

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

**João Gabriel Alves  
Joao Victor dos Anjos Sales  
Jônatas Fernandes Ferreira  
Kelly Marques  
Marco Willy Azevedo Gomes  
Thiago Vinicius Costa Guimaraes**

**PROJETO DE INFRAESTRUTURA DE REDES - UNIVERSIDADE PROGRESSUS**

Belo Horizonte  
2024

**João Gabriel Alves**  
**Joao Victor dos Anjos Sales**  
**Jônatas Fernandes Ferreira**  
**Kelly Marques**  
**Marco Willy Azevedo Gomes**  
**Thiago Vinicius Costa Guimaraes**

## **PROJETO DE INFRAESTRUTURA DE REDES - UNIVERSIDADE PROGRESSUS**

Trabalho apresentado como requisito parcial à  
aprovação na disciplina Projeto: Projeto da  
Infraestrutura de Rede - Turma 01 - 2024/1

Professor(a):

Fabio Leandro Rodrigues Cordeiro

Belo Horizonte  
ano

## SUMÁRIO

<b>1. INTRODUÇÃO</b>	4
1.1. Proposta	4
1.2. História	4
1.3. Tamanho da Empresa	4
1.4. Serviços	5
1.5. Infraestrutura	5
1.6. Projeto Packet Tracer	6
<b>2. SERVIÇOS</b>	7
2.1. Serviços On Premises	7
2.1.1. DHCP	7
2.1.2. AD/DNS	12
2.2. Serviços em Nuvem (AWS)	22
2.2.1. SMTP	23
2.2.2. WEB/APLICAÇÃO	27
2.2.3. PROXY	36
<b>3. MONITORAMENTO DE RECURSOS</b>	52
3.1. Monitoramento On Premises	52
3.1.1. Servidor AD/DNS	
3.1.2. Estações de Trabalho	
<b>4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>	65
4.1. PSI UNIVERSIDADE PROGRESSUS	65
4.2. CARTILHA PSI	76

## **1. INTRODUÇÃO**

Um novo campus de uma Faculdade na Região Metropolitana de uma das capitais do país

### **1.1. Proposta**

A proposta deste projeto consiste na criação de um sistema de infraestrutura de redes para um novo campus de uma faculdade. A iniciativa surge com o objetivo de trazer uma infraestrutura de redes robusta, inteligente e inovadora que promova uma experiência acadêmica excepcional. Tal infraestrutura se tornará não apenas um facilitador tecnológico, mas um pilar essencial na construção do conhecimento, e melhoria das atuais demandas que vem com a criação de um novo campus de faculdade.

### **1.2. História**

Havia uma cidade na Região Metropolitana de Belo Horizonte, onde os alunos que migravam do ensino médio para o ensino superior enfrentavam o dilema de se mudar para outra cidade ou encarar longas horas no trânsito e transporte público para seguir suas perspectivas acadêmicas. Sentindo essa necessidade, Joel Muniz Cabral fundou a filial da Universidade Progressus. O objetivo dessa filial sempre foi proporcionar uma educação holística, integrando disciplinas tradicionais com as mais recentes descobertas em ciência, tecnologia e artes. Os cursos foram desenvolvidos com uma abordagem interdisciplinar, incentivando os alunos a explorar conexões entre diferentes campos do conhecimento. A infraestrutura de redes foi pensada para ser a mais moderna e eficaz possível, aprimorando a experiência acadêmica.

### **1.3. Tamanho da Empresa**

A universidade conta com a sede localizada na capital de Minas Gerais, possui mais 4 unidades espalhadas na região metropolitana de Belo Horizonte, totalizando cerca de 200 funcionários e mais de 1000 alunos que utilizam a infraestrutura da rede.

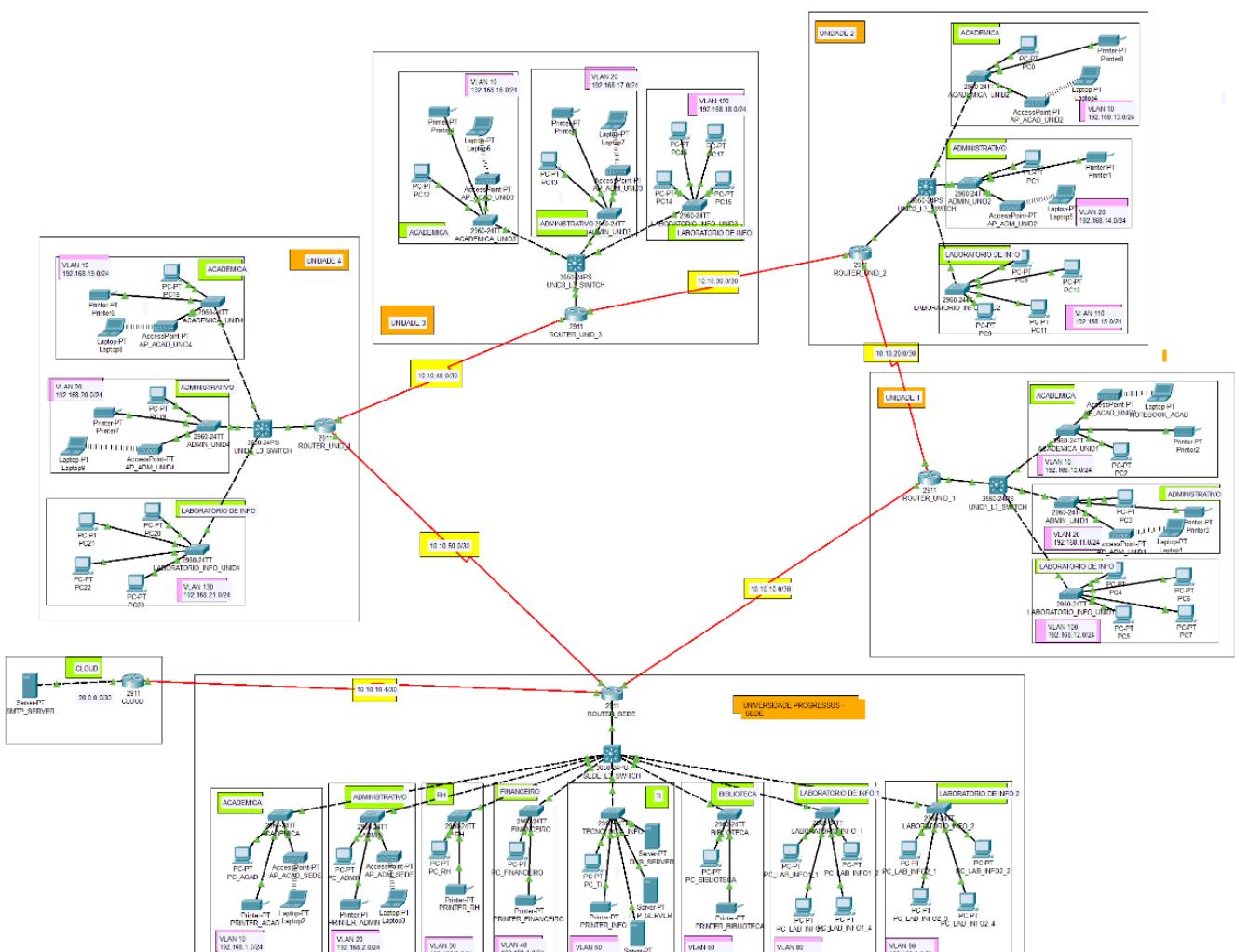
### **1.4. Serviços**

- Portal Web
- Sistema de gestão de Aluno/Estágio
- Sistema de gestão de funcionário
- Aplicativo de gestão de Aluno
- Plataforma ead
- Plataforma de biblioteca física/virtual
- email
- vpn
- domínio
- laboratório de informática
- impressoras
- CCTV/CFTV
- Wi-Fi
- Cartão mifare

## 1.5. Infraestrutura

- Nuvem EC2 -> apache
- office365 web/ exchange
- local/ nuvem (tomcat/apache)
- moodle/canvas
- sistema de node
- dhcp
- vpn
- AD/GPO
- proxy
- dns

## 1.6. Projeto Packet Tracer



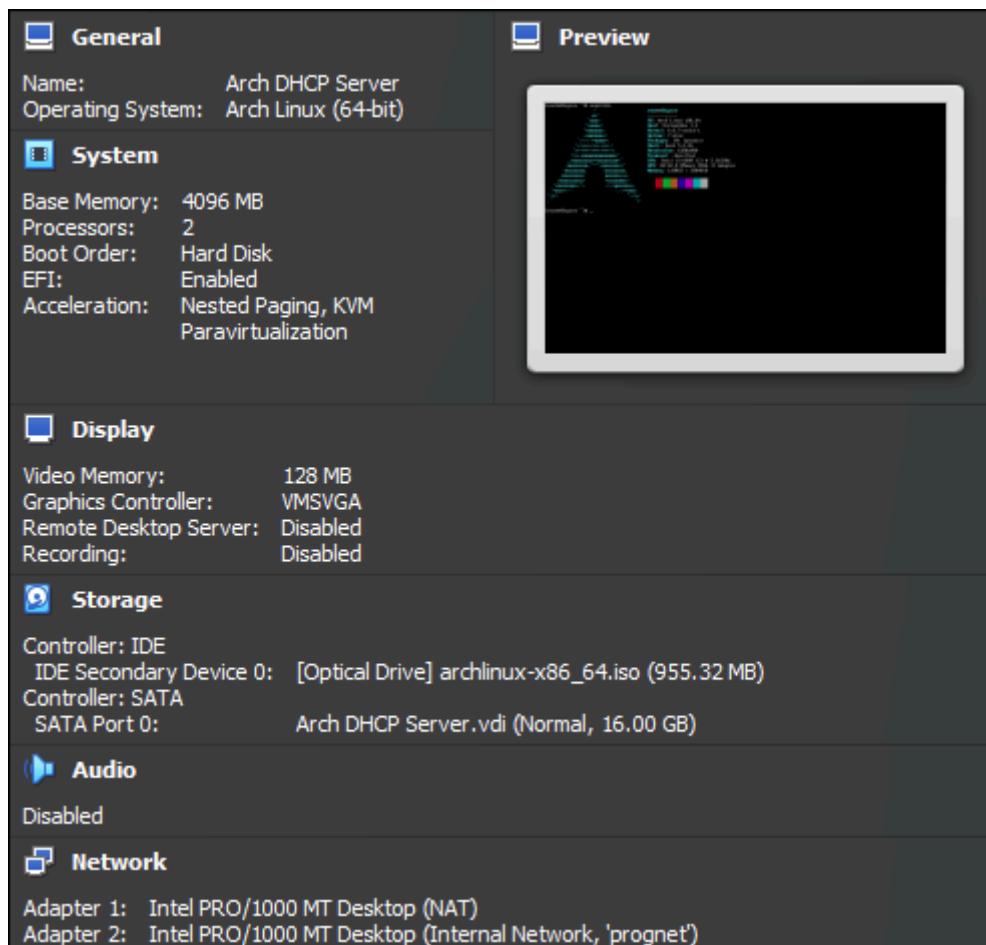
## 2. SERVIÇOS

### 2.1. SERVIÇOS ON PREMISES

#### 2.1.1. DHCP

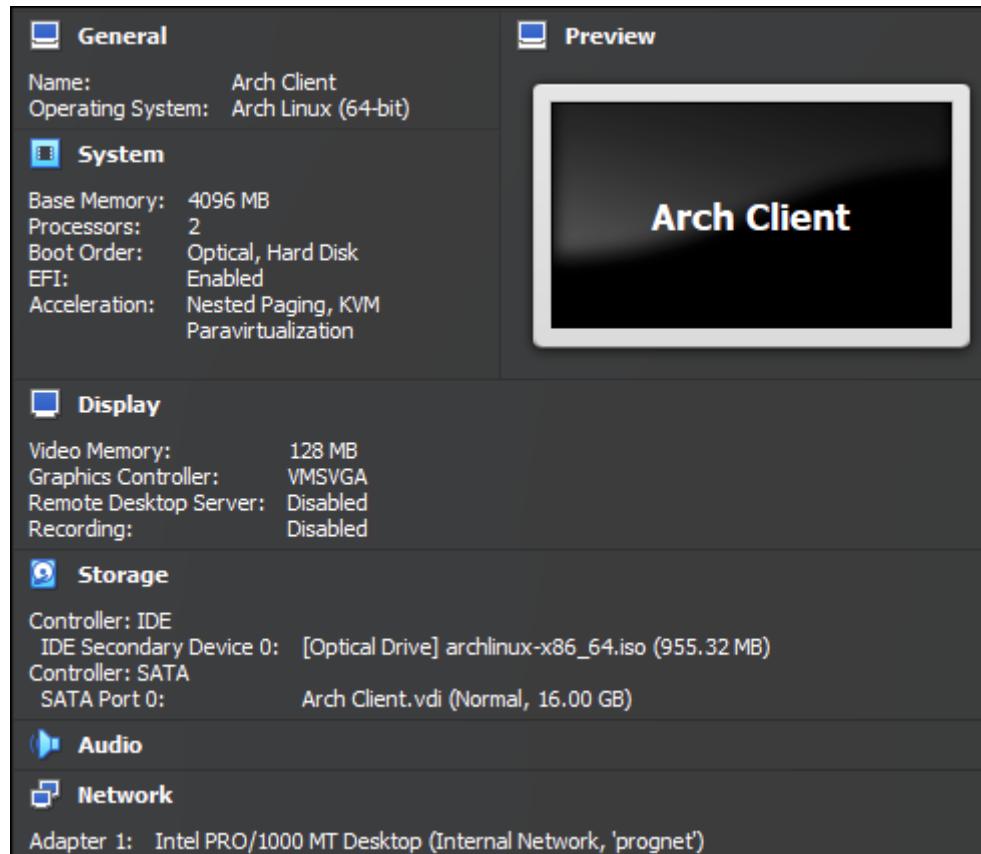
O servidor DHCP será criado no virtual box da Oracle. Abaixo, encontram-se as especificações das VMs utilizadas, a ISO e o software utilizado para servir os IPs na rede interna do VBox.

- VM. Servidor DHCP:
  - Memória 4096 MB / 2 núcleos;
  - Vídeo 128MB;
  - Memória Interna: 16GB;
  - 2 Adaptadores de rede: 1 NAT (para instalação); 1 Interno;



- VM Cliente:
  - Memória 4096 MB / 2 núcleos;

- Vídeo 128MB;
- Memória Interna: 16GB;
- 1 Adaptador de rede: Interno;



Em seguida, tendo nosso Arch Linux já instalado, acessaremos o root ou um usuário (como for da preferência do admin) e iremos para nossa configuração do DHCPD (ISC DHCP

[https://kb.isc.org/v1/docs/isc-dhcp-44-manual-pages-dhcpd#configuration\\_manpages](https://kb.isc.org/v1/docs/isc-dhcp-44-manual-pages-dhcpd#configuration_manpages)).

```
[root@dhcpsrv ~]# cat /etc/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;
authoritative;
subnet 192.168.100.0 netmask 255.255.255.0 {
    range 192.168.100.10 192.168.100.100;
    option routers 192.168.100.1;
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.100.255;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
}
log-facility local7;
```

Vejamos que temos a subnet declarada para o IP local 192.168.100.0/24 entregando IPs do limite .10 até .100. Seu Gateway configurado como .1 e o DNS público da Google, também poderia ser da CloudFlare 1.1.1.1. Agora definimos o IP estático para a interface enp0s8:

```
[root@dhcpsrv ~]# cat /etc/systemd/network/20-wired.network
[Match]
Name=enp0s8

[Network]
Address=192.168.100.1/24
```

Ao reiniciamos o serviço com \$ systemctl restart dhcpcd4.service ; Poderemos verificar o status do nosso servidor DHCP ao executar o mesmo comando do systemctl para status:

```
[root@dhcpsrv ~]# systemctl status dhcpcd4.service
● dhcpcd4.service - IPv4 DHCP server
   Loaded: loaded (/usr/lib/systemd/system/dhcpcd4.service; enabled; preset: disabled)
     Active: active (running) since Wed 2024-04-24 11:07:07 -03; 3min 55s ago
       Process: 738 ExecStart=/usr/bin/dhcpcd -4 -q -cf /etc/dhcpcd.conf -pf /run/dhcpcd4/dhcpcd.pid (code=exited, status=0/SUCCESS)
      Main PID: 739 (dhcpcd)
         Tasks: 1 (limit: 4664)
        Memory: 4.4M (peak: 6.4M)
          CPU: 17ms
         CGroup: /system.slice/dhcpcd4.service
                   └─739 /usr/bin/dhcpcd -4 -q -cf /etc/dhcpcd.conf -pf /run/dhcpcd4/dhcpcd.pid
```

Abaixo a configuração completa em uma captura de tela:

```

Arch DHCP Server [Running] - Oracle VM VirtualBox
[root@dhcpsrv ~]# systemctl status dhcpd4.service    status do daemon
● dhcpd4.service - IPv4 DHCP server
   Loaded: loaded (/usr/lib/systemd/system/dhcpd4.service; enabled; preset: disabled)
     Active: active (running) since Wed 2024-04-24 11:07:07 -03: 3min 55s ago
       PID: 739 (dhcpd)
      Tasks: 1 (limit: 4664)
     Memory: 4.4M (peak: 6.4M)
        CPU: 17ms
       CGroup: /system.slice/dhcpd4.service
               └─739 /usr/bin/dhcpd -4 -q -cf /etc/dhcpd.conf -pf /run/dhcpd4/dhcpd.pid

Apr 24 11:07:07 dhcpsrv dhcpd[739]: Wrote 0 leases to leases file.
Apr 24 11:07:07 dhcpsrv dhcpd[739]:
Apr 24 11:07:07 dhcpsrv dhcpd[739]: No subnet declaration for enp0s3 (10.0.2.15).          rede nat do vbox
Apr 24 11:07:07 dhcpsrv dhcpd[739]: ** Ignoring requests on enp0s3. If this is not what      deixei sem declarar
Apr 24 11:07:07 dhcpsrv dhcpd[739]: you want, please write a subnet declaration
Apr 24 11:07:07 dhcpsrv dhcpd[739]: in your dhcpd.conf file for the network segment
Apr 24 11:07:07 dhcpsrv dhcpd[739]: to which interface enp0s3 is attached. **
Apr 24 11:07:07 dhcpsrv dhcpd[739]:
Apr 24 11:07:07 dhcpsrv dhcpd[739]: Server starting service.
Apr 24 11:07:07 dhcpsrv systemd[1]: Started IPv4 DHCP server.
[root@dhcpsrv ~]# ip addr show enp0s8
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:41:f3:77 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.1/24 brd 192.168.100.255 scope global enp0s8
        valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe41:f377/64 scope link proto kernel ll
            valid_lft forever preferred_lft forever
[root@dhcpsrv ~]# cat /etc/systemd/network/20-wired.network
[Match]
Name=enp0s8      static ip conf

[Network]
Address=192.168.100.1/24
[root@dhcpsrv ~]# cat /etc/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;
authoritative;
subnet 192.168.100.0 netmask 255.255.255.0 {           declarando subnet
    range 192.168.100.10 192.168.100.100;             conf do dhcp
    option routers 192.168.100.1;
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.100.255;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
}
log-facility local7;
[root@dhcpsrv ~]#

```

Abaixo os IPs já registrados (leases):

- “archiso” sendo a vm enquanto estava instalando o cliente com o DHCP já executando:
- “cliente” já sendo a vm com a gnu/linux arch instalada.

```
[root@dhcpsrv ~]# cat /var/lib/dhcp/dhcpd.leases
# The format of this file is documented in the dhcpcd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.4.3-P1

# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

server-uid "\000\001\000\001-\273\316\213\010\000'AN363w";

lease 192.168.100.10 {
    starts 3 2024/04/24 14:18:31;
    ends 3 2024/04/24 14:28:31;
    cltt 3 2024/04/24 14:18:31;
    binding state active;
    next binding state free;
    rewind binding state free;
    hardware ethernet 08:00:27:cb:b1:69;
    uid "\377\3424?>\000\002\000\000\253\021\342g\370U\375' j\321";
    client-hostname "archiso";
}
lease 192.168.100.10 {
    starts 3 2024/04/24 14:18:31;
    ends 3 2024/04/24 14:28:31;
    tstp 3 2024/04/24 14:28:31;
    cltt 3 2024/04/24 14:18:31;
    binding state free;
    hardware ethernet 08:00:27:cb:b1:69;
    uid "\377\3424?>\000\002\000\000\253\021\342g\370U\375' j\321";
}
lease 192.168.100.11 {
    starts 3 2024/04/24 14:39:03;
    ends 3 2024/04/24 14:49:03;
    cltt 3 2024/04/24 14:39:03;
    binding state active;
    next binding state free;
    rewind binding state free;
    hardware ethernet 08:00:27:cb:b1:69;
    uid "\001\010\000'\313\261i";
    client-hostname "cliente";
}
```

Acessando nosso cliente, podemos ver que os IPs estão corretamente sendo entregues:

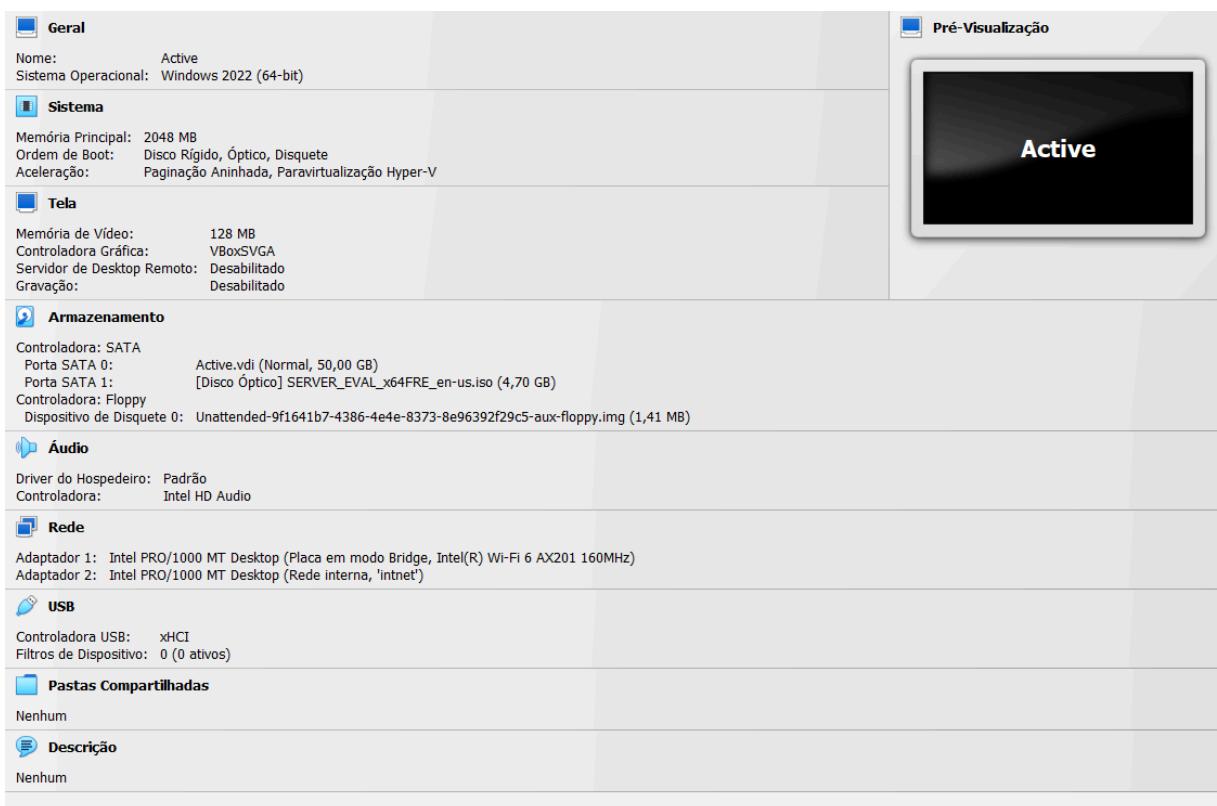
- 192.168.100.11 foi entregue corretamente para o host “cliente”.

```
[gbr@cliente ~]$ ip add show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cb:b1:69 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.11/24 brd 192.168.100.255 scope global dynamic noprefixroute enp0s3
        valid_lft 552sec preferred_lft 552sec
    inet6 fe80::c4b1:fb74:e954:28c5/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

## 2.1.2 AD/DNS

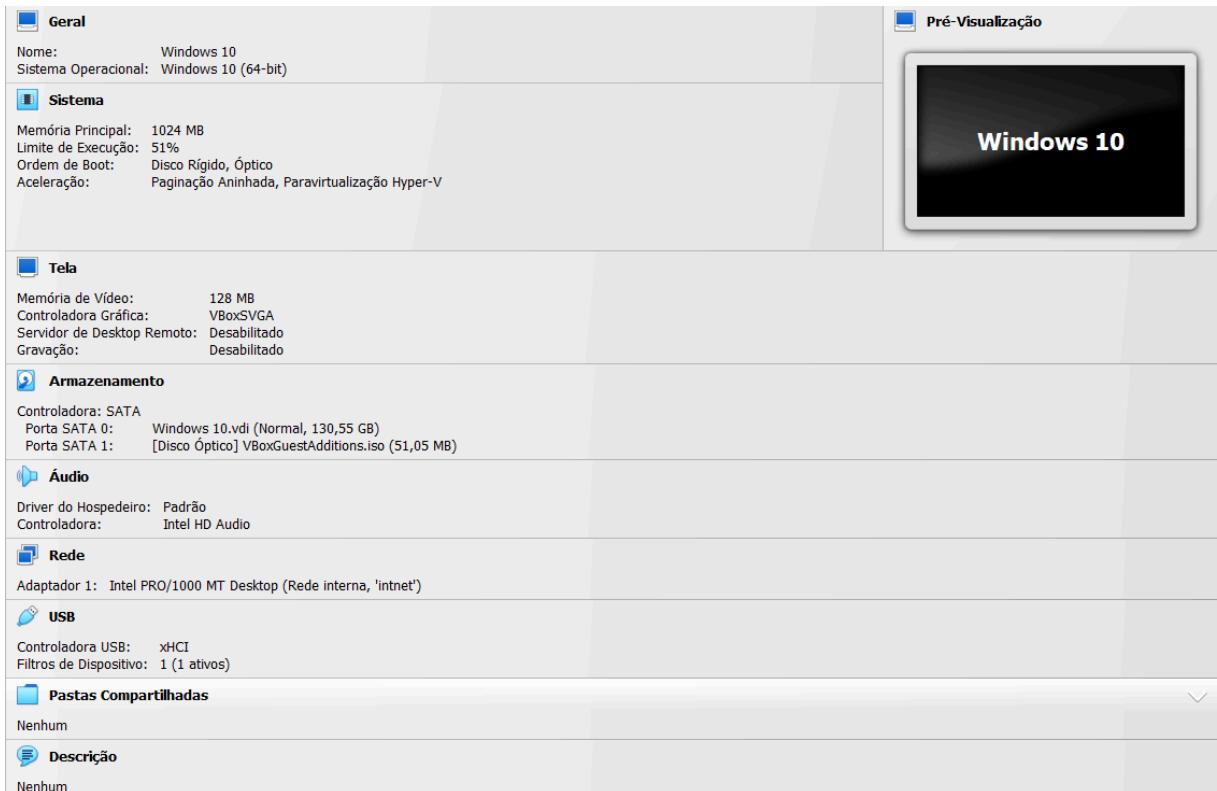
O servidor de Active Directory foi virtualizado utilizando a iso do Windows Server 2022 e o Virtual Box. Abaixo, encontram-se as especificações das VMs utilizadas, a ISO e o software utilizado para servir os IPs na rede interna do VBox.

- VM. Servidor AD/DNS:
  - Memória 2048MB / 1 núcleos;
  - Vídeo 128MB;
  - Memória Interna: 50GB;
  - 2 Adaptadores de rede: 1 Bridge; 1 Interno;

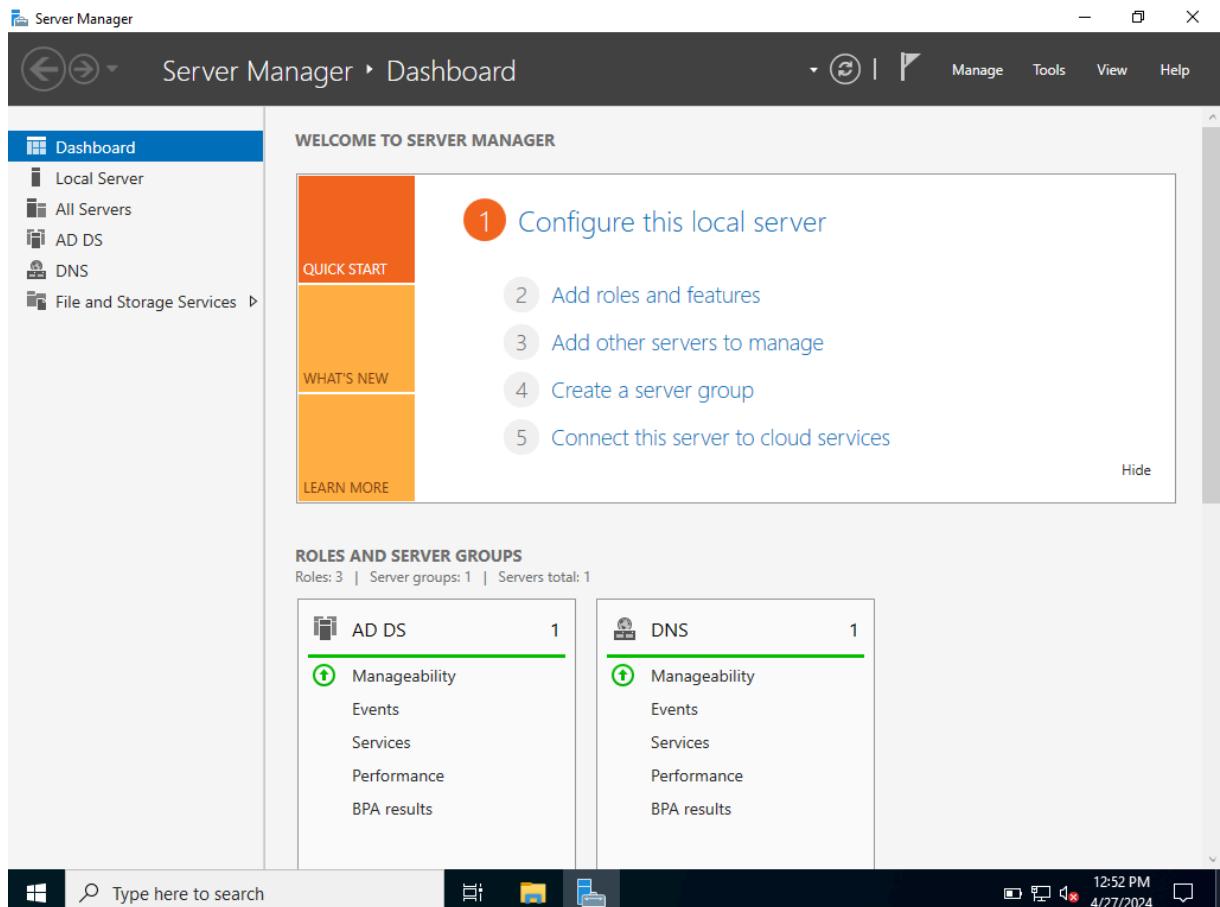


- VM Cliente:

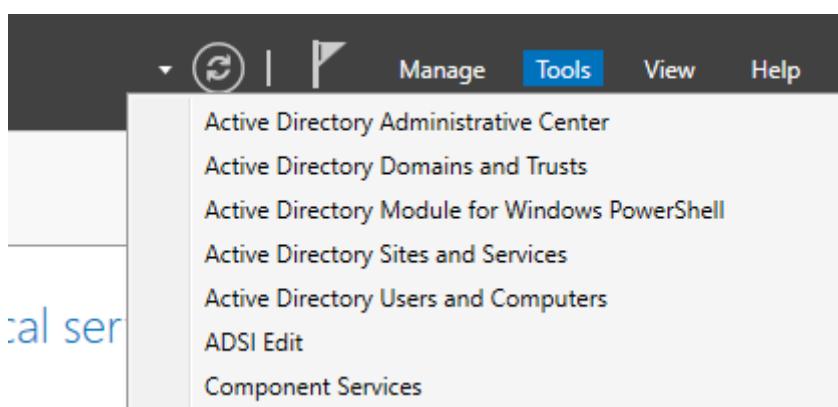
- Memória 1024 MB / 1 núcleos;
- Vídeo 128MB;
- Memória Interna 130GB;
- 1 Adaptador de rede: Interno;



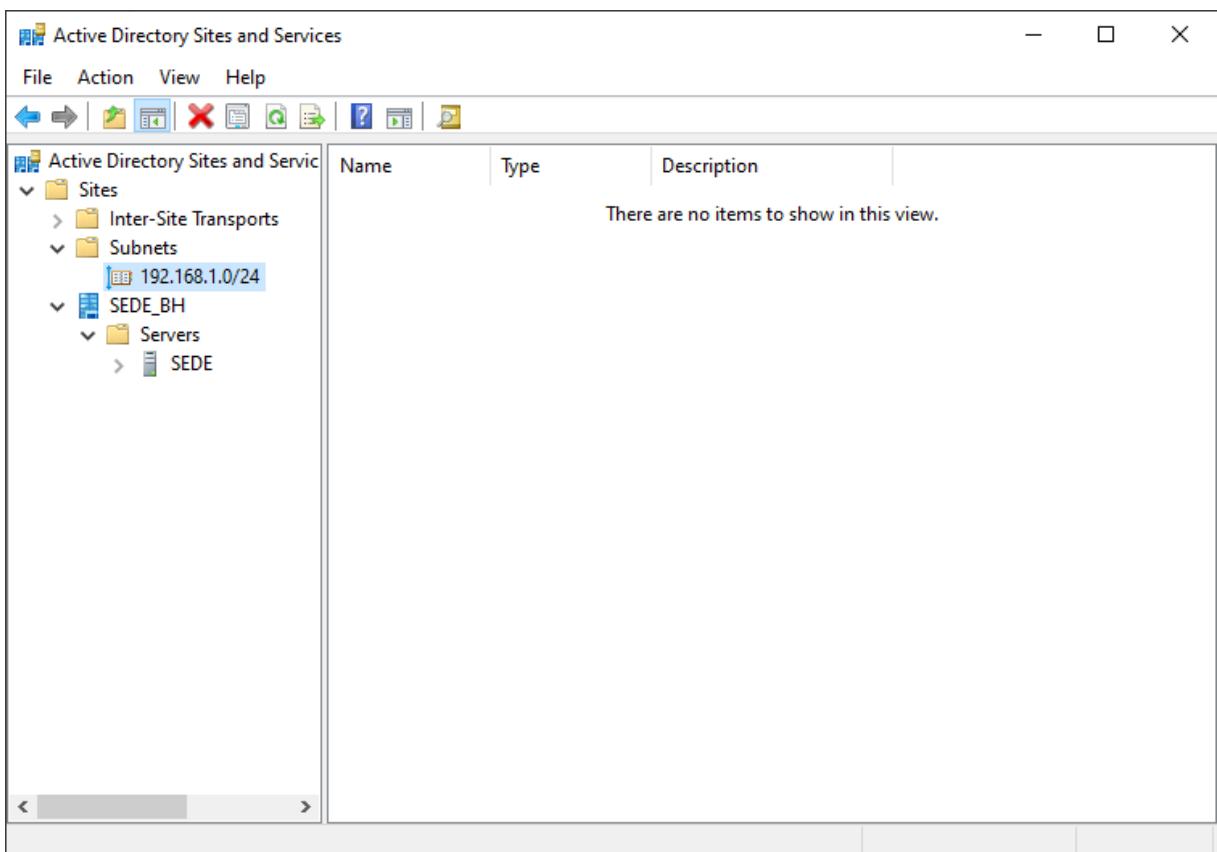
Ao iniciar o servidor podemos identificar os serviços instalados e inicializados juntamente com inicialização do sistema. O servidor possui O active directory (AD/DS) e o DNS.



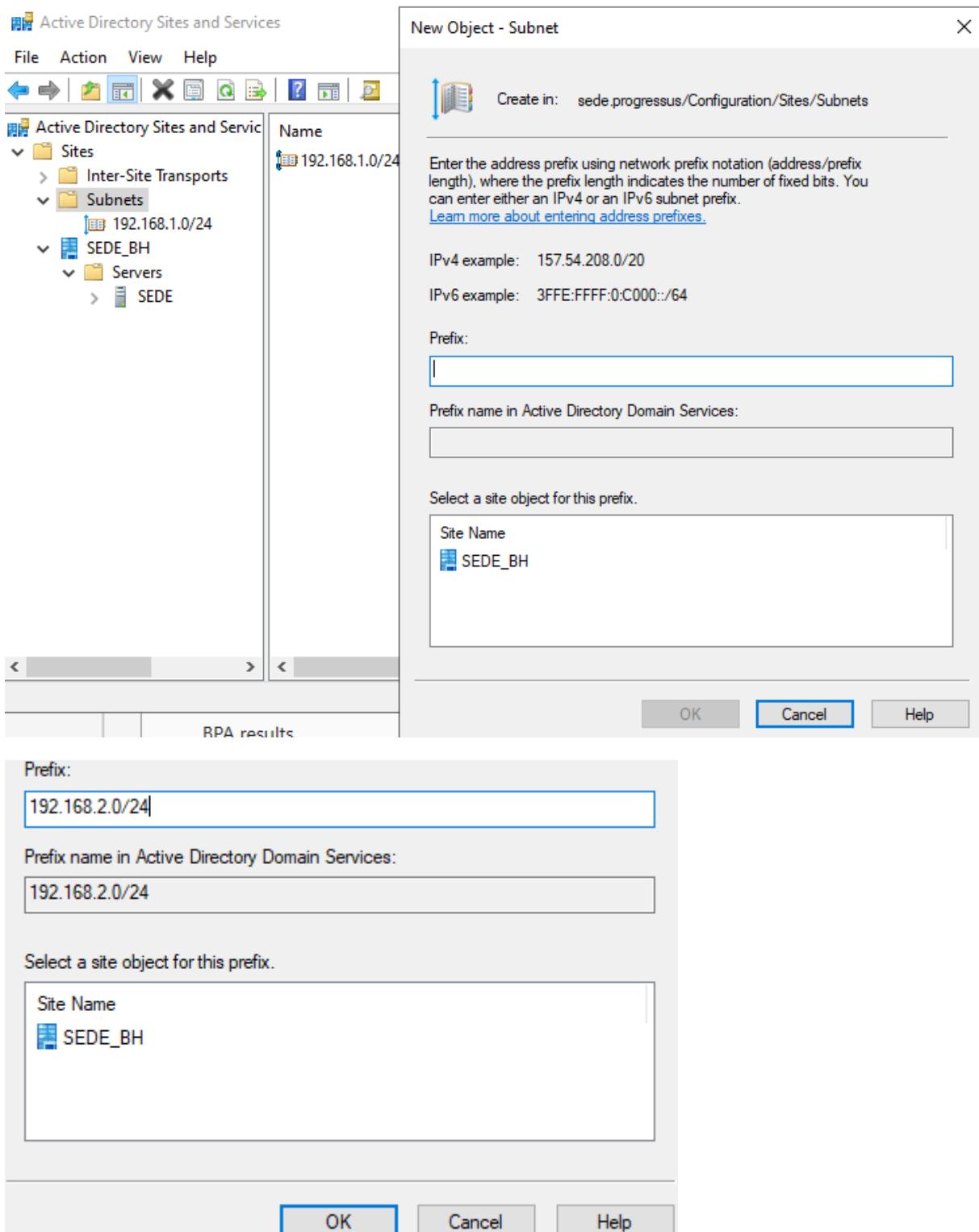
No canto superior direito ao clicar em “Tools” podemos identificar as ferramentas do Active Directory. Para o nosso Caso vamos utilizar apenas as ferramentas: Site e Serviços e Usuários e Computadores, para que possamos fazer o controle dos domínios e dos usuários e das estações.



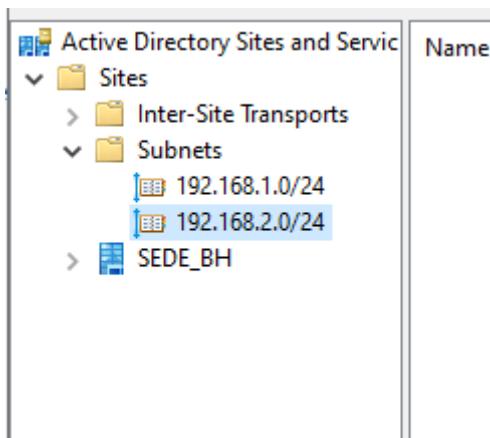
Ao clicarmos em Sites e Serviços um nova janela será aberta contendo as informações sobre o domínio, as subnets e os servidores, neste caso, foi criado apenas uma subnet com o 192.168.1.0/24, sendo assim, é possível até 254 estações nesta subnet.



Para incluir outra subnet, pode clicar com o botão direito do mouse sobre a pasta de subnet, em seguida clicar em nova subnet. Uma nova janela será aberta onde devemos selecionar o domínio e preencher o campo de prefixo, o campo aceita os padrões de IPv4 e IPv6. Após preencher o campo é só clicar em Ok.



Após clicar em ok, podemos observar que a nova subnet foi criada de acordo com os parâmetros informados.

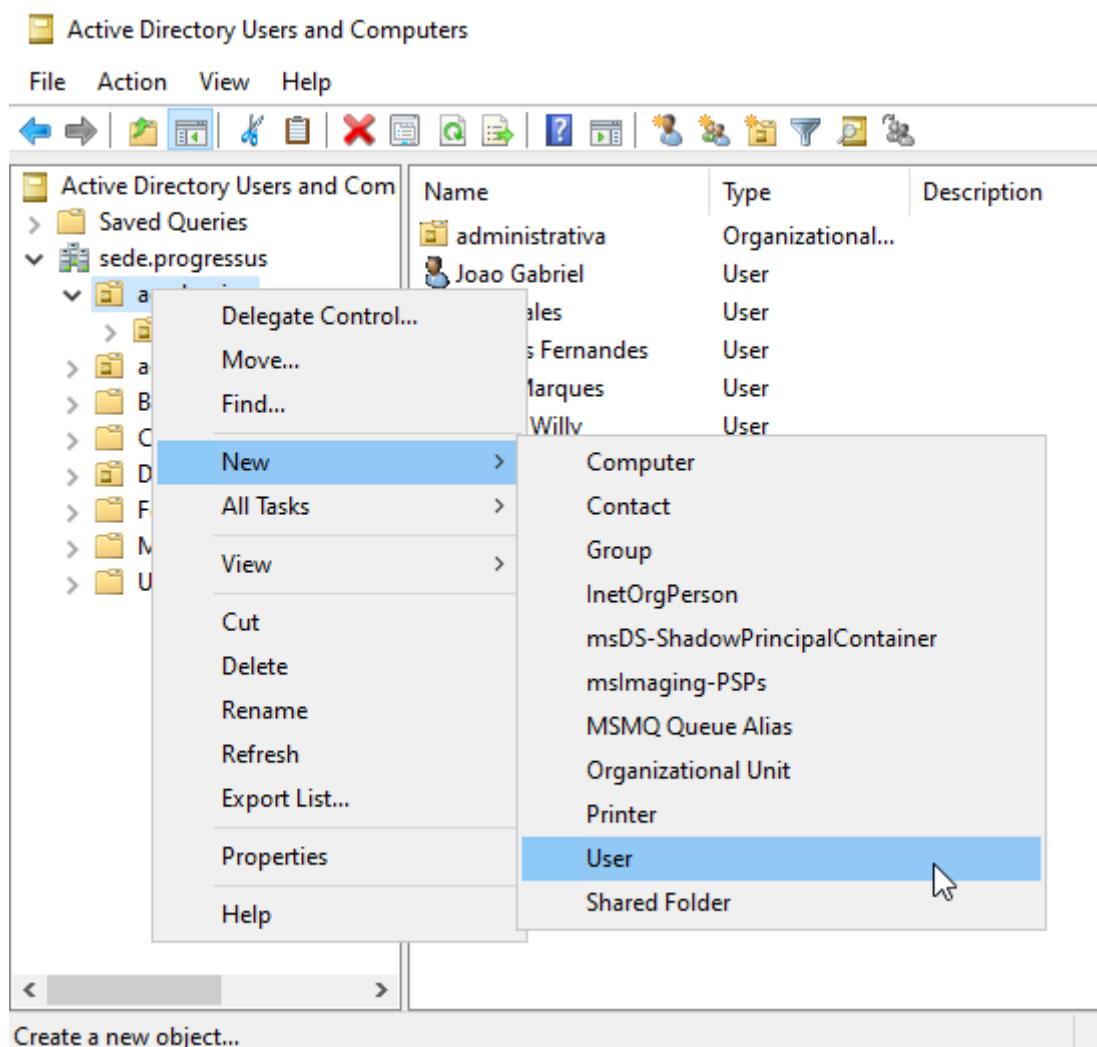


Ao clicarmos novamente em “Tools” em seguida “Usuários e Computadores”, uma nova janela será aberta, onde podemos ver as informações dos domínios, pastas(organizações/grupos de trabalhos) e os usuários.

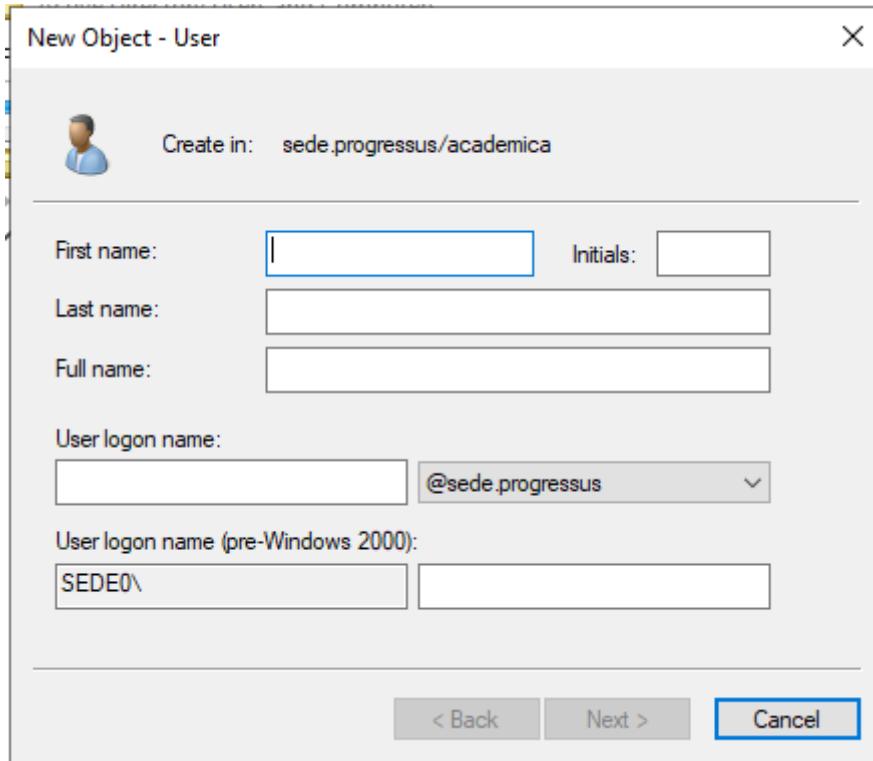
The screenshot shows the 'Active Directory Users and Computers' management console. The left navigation pane shows the 'sede.progressus' domain container expanded, with its subcontainers like 'academica', 'administrativa', 'BuiltIn', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Managed Service Accounts', and 'Users' listed. The right pane displays a table of users:

Name	Type	Description
administrativa	Organizational...	
Joao Gabriel	User	
Joao Sales	User	
Jonatas Fernandes	User	
Kelly Marques	User	
Marco Willy	User	
Thiago Vinicius	User	

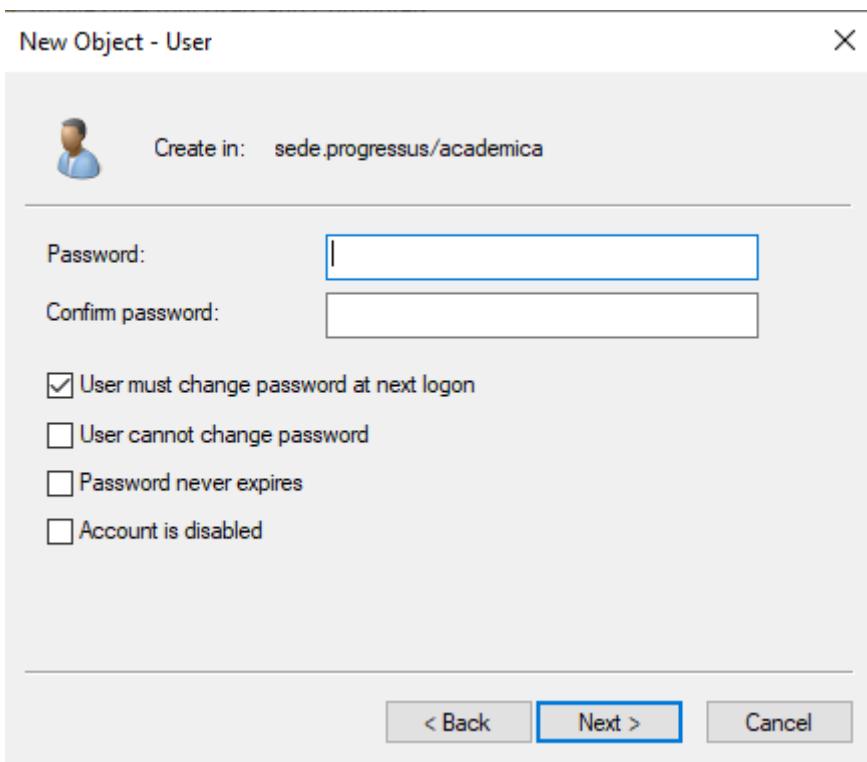
Para adicionar novos usuários, basta clicar com o botão direito no grupo que deseja adicionar o usuário ao abrir o menu de opções selecione: novo > usuário e uma nova janela será aberta.



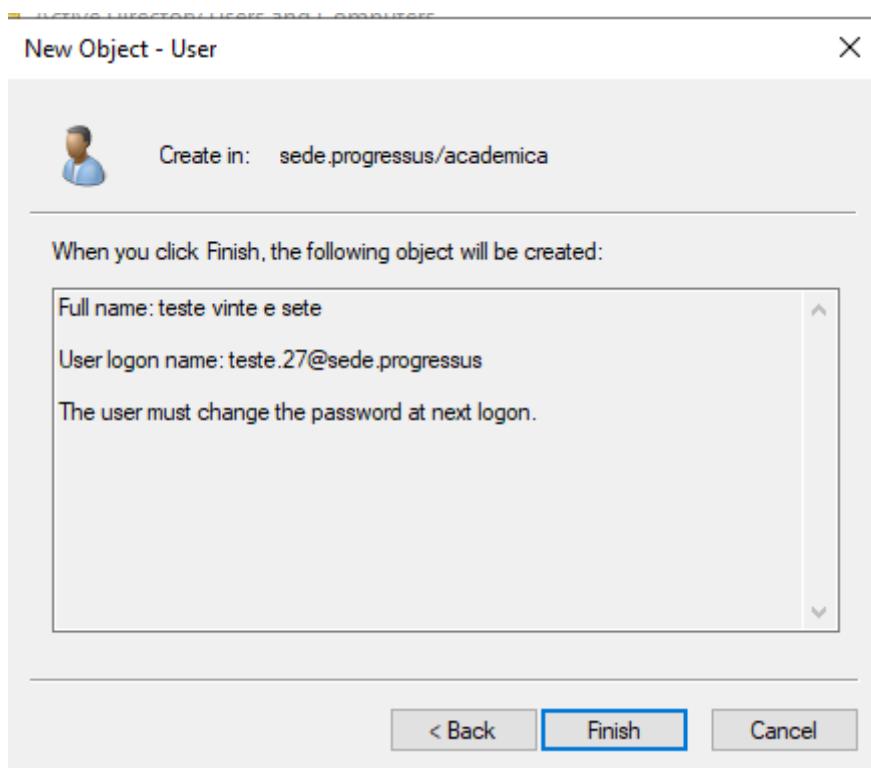
Ao abrir a janela devemos preencher o nome e sobrenome do usuário, logon do usuário (que será utilizado para fazer o logon nas estações), após preencher devemos clicar em próximo.



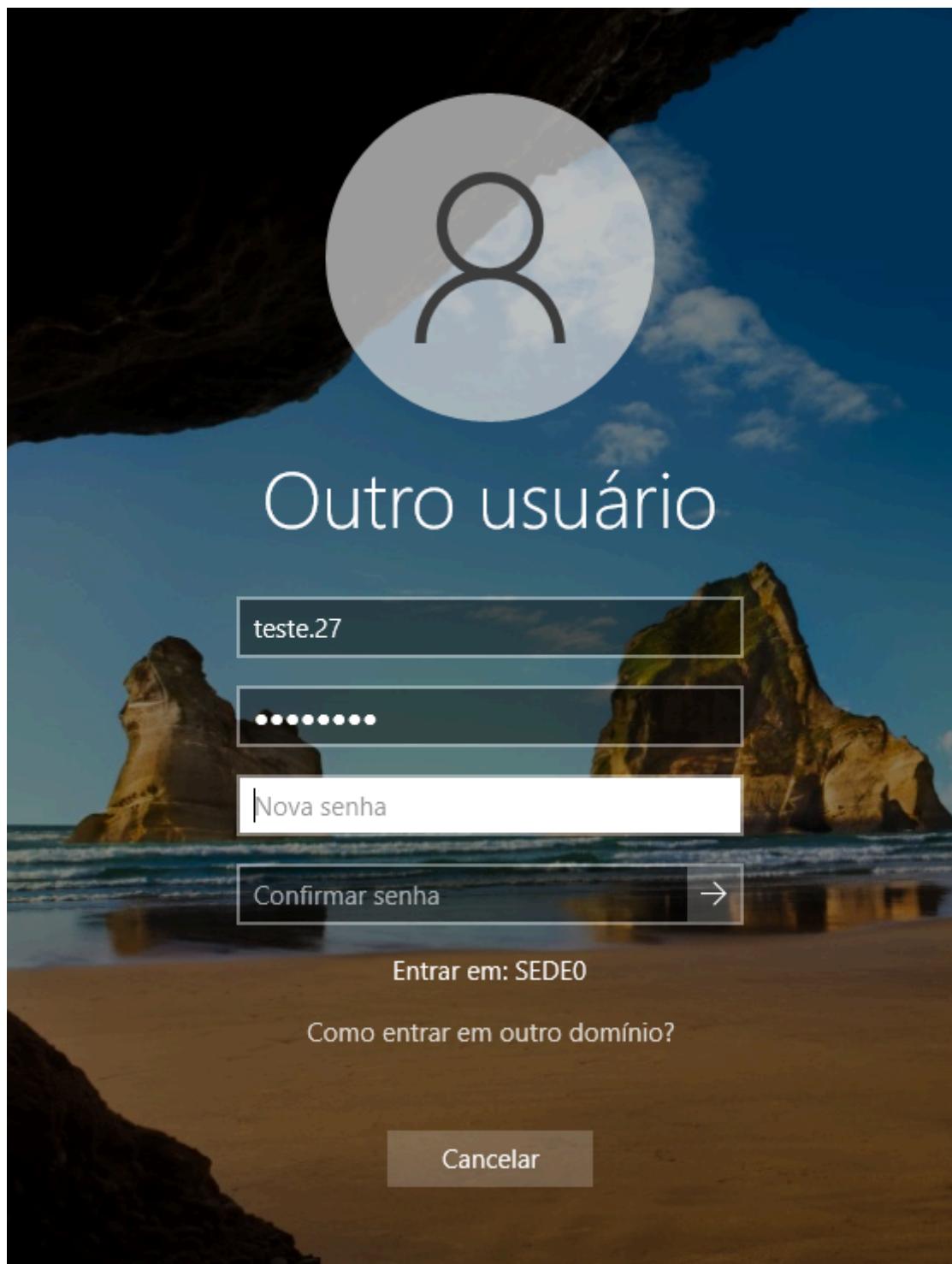
Na tela seguinte devemos escolher uma senha provisória para o usuário, caso contrário, desmarque a primeira opção.



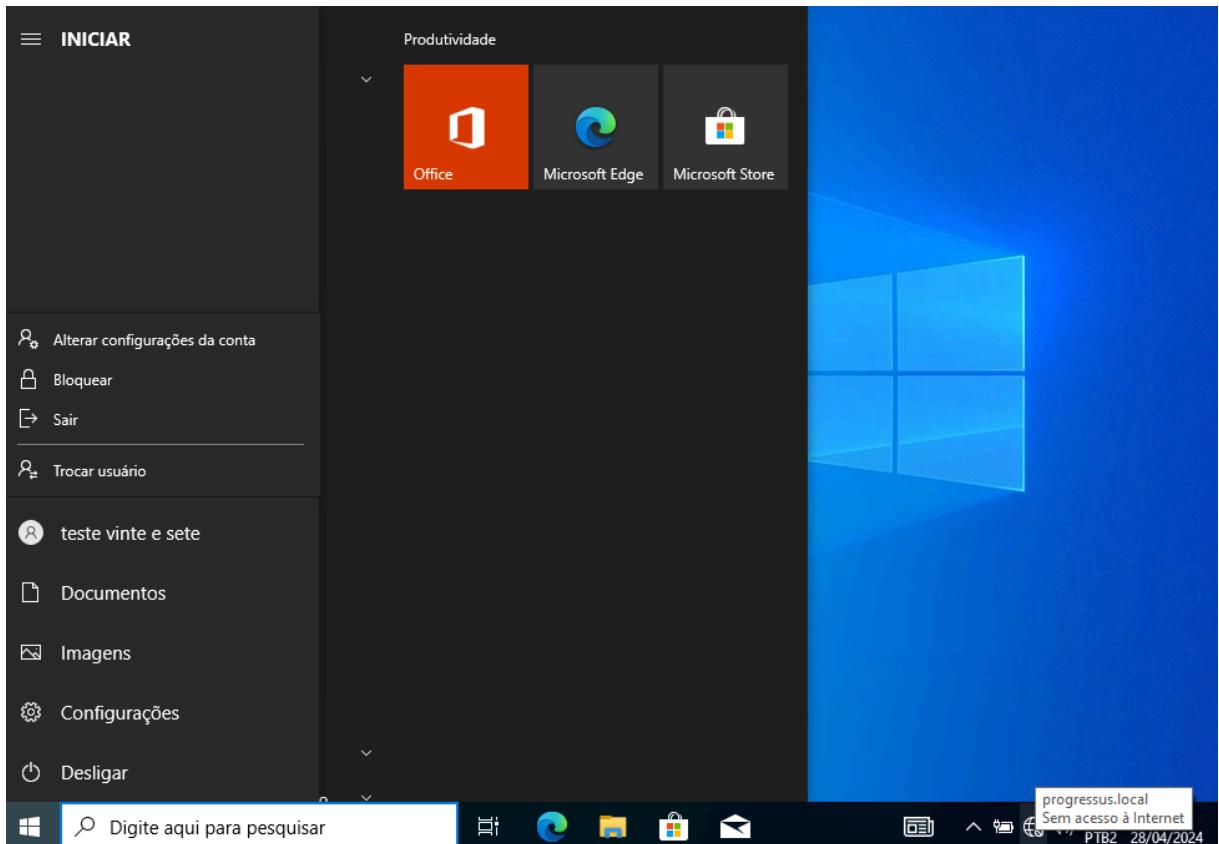
Ao preencher a senha e clicar em próximo somos direcionados para tela de informações, onde podemos visualizar as informações do usuário que está sendo criado, possibilitando ajustes ou correções antes de finalizar o cadastro.



Ao tentar acessar com usuário criado na estação, foi solicitado a alteração da senha.



Ao fazer o logon, podemos ver que a máquina já está rede da universidade progressus, porém, não possui conexão com a internet.



## 2.2. SERVIÇOS EM NUVEM (AWS)

### 2.2.1. SMTP

Configuramos uma instância EC2 usando a AMI Debian no nível gratuito com 16GB de espaço interno. O tipo de instância selecionado foi t2.micro, adequado para testes. As configurações de grupo de segurança foram ajustadas para permitir tráfego SMTP.

[Software Image \(AMI\)](#)

Debian 12 (20231013-1532)

ami-058bd2d568351da34

[Virtual server type \(instance type\)](#)

t2.micro

[Firewall \(security group\)](#)

New security group

[Storage \(volumes\)](#)

1 volume(s) - 16 GiB

Após a instância estar operacional, realizamos a conexão via SSH, usando a chave privada associada. Isso nos permitiu acessar o terminal do servidor onde o Postfix seria configurado.

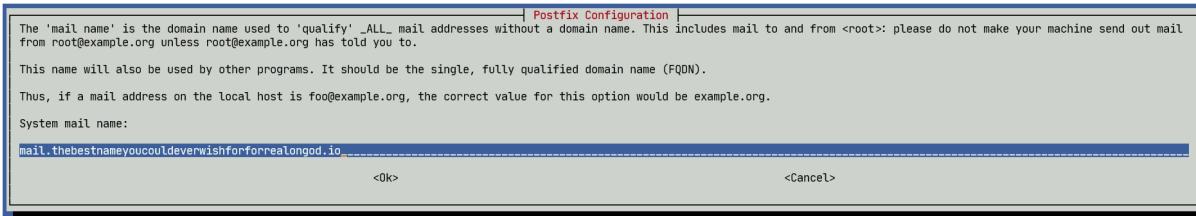
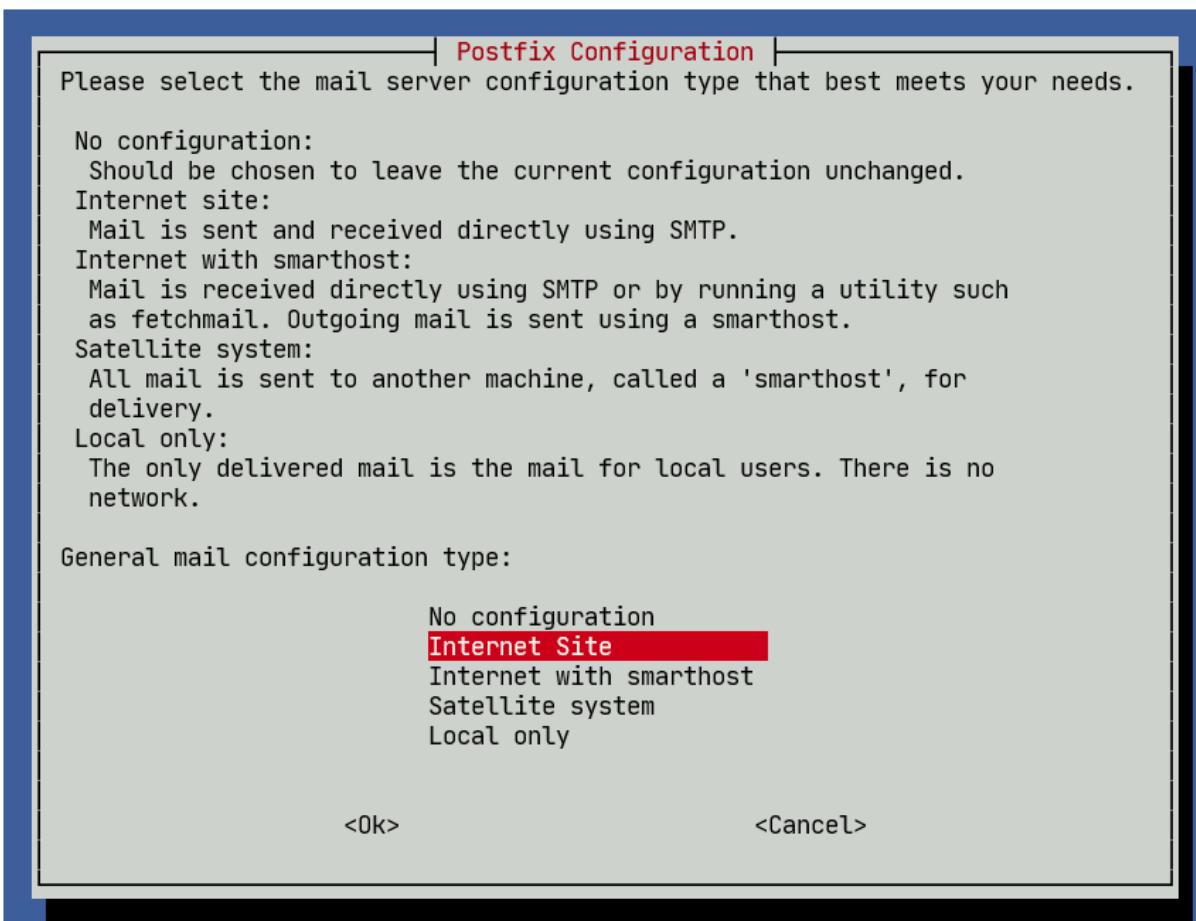
Comando (~dir\_da\_chave\_ssh):

ssh -i "your-key-pair.pem" ec2-user@ec2-xx-xx-xx-xx.compute-1.amazonaws.com

```
$ ssh -i "iaheohre.pem" admin@ec2-54-221-27-230.compute-1.amazonaws.com
```

No terminal conectado, executamos o comando [sudo apt install postfix](#). Durante a instalação, escolhemos a opção "Internet Site" e configuramos o "nome do sistema de correio" como [mail.exemplo.local](#).

```
admin@ip-172-31-30-110:~$ sudo apt update
Get:1 file:/etc/apt/mirrors/debian.list Mirrorlist [38 B]
Get:5 file:/etc/apt/mirrors/debian-security.list Mirrorlist [47 B]
Get:2 https://cdn-aws.deb.debian.org/debian bookworm InRelease [151 kB]
Get:3 https://cdn-aws.deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Get:4 https://cdn-aws.deb.debian.org/debian bookworm-backports InRelease [56.5 kB]
Get:6 https://cdn-aws.deb.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Get:7 https://cdn-aws.deb.debian.org/debian bookworm/main Sources [9489 kB]
Get:8 https://cdn-aws.deb.debian.org/debian bookworm/main amd64 Packages [8786 kB]
Get:9 https://cdn-aws.deb.debian.org/debian bookworm/main Translation-en [6109 kB]
Get:10 https://cdn-aws.deb.debian.org/debian bookworm-updates/main Sources [17.9 kB]
Get:11 https://cdn-aws.deb.debian.org/debian bookworm-updates/main amd64 Packages [13.8 kB]
Get:12 https://cdn-aws.deb.debian.org/debian bookworm-updates/main Translation-en [16.0 kB]
Get:13 https://cdn-aws.deb.debian.org/debian bookworm-backports/main Sources [204 kB]
Get:14 https://cdn-aws.deb.debian.org/debian bookworm-backports/main amd64 Packages [192 kB]
Get:15 https://cdn-aws.deb.debian.org/debian bookworm-backports/main Translation-en [161 kB]
Get:16 https://cdn-aws.deb.debian.org/debian-security bookworm-security/main Sources [91.6 kB]
Get:17 https://cdn-aws.deb.debian.org/debian-security bookworm-security/main amd64 Packages [155 kB]
Get:18 https://cdn-aws.deb.debian.org/debian-security bookworm-security/main Translation-en [94.3 kB]
Fetched 25.6 MB in 4s (6436 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
52 packages can be upgraded. Run 'apt list --upgradable' to see them.
admin@ip-172-31-30-110:~$ sudo apt install postfix
```



Editamos o arquivo `/etc/postfix/main.cf`, onde configuramos `myhostname` como `mail.exemplo.local`. Ajustamos outras configurações relevantes, como `mydomain` para `exemplo.local` e `myorigin` para `$mydomain`.

```
admin@ip-172-31-30-110:~$ sudo vi /etc/postfix/main.cf_
```

Nosso arquivo final ficaria como:

```
# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname
mail_spool_directory = /var/mail
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

readme_directory = no

# See http://www.postfix.org/COMPATIBILITY_README.html -- default to 3.6 on
# fresh installs.
compatibility_level = 3.6


# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_CApth=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache


smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = mail.thebestnameyoucouldeverwishforforrealongod.io
alias_maps = hash:/etc/aliases
mydomain = thebestnameyoucouldeverwishforforrealongod.io
alias_database = hash:/etc/aliases
myorigin = $mydomain
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

Para aplicar as novas configurações, reiniciamos o Postfix utilizando o comando `sudo systemctl restart postfix`. Esse passo assegurou que o servidor de e-mail começasse a operar com as configurações atualizadas.

```
admin@ip-172-31-30-110:~$ sudo systemctl restart postfix_
```

Testamos a funcionalidade de envio de e-mails com o comando `echo "Teste de email" | mail -s "Assunto Teste" admin@localhost`. A execução bem-sucedida deste teste indicou a operacionalidade do Postfix.

```
admin@ip-172-31-30-110:~$ sudo apt install mailutils_
```

```
admin@ip-172-31-30-110:~$ echo "Teste de email" | mail -s "Assunto Teste" admin@localhost
```

Utilizamos o comando `mail` para inspecionar o correio local.

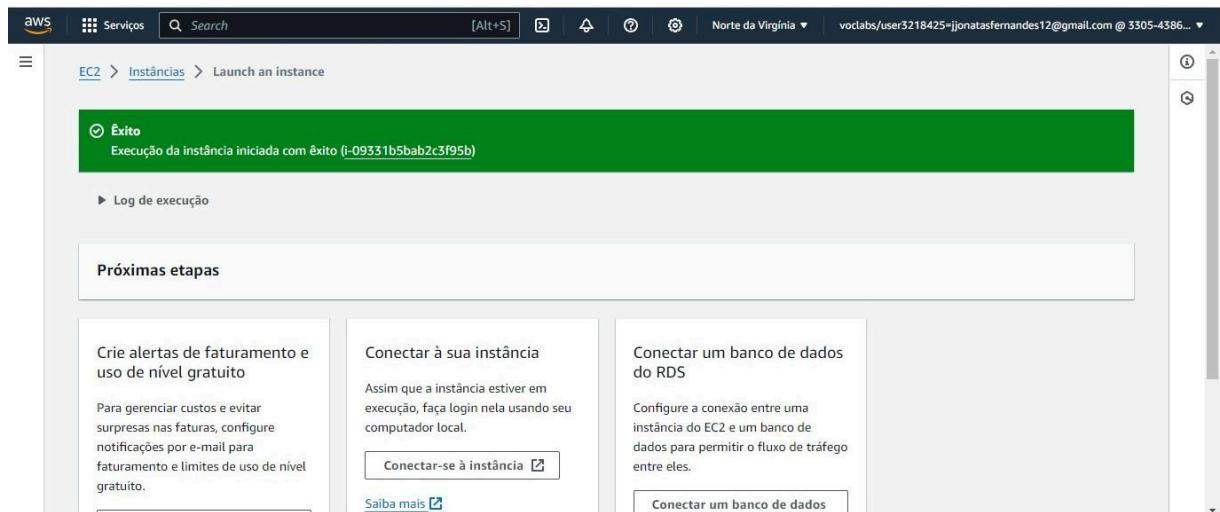
```
admin@ip-172-31-30-110:~$ mail
"/var/mail/admin": 1 message 1 new
>N 1 Debian Sun Apr 28 12:20 13/511 Assunto Teste
?
```

Por fim, examinamos os registros do Postfix com o comando `cat /var/log/mail.log`. Este exame nos permitiu verificar se havia erros ou outras questões impactando a funcionalidade do servidor de e-mails.

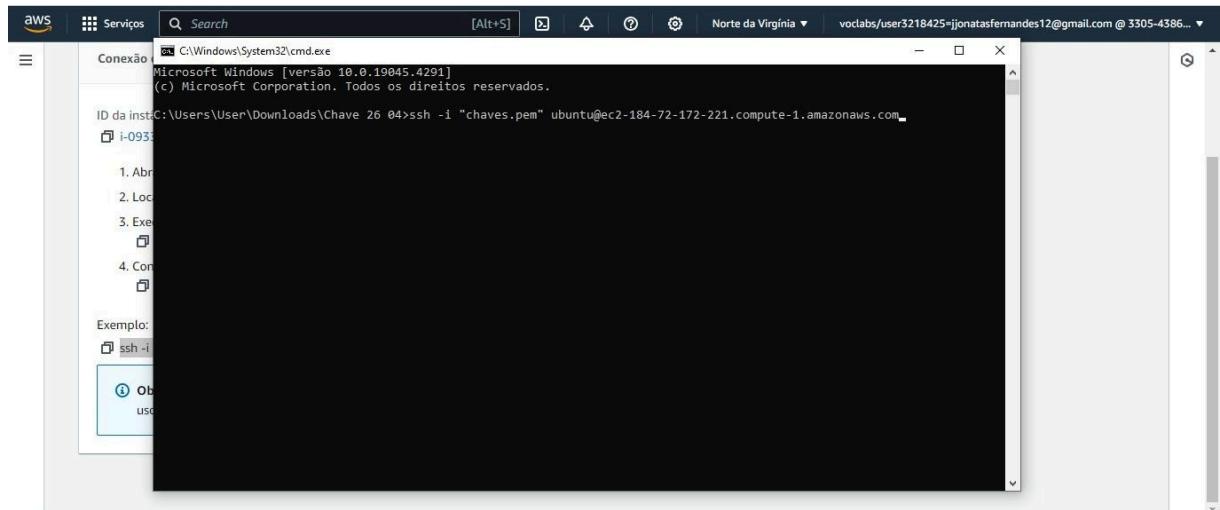
```
admin@ip-172-31-30-110:~$ cat /var/log/mail.log
2024-04-28T12:26:47.670119+00:00 ip-172-31-30-110 postfix/pickup[1899]: A385549029: uid=1000 from=<admin@ip-172-31-30-110>
```

## 2.2.2. WEB/APLICAÇÃO

No painel do EC2, criei e configurei uma instância de servidor.



Após criada e configurada, conectei a ela usando SSH.



```

aws Serviços Search [Alt+S] Conexão Norte da Virgínia v vclabs/user3218425=jjonatasfernandes12@gmail.com @ 3305-4386... ▾
ubuntu@ip-172-31-28-45:~ 
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro

ID da instância: i-093...
System information as of Fri Apr 26 13:06:03 UTC 2024
  System load: 0.03      Processes:          107
  Usage of /: 23.2% of 6.71GB   Users logged in:     0
  Memory usage: 20%           IPv4 address for enX0: 172.31.28.45
  Swap usage:  0%
  1. Abrir terminal
  2. Localizar
  3. Executar
    Expanded Security Maintenance for Applications is not enabled.
  4. Configurar
    0 updates can be applied immediately.
  5. Conectar
    Enable ESM Apps to receive additional future security updates.
    See https://ubuntu.com/esm or run: sudo pro status

Exemplo:
  ssh -i The programs included with the Ubuntu system are free software;
  the exact distribution terms for each program are described in the
  individual files in /usr/share/doc/*/*copyright.

  ⓘ Observe que o Ubuntu vem com ABSOLUTAMENTE NÃO GARANTIA, na medida permitida por
  a lei aplicável.

  To run a command as administrator (user "root"), use "sudo <command>".
  See "man sudo_root" for details.

ubuntu@ip-172-31-28-45:~$ 

```

CloudShell © 2024, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

```

aws Serviços Search [Alt+S] Conexão Norte da Virgínia v vclabs/user3218425=jjonatasfernandes12@gmail.com @ 3305-4386... ▾
ubuntu@ip-172-31-28-45:~ 
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease [256 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [89.7 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [90.8 kB]
ID da instância: i-093...
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 Packages [1401 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main Translation-en [513 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [112 B]
Get:9 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [116 B]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/restricted amd64 Packages [93.9 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/restricted Translation-en [18.7 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [112 B]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [116 B]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [112 B]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [116 B]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 c-n-f Metadata [116 B]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 c-n-f Metadata [116 B]
Fetcher: 28.1 MB in 5s (5193 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
ubuntu@ip-172-31-28-45:~$ 

```

CloudShell © 2024, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

Logo após foi feita a instalação do Apache.

```

aws Serviços Search [Alt+S] Norte da Virginia v vocabs/user3218425=jonatasfernandes12@gmail.com @ 3305-4386... v
Conexão: ubuntu@ip-172-31-28-45:~ 
ID da instância: i-093
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/universe amd64 c-n-f Metadata [116 B]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 c-n-f Metadata [116 B]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 c-n-f Metadata [116 B]
Fetched 28.1 MB in 5s (5193 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
1. Abrir o terminal
2. Localizar o diretório da instância
3. Executar o comando 'sudo apt update'
4. Comando 'sudo apt install apache2'
Exemplo: The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
  liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64
  liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 2081 kB of archives.
After this operation, 8887 kB of additional disk space will be used.
Do you want to continue? [Y/n]

```

CloudShell © 2024, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

Habilitado e ativado.

```

aws Serviços Search [Alt+S] Norte da Virginia v vocabs/user3218425=jonatasfernandes12@gmail.com @ 3305-4386... v
EC2 > Instâncias
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.

► Log de sistema
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-28-45:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
  Active: active (running) since Fri 2024-04-26 13:08:40 UTC; 27s ago
    Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2083 (apache2)
      Tasks: 55 (limit: 1130)
     Memory: 5.4M (peak: 5.6M)
        CPU: 38ms
       CGroup: /system.slice/apache2.service
           └─2083 /usr/sbin/apache2 -k start
              ├─2086 /usr/sbin/apache2 -k start
              ├─2087 /usr/sbin/apache2 -k start
              └─2088 /usr/sbin/apache2 -k start

Para gerenciar seu servidor web, use o comando 'systemctl'.
notificações de faturamento são gratuitas.

```

Saiba mais Conectar um banco de dados CloudShell © 2024, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

Nesse passo foi feito a configuração do Firewall HTTP.

```

aws Serviços Search [Alt+S] Norte da Virgínia v vocabs/user3218425=jonatasfernandes12@gmail.com @ 3305-4386...
Conexão ID da instância i-0933 No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
1. Abrir apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Fri 2024-04-26 13:08:40 UTC; 27s ago
     Docs: https://httpd.apache.org/docs/2.4/
          Main PID: 2083 (apache2)
             Tasks: 55 (limit: 1130)
            Memory: 5.4M (peak: 5.6M)
              CPU: 38ms
            CGroup: /system.slice/apache2.service
                    └─2083 /usr/sbin/apache2 -k start
                     ├─2086 /usr/sbin/apache2 -k start
                     └─2087 /usr/sbin/apache2 -k start
Exemplo: ssh -i
        ⓘ Outras opções
          Usuário
          Rules updated
          Rules updated (v6)
ubuntu@ip-172-31-28-45:~$ 

```

CloudShell © 2024, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

## A devida ativação do firewall.

```

ubuntu@ip-172-31-28-45:~$ 
  Active: active (running) since Fri 2024-04-26 13:08:40 UTC; 27s ago
    Docs: https://httpd.apache.org/docs/2.4/
  Main PID: 2083 (apache2)
    Tasks: 55 (limit: 1130)
   Memory: 5.4M (peak: 5.6M)
     CPU: 38ms
    CGroup: /system.slice/apache2.service
            ├─2083 /usr/sbin/apache2 -k start
            ├─2086 /usr/sbin/apache2 -k start
            └─2087 /usr/sbin/apache2 -k start

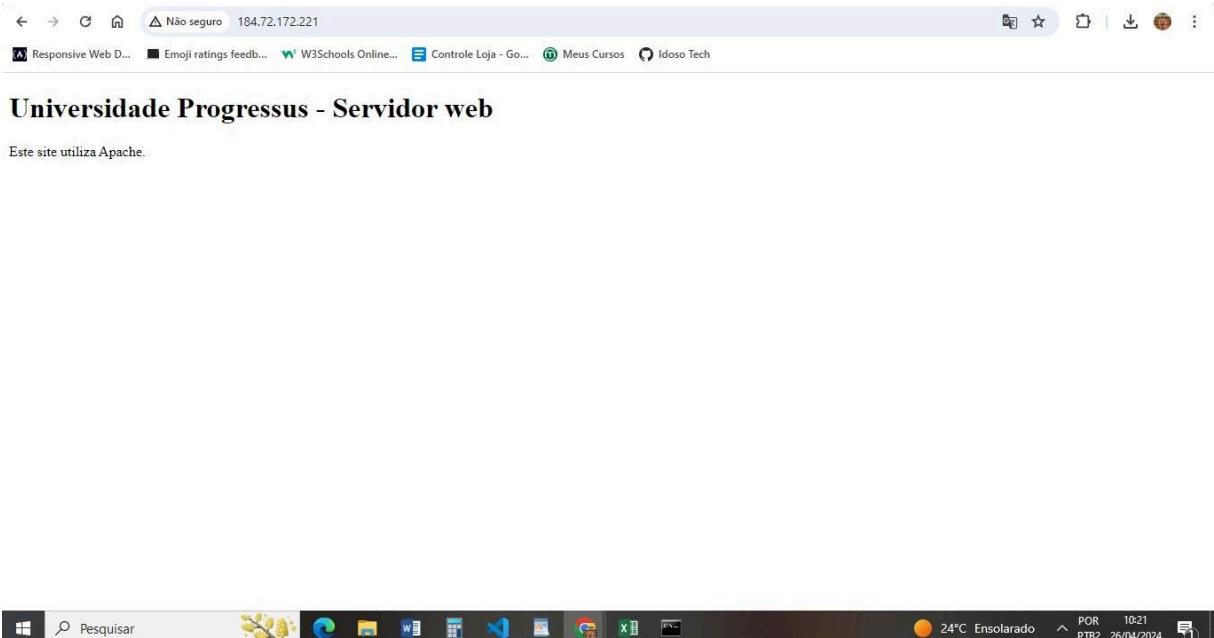
Apr 26 13:08:40 ip-172-31-28-45 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Apr 26 13:08:40 ip-172-31-28-45 systemd[1]: Started apache2.service - The Apache HTTP Server.
ubuntu@ip-172-31-28-45:~$ sudo ufw allow 'Apache'
Rules updated
Rules updated (v6)
ubuntu@ip-172-31-28-45:~$ sudo ufw status
Status: inactive
ubuntu@ip-172-31-28-45:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
ubuntu@ip-172-31-28-45:~$ sudo ufw status
Status: active

To           Action      From
--           -----      ---
Apache        ALLOW      Anywhere
Apache (v6)   ALLOW      Anywhere (v6)

ubuntu@ip-172-31-28-45:~$ 

```

Servidor Web da Universidade Progressus



## Instalando JDK para o servidor de aplicação

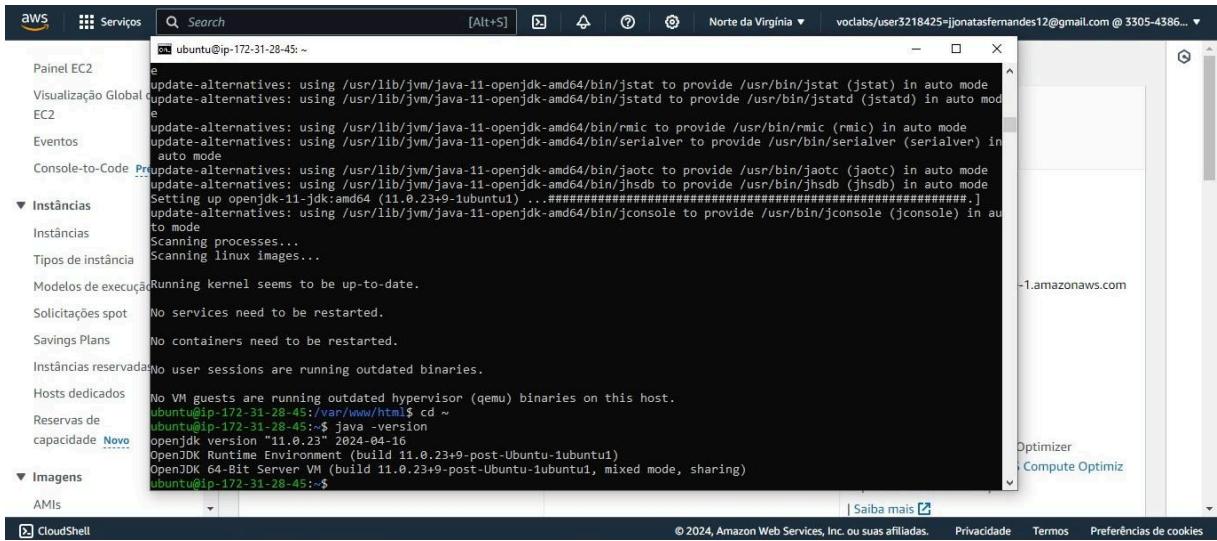
```

aws Serviços Search [Alt+S] 24°C Ensolarado POR 10:21 PTB2 26/04/2024
Norte da Virgínia v vocabs/user3218425=jjonatasfernandes12@gmail.com @ 3305-4386...
ubuntu@ip-172-31-28-45:~ update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jstack to provide /usr/bin/jstack (jstack) in auto mode
e update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jstat to provide /usr/bin/jstat (jstat) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jstatd to provide /usr/bin/jstatd (jstatd) in auto mode
e update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/rmic to provide /usr/bin/rmic (rmic) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/serialver to provide /usr/bin/serialver (serialver) in auto mode
auto mode update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jaotc to provide /usr/bin/jaotc (jaotc) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jhsdb to provide /usr/bin/jhsdb (jhsdb) in auto mode
Setting up openjdk-11-jdk-amd64 (11.0.23+9-1ubuntu1) ...#####
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jconsole to provide /usr/bin/jconsole (jconsole) in auto mode
to mode
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
Savings Plans
No containers need to be restarted.
Instâncias reservadas
No user sessions are running outdated binaries.
Hosts dedicados
Reservas de capacidade Novo
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-28-45:/var/www/html$ cd ~
ubuntu@ip-172-31-28-45:~$ sudo apt install openjdk-11-jdk

```

© 2024, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

## Verificando a versão instalada



```

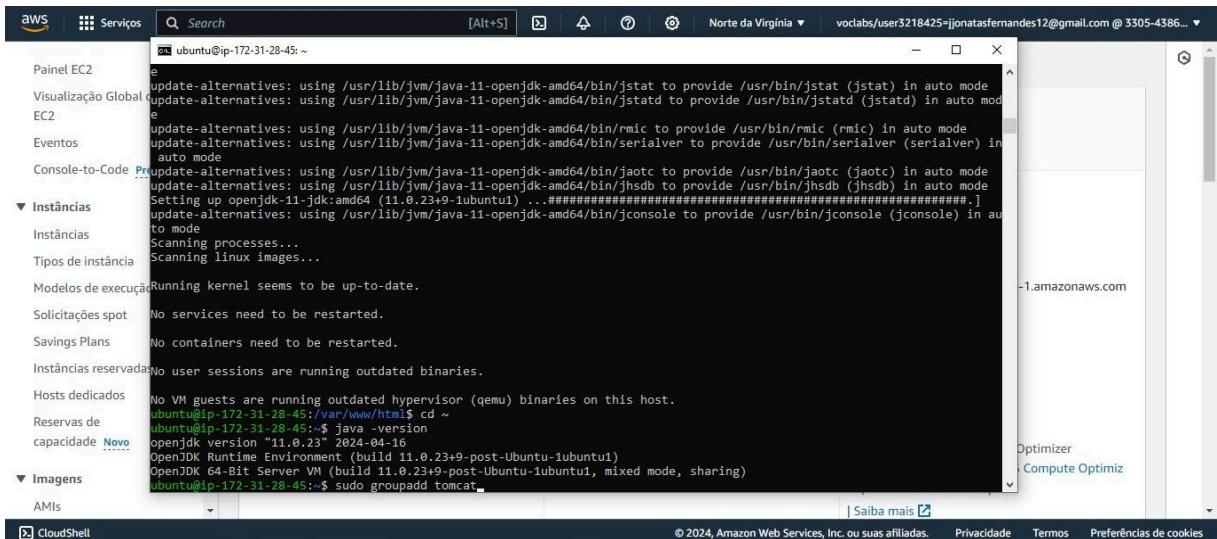
aws Serviços Search [Alt+S] Norte da Virgínia v vocabs/user3218425=jonatasfernandes12@gmail.com @ 3305-4386... ▾
Painel EC2
Visualização Global
EC2
Eventos
Console-to-Code
Instâncias
Instâncias
Tipos de instância
Modelos de execução
Solicitações spot
Savings Plans
Instâncias reservadas
Hosts dedicados
Reservas de capacidade Novo
Imagens
AMIs
CloudShell

ubuntu@ip-172-31-28-45:~ e
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jstat to provide /usr/bin/jstat (jstat) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jstatd to provide /usr/bin/jstatd (jstatd) in auto mode
e
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/rmic to provide /usr/bin/rmic (rmic) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/serialver to provide /usr/bin/serialver (serialver) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jaotc to provide /usr/bin/jaotc (jaotc) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jhsdb to provide /usr/bin/jhsdb (jhsdb) in auto mode
Setting up openjdk-11-jdk:amd64 (11.0.23+9-1ubuntu1) ...#####
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jconsole to provide /usr/bin/jconsole (jconsole) in auto mode
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-28-45:~/var/www/html$ cd ~
ubuntu@ip-172-31-28-45:$ java -version
openjdk version "11.0.23" 2024-04-16
OpenJDK Runtime Environment (build 11.0.23+9-post-Ubuntu-1ubuntu1)
OpenJDK 64-Bit Server VM (build 11.0.23+9-post-Ubuntu-1ubuntu1, mixed mode, sharing)
ubuntu@ip-172-31-28-45:$

  Saiba mais ▾
© 2024, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

```

## Configurando Tomcat para Servidor



```

aws Serviços Search [Alt+S] Norte da Virgínia v vocabs/user3218425=jonatasfernandes12@gmail.com @ 3305-4386... ▾
Painel EC2
Visualização Global
EC2
Eventos
Console-to-Code
Instâncias
Instâncias
Tipos de instância
Modelos de execução
Solicitações spot
Savings Plans
Instâncias reservadas
Hosts dedicados
Reservas de capacidade Novo
Imagens
AMIs
CloudShell

ubuntu@ip-172-31-28-45:~ e
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jstat to provide /usr/bin/jstat (jstat) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jstatd to provide /usr/bin/jstatd (jstatd) in auto mode
e
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/rmic to provide /usr/bin/rmic (rmic) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/serialver to provide /usr/bin/serialver (serialver) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jaotc to provide /usr/bin/jaotc (jaotc) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jhsdb to provide /usr/bin/jhsdb (jhsdb) in auto mode
Setting up openjdk-11-jdk:amd64 (11.0.23+9-1ubuntu1) ...#####
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jconsole to provide /usr/bin/jconsole (jconsole) in auto mode
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-28-45:~/var/www/html$ cd ~
ubuntu@ip-172-31-28-45:$ java -version
openjdk version "11.0.23" 2024-04-16
OpenJDK Runtime Environment (build 11.0.23+9-post-Ubuntu-1ubuntu1)
OpenJDK 64-Bit Server VM (build 11.0.23+9-post-Ubuntu-1ubuntu1, mixed mode, sharing)
ubuntu@ip-172-31-28-45:$ sudo groupadd tomcat
  Saiba mais ▾
© 2024, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

```

## Criando usuário Tomcat.

```

ubuntu@ip-172-31-28-45:~ 
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jstat to provide /usr/bin/jstat (jstat) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jstadv to provide /usr/bin/jstadv (jstadv) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/rmic to provide /usr/bin/rmic (rmic) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/serialver to provide /usr/bin/serialver (serialver) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jactc to provide /usr/bin/jactc (jactc) in auto mode
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jhsdb to provide /usr/bin/jhsdb (jhsdb) in auto mode
Setting up openjdk-11-jdk:amd64 (11.0.23+9-1ubuntu1) ...#####
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jconsole to provide /usr/bin/jconsole (jconsole) in auto mode
to mode
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-28-45:~$ cd ~
ubuntu@ip-172-31-28-45:~$ java -version
openjdk version "11.0.23" 2024-04-16
OpenJDK Runtime Environment (build 11.0.23+9-post-Ubuntu-1ubuntu1)
OpenJDK 64-Bit Server VM (build 11.0.23+9-post-Ubuntu-1ubuntu1, mixed mode, sharing)
ubuntu@ip-172-31-28-45:~$ sudo groupadd tomcat
ubuntu@ip-172-31-28-45:~$ sudo useradd -s /bin/false -g tomcat -d /opt/tomcat tomcat

```

© 2024, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

25°C Ensolarado POR 10:25 PTB2 26/04/2024

## Baixando Tomcat

```

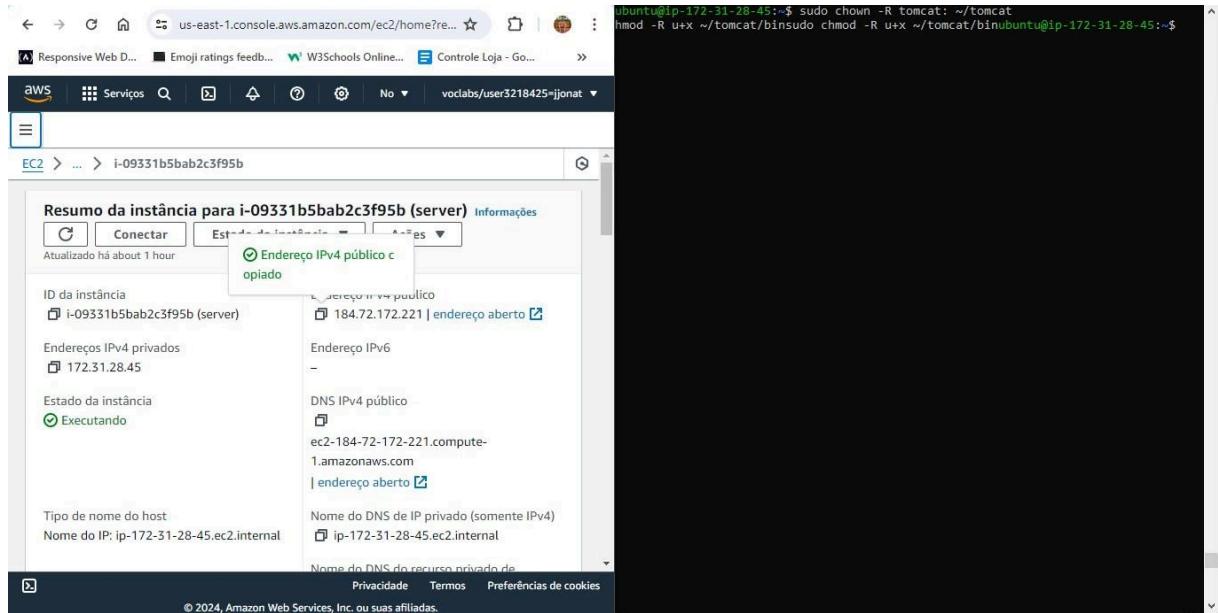
ubuntu@ip-172-31-28-45:~ 
Setting up openjdk-11-jdk:amd64 (11.0.23+9-1ubuntu1) ...#####
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/jconsole to provide /usr/bin/jconsole (jconsole) in auto mode
to mode
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-28-45:~$ cd ~
ubuntu@ip-172-31-28-45:~$ java -version
openjdk version "11.0.23" 2024-04-16
OpenJDK Runtime Environment (build 11.0.23+9-post-Ubuntu-1ubuntu1)
OpenJDK 64-Bit Server VM (build 11.0.23+9-post-Ubuntu-1ubuntu1, mixed mode, sharing)
ubuntu@ip-172-31-28-45:~$ sudo groupadd tomcat
ubuntu@ip-172-31-28-45:~$ cd /tmp
ubuntu@ip-172-31-28-45:~/tmp$ curl -O https://dlcdn.apache.org/tomcat/tomcat-9/v9.0.68/bin/apache-tomcat-9.0.68.tar.gz
% Total % Received % Xferd Average Speed Time Time Current
          Dload Upload Total Spent Left Speed
100  196 100  196  0     0  444  0 --:--:--:--:--:-- 443
ubuntu@ip-172-31-28-45:~/tmp$ 

```

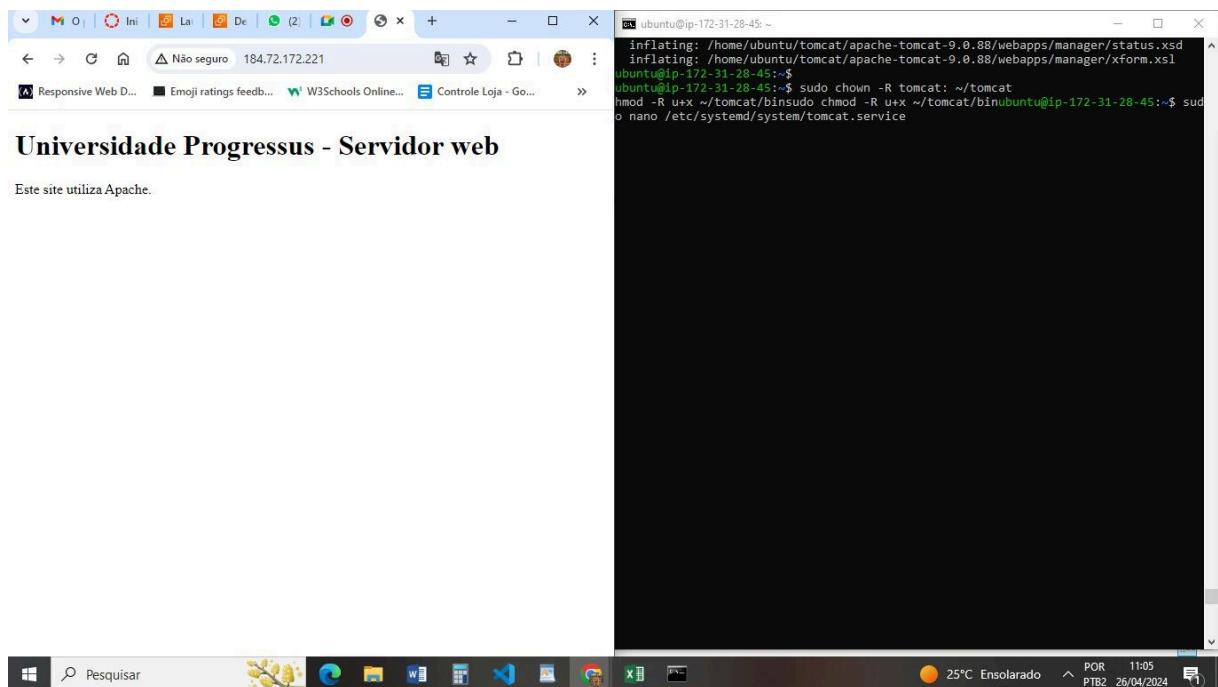
© 2024, Amazon Web Services, Inc. ou suas afiliadas. Privacidade Termos Preferências de cookies

Próxima do registro POR 10:27 PTB2 26/04/2024

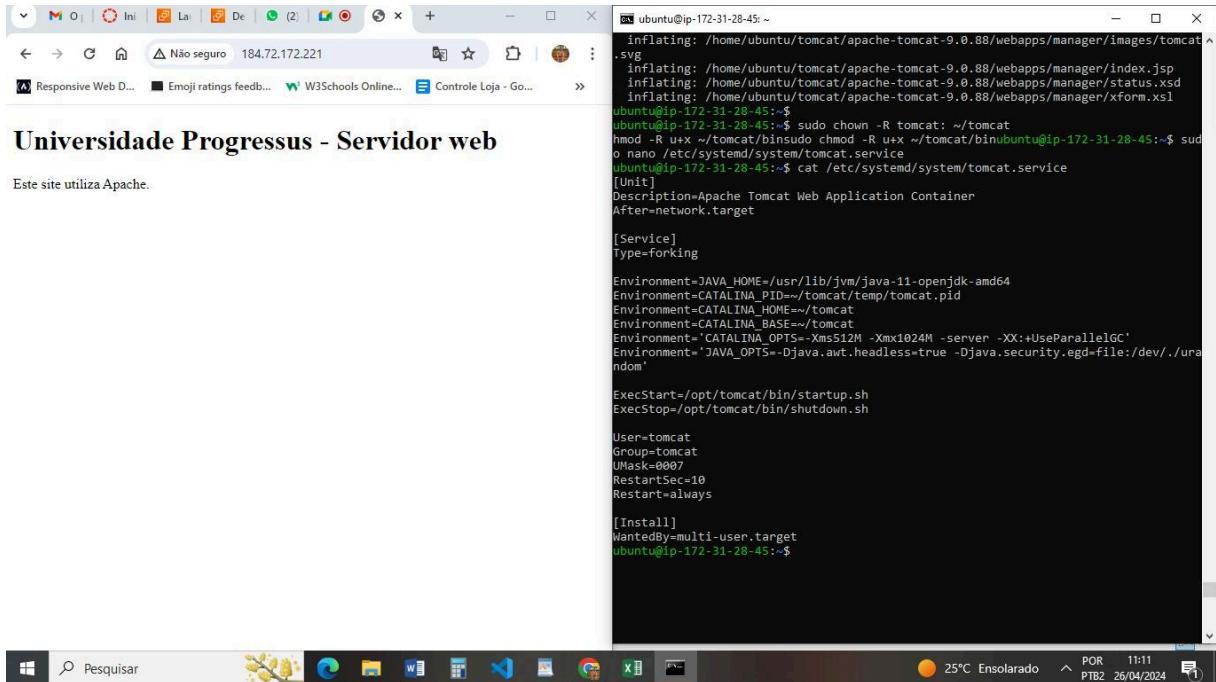
## Alterando as permissões do Tomcat .



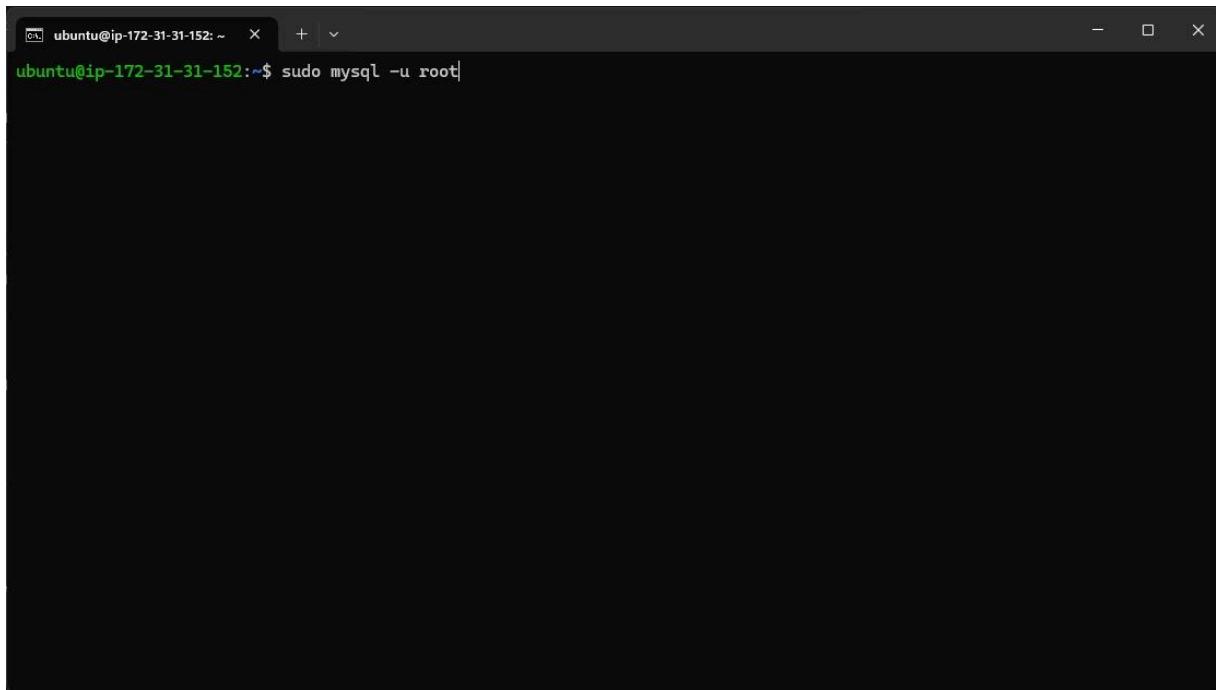
## Criando o arquivo de serviço systemd.



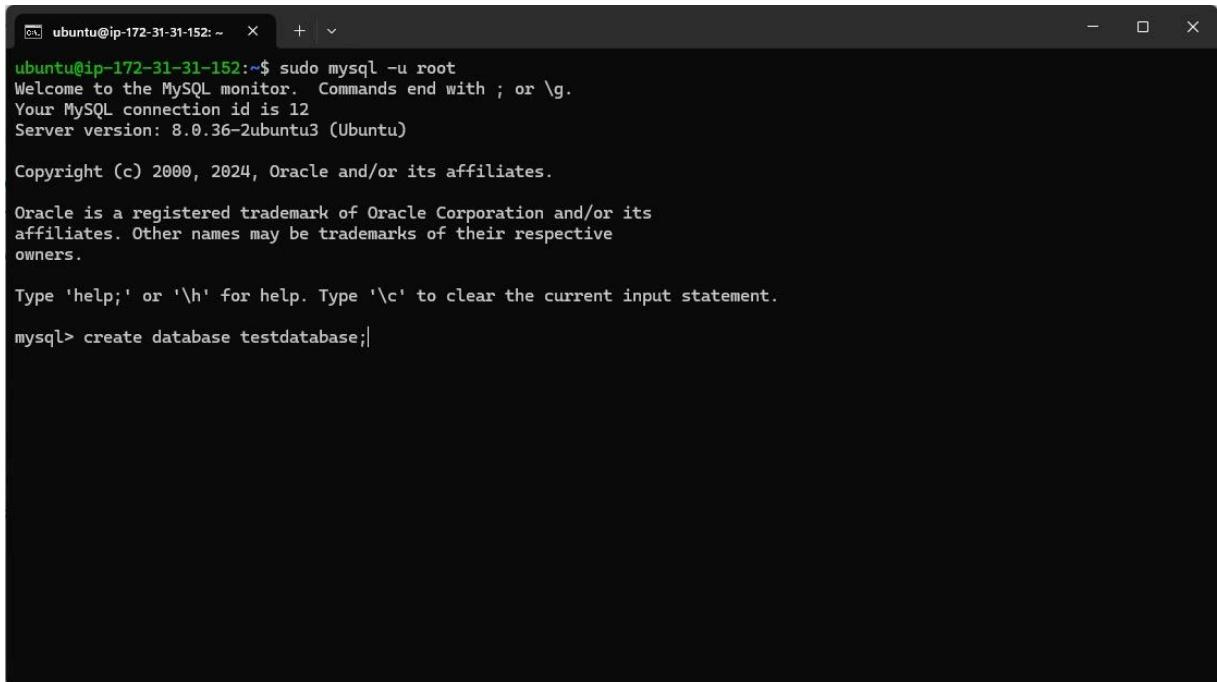
## Variáveis de update .



## Acesso ao banco de Dados.



## Criando o Database



```
ubuntu@ip-172-31-31-152:~$ sudo mysql -u root
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.36-2ubuntu3 (Ubuntu)

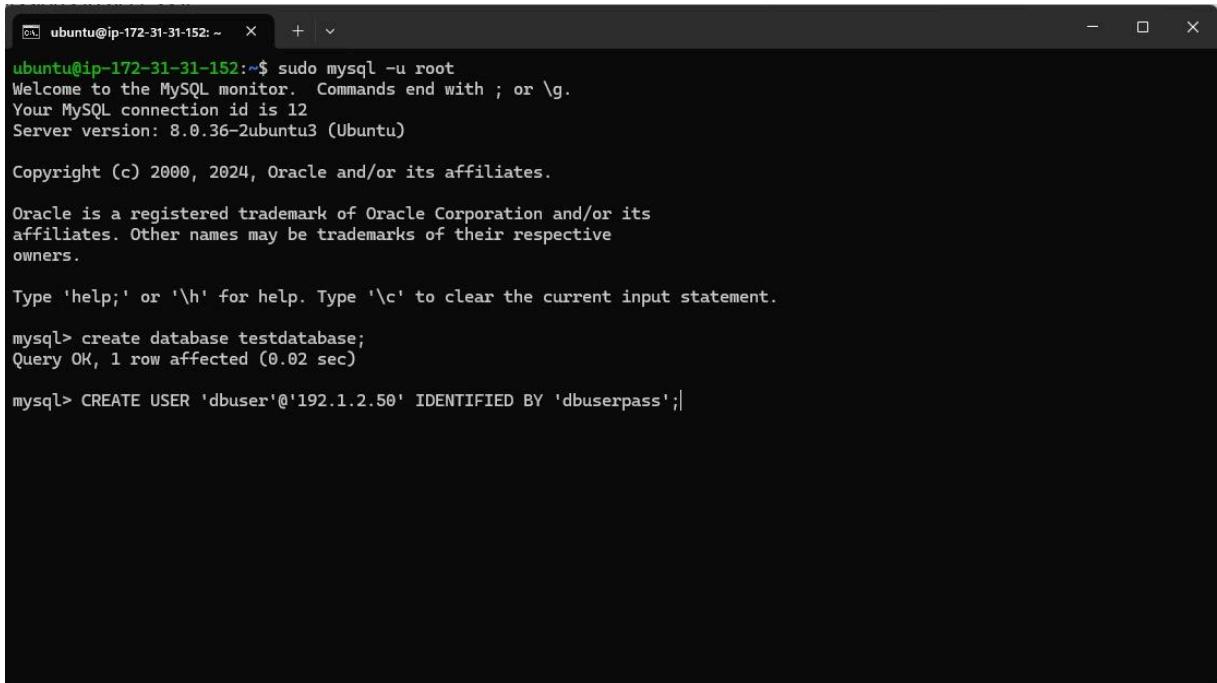
Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database testdatabase;
```

Criando um usuário com nome e senha.



```
ubuntu@ip-172-31-31-152:~$ sudo mysql -u root
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.36-2ubuntu3 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database testdatabase;
Query OK, 1 row affected (0.02 sec)

mysql> CREATE USER 'dbuser'@'192.1.2.50' IDENTIFIED BY 'dbuserpass';
```

Concedendo permissões ao usuário criado.

```

ubuntu@ip-172-31-31-152:~$ sudo mysql -u root
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.36-2ubuntu3 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database testdatabase;
Query OK, 1 row affected (0.02 sec)

mysql> CREATE USER 'dbuser'@'192.1.2.50' IDENTIFIED BY 'dbuserpass';
ERROR 1396 (HY000): Operation CREATE USER failed for 'dbuser'@'192.1.2.50'
mysql> CREATE USER 'root'@'192.1.2.50' IDENTIFIED BY 'dbuserpass';
Query OK, 0 rows affected (0.01 sec)

mysql> GRANT ALL PRIVILEGES ON testdb.* TO 'root' @'192.1.2.50';

```

Atualizando permissões.

```

ubuntu@ip-172-31-31-152:~$ sudo mysql -u root
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.36-2ubuntu3 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database testdatabase;
Query OK, 1 row affected (0.02 sec)

mysql> CREATE USER 'dbuser'@'192.1.2.50' IDENTIFIED BY 'dbuserpass';
ERROR 1396 (HY000): Operation CREATE USER failed for 'dbuser'@'192.1.2.50'
mysql> CREATE USER 'root'@'192.1.2.50' IDENTIFIED BY 'dbuserpass';
Query OK, 0 rows affected (0.01 sec)

mysql> GRANT ALL PRIVILEGES ON testdb.* TO 'root' @'192.1.2.50';
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;

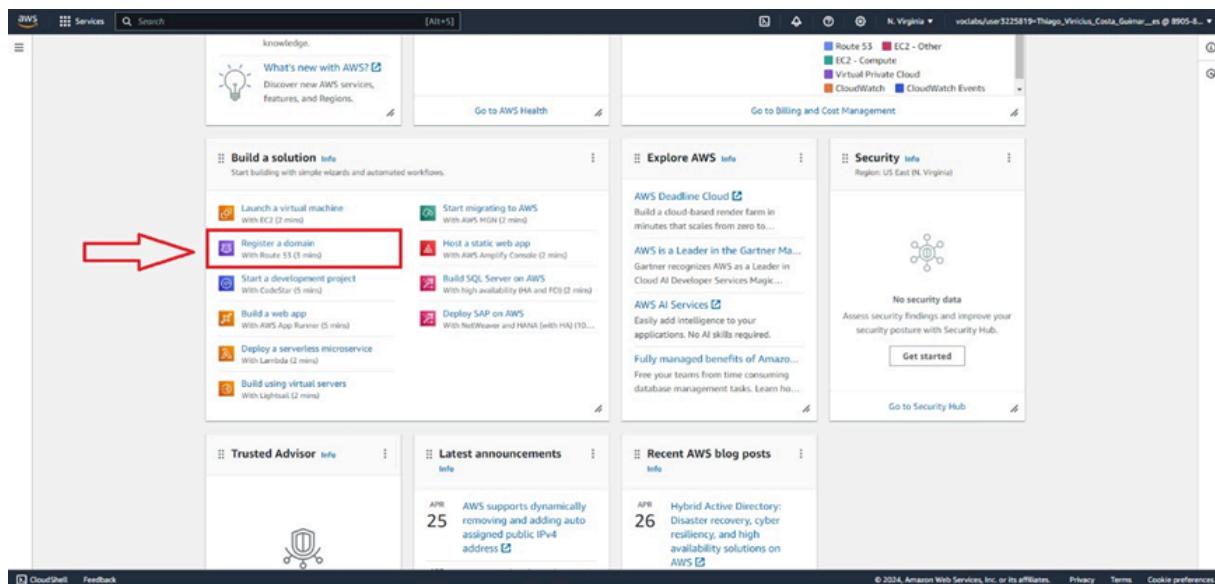
```

Visualizando o banco de dados criado.

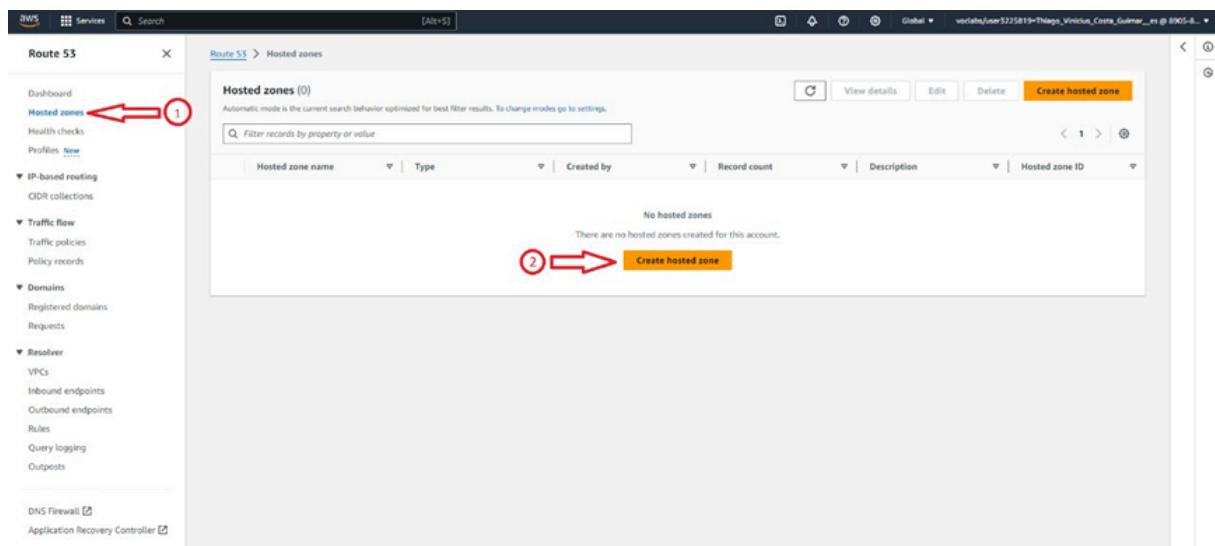
```
ubuntu@ip-172-31-31-152: ~ + ~ Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Type 'help;' or '\h' for help. Type '\c' to clear the current input statement. mysql> create database testdatabase; Query OK, 1 row affected (0.02 sec) mysql> CREATE USER 'dbuser'@'192.1.2.50' IDENTIFIED BY 'dbuserpass'; ERROR 1396 (HY000): Operation CREATE USER failed for 'dbuser'@'192.1.2.50' mysql> CREATE USER 'root'@'192.1.2.50' IDENTIFIED BY 'dbuserpass'; Query OK, 0 rows affected (0.01 sec) mysql> GRANT ALL PRIVILEGES ON testdb.* TO 'root' @'192.1.2.50'; Query OK, 0 rows affected (0.00 sec) mysql> FLUSH PRIVILEGES; Query OK, 0 rows affected (0.00 sec) mysql> SHOW DATABASES LIKE 'testdatabase'; +-----+ | Database (testdatabase) | +-----+ | testdatabase | +-----+ 1 row in set (0.00 sec) mysql> |
```

### 2.2.3. DNS

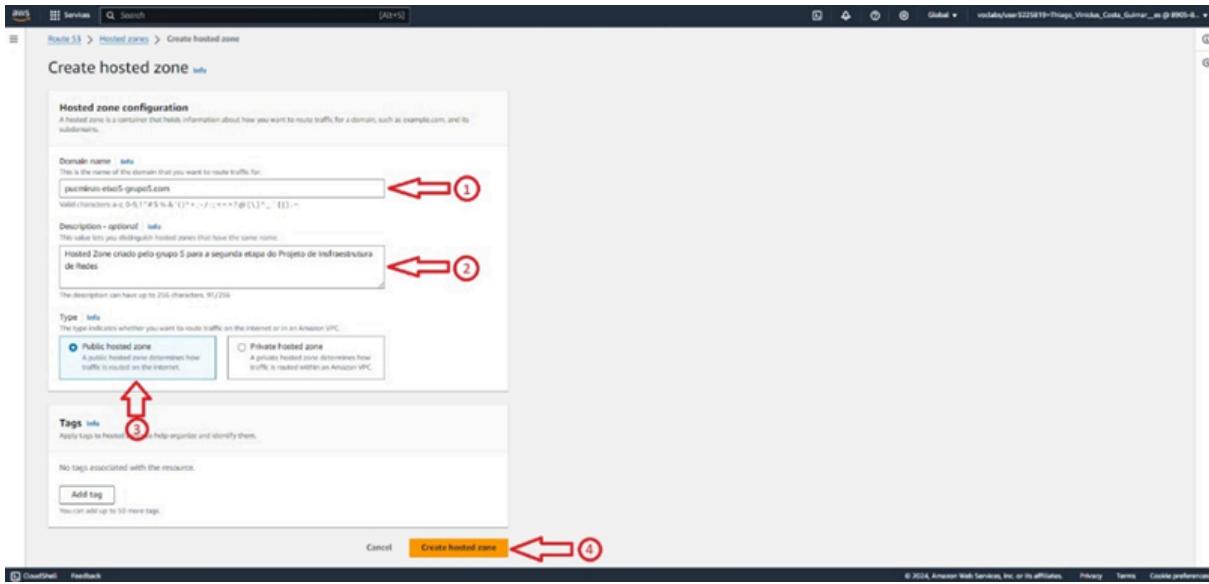
A configuração do sistema de DNS utilizou a ferramenta/serviço *Route 53* disponibilizado pela AWS (Amazon Web Services), para que o acesso do servidor fosse feito através de um domínio.



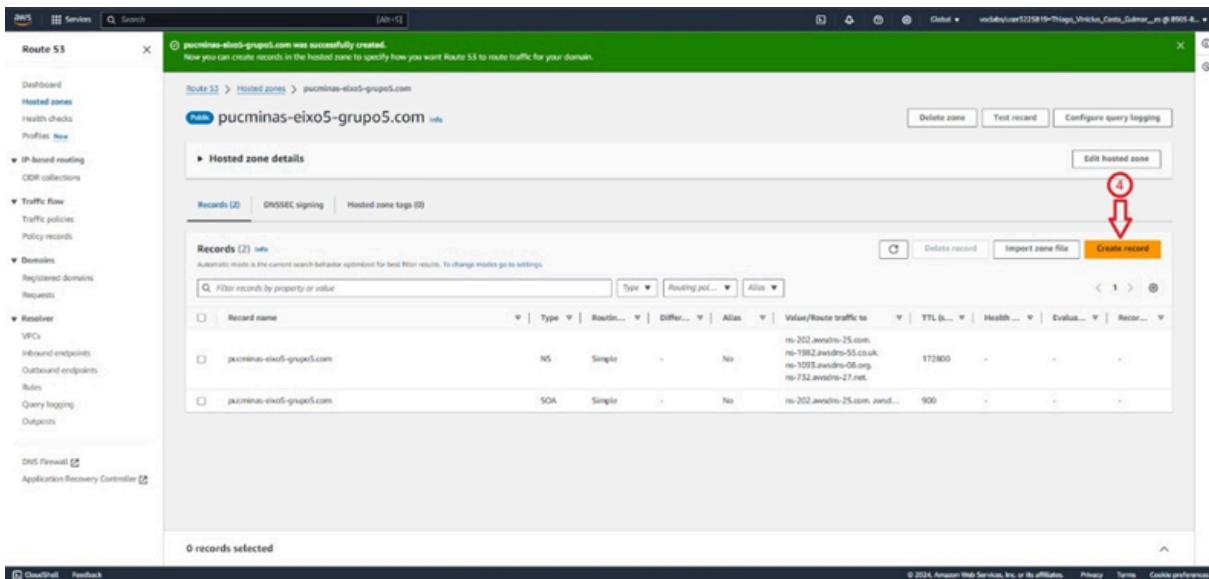
A figura acima indica a área em que é feito o acesso do serviço *Route 53*, sendo encontrado na aba “*Build a solution*” (*Construa uma solução*).



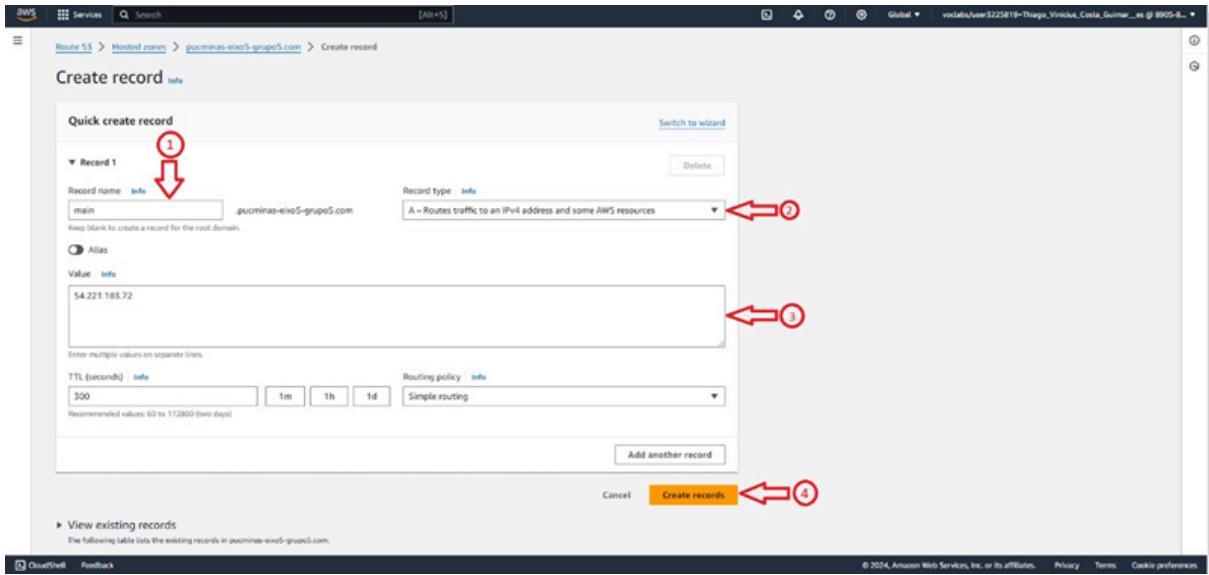
Após o acesso ao Route 53, é necessário que seja acessado a área de *Hosted Zones*, podendo ser encontrado na aba lateral esquerda (passo 1), e seja clicado no botão “*Create a Hosted Zone*” (passo 2).



O botão “*Create a Hosted Zone*” na tela anterior redireciona o usuário para o formulário de criação, em que será preenchido o nome do domínio, a descrição, e o tipo da hosted zone (passos 1, 2 e 3 respectivamente). Após o preenchimento dessas informações, o usuário irá criar a zona clicando no botão de confirmação (passo 4).



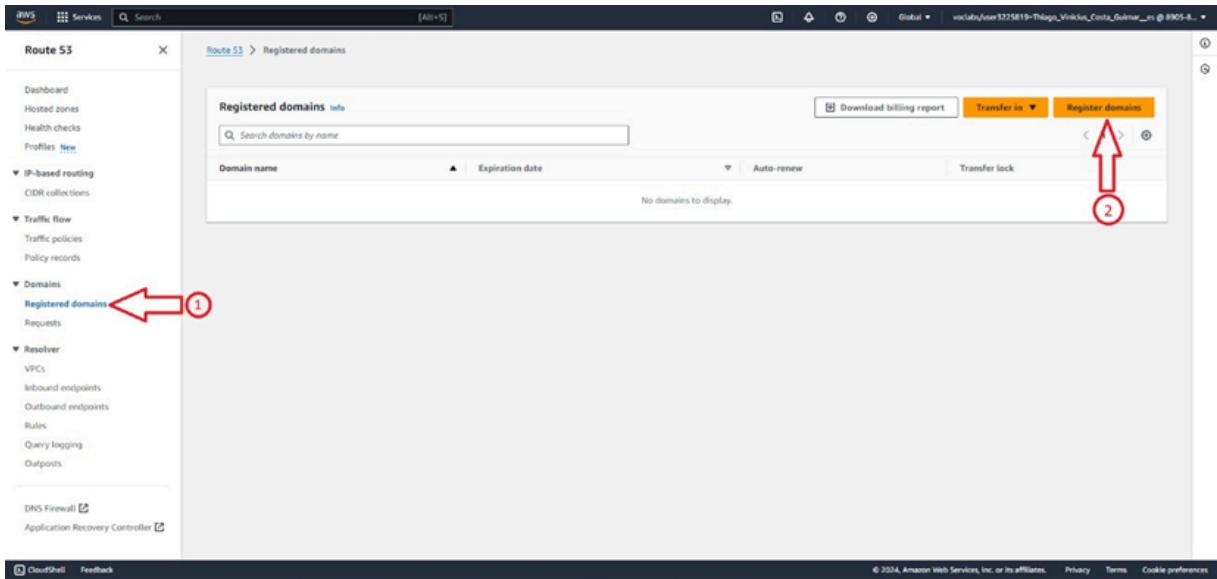
Após a criação da Hosted Zone, é apresentado uma mensagem para o usuário informando que que a zona foi criada com sucesso, e após isso o usuário irá criar um “*Record*”, que será responsável por acessar subdomínios do DNS, a ação pode ser feita através do botão “*Create Record*” (passo 4).



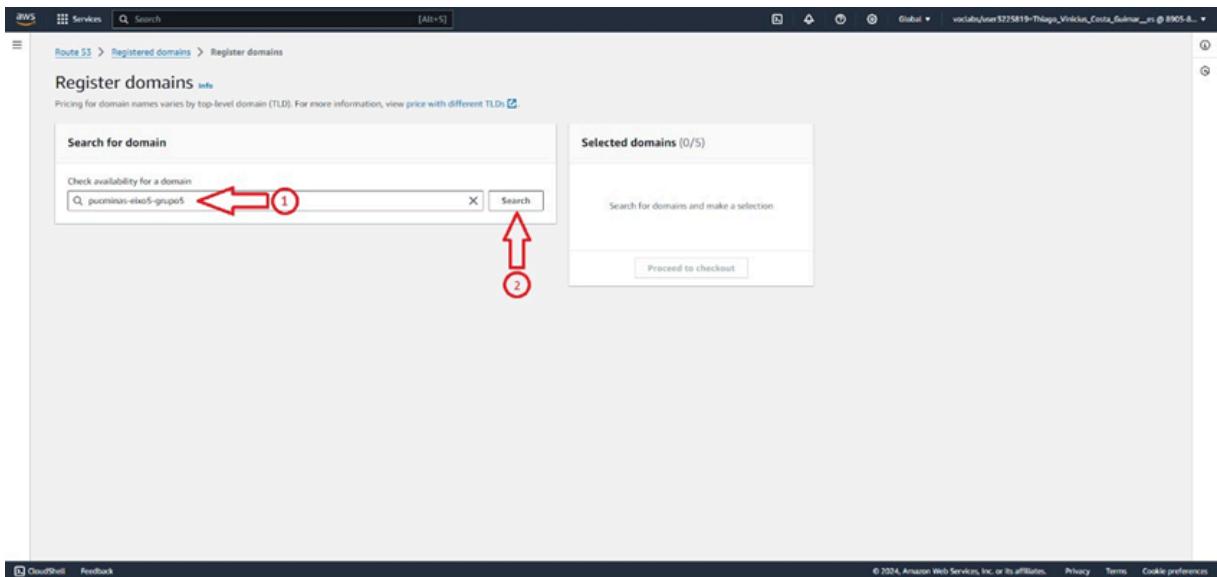
A botão “*Create Record*” na tela anterior, redireciona o usuário para o formulário de criação, em que será preenchido o nome (passo 1), o tipo (passo 2) e o valor, responsável por acessar a página ou endereço para o qual o usuário deseja utilizar (passo 3), e dada as informações, ao clicar no botão “*Create Records*” cria o record desejado.

Record name	Type	Routing	Alias	Value/Route traffic to	TTL (seconds)	Health	Evaluate	Records
pucminas-eixo5-grupo5.com	NS	Simple	No	ns-202.awsdns-25.com. ns-1982.awsdns-55.co.uk. ns-1093.awsdns-08.org. ns-732.awsdns-27.net.	172800	-	-	3
pucminas-eixo5-grupo5.com	SOA	Simple	No	ns-202.awsdns-25.com.awsd...	900	-	-	1
main.pucminas-eixo5-grupo5.com	A	Simple	No	54.221.183.72	300	-	-	1

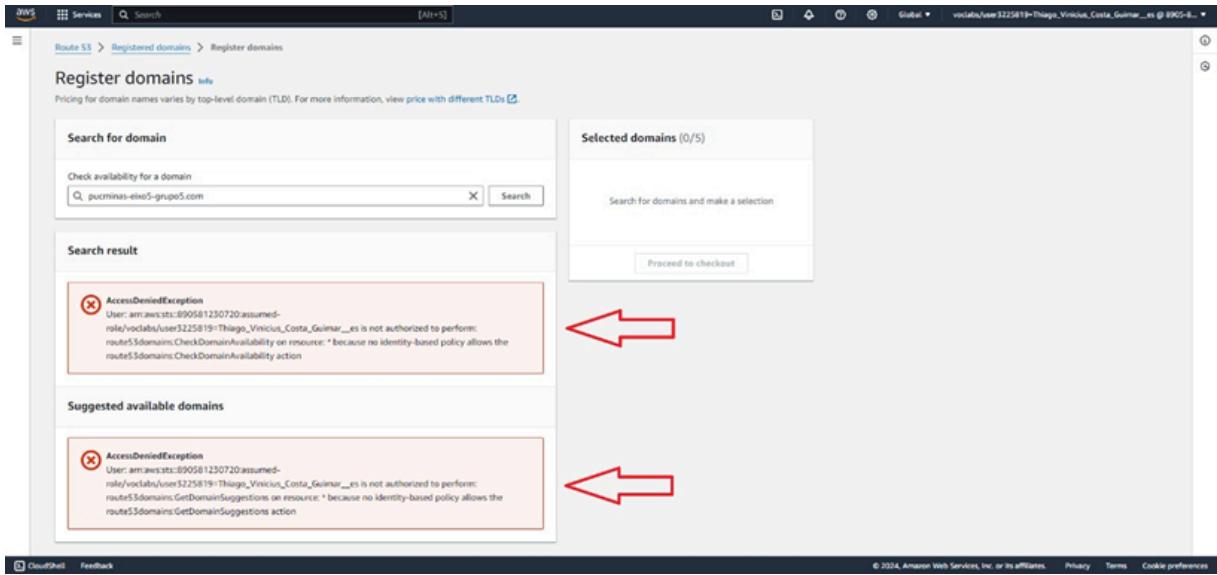
Após a criação, o sistema informa que o record foi criado com sucesso, e é possível ter uma visão geral da hosted zone com todas as rotas configuradas.



Para o registro do domínio online, é necessário que o usuário acesse a área “*Registered Domains*” na aba lateral esquerda (passo 1), e clique no botão “*Register Domain*” (passo 2).



Será aberto um formulário de criação, em que será solicitado do usuário o domínio desejado (passo 1), para que seja feita uma verificação de disponibilidade, para isso o usuário irá clicar no botão “*Search*” (passo 2).



De acordo com os testes feitos pelo grupo, o AWS não está permitindo os usuários de criarem um domínio utilizando seus recursos nativos, informando um erro no qual o usuário não está autorizado para realizar a ação de criar um domínio.

## 2.2.4. PROXY

Configuramos uma instância EC2 usando a AMI Debian no nível gratuito com 16GB de espaço interno. O tipo de instância selecionado foi t2.micro, adequado para testes.

Instance ID	Public IPv4 address
▀ i-0fd0d30480af1f7cf (Proxy Server)	▀ 3.92.60.131   <a href="#">open address</a> □
IPv6 address	Instance state
-	▀ <span style="color: green;">Running</span>
Hostname type	Private IP DNS name (IPv4 only)
IP name: ip-172-31-84-155.ec2.internal	▀ ip-172-31-84-155.ec2.internal
Answer private resource DNS name	Instance type
IPv4 (A)	t2.micro
Auto-assigned IP address	VPC ID
▀ 3.92.60.131 [Public IP]	▀ vpc-0c8e4f3d29b9d749e □
IAM Role	Subnet ID
-	▀ subnet-0ff6e4179108c855f □
IMDSv2	
Required	

Após a instância estar operacional, realizamos a conexão via SSH, usando a chave privada associada. Isso nos permitiu acessar o terminal do servidor onde o Squid proxy seria configurado.

```
$ ssh -i "proxy.pem" admin@ec2-3-92-60-131.compute-1.amazonaws.com
```

No terminal conectado, executamos o comando `sudo apt install squid` para instalar o serviço de proxy. Após a instalação executamos o comando para verificar se o serviço estava rodando normalmente:

```
$ sudo systemctl status squid.service
```

```
admin@ip-172-31-84-155:~$ sudo systemctl status squid.service
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; preset: enabled)
   Active: active (running) since Tue 2024-04-16 21:55:03 UTC; 39min ago
     Docs: man:squid(8)
 Process: 2081 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
 Main PID: 2085 (squid)
   Tasks: 4 (limit: 1141)
  Memory: 20.7M
    CPU: 800ms
   CGroup: /system.slice/squid.service
           └─2085 /usr/sbin/squid --foreground -sYC
             ├─2087 "(squid-1)" --kid squid-1 --foreground -sYC
             ├─2088 "(logfile-daemon)" /var/log/squid/access.log
             ├─2089 "(pinger)"

Apr 16 21:55:03 ip-172-31-84-155 squid[2087]: Using Least Load store dir selection
Apr 16 21:55:03 ip-172-31-84-155 squid[2087]: Set Current Directory to /var/spool/squid
Apr 16 21:55:03 ip-172-31-84-155 squid[2087]: Finished loading MIME types and icons.
Apr 16 21:55:03 ip-172-31-84-155 squid[2087]: HTCP Disabled.
Apr 16 21:55:03 ip-172-31-84-155 squid[2087]: Pinger socket opened on FD 14
Apr 16 21:55:03 ip-172-31-84-155 squid[2087]: Squid plugin modules loaded: 0
Apr 16 21:55:03 ip-172-31-84-155 squid[2087]: Adaptation support is off.
Apr 16 21:55:03 ip-172-31-84-155 squid[2087]: Accepting HTTP Socket connections at conn3 local=[ :: ]:80 remote=[ :: ] FD 12 flags=9
Apr 16 21:55:03 ip-172-31-84-155 systemd[1]: Started squid.service - Squid Web Proxy Server.
Apr 16 21:55:04 ip-172-31-84-155 squid[2087]: storeLateRelease: released 0 objects
admin@ip-172-31-84-155:~$
```

O próximo passo após verificar que o serviço está rodando corretamente foi configurar quais domínios deveriam ser bloqueados pelo proxy. A mérito de demonstração escolhemos os seguintes domínios:

- facebook.com
- youtube.com
- twitter.com

Para adicionar essa regra de bloqueio ao proxy precisamos abrir o arquivo de configuração com o seguinte comando:

```
$ sudo nano /etc/squid/squid.conf
```

No arquivo de configuração precisamos adicionar as regras de bloqueio assim como as regras de quais faixas de IP que seriam permitidas

```

GNU nano 7.2                               /etc/squid/squid.conf *
acl toblock dstdomain .facebook.com .youtube.com .twitter.com
http_access deny toblock

acl allowed_client src ||
http_access allow allowed_client

acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8               # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10            # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16           # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12            # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16           # RFC 1918 local private network (LAN)
acl localnet src fc00::/7                # RFC 4193 local private network range
acl localnet src fe80::/10               # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80      # http
acl Safe_ports port 21      # ftp
acl Safe_ports port 443     # https
acl Safe_ports port 70      # gopher
acl Safe_ports port 210     # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280     # http-mgmt
acl Safe_ports port 488     # gss-http
acl Safe_ports port 591     # filemaker
acl Safe_ports port 777     # multiling http
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
include /etc/squid/conf.d/*.conf

^G Help      ^O Write Out   ^W Where Is    ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File   ^\ Replace     ^U Paste      ^J Justify    ^Y Go To Line M-E Redo
                                         M-A Set Mark
                                         M-6 Copy

```

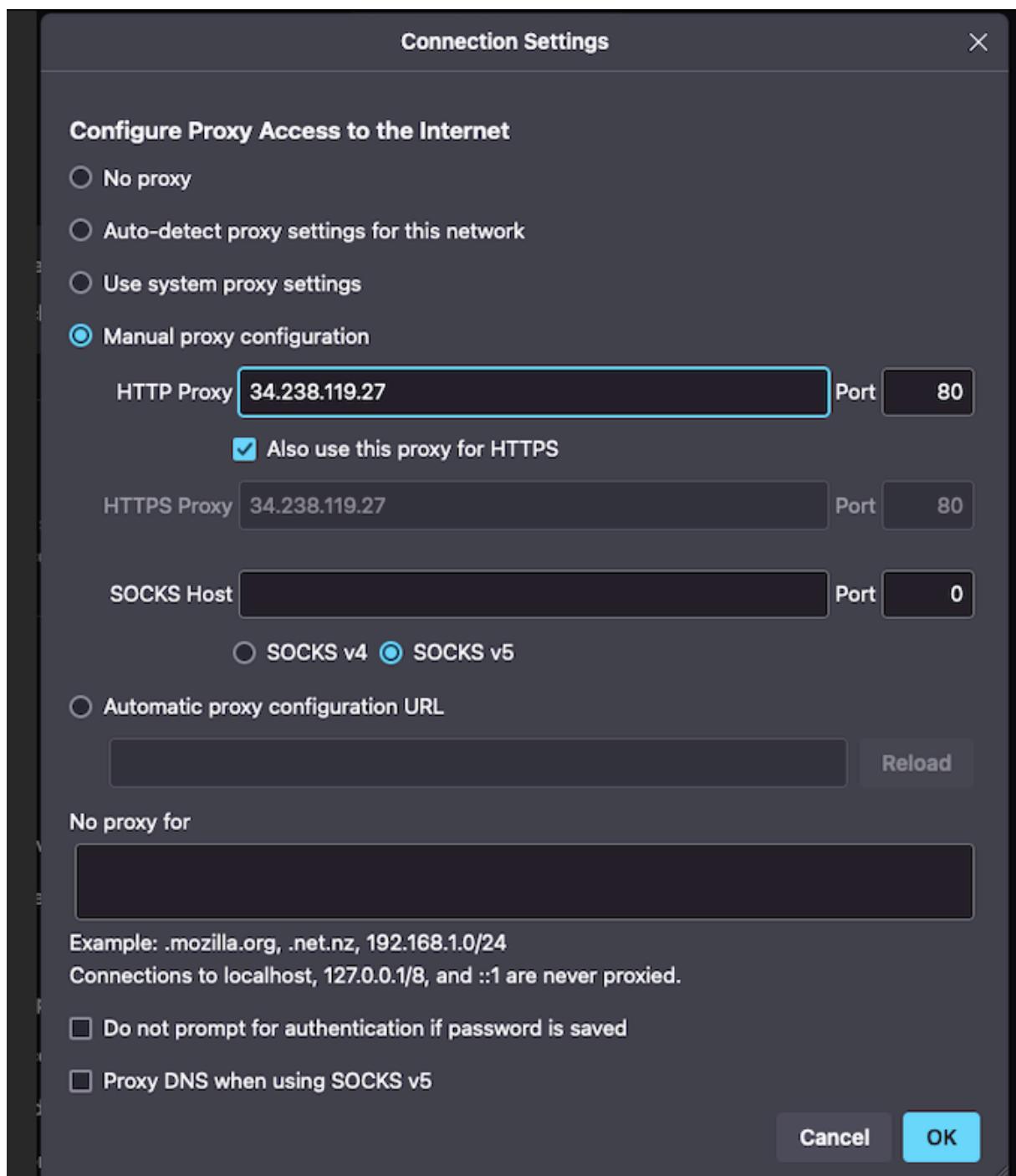
Após adicionar as configurações de bloqueio, precisamos reiniciar o serviço de proxy com o seguinte comando:

```
$ sudo systemctl restart squid.service
```

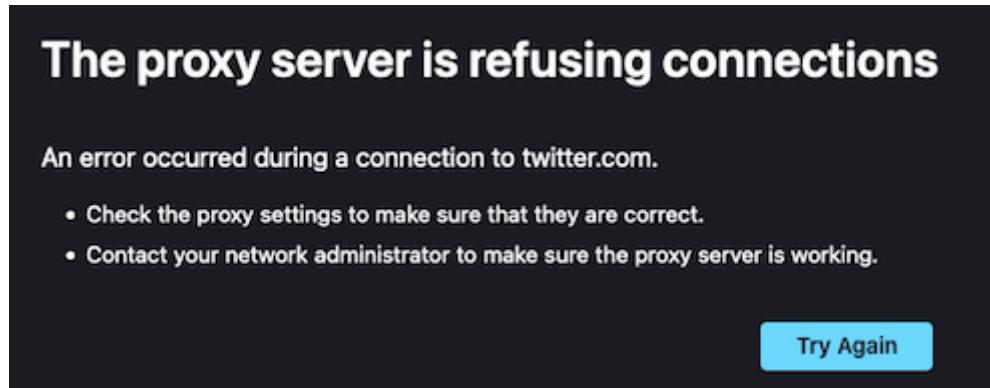
E depois verificar se o serviço estava rodando normalmente com

```
$ sudo systemctl status squid.service
```

Após garantir que o serviço estava rodando normalmente, precisamos configurar uma máquina para acessar a internet através do nosso serviço de proxy. Para testar o acesso via proxy o browser Firefox foi utilizado para fazer o teste. Com Firefox aberto, através do menu Settings > Network Connections adicionamos o IP público da máquina virtual na AWS:



Com o servidor de proxy configurado, tentamos acessar um dos sites bloqueados, e o browser realmente não deixou a navegação ser concluída com a seguinte mensagem:



"O servidor de proxy está recusando conexões"

Indicando que nossa configuração funcionou. Ao tentar acessar qualquer outro site, o browser navegou no site normalmente.

Para verificar se de fato nossas requisições estavam passando pelo proxy, acessamos a máquina da AWS novamente via SSH e rodamos o seguinte comando:

```
$ sudo tail -f /var/log/squid/access.log
```

Este comando mostra os logs de acesso do Squid, nosso serviço de proxy e nele conseguimos ver que o acesso aos domínios bloqueados retornaram um código 403 que significa

403—*Forbidden: The client does not have the access right for the content*

403—*Proibido: O cliente não tem direito de acesso ao conteúdo*

```
admin@ip-172-31-84-155:~$ sudo tail -f /var/log/squid/access.log
1713305904.291      2 188.          TCP_MISS/502 4215 POST http://event.wps.com/old/dynamic/api/dynamicParam/v1/app/cfcfd627ef2
5f - HIER_NONE/- text/html
1713306204.292      1 188.          TCP_MISS/502 4215 POST http://event.wps.com/old/dynamic/api/dynamicParam/v1/app/cfcfd627ef2
5f - HIER_NONE/- text/html
1713306451.089      171121 188.    TCP_TUNNEL/200 2764 CONNECT contile.services.mozilla.com:443 - HIER_DIRECT/34.117.237.239
1713306484.284      6 188.          TCP_MISS/200 726 GET http://ocsp.digicert.com/ME8wTTBLMEkwRzAHBgUrDgMCGgQU6468nUcrfgKRdxkj
wcUeV7UEFLPD5KT5ocXYrjZBzB AHAMq6rRzsTpMjWlHQITj3 - HIER_DIRECT/192.229.211.108 application/ocsp-response
1713306504.294      2 188.          TCP_MISS/502 4215 POST http://event.wps.com/old/dynamic/api/dynamicParam/v1/app/cfcfd627ef2
5f - HIER_NONE/- text/html
1713306566.541      3 188.          TCP_MISS/200 883 GET http://ocsp.digicert.com/ME8wTTBLMEkwRzAHBgUrDgMCGgQU6468nUcrfgKRdxkj
AWIBVe4EFAPeUDVW0Uy7ZvCj4h: AHACdC6qF8q0IccXuxX2F8%2FQyg - HIER_DIRECT/192.229.211.108 application/ocsp-response
1713306766.312      2352 188.    TCP_TUNNEL/200 303308 CONNECT miro.medium.com:443 - HIER_DIRECT/162.159.152.4 -
1713306804.292      2 188.          TCP_MISS/502 4215 POST http://event.wps.com/old/dynamic/api/dynamicParam/v1/app/cfcfd627ef2
5f - HIER_NONE/- text/html
1713306937.555      171149 188.    TCP_TUNNEL/200 132546 CONNECT miro.medium.com:443 - HIER_DIRECT/162.159.152.4 -
1713306939.563      177549 188.    TCP_TUNNEL/200 6861 CONNECT medium.com:443 - HIER_DIRECT/162.159.153.4 -
1713307027.160      0 188.          TCP_DENIED/403 4044 CONNECT www.facebook.com:443 - HIER_NONE/- text/html
1713307030.316      0 188.          NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -
1713307033.999      0 188.          TCP_DENIED/403 4029 CONNECT youtube.com:443 - HIER_NONE/- text/html
1713307034.364      331 188.        TCP_TUNNEL/200 1477 CONNECT safebrowsing.googleapis.com:443 - HIER_DIRECT/142.251.167.95 -
1713307038.046      0 188.          TCP_DENIED/403 4029 CONNECT youtube.com:443 - HIER_NONE/- text/html
1713307042.101      0 188.          NONE_NONE/000 0 - error:transaction-end-before-headers - HIER_NONE/- -

```

## 2.2.5. FTP

### Servidores Hospedados em Nuvem

Instância lab AWS:

The screenshot shows the AWS Academy Learner Lab interface. On the left is a sidebar with navigation links: Conta, Painel de controle, Cursos, Calendário, Caixa de entrada, Histórico, and Ajuda. The main area has tabs for Página inicial, Módulos, and Fóruns. The Página inicial tab is active, showing a terminal window with the command 'eee\_W\_3146179@runweb122992:~\$'. The terminal window also displays the AWS logo. At the top, there's a header with the URL 'awsacademy.instructure.com/courses/78849/modules/items/7114094', a progress bar showing 'Used \$0.4 of \$100', and a timer '03:35'. Below the terminal are buttons for 'Start Lab', 'End Lab', 'AWS Details', 'Readme', and 'Reset'. To the right of the terminal is a sidebar titled 'Learner Lab' containing links to various AWS documentation topics such as Environment Overview, Environment Navigation, Access the AWS Management Console, Region restriction, Service usage and other restrictions, Using the terminal in the browser, Running AWS CLI commands, Using the AWS SDK for Python, Preserving your budget, Accessing EC2 Instances, SSH Access to EC2 Instances, SSH Access from Windows, and SSH Access from a Mac.

Instâncias EC2:

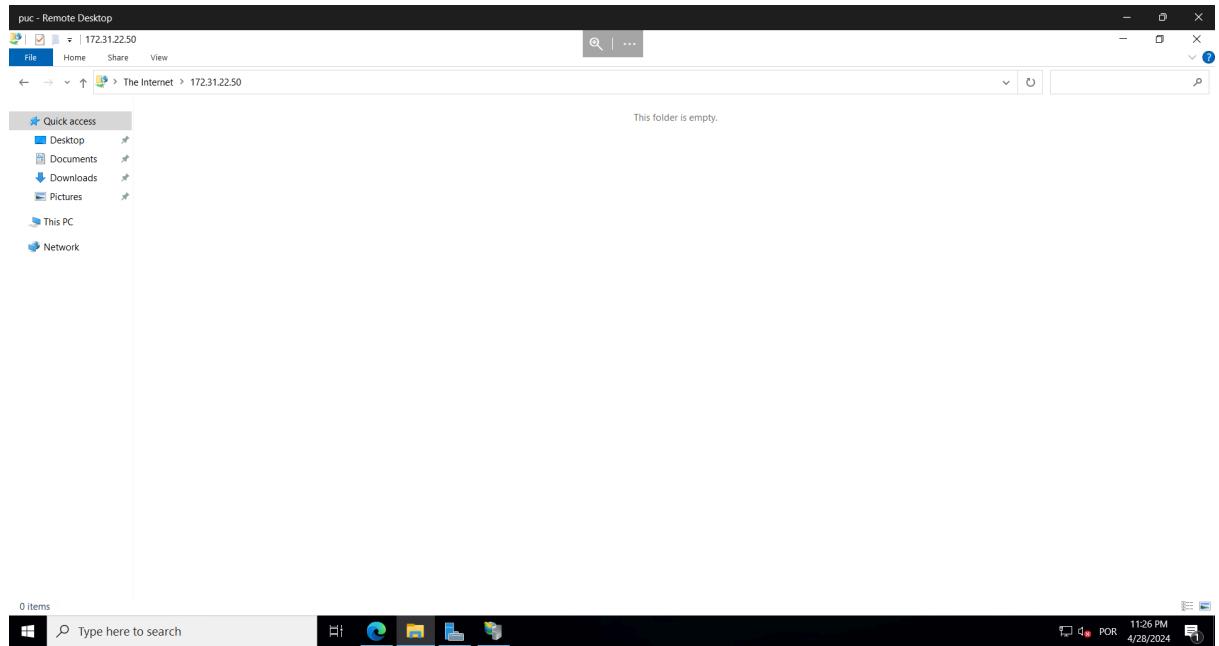
The screenshot shows the AWS EC2 Instances page. The left sidebar includes options like Painel EC2, Visão global do EC2, Events, Console-to-Code Preview, Imagens (AMIs, Catalogo AMI, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity, Reservations), Loja de blocos elásticos (Volumes, Instantâneos), Segurança de rede (Grupos de segurança, IPs elásticos), and CloudShell/Opinião. The main content area displays a table titled 'Instances (2) Info' with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4. Two instances are listed: 'PUC WINDOWS' (i-0a9128b92dd4f4d0f, Running, t2.micro, 2/2 checks passed, us-east-1d, ec2-34-230-1) and 'PUC' (i-0490073aa4cf51d03, Running, t2.micro, 2/2 checks passed, us-east-1c, ec2-3-88-162). A modal window titled 'Select an instance' is open at the bottom.

### - Servidor Windows:

- Nome: i-0a9128b92dd4f4d0f
- Endereço DNS: ec2-34-230-18-242.compute-1.amazonaws.com
- Usuário de Acesso: Administrator

The screenshot shows the AWS EC2 Instance Details page for the instance i-0a9128b92dd4f4d0f (PUC WINDOWS). The left sidebar is identical to the previous screenshot. The main content area is titled 'Instance summary for i-0a9128b92dd4f4d0f (PUC WINDOWS) Info'. It provides detailed information about the instance, including its ID, state, type, and network settings. At the bottom, there are tabs for Details, Status and alarms New, Monitoring, Security, Networking, Storage, and Tags. A note at the bottom right encourages users to opt-in to AWS Compute Optimizer.

Conectado via Remote Desktop.

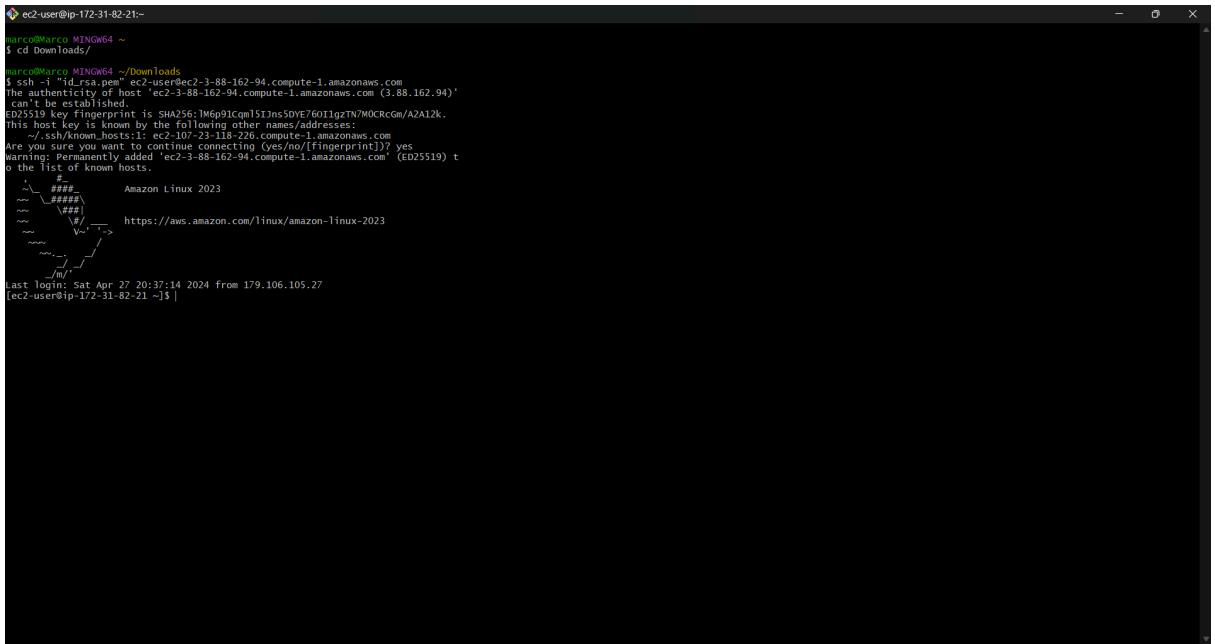


### - Servidor Linux:

- Nome: i-0490073a4c0f51d03
- Endereço DNS: ec2-3-88-162-94.compute-1.amazonaws.com
- Usuário de Acesso: ec2-user

The screenshot shows the AWS CloudWatch Metrics interface. At the top, there's a search bar and a navigation bar with tabs like 'Metrics', 'Logs', and 'CloudWatch Metrics'. Below the search bar, there's a dropdown menu for 'Region' set to 'Norte da Virgínia'. The main area displays a line graph titled 'CPU Utilization' with two data series: 'CPU Utilization' and 'CPU Utilization (estimated)'. The graph shows a fluctuating line between 0% and 100% over a period of time. At the bottom, there's a legend, a 'Details' button, and other navigation links.

Conectado via shell.



Marco@Marco MINGW64 ~  
\$ cd Downloads/  
\$ ssh -o StrictHostKeyChecking=no ec2-user@ec2-3-88-162-94.compute-1.amazonaws.com  
The authenticity of host 'ec2-3-88-162-94.compute-1.amazonaws.com (3.88.162.94)'  
can't be established.  
ED25519 key fingerprint is SHA256:IM6p91Cqm151Jn5OYE760IJgTN7MCRcGm/AzA12k.  
This host key is known by the following user names/addresses:  
Marco@179.106.105.21:22  
Marco@179.106.105.21:22  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'ec2-3-88-162-94.compute-1.amazonaws.com' (ED25519) to the list of known hosts.  
Last login: Sat Apr 27 20:37:14 2024 from 179.106.105.21  
[ec2-user@ip-172-31-82-21 ~]\$

### 3. MONITORAMENTO DE RECURSOS

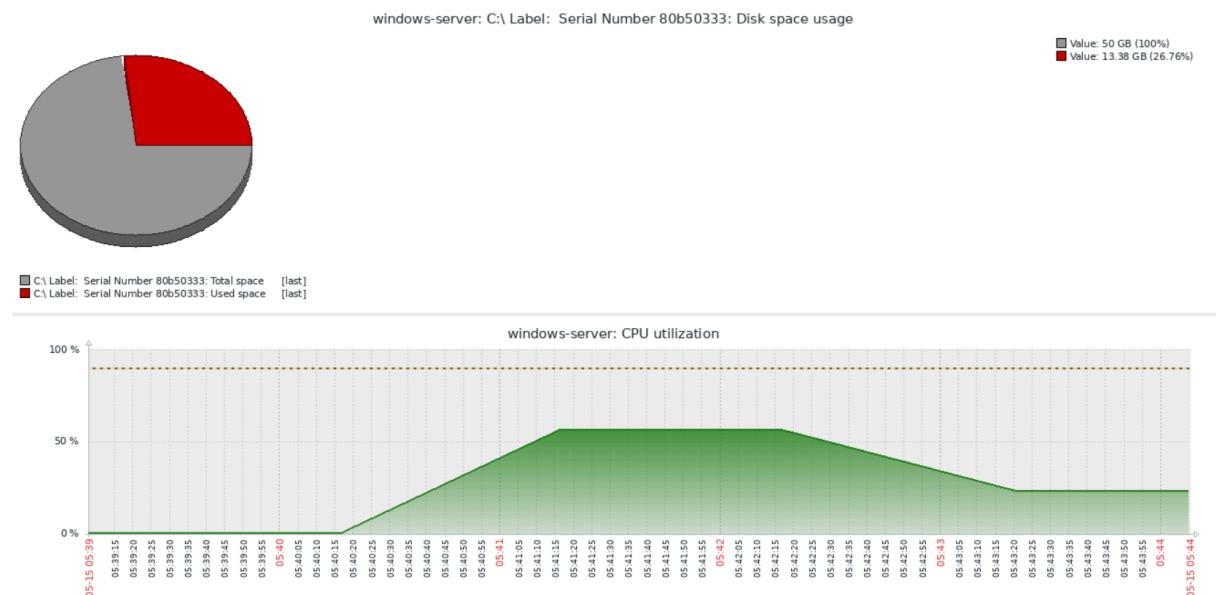
#### 3.1. MONITORAMENTO ON PREMISES

##### 3.1.1. SERVIDOR AD/DNS

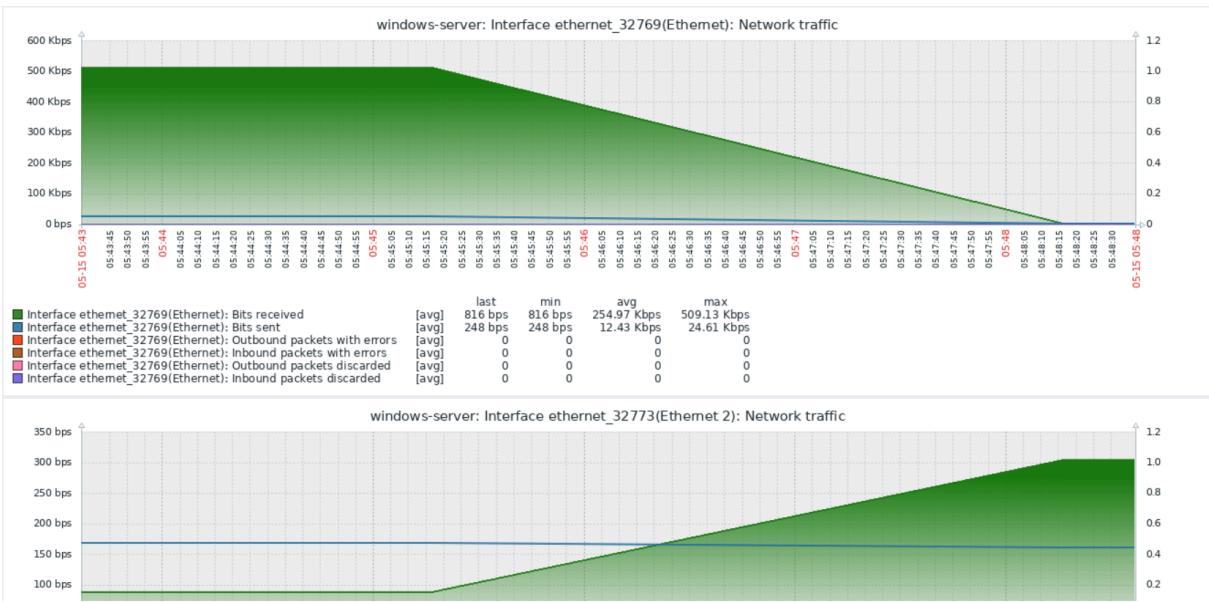
No dashboard contém os hosts que estão sendo monitorados pelo Zabbix appliance, neste caso, possui o windows-server com ip 192.168.1.212 e porta 161 aberta para o monitoramento e o windows-10 com ip 192.168.1.71 e porta 161 aberta para monitoramento.

Ao acessar os graphs, o zabbix fornece as seguintes informações do host:

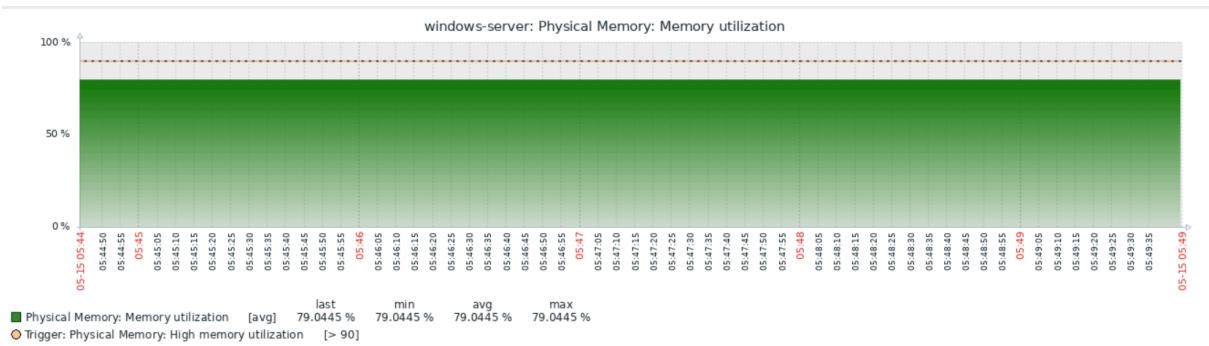
- Uso de disco
- Uso de CPU



- Tráfego de rede (por interfaces)



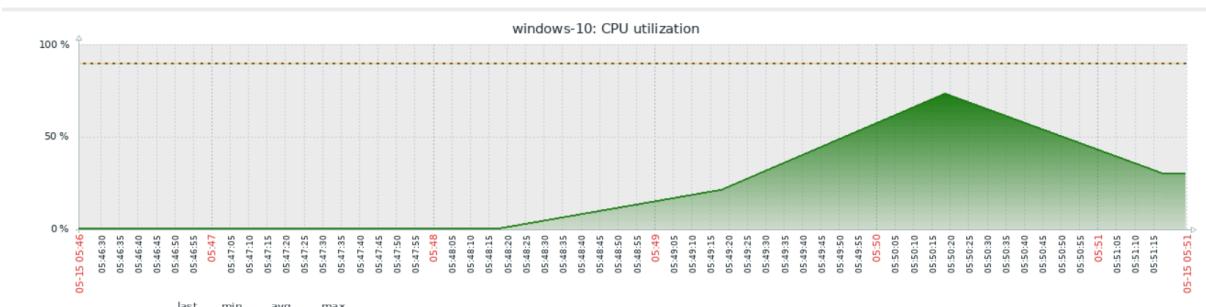
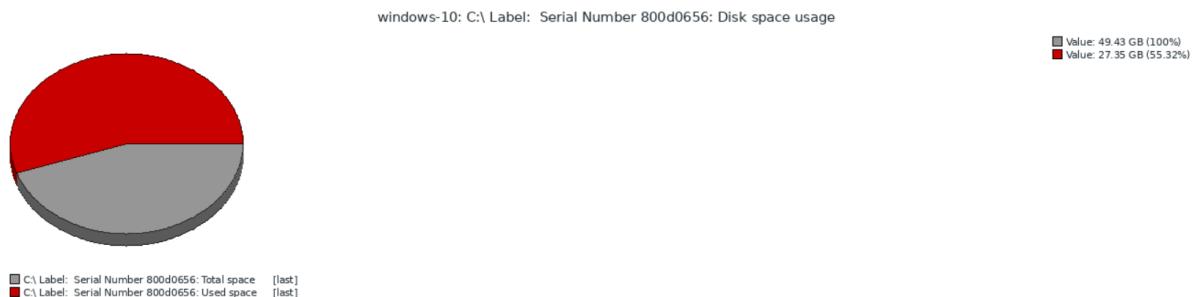
- Uso de memória RAM



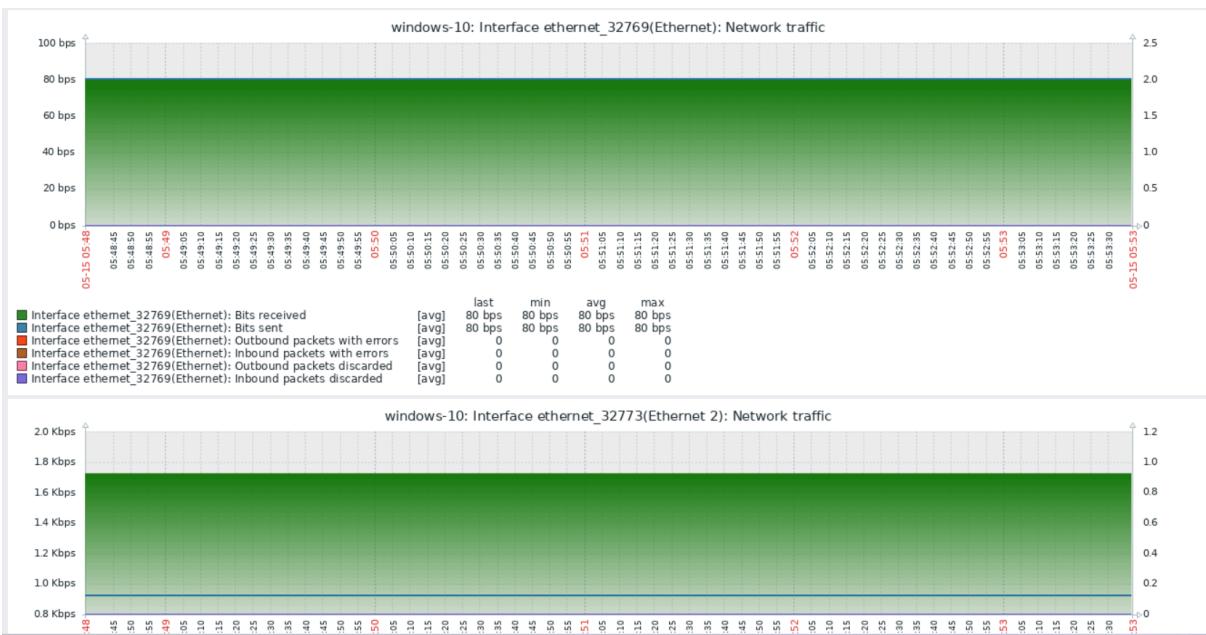
## 2.1.2 ESTAÇÃO DE TRABALHO

Ao acessar os graphs da estação de trabalho windows-10, o zabbix fornece as seguintes informações do host:

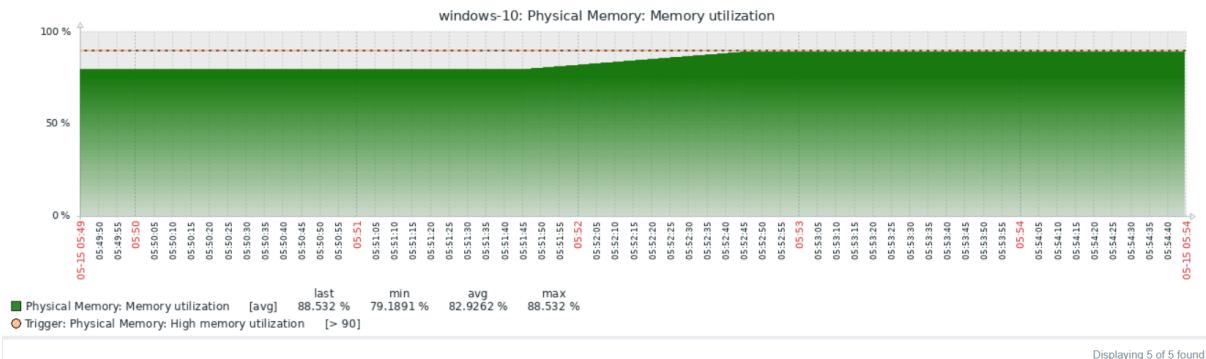
- Uso de disco
- Uso de CPU



- Tráfego de rede (por interfaces)



## - Uso de memória RAM



### 3.1.3. SERVIDOR DHCP

Foi-se tentado fazer a conexão entre o Zabbix Appliance (NIC Bridged) e o servidor DHCP para visualização no Host, todas as tentativas falharam em realizar essa comunicação. Houve a tentativa de conectar via Agent pela porta 10050 e via SNMP pelo mesmo endereço.

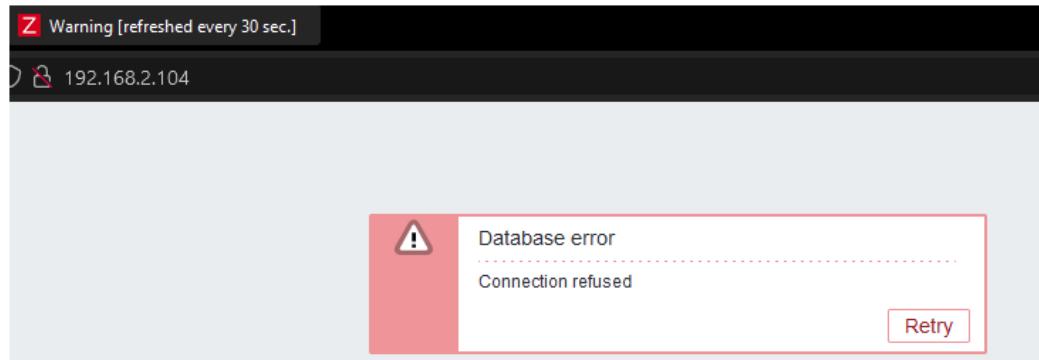
No início, foi-se cogitado a possibilidade de fazer a comunicação caso o servidor DHCP também estivesse com sua NIC ponteada (Bridged) mas sem sucesso. Mesmo possuindo um IP local 192.168.2.105 (Servidor DHCP) e 192.168.2.104 (Zabbix Appliance), mas infelizmente não foi possível obter sucesso.

Ao usar a rede Interna do DHCP com o Zabbix, eles passam a se comunicar mas o host perde a conexão pois o Zabbix assume um endereço IP vindo do servidor DHCP.

Abaixo é possível verificar que o servidor DHCP está funcionando e entregando IPs corretamente no range 192.168.42.100-199.

```
Client [Running] - Oracle VM VirtualBox
root@archlinux: ~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8a:72:41 brd ff:ff:ff:ff:ff:ff
    inet 192.168.42.101/24 brd 192.168.42.255 scope global dynamic enp0s3
        valid_lft 7189sec preferred_lft 7189sec
        inet6 fe80::a67d:6d3c:71d4:64 scope link noprefixroute
            valid_lft forever preferred_lft forever
root@archlinux: ~#
DHCP Server [Running] - Oracle VM VirtualBox
root@archlinux: ~# systemctl status kea-dhcp4
● kea-dhcp4.service - ISC Kea IPv4 DHCP daemon
   Loaded: loaded (/usr/lib/systemd/system/kea-dhcp4.service; enabled; preset: disabled)
     Active: active (running) since Sun 2024-05-19 11:23:54 -03; 7mi
n ago
      Docs: man:kea-dhcp4(8)
      Main PID: 959 ('kea-dhcp4')
         Tasks: 7 (limit: 4663)
        Memory: 15.0M (peak: 15.5M)
          CPU: 103ms
         CGroup: /system.slice/kea-dhcp4.service
              └─ 959 /usr/bin/kea-dhcp4 -c /etc/kea/kea-dhcp4.conf
```

O erro no banco de dados do servidor Zabbix (acessado pelo Host enquanto a appliance está em execução).



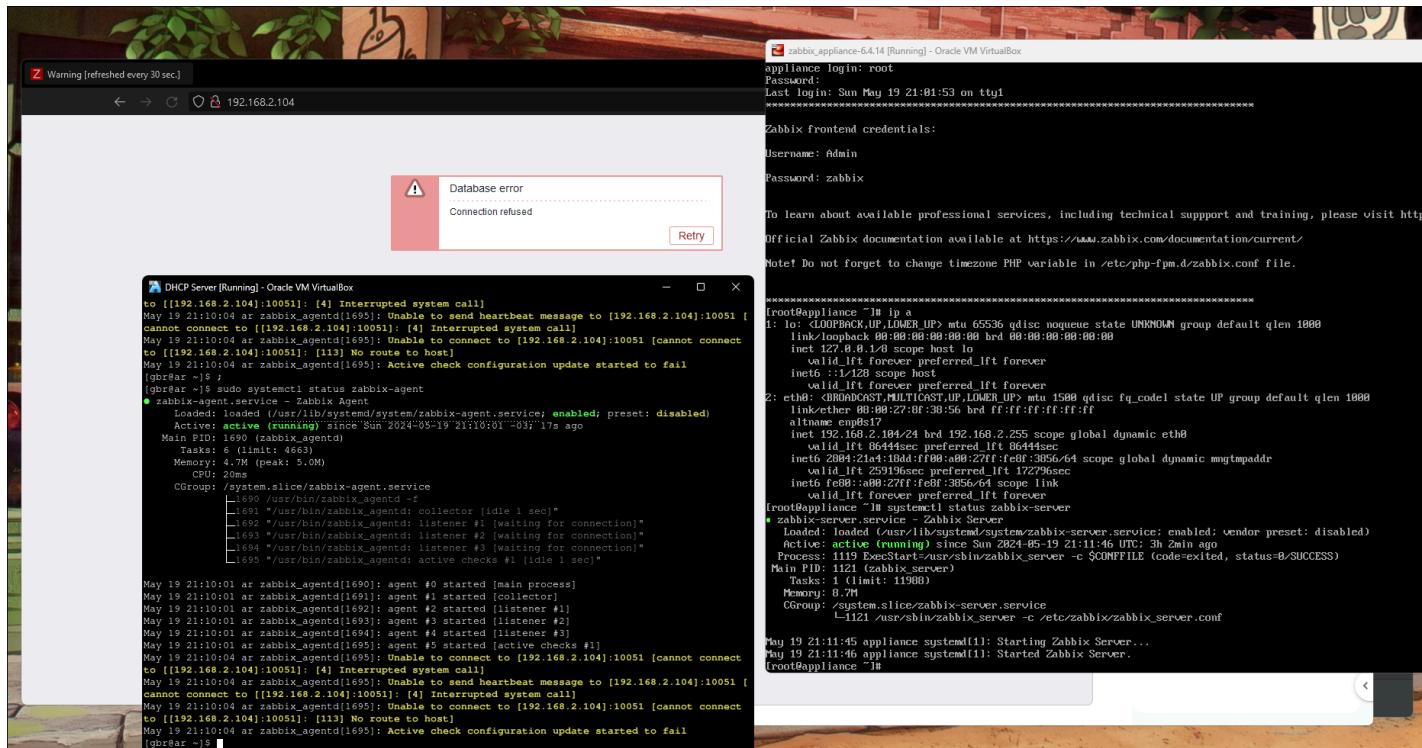
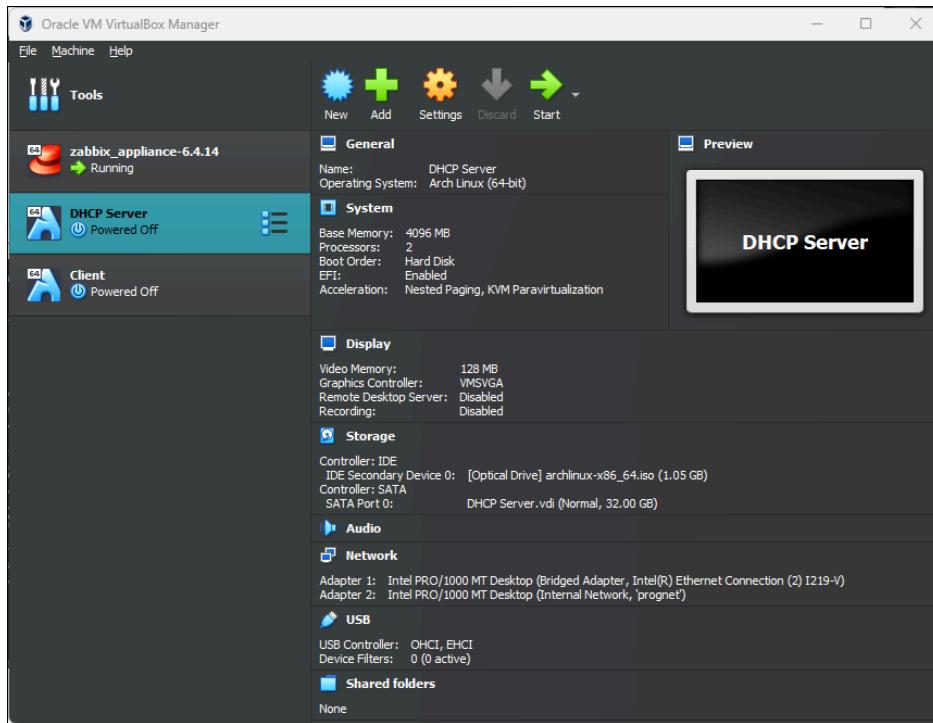
Podemos ver o zabbix-appliance executando normalmente e com seu endereço 192.168.2.104, ele assumiu esse endereço ao se comunicar com o servidor DHCP, seu acesso no Host (visto acima) veio a falhar inesperadamente, pois foi possível criar o um 'host' para monitoramento antes da falha no banco de dados.

```
zabbix_appliance-64.14 [Running] - Oracle VM VirtualBox
AlmaLinux 8.9 (Midnight Onicia)
Kernel 4.18.0-513.24.1.el8_9.x86_64 on an x86_64
appliance login: root
Password:
Last login: Sun May 19 20:58:22 on ttys1
*****
Zabbix frontend credentials:
Username: Admin
Password: zabbix

To learn about available professional services, including technical support and training, please visit https://www.zabbix.com/services
Official Zabbix documentation available at https://www.zabbix.com/documentation/current
Note! Do not forget to change timezone PHP variable in /etc/php-fpm.d/zabbix.conf file.

*****
[root@appliance ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:00:27:0f:38:56 brd ff:ff:ff:ff:ff:ff
    altname enp0s17
    inet 192.168.2.104/24 brd 192.168.2.255 scope global dynamic eth0
        valid_lft 86445sec preferred_lft 86445sec
    inet6 2002:1a4:10dd:ff00:00:27ff:fe0f:3856/64 scope global dynamic mngtmpaddr
        valid_lft 259199sec preferred_lft 172799sec
    inet6 fe00::0:ff:fe0f:3856/64 scope link
        valid_lft forever preferred_lft forever
[root@appliance ~]#
```

Configuração do VirtualBox com NIC ponteada no servidor DHCP.



É possível ver que tanto zabbix-server e zabbix-agent estão ativos mas a conexão não é feita, mesmo conectados na mesma subnet, tendo o DHCP 2 NICs (1 Interno 192.168.42.42

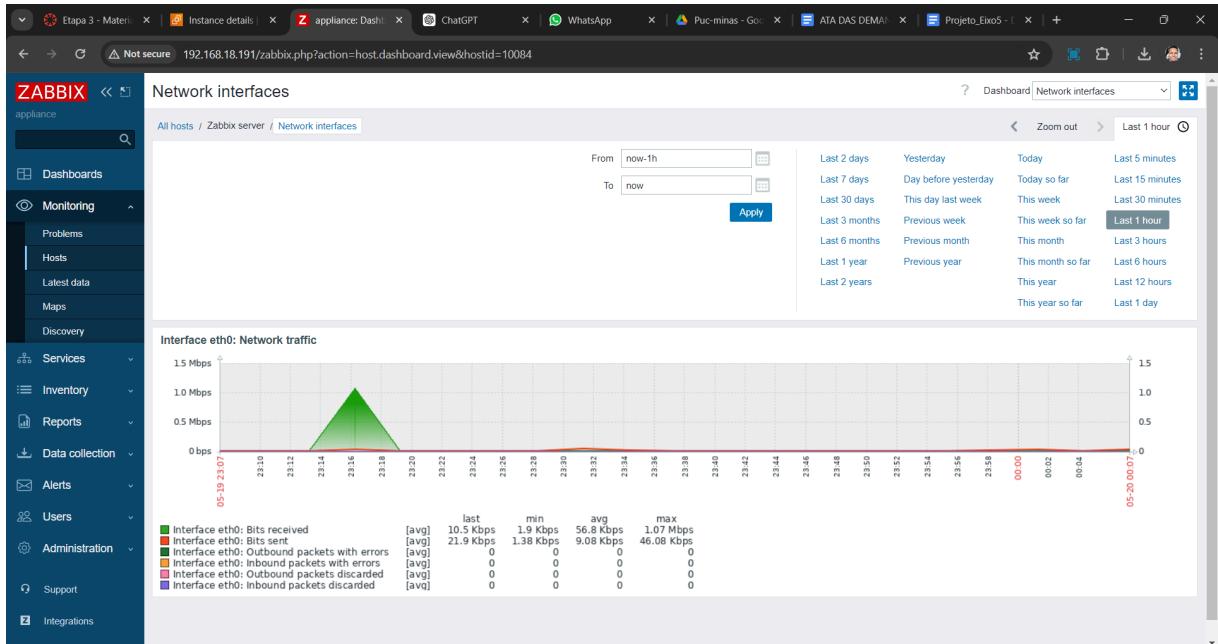
e 1 Ponteada 192.168.2.105). A rede interna é reservada para clientes que conectam-se ao ip ..42.42. Enquanto o adaptador ponteado deveria permitir a conexão mas não foi o caso.

### 3.1.4. SERVIDOR FTP

Ao acessar os graphs do servidor FTP local (windows), o zabbix fornece as seguintes informações do host:

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
192.168.18.102	Items	Triggers	Graphs	Discovery	Web				Enabled	None			
Zabbix server	Items 146	Triggers 84	Graphs 27	Discovery 5	Web	127.0.0.1:10050	Linux by Zabbix agent, Zabbix server health		Enabled	ZBX	None		

Gráfico de utilização de rede:



Conexão do servidor AWS ao servidor de monitoramento.

```
ubuntu@ip-172-31-18-146:~$ sudo systemctl status zabbix-agent
No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-18-146:~$ sudo nano /etc/vsftpd.conf
ubuntu@ip-172-31-18-146:~$ sudo systemctl restart vsftpd
ubuntu@ip-172-31-18-146:~$ sudo service vsftpd restart
ubuntu@ip-172-31-18-146:~$ sudo systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
    Loaded: loaded (/usr/lib/systemd/system/zabbix-agent.service; enabled; preset: enabled)
      Active: active (running) since Sun 2024-05-19 23:18:39 UTC; 4min 55s ago
        Main PID: 5956 (zabbix_agentd)
          Tasks: 6 (limit: 1130)
        Memory: 5.1M (peak: 5.7M)
          CPU: 88ms
        CGroup: /system.slice/zabbix-agent.service
                └─5956 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf
                  ├─5960 "/usr/sbin/zabbix_agentd: collector [idle 1 sec]"
                  ├─5961 "/usr/sbin/zabbix_agentd: listener #1 [waiting for connection]"
                  ├─5962 "/usr/sbin/zabbix_agentd: listener #2 [waiting for connection]"
                  ├─5963 "/usr/sbin/zabbix_agentd: listener #3 [waiting for connection]"
                  ├─5964 "/usr/sbin/zabbix_agentd: active checks #1 [idle 1 sec]"

May 19 23:18:39 ip-172-31-18-146 systemd[1]: Started zabbix-agent.service - Zabbix Agent.
ubuntu@ip-172-31-18-146:~$
```

## 3.2. MONITORAMENTO NA NUVEM

### 3.2.1. SERVIDOR SQUID PROXY

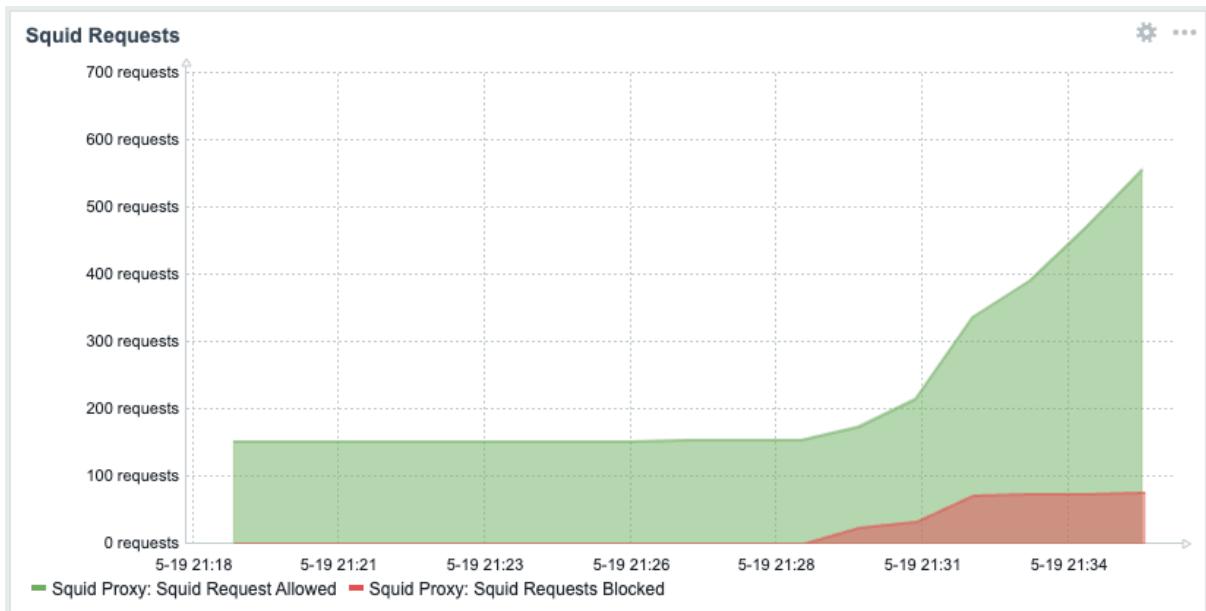
Antes de configurar as métricas no Zabbix, precisamos instalar o agente do Zabbix no servidor de proxy com o comando:

```
$ sudo apt install zabbix-agent
```

Após instalar o agente, precisamos configurá-lo para acessar o IP do servidor Zabbix. Também precisamos adicionar quais métricas devem ser enviadas para o servidor do Zabbix. Abaixo seguem as alterações que precisaram ser feitas no arquivo de configuração do agente (`/etc/zabbix/zabbix_agentd.conf`):

```
# IP do servidor Zabbix
Server=54.90.111.115
ActiveServer=54.90.111.115
# Nome do servidor de proxy
Hostname=squid-server
# Comando para mostrar quantidade de requisições bloqueadas
UserParameter=squid.requests_blocked,grep "TCP_DENIED" /var/log/squid/access.log | wc -l
# Comando para mostrar quantidade de requisições permitidas
UserParameter=squid.requests_allowed,grep -v "TCP_DENIED" /var/log/squid/access.log | wc -l
# Comando para mostrar uso de banda
UserParameter=squid.bandwidth_usage,awk '{sum+=$5} END {print sum}' /var/log/squid/access.log
```

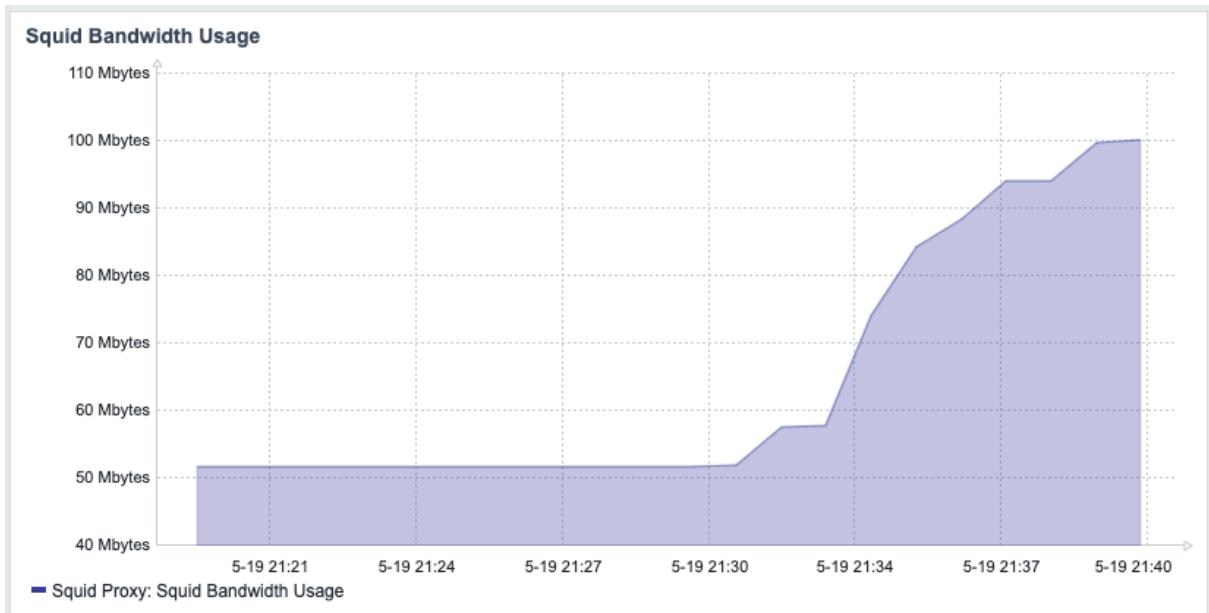
Para verificar quantas requisições estão sendo processadas pelo servidor criamos um gráfico que demonstra a quantidade de requisições bloqueadas versus a quantidade de requisições permitidas.



Também adicionamos contadores para demonstrar o número de requisições em tempo real



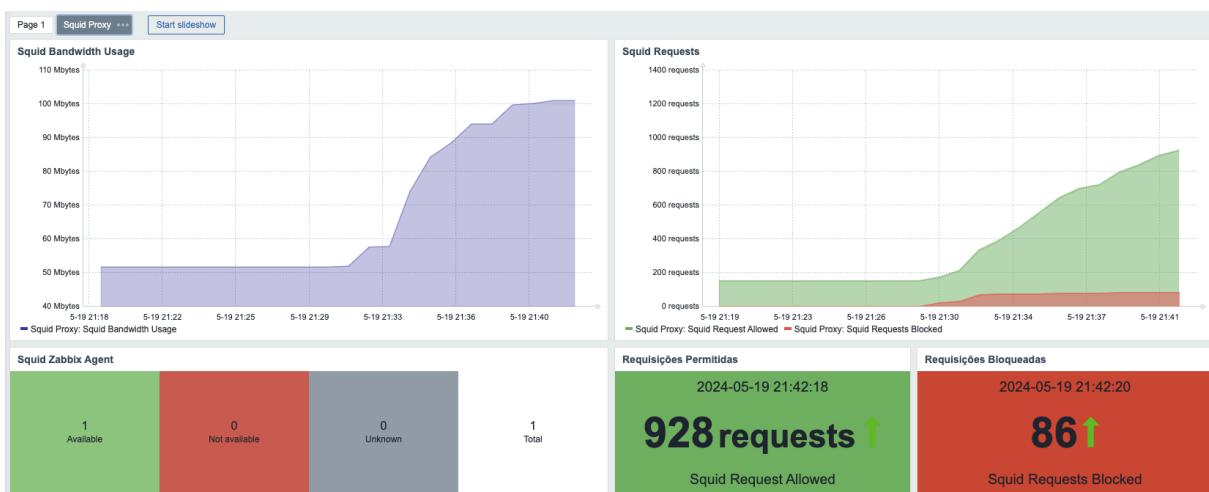
Uma outra métrica que adicionamos foi a métrica de uso de banda do servidor de proxy



E por último, uma métrica para indicar se o agente do zabbix rodando dentro do servidor de proxy está ativo



Criamos um dashboard específico que serve para mostrar apenas métricas do servidor de proxy, abaixo pode-se visualizar como



### 3.2.2. SERVIDORES WEB

O monitoramento dos servidores foi feito fazendo a criação de um Host no Zabbix, acessando a aba lateral, clicando em “Configuration” e “Hosts”, sendo inserido o nome, grupo e o IP.

Após a criação, para o monitoramento do servidor criado, foi criado um item no “Host” para que fosse especificado o endereço e forma de monitoramento que seria feito para o servidor a ser monitorado.

Sendo informado, o nome, tipo como HTTP Agent, key, url e modo de requisição, que foi configurado como “Headers”, para verificar o Header da resposta obtida na requisição HTTP.

Foi realizado um teste antes de salvar o item criado, para verificar qual seria o retorno do servidor, obtendo a resposta HTTP 200, indicando sucesso na requisição e que o servidor estava com status online.

Name	Triggers	Key	Interval	History	Trends	Type	Status	Tags	Info
server-web		server-web	30s	90d	Trends	HTTP agent	Enabled		

O item criado fica disponível para acesso dentro do Host criado, podendo ser verificado o seu status e se o monitoramento está ativo ou não dentro do Zabbix.

### 3.1.4. SERVIDOR SMTP

Devidamente configurado para o endereço: 54.90.111.115 aguardando conexão.

```
ubuntu@ip-172-31-25-72:~$ systemctl status zabbix-agent
● zabbix-agent.service - Zabbix Agent
   Loaded: loaded (/usr/lib/systemd/system/zabbix-agent.service; enabled; preset: enabled)
   Active: active (running) since Sun 2024-05-19 23:13:38 UTC; 1h 8min ago
     Process: 3316 ExecStart=/usr/sbin/zabbix_agentd -c $CONFFILE (code=exited, status=0/SUCCESS)
    Main PID: 3318 (zabbix_agentd)
      Tasks: 6 (limit: 1130)
     Memory: 4.9M (peak: 5.6M)
        CPU: 891ms
       CGroup: /system.slice/zabbix-agent.service
               └─3318 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf
                  ├─3319 "/usr/sbin/zabbix_agentd: collector [idle 1 sec]"
                  ├─3320 "/usr/sbin/zabbix_agentd: listener #1 [waiting for connection]"
                  ├─3321 "/usr/sbin/zabbix_agentd: listener #2 [waiting for connection]"
                  ├─3322 "/usr/sbin/zabbix_agentd: listener #3 [waiting for connection]"
                  └─3323 "/usr/sbin/zabbix_agentd: active checks #1 [idle 1 sec]"

May 19 23:13:38 ip-172-31-25-72 systemd[1]: Starting zabbix-agent.service - Zabbix Agent...
May 19 23:13:38 ip-172-31-25-72 systemd[1]: Started zabbix-agent.service - Zabbix Agent.
```

## 4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

### 4.1 PSI UNIVERSIDADE PROGRESSUS



#### **Política de Segurança da Informação da Universidade Progressus**

**Versão:** 1.0

**Classificação:** Interna

**Última revisão:** 15 de Junho de 2024

---

#### **Índice**

1. Introdução
2. Objetivos
3. Abrangência
4. Diretrizes Gerais
  - 4.1 Interpretação
  - 4.2 Propriedade
  - 4.3 Classificação da Informação
  - 4.4 Controle de Acesso
  - 4.5 Internet
  - 4.6 Correio Eletrônico
  - 4.7 Rede Sem Fio (Wi-Fi)
  - 4.8 Recursos de TIC Institucionais
  - 4.9 Recursos de TIC Particulares
  - 4.10 Armazenamento de Informações
  - 4.11 Repositórios Digitais
  - 4.12 Mídias Sociais
  - 4.13 Mesa Limpa e Tela Limpa
  - 4.14 Áudio, Vídeos e Fotos
  - 4.15 Uso de Imagem, Som da Voz e Nome
  - 4.16 Aplicativos de Comunicação
  - 4.17 Monitoramento
  - 4.18 Combate à Intimidação Sistemática (Bullying)
  - 4.19 Contratos de Trabalho e de Prestação de Serviços
  - 4.20 Segurança da Informação
5. Papéis e Responsabilidades
  - 5.1 Todos
  - 5.2 Gestores e Coordenadores
  - 5.3 Colaboradores
6. Disposições Finais
7. Documentos de Referência
8. Apêndice A – Siglas, Termos e Definições



## 1. Introdução

A Universidade Progressus é uma instituição de ensino, que tem por finalidade a formação de qualidade, pesquisa, inovação, desenvolvimento econômico e cultural, tem como missão a contribuição para o progresso social e individual. Através do ensino de excelência, pesquisas e extensões.

Com o avanço tecnológico e a crescente aplicação da internet no dia a dia da instituição, é essencial estabelecer parâmetros para padronizar e normatizar a segurança no âmbito humano e tecnológico, para que seja garantida a qualidade de ensino e o acesso à informação.

Portanto, como forma de reconhecer a importância da segurança da informação para a proteção de dados e ativos contra as ameaças e vulnerabilidades, a Universidade Progressus apresenta neste documento diretrizes, normas e procedimentos propostos à proteção da informação.

## 2. Objetivos

A Política de Segurança da Informação (PSI) é aplicável ao ambiente estudantil, acadêmico e administrativo e tem por objetivos:

- Estabelecer diretrizes estratégicas e princípios para a proteção dos ativos tangíveis e intangíveis.
- Nortear a tomada de decisão e a realização das atividades profissionais e educacionais de todos os colaboradores.
- Construir uma cultura de uso seguro das informações.
- Preservar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a legalidade das informações.
- Definir normas e procedimentos específicos de segurança da informação.

## 3. Abrangência

Esta PSI é um normativo interno, com valor jurídico e aplicabilidade imediata e irrestrita a todos os alunos e colaboradores, para os ambientes estudantil, acadêmico e administrativo, que venham a ter acesso e/ou utilizam as informações, os recursos de TIC e/ou demais ativos tangíveis ou intangíveis da universidade.

## 4. Diretrizes Gerais

### 4.1 Interpretação



4.1.1 Para efeito desta PSI, são adotadas as siglas, os termos e definições constantes no Apêndice A.

4.1.2 Esta PSI deve ser interpretada de forma restritiva, com casos excepcionais necessitando autorização prévia.

#### **4.2 Propriedade**

4.2.1 As informações geradas, acessadas, recebidas, manuseadas e armazenadas são de propriedade e de direito de uso exclusivo da universidade.

4.2.2 Os recursos de TIC fornecidos para atividades educacionais e profissionais são de propriedade da universidade.

4.2.3 Todos os ativos tangíveis e intangíveis da universidade devem ser utilizados apenas para fins institucionais. 4.2.4 A utilização das marcas, identidade visual e demais sinais distintivos da universidade devem ser autorizados previamente.

#### **4.3 Classificação da Informação**

4.3.1 As informações devem ser classificadas como:

- **Públicas:** Podem ser divulgadas sem restrições.
- **Internas:** Devem ser acessadas apenas por membros da universidade.
- **Confidenciais:** Requerem tratamento especial e acesso restrito.

4.3.2 Informações não públicas devem ser rotuladas no momento de sua criação.

4.3.3 Colaboradores devem tratar todas as informações não rotuladas como internas até que a classificação correta seja determinada.

4.3.4 Dados pessoais e informações sensíveis devem ser protegidos com mecanismos de segurança adequados, como criptografia.

#### **4.4 Controle de Acesso**

4.4.1 Cada aluno e colaborador receberá uma identidade digital individual e intransferível.

4.4.2 Identidades digitais são monitoradas e controladas pela equipe de TI.

4.4.3 O acesso a áreas físicas críticas é restrito a indivíduos autorizados e deve ser protegido por medidas de segurança apropriadas, como controle de acesso por crachá.

4.4.4 Logs de acesso devem ser mantidos para auditoria e revisão periódica.



#### **4.5 Internet**

4.5.1 O acesso à internet é concedido para fins educacionais e administrativos, e deve ser utilizado em conformidade com as leis vigentes e políticas institucionais.

4.5.2 É proibido o acesso a sites com conteúdo impróprio, ilegal ou que possam comprometer a segurança da informação.

#### **4.6 Correio Eletrônico**

4.6.1 O uso do correio eletrônico deve ser restrito a atividades educacionais e profissionais.

4.6.2 Correios eletrônicos devem ser protegidos contra spam, phishing e outras ameaças.

4.6.3 Mensagens de correio eletrônico devem ser arquivadas de acordo com as políticas de retenção de dados.

#### **4.7 Rede Sem Fio (Wi-Fi)**

4.7.1 A universidade oferece rede sem fio para finalidades educacionais e administrativas.

4.7.2 Apenas usuários autorizados podem acessar a rede sem fio.

4.7.3 Redes sem fio devem ser protegidas por senhas fortes e mecanismos de criptografia.

#### **4.8 Recursos de TIC Institucionais**

4.8.1 Recursos de TIC são destinados a finalidades educacionais e profissionais.

4.8.2 É vedado o armazenamento de arquivos pessoais nos recursos de TIC da universidade.

4.8.3 Os arquivos institucionais devem ser armazenados em servidores dedicados, com backup regular.

4.8.4 A equipe de TI é responsável pela manutenção e atualização dos recursos de TIC.

#### **4.9 Recursos de TIC Particulares**

4.9.1 A conexão de recursos de TIC particulares à rede da universidade é restrita e deve seguir diretrizes específicas.



4.9.2 Dispositivos móveis particulares devem ser protegidos com senhas e softwares de segurança.

4.9.3 É proibido o uso de dispositivos particulares para armazenar informações confidenciais da universidade sem autorização.

#### **4.10 Armazenamento de Informações**

4.10.1 Informações devem ser armazenadas nos locais apropriados e destinados a esse fim.

4.10.2 A universidade pode solicitar a remoção de conteúdos que ofereçam riscos ou violem normas.

4.10.3 Dados sensíveis devem ser armazenados com criptografia e acesso restrito.

#### **4.11 Repatórios Digitais**

4.11.1 Repatórios digitais são destinados ao armazenamento e compartilhamento de informações institucionais.

4.11.2 É vedado armazenar informações institucionais em repatórios digitais particulares.

4.11.3 Acesso a repatórios digitais deve ser controlado e monitorado.

#### **4.12 Mídias Sociais**

4.12.1 O uso de mídias sociais deve ser responsável e conforme os direitos e deveres estabelecidos pela universidade.

4.12.2 É proibido compartilhar informações confidenciais ou sensíveis da universidade em mídias sociais.

#### **4.13 Mesa Limpa e Tela Limpa**

4.13.1 Informações da universidade não devem ficar expostas em áreas comuns ou de trânsito de pessoas.

4.13.2 Colaboradores devem bloquear suas estações de trabalho ao se afastar.

4.13.3 Documentos confidenciais devem ser guardados em locais seguros quando não estiverem em uso.

#### **4.14 Áudio, Vídeos e Fotos**



4.14.1 A captura de imagens, vídeos ou áudios deve ser previamente autorizada pela universidade.

4.14.2 É proibido compartilhar gravações sem autorização expressa.

#### **4.15 Uso de Imagem, Som da Voz e Nome**

4.15.1 A universidade pode usar a imagem dos alunos para fins institucionais, respeitando a integridade dos envolvidos.

4.15.2 O uso de imagens deve ser feito de forma a não expor os indivíduos ao ridículo ou constrangimento.

#### **4.16 Aplicativos de Comunicação**

4.16.1 O uso de aplicativos de comunicação deve ser feito de forma responsável e segura.

4.16.2 Informações sensíveis não devem ser compartilhadas por aplicativos de comunicação sem medidas de segurança adequadas.

#### **4.17 Monitoramento**

4.17.1 A universidade realiza o monitoramento de atividades para proteger seus ambientes físicos e lógicos.

4.17.2 Logs de monitoramento são mantidos para análise e auditoria.

#### **4.18 Combate à Intimidação Sistemática (Bullying)**

4.18.1 Todos devem participar de campanhas contra a violência e intimidação sistemática.

4.18.2 Incidentes de bullying devem ser reportados imediatamente às autoridades competentes da universidade.

#### **4.19 Contratos de Trabalho e de Prestação de Serviços**

4.19.1 A GTI deve desativar as identidades digitais de alunos ou colaboradores desligados.

4.19.2 Alunos ou colaboradores devem excluir informações institucionais de dispositivos particulares ao término do contrato.

4.19.3 Contratos de prestação de serviços devem incluir cláusulas de confidencialidade e segurança da informação.



#### **4.20 Segurança da Informação**

- 4.20.1 Informações devem ser transmitidas com cautela, confirmando a identidade do solicitante.
- 4.20.2 A universidade mantém processos de salvaguarda e restauração de arquivos críticos.
- 4.20.3 Dados descartados devem ser destruídos de forma segura para impedir a recuperação.

### **5. Papéis e Responsabilidades**

#### **5.1 Todos**

- 5.1.1 Conhecer e disseminar as regras da Política de Segurança da Informação.
- 5.1.2 Proteger os ativos tangíveis e intangíveis da universidade.
- 5.1.3 Reportar incidentes de segurança imediatamente.
- 5.1.4 Participar de programas de treinamento e conscientização sobre segurança da informação.

#### **5.2 Gestores e Coordenadores**

- 5.2.1 Orientar suas equipes quanto ao uso seguro dos ativos e informações da universidade.
- 5.2.2 Assegurar o cumprimento das políticas de segurança da informação em suas áreas de responsabilidade.
- 5.2.3 Participar da investigação de incidentes de segurança relacionados às suas equipes.

#### **5.3 Colaboradores**

- 5.3.1 Utilizar mídias sociais com responsabilidade e preservar a imagem da universidade.
- 5.3.2 Cumprir todas as diretrizes e práticas estabelecidas na política de segurança da informação.
- 5.3.3 Reportar imediatamente qualquer incidente ou suspeita de violação de segurança.



## 6. Disposições Finais

Este documento deve ser interpretado conforme as leis brasileiras e em conjunto com outras normas da universidade. Quaisquer infrações estão sujeitas a sanções previstas nos contratos e normas institucionais.

## 7. Documentos de Referência

- ABNT NBR ISO/IEC 27001:2013
- ABNT NBR ISO/IEC 27002:2013
- ABNT NBR ISO/IEC 27014:2013
- Norma ISO/IEC 27005:2011
- COBIT 5® Foundation

## 8. Apêndice

### A – Siglas, Termos e Definições

#### A

- **Ativo:** Qualquer coisa que tenha valor para a instituição e precisa ser adequadamente protegida.
- **Ameaça:** Causa potencial de um incidente indesejado, que pode resultar em dano à instituição.

#### B

- **Backup:** Salvaguarda de sistemas ou arquivos, realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de retorno.

#### C

- **Confidencialidade:** Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e sejam devidamente protegidas do conhecimento alheio.
- **CRC:** Centro de Recursos Computacionais, vinculado ao ICEI.

#### D

- **Dados:** Conjunto de fatos, valores ou ocorrências em estado bruto, que, quando processados ou agrupados, produzem informações.
- **Datacenter:** Ambiente altamente crítico, projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede.

**E**

- **Encriptação:** Processo de codificação de informações para proteger seu conteúdo durante a transmissão e armazenamento.

**F**

- **Firewall:** Dispositivo de segurança de uma rede de computadores que monitora, autoriza e bloqueia o tráfego que entra e sai da rede.

**I**

- **Integridade:** Garantia de que as informações estejam íntegras durante o seu ciclo de vida.
- **Identidade Digital:** Identificação do usuário em ambientes lógicos, sendo composta por login e senha ou por outros mecanismos de identificação e autenticação.

**M**

- **Monitoramento:** Processo de registro e análise de atividades em sistemas de informação para garantir segurança e conformidade.

**R**

- **Risco:** Possibilidade de uma ameaça explorar uma vulnerabilidade de um ativo para prejudicar a instituição.
- **Recursos de TIC:** Todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação.

**S**

- **Segurança da Informação:** Preservação da confidencialidade, integridade e disponibilidade da informação na instituição.

**W**

- **Wi-Fi:** Abreviação de Wireless Fidelity, tecnologia de comunicação sem fio.

**A – Procedimentos**

**Controle de Acesso:** O controle de acesso tem como objetivo a restrição do acesso de dados confidenciais da Universidade para usuários devidamente autorizados, para seu cumprimento, sendo necessário a aplicação das seguintes medidas:





- **Autenticação Multifator (MFA):** Autenticação através de dois ou mais fatores, por senhas, biometrias, tokens físicos, aplicativos de autorização, em que o usuário somente terá seu acesso liberado após cumprir todas as exigências de autenticação;
- **Níveis de Acesso:** Os usuários terão seus níveis atribuídos de acordo com sua atuação dentro da universidade, podendo haver bloqueios de acesso caso não tenha o acesso autorizado;
- **Monitoramento:** Documentos de acompanhamento das atividades que foram realizadas, cada acesso devidamente registrado para que o setor responsável analise, verifique e gere relatórios.

**Segurança Cibernética:** A segurança cibernética tem como objetivo proteger os servidores da Universidade Progressus contra os ataques cibernéticos, como malwares, spywares, DoS, phishing e invasões, sendo necessário a aplicação das seguintes medidas:

- **Softwares de Segurança:** A instalação de softwares de segurança que analisem e verifiquem os possíveis ataques que podem ocorrer aos servidores da universidade, como antivírus, firewall e anti-malwares;
- **Testes de Vulnerabilidade:** Deve ser feito periodicamente pela Universidade testes que verifiquem falhas de segurança nos servidores, para que possam ser identificados e corrigidos;
- **Políticas de Segurança da Rede:** A rede deve ter regras que possam proteger e limitar os acessos de pessoas e serviços não autorizados, para que evite possíveis ataques.

**Backup de Dados:** O backup de dados tem como objetivo a garantia da recuperação e manutenção dos dados da Universidade de maneira segura, para cenários de perda, sinistros ou falhas do sistema, sendo necessário a aplicação das seguintes medidas:

- **Rotina de Backup:** O backup deve ser feito periodicamente, podendo ser escolhido o tipo incremental, sua frequência deverá ser diária e os dados serão mantidos em um servidor físico interno da Universidade, e um servidor na nuvem pago;
- **Teste de Backups:** Os backups feitos anteriormente devem ser verificados e analisados se estão com os dados corretos, e se estão podendo ser recuperados do seu servidor de origem para outro servidor, como forma de garantir a sua qualidade;



- **Plano de Recuperação de Sinistros:** A Universidade deve ter um plano visando o acontecimento de desastres, no qual pode ocorrer a perca massiva de dados armazenados no servidor in loco, tendo que ser feita a recuperação de dados de acordo com o armazenamento em nuvem pago.

**Proteção de Informações Estratégicas:** A existência de dados estratégicos da Universidade mostra a necessidade de aplicação de regras que tenham como objetivo a garantia da confidencialidade e integridade dessas informações, para a sua aplicação devem ser aplicadas as seguintes medidas:

- **Classificação de Informações:** Os dados contidos no armazenamento dos servidores da Universidade devem ser classificados como dados de pessoas, financeiros, pesquisas, infraestrutura, ensino, reputação e segurança, para que possam ser distinguidos de acordo com a sua confidencialidade;
- **Controle de Acesso:** A visualização dos dados deve ser permitida de acordo com o nível atribuído a pessoa, para que haja a restrição de acesso caso o usuário não possua autorização;
- **Criptografia de Informações:** As informações dos tipos: pessoas, financeiros, infraestrutura e segurança devem ser criptografados;

UNIVERSIDADE  
PROGRESSUS

## 4.2. CARTILHA PSI


  
**CARTILHA DE SEGURANÇA DA INFORMAÇÃO**

**DIRETRIZES GERAIS**

**19. Contratos de Trabalho e de Prestação de Serviços**

Identidades digitais de ex-alunos e ex-colaboradores são desativadas ao término do vínculo. Exclua informações institucionais de dispositivos pessoais após o término do contrato.

**20. Segurança da Informação**

Transmita informações com cautela e confirme a identidade do solicitante. Descarte dados de forma segura para impedir recuperação não autorizada.

**PAPÉIS E RESPONSABILIDADES**

**TODOS**

- Conhecer e seguir as diretrizes da PSI.
- Proteger os ativos da universidade.
- Reportar incidentes de segurança imediatamente.
- Participar de programas de treinamento e conscientização.

**COLABORADORES**

- Utilizar mídias sociais com responsabilidade.
- Seguir todas as diretrizes de segurança da informação.
- Reportar qualquer incidente ou suspeita de violação de segurança.

Para mais informações ou dúvidas sobre a Política de Segurança da Informação, entre em contato com a equipe de TI da Universidade Progressus.

Esta cartilha foi desenvolvida para ajudar você a entender e seguir as principais diretrizes da nossa Política de Segurança da Informação. Proteger nossas informações é uma responsabilidade de todos. Contamos com a sua colaboração.

**DIRETRIZES GERAIS**

**1. Interpretação**

A PSI deve ser interpretada de forma restritiva, com casos excepcionais necessitando autorização prévia.

**3. Classificação da Informação**

Informações devem ser classificadas como públicas, internas ou confidenciais. Dados pessoais e informações sensíveis devem ser protegidos adequadamente.

**5. Uso da Internet**

O acesso à internet deve ser utilizado para fins educacionais e administrativos, respeitando as leis e políticas institucionais. É proibido acessar sites com conteúdo impróprio ou ilegal.

**7. Rede Sem Fio (Wi-Fi)**

A rede Wi-Fi da universidade é destinada a fins educacionais e administrativos. Acesso à rede é permitido apenas a usuários autorizados e deve ser protegido por senhas fortes.

**2. Propriedade**

Todas as informações geradas, acessadas, recebidas, manuseadas ou armazenadas são de propriedade da universidade. Os recursos de TIC devem ser utilizados apenas para fins institucionais.

**4. Controle de Acesso**

Cada usuário recebe uma identidade digital individual e intransférivel. Acesso a áreas físicas e digitais é monitorado e controlado.

**6. Correio Eletrônico**

O uso do correio eletrônico é restrito a atividades educacionais e profissionais. Proteja suas contas de e-mail contra ameaças como spam e phishing.

**8. Recursos de TIC Institucionais**

Recursos de TIC são para uso educacional e profissional. Arquivos institucionais devem ser armazenados em servidores dedicados com backup regular.

**9. Recursos de TIC Particulares**

A conexão de dispositivos pessoais à rede da universidade é restrita e deve seguir diretrizes específicas. Dispositivos pessoais não devem armazenar informações confidenciais sem autorização.

**11. Reppositórios Digitais**

Repositórios digitais são para armazenamento de informações institucionais. É proibido armazenar informações da universidade em repositórios pessoais.

**13. Mesa Limpa e Tela Limpa**

Não deixe informações da universidade expostas em áreas comuns. Bloqueie suas estações de trabalho ao se afastar.

**15. Uso de Imagem, Voz e Nome**

A universidade pode usar a imagem dos alunos para fins institucionais, respeitando a integridade dos envolvidos.

**17. Monitoramento**

A universidade monitora atividades para proteger seus ambientes físicos e digitais.

**10. Armazenamento de Informações**

Informações devem ser armazenadas em locais apropriados e seguros. Dados sensíveis devem ser protegidos com criptografia.

**12. Mídias Sociais**

Utilize mídias sociais de forma responsável, sem compartilhar informações confidenciais da universidade.

**14. Áudio, Vídeos e Fotos**

A captura de imagens, vídeos ou áudios deve ser previamente autorizada pela universidade.

**16. Aplicativos de Comunicação**

Use aplicativos de comunicação de forma responsável e segura.

**18. Combate ao Bullying**

Participe de campanhas contra bullying e reporte incidentes imediatamente.