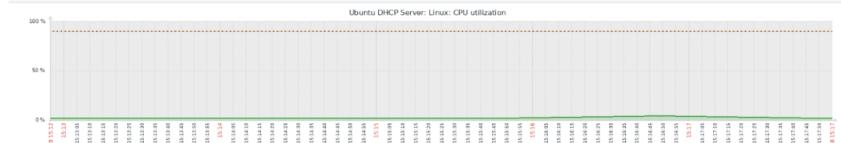
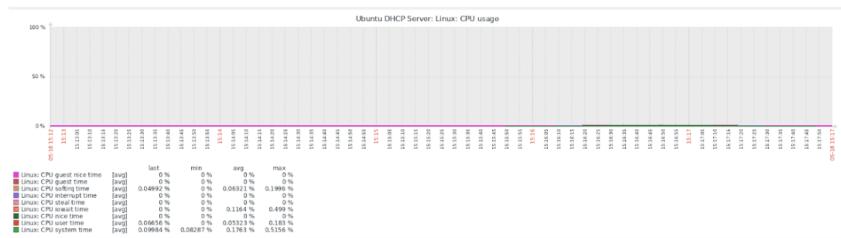
Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashb
Ubuntu DHCP Server	192.168.18.78:161	OK	class: os target: linux	Enabled	Latest data 72	Problems	Graphs 12	Dashb
Zabbix server	127.0.0.1:1050	CRITICAL	class: os class: software target: linux ***	Enabled	Latest data 146	Problems	Graphs 27	Dashb





7.7 Servidor DHCP Local





8 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação ou PSI é um documento que procura estabelecer diretrizes abrangentes, procedimentos e protocolos para proteger ativos digitais, garantir a confidencialidade, integridade e disponibilidade da informação, e mitigar ameaças cibernéticas dentro de uma organização.

Este documento serve como um quadro fundamental para gerenciar riscos cibernéticos e manter um ambiente de computação seguro. Ele descreve as responsabilidades organizacionais, define o uso aceitável de recursos e delimita procedimentos para resposta a incidentes e recuperação.

Suas diretrizes tem como objetivo estabelecer uma cultura de segurança dentro da organização, fornecendo orientação e padrões para proteger contra possíveis ameaças cibernéticas e garantir a resiliência de sistemas críticos e ativos de dados.

9 FOLDER DE SEGURANÇA DA INFORMAÇÃO

Política de segurança da Informação

Objetivo

O objetivo desta política é assegurar que todas as informações da ONG Quatro Patas estejam protegidas contra ameaças internas e externas, garantindo a continuidade das nossas operações e mantendo a confiança dos nossos clientes, parceiros e colaboradores.

A Política de Segurança da Informação tem como propósito orientar e definir todas as diretrizes e responsabilidades da organização, seus colaboradores e parceiros no que diz respeito ao tratamento e à preservação das informações. Ao estabelecer essas diretrizes, buscamos assegurar que as informações sejam gerenciadas de forma segura e eficiente, protegendo dados sensíveis e confidenciais de qualquer tipo de risco.



Abrangência

Esta PSI é um normativo interno, aplicável a todos os colaboradores que venham a ter acesso e/ou utilizarem informações, recursos TIC e demais ativos intangíveis da ONG4P. Este normativo tem valor jurídico e aplicabilidade imediata.

Papéis e responsabilidades

Todos:

É de responsabilidade de todos os colaboradores da ONG4P estar atualizado sobre as políticas de segurança da instituição e auxiliar na instrução de novos membros sobre as mesmas.

Manter sigilo perante a informações confidenciais e seguir as instruções de contenção de riscos em caso de suspeita de ataques cibernéticos à instituição.

Não compartilhar informações internas da instituição.

Colaboradores:

Evitar exposição desnecessária em meios de comunicação pública, tais como redes sociais, das rotinas e procedimentos realizados dentro ou relacionados às atividades da ONG4P.

Não transportar, compartilhar ou mover informações internas da ONG4P e parceiros para fora das dependências da instituição, salvo casos previamente autorizados pelos superiores responsáveis.

Gestores:

É de responsabilidade da diretoria e gestores informar e manter colaboradores, sob a sua responsabilidade, atualizados sobre a política de segurança vigente.

Supervisionar e manter-se informado sobre os procedimentos que possam gerar riscos.

Contribuir ativamente para a investigação de incidentes de segurança da informação

Quatro Patas Solidárias



POLÍTICA DE SEGURANÇA

Aponte o seu celular para o QR code e leia a Política de Segurança da informação completa.



Diretrizes específicas

Internet

O uso da internet na nossa ONG é regulamentado e monitorado para garantir a proteção completa dos dados. É essencial utilizar a internet de maneira responsável, evitando acessar sites não autorizados, baixar conteúdo suspeito e compartilhar informações oficiais sem autorização. O acesso à internet é concedido aos profissionais por meio de uma identidade digital (login e senha) intransferível, sendo o titular o único responsável pelas ações e/ou danos decorrentes do seu uso.

Senhas

Recomendamos aos colaboradores a criação de senhas seguras, que devem conter no mínimo 12 caracteres, incluindo letras maiúsculas e minúsculas, números e símbolos, evitando o uso de informações pessoais facilmente identificáveis. Nossa política exige a atualização periódica das senhas. Lembramos que as senhas são pessoais e não devem ser compartilhadas com ninguém, nem mesmo com outros colaboradores da ONG Quatro Patas, independentemente do cargo.

Redes sem fio

Na ONG Quatro Patas, nossa rede Wi-Fi é exclusivamente para uso profissional e administrativo. Apenas colaboradores autorizados têm acesso, garantindo a segurança dos dados. Visitantes e fornecedores podem acessar mediante autorização prévia. O uso de Wi-Fi público para acessar informações da organização é estritamente proibido, prevenindo potenciais ameaças à segurança.

Email

Para manter a segurança das nossas informações, é importante seguir algumas diretrizes simples:

Evite usar o email da organização para receber promoções ou correspondências pessoais. Não abra emails de remetentes desconhecidos ou suspeitos, e tenha cuidado especial com anexos, especialmente aqueles com extensões incomuns como .EXE, .MSI, .BAT, .CIM, .CMD. Verifique sempre se os sites para os quais você é redirecionado têm conexão segura (HTTPS / ícone do cadeado ao lado da URL). E, por fim, desconfie de arquivos que exigem senha para serem abertos. Todos os colaboradores devem evitar enviar informações sensíveis por email e, quando viável, utilizar criptografia para mensagens contendo dados confidenciais.

Recursos de TI

Os recursos de Tecnologia da Informação da ONG Quatro Patas, incluindo servidores de arquivo, acesso à internet, email e equipamentos individuais, são estritamente destinados ao uso institucional. É fundamental que os colaboradores evitem utilizar esses recursos para fins pessoais. Além disso, é crucial zelar pelo equipamento fornecido pela organização, garantindo sua integridade contra danos e preservando sua segurança contra furtos. Juntos, mantemos nossos recursos operacionais eficientes e protegidos para apoiar nossa missão.

Segurança da Informação

Todos os colaboradores da ONG 4 Patas devem estar cientes das políticas e procedimentos de segurança da informação e seguir as diretrizes estabelecidas para proteger os dados da organização.

É fundamental proteger a confidencialidade, integridade e disponibilidade das informações da ONG, adotando medidas de segurança adequadas e reportando qualquer incidente de segurança à equipe de TI.

Classificação da informação

Para que as informações sejam adequadamente protegidas, cabe ao colaborador realizar a classificação no momento em que for gerada a informação, para garantir a devida confidencialidade, especialmente no caso de conteúdos e dados pessoais.

- Informação pública: informação que pode ou deve ser tornada disponível para distribuição pública. Sua divulgação não causa qualquer dano à instituição e aos profissionais.
- Informação interna: informação que pode ser divulgada para os cliente e profissionais da instituição, enquanto estiverem desempenhando atividades profissionais. Sua divulgação não autorizada ou acesso indevido podem causar impactos institucionais.
- Informação confidencial: informação exclusiva a quem se destina. Requer tratamento especial. Contém dados pessoais e/ou sigilosos, que, se divulgados, podem afetar a reputação e a imagem da instituição ou causar impactos graves, sob o aspecto financeiro, legal e normativo.

Nossa política de segurança da informação define regras claras para o manuseio de dados, adaptadas ao nível de confidencialidade. É de extrema importância que as regras sejam respeitadas para garantir a integridade e a proteção dos nossos dados sensíveis.

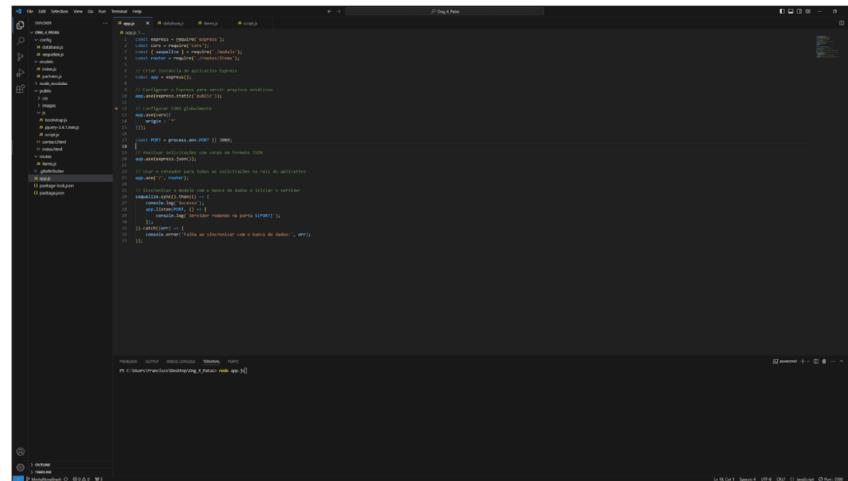
Quatro Patas Solidárias



10 APLICAÇÃO BACK-END

10.1 Implementação

A aplicação foi criada em node, utilizando express e back-end simples.



```

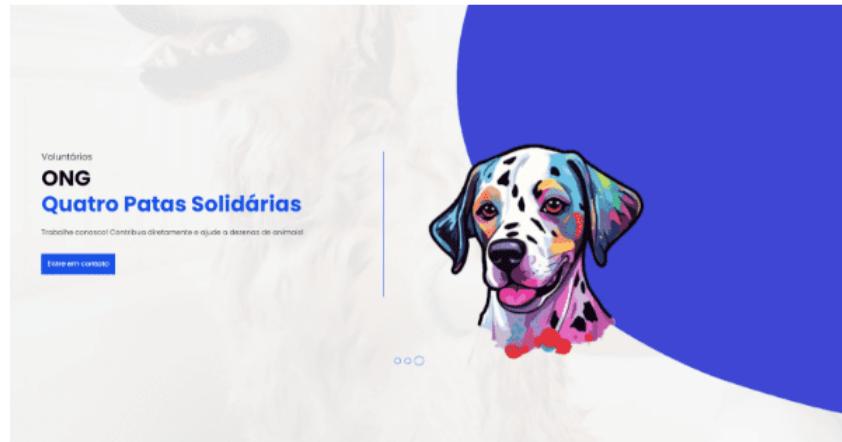
const express = require('express');
const cors = require('cors');
const bodyParser = require('body-parser');
const app = express();
const PORT = process.env.PORT || 3000;

app.use(cors());
app.use(bodyParser.json());

app.get('/quatro-patas', (req, res) => {
  res.send('Olá, mundo!');
});

app.listen(PORT, () => {
  console.log(`Servidor rodando na porta ${PORT}`);
});
  
```

O front-end foi feito utilizando javascript com jquery e bootstrap, priorizando recursividade e simplicidade de uso seja mobile ou desktop.



Sobre nós

A missão da Quatro Patas Solidárias é de extrema importância, pois visa proporcionar cuidado e proteção aos cães que se encontram em situação de vulnerabilidade. A organização trabalha para garantir o resgate, castração, vacinação, adoção, hospedagem, educação e conscientização sobre a causa animal, a organização não apenas ajuda os animais diretamente, mas também trabalha para promover uma mudança de mentalidade e comportamento em relação aos direitos dos animais.



Entre em contato

Visite uma de nossas unidades, adote ou ajude animais conosco, basta preencher o formulário abaixo!

Quatro Patas Solidárias

Trabalhe conosco! Contribua diretamente e ajude a dezenas de animais!

[Entre em contato](#)

O back-end do código foi feito de maneira a já se conectar com o banco criado na AWS

```

module.exports = {
  dialect: 'postgres',
  username: 'postgres',
  password: 'RcJoosonevjs0tXxFiQ',
  host: 'ong-quatro-patas.cyafqex6p0ng.us-east-1.rds.amazonaws.com',
  port: 5432,
  database: 'postgres',
  dialectOptions: {
    ssl: {
      require: true,
      rejectUnauthorized: false
    }
  }
};

```

10.2 Estudo de Vulnerabilidades

Dentre as vulnerabilidades que podem ser encontrada em aplicações back-end com nodeJs destaca-se os ataques de enjeção, tais como SQL Injection, NoSQL Injection e OS Command Injection. Estes ataques ocorrem quando as informações de dados de entrada fornecidas pelo usuário não são devidamente sanitizadas e relazam comandos na base de banco de dados da aplicação ou no próprio sistema operacional.

Identifica-se como outra vulnerabilidade comum a sistemas nodeJS o Cross-Site Scripting ou XSS, neste ataque são inseridos scripts maliciosos em páginas web afetando seus usuários.

Pode-se destacar também a necessidade de proteção de dados sensíveis, tais como senhas e tokens do usuário final, evitando a exposição indevida destas informações. Vulnerabilidades como Server-Side Request Forgery (SSRF) e ataques de negação de serviço (DoS) também representam ameaças significativas, exigindo medidas proativas de mitigação, como implementação de HTTPS, uso de middlewares de segurança e realização regular de auditorias de segurança e testes de penetração.

Recomenda-se também a atualização recorrente de pacotes e dependências de terceiros via npm para correção de falhas se segurança já mapeadas.

11 CONCLUSÃO

O projeto de infraestrutura de rede para a ONG Quatro Patas sublinha a eficácia dos processos implementados para melhorar a operação da organização. A escolha de uma topologia de rede em anel foi fundamental para garantir comunicação eficiente e redundância, enquanto a utilização de servidores hospedados na AWS proporcionou uma plataforma robusta e segura para as aplicações da ONG. A implementação de servidores Apache e NodeJS, juntamente com a configuração de um banco de dados relacional na AWS, assegurou a integridade e disponibilidade dos dados críticos. Adicionalmente, a configuração de servidores DHCP e FTP, bem como a aplicação de políticas de segurança, fortaleceu a segurança e a gestão da rede. Esses processos não apenas otimizaram a infraestrutura tecnológica da ONG, mas também estabeleceram uma base sólida para futuras expansões e melhorias, assegurando a continuidade e eficácia dos serviços prestados.

12 REFERÊNCIAS

AS VULNERABILIDADES mais comuns em aplicações Web: detecção e mitigação. [S. l.], 19 mar. 2024. Disponível em: <https://www.redbelt.com.br/blog/as-vulnerabilidades-mais-comuns-em-aplicacoes-web-deteccao-e-mitigacao/>. Acesso em: 27 jun. 2024

PACKET Tracer. [S. l.], 2024. Disponível em: <https://www.netacad.com/pt-br/courses/packet-tracer/teaching>. Acesso em: 11 mar. 2024.

DOCUMENTATION: These pages are created to help users successfully manage their monitoring tasks with Zabbix, from the simple to the more complex.. [S. l.], 2024. Disponível em: <https://www.zabbix.com/manuals>. Acesso em: 1 maio 2024.