



CURSO DE TECNOLOGIA EM DEFESA CIBERNÉTICA

ATIVIDADE DO CAP 6 - Monitoração usando Zabbix!

Kraków – Polônia

Junho/2021

Ian Alberto Ribeiro Christani

ATIVIDADE DO CAP 6 - Monitoração usando Zabbix!

Kraków – Polônia

Junho/2021

SUMÁRIO

1. INTRODUÇÃO.....4

2. DESENVOLVIMENTO.....5

3. CONCLUSÃO.....6

REFERÊNCIAS.....7

1 INTRODUÇÃO

Nessa atividade o objetivo é instalar um aplicativo para monitorar os serviços de um servidor web. Vamos usar o Zabbix e esse trabalho contempla a instalação de forma a adequar o serviço ao site da Feirinha Orgânica. Também está incluso no roteiro a instalação do serviço de FTP para a empresa. Este será feito inicialmente.

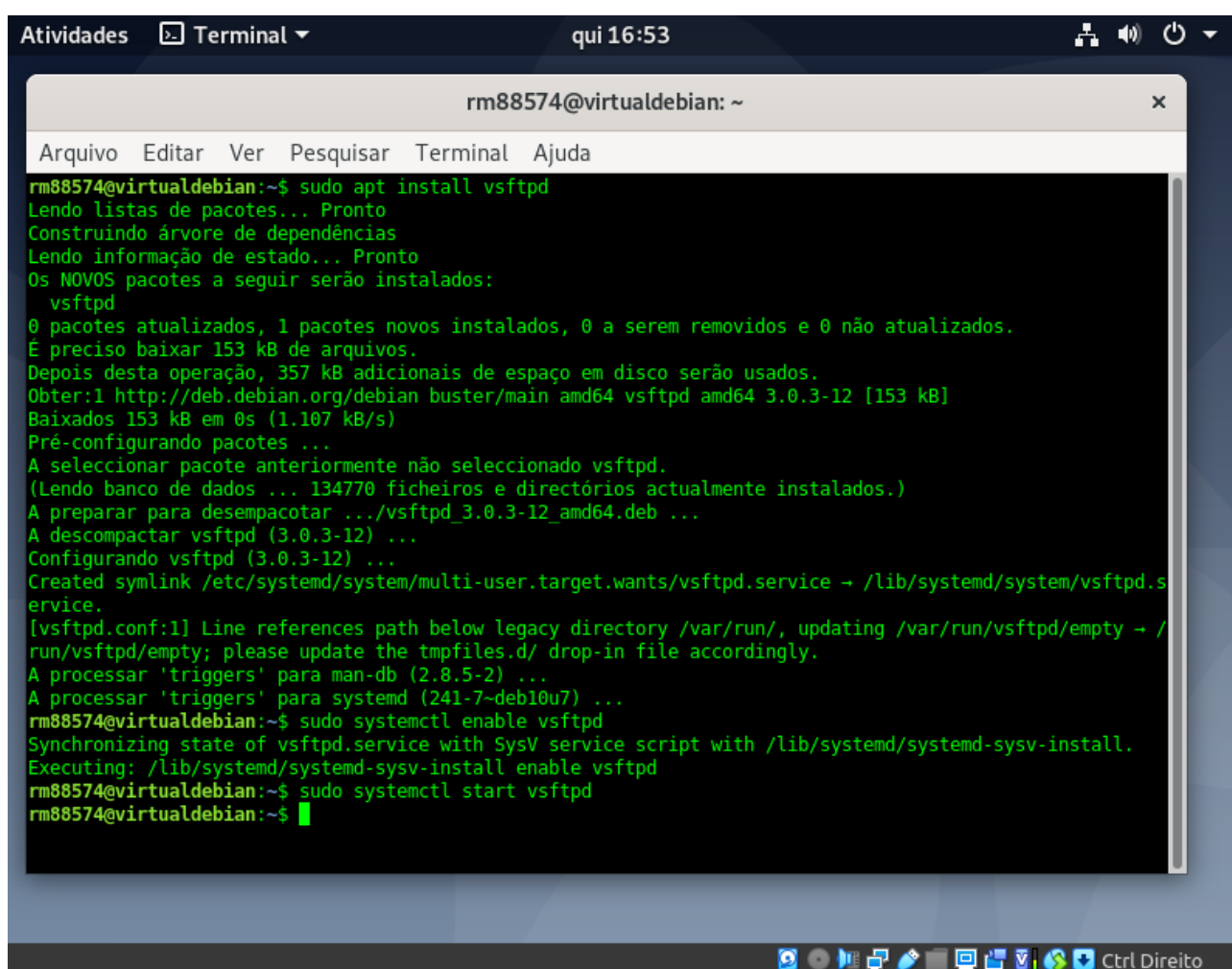
2 DESENVOLVIMENTO

Vamos instalar o serviço de FTP:

```
sudo apt install vsftpd
```

```
sudo systemctl enable vsftpd
```

```
sudo systemctl start vsftpd
```



```
Atividades Terminal qui 16:53
rm88574@virtualdebian: ~
Arquivo Editar Ver Pesquisar Terminal Ajuda
rm88574@virtualdebian:~$ sudo apt install vsftpd
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
Os NOVOS pacotes a seguir serão instalados:
  vsftpd
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
É preciso baixar 153 kB de arquivos.
Depois desta operação, 357 kB adicionais de espaço em disco serão usados.
Obter:1 http://deb.debian.org/debian buster/main amd64 vsftpd amd64 3.0.3-12 [153 kB]
Baixados 153 kB em 0s (1.107 kB/s)
Pré-configurando pacotes ...
A seleccionar pacote anteriormente não seleccionado vsftpd.
(Lendo banco de dados ... 134770 ficheiros e directórios actualmente instalados.)
A preparar para desempacotar .../vsftpd_3.0.3-12_amd64.deb ...
A descompactar vsftpd (3.0.3-12) ...
Configurando vsftpd (3.0.3-12) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.service.
[vsftpd.conf:1] Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
A processar 'triggers' para man-db (2.8.5-2) ...
A processar 'triggers' para systemd (241-7-deb10u7) ...
rm88574@virtualdebian:~$ sudo systemctl enable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
rm88574@virtualdebian:~$ sudo systemctl start vsftpd
rm88574@virtualdebian:~$
```

Editando as configurações padrão do serviço FTP:

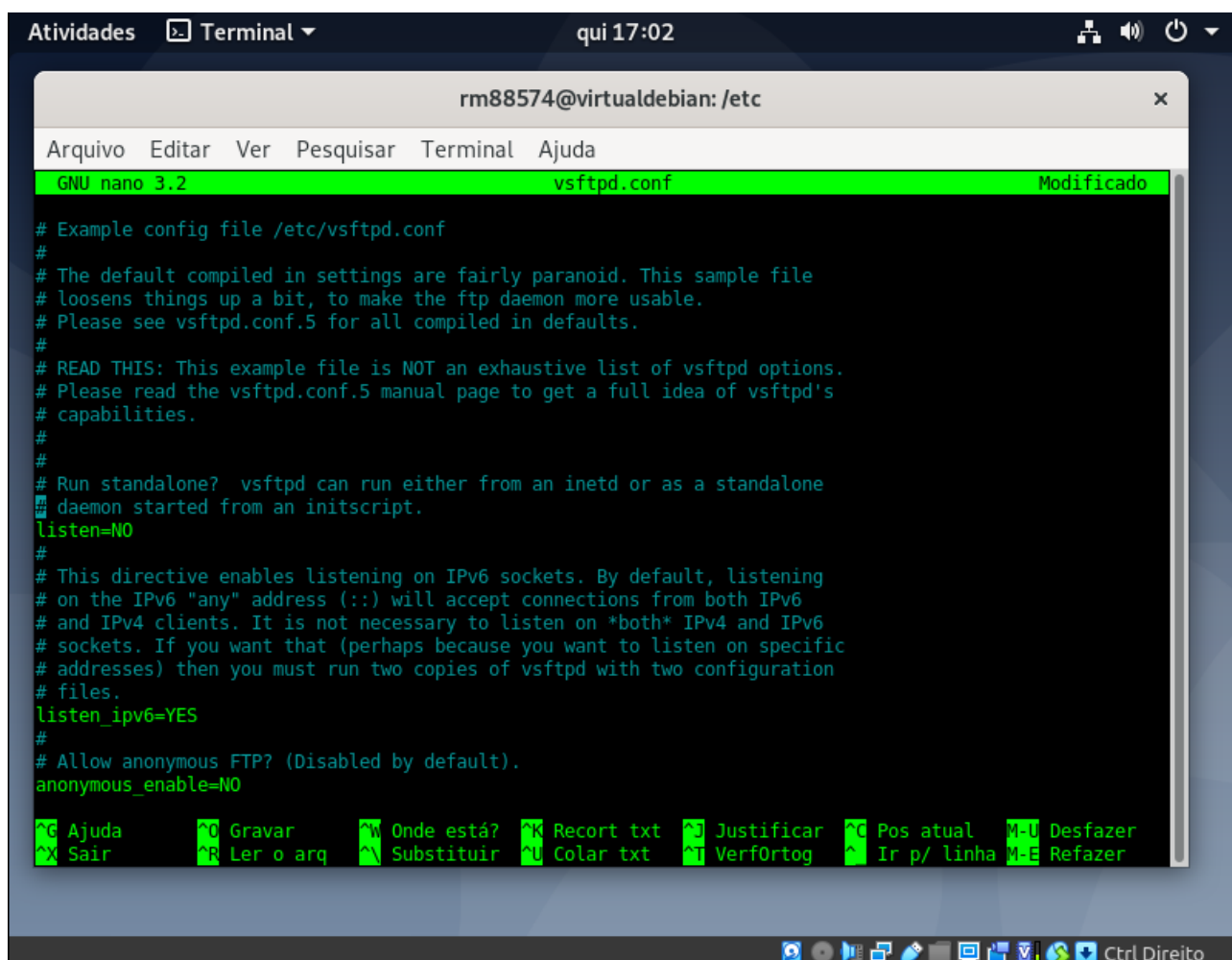
No diretório `/etc/vsftpd.conf`

ftpd_banner=Bem-vindo ao FTP da Feirinha Organica

listen_ipv6=YES

anonymous_enable=NO

chroot_local_user=YES



The screenshot shows a terminal window titled "rm88574@virtualdebian: /etc" with a nano 3.2 editor open to the file "vsftpd.conf". The editor's status bar indicates "Modificado". The configuration file content is as follows:

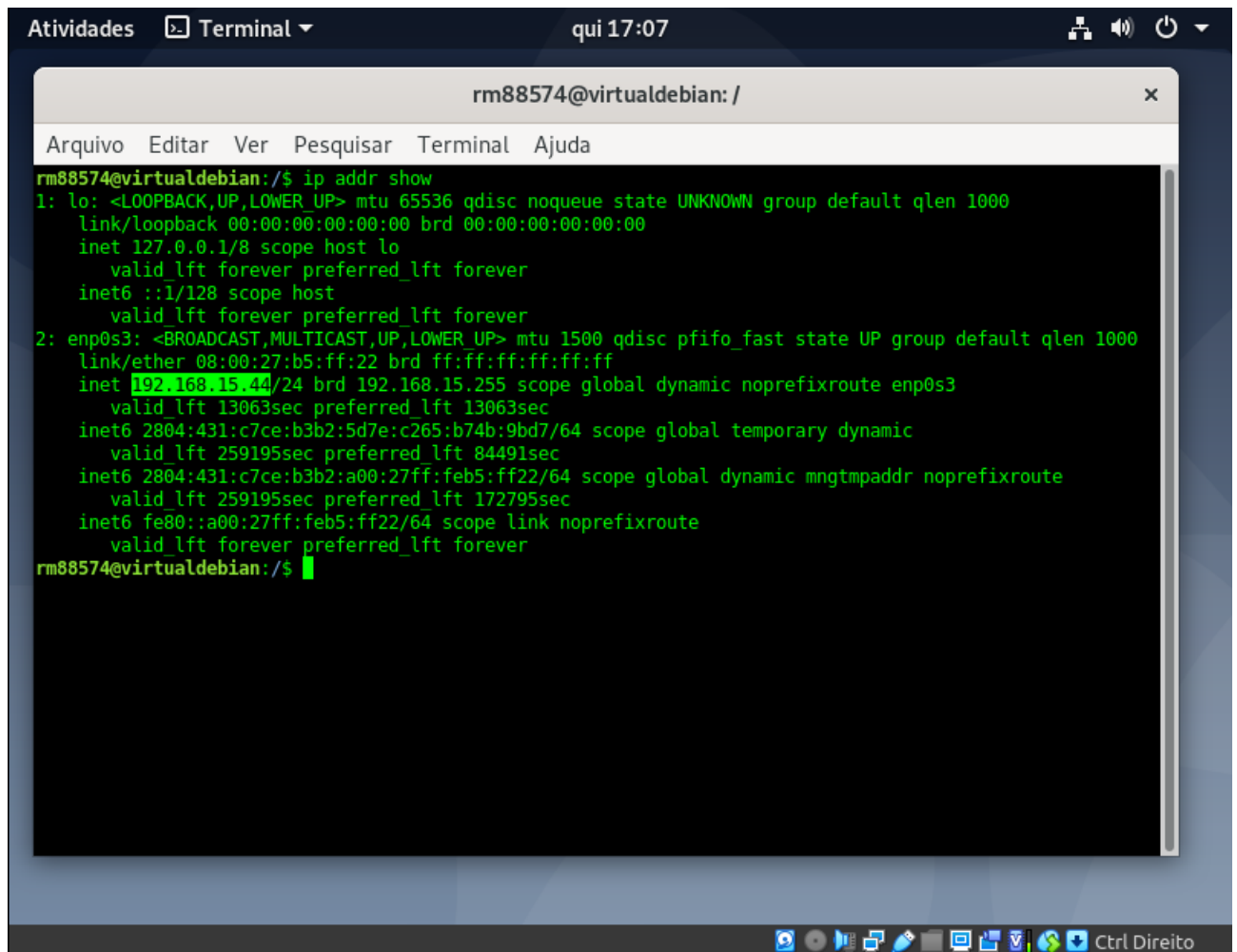
```
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (:::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
```

At the bottom of the terminal, there is a taskbar with various icons and a "Ctrl Direito" button.

Depois de reiniciar o serviço de FTP para as configurações fazerem efeito, vamos agora testando o serviço FTP

Na máquina virtual:

ip addr show



The screenshot shows a terminal window titled "rm88574@virtualdebian: /". The terminal output of the command "ip addr show" is as follows:

```
rm88574@virtualdebian:/$ ip addr show
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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:b5:ff:22 brd ff:ff:ff:ff:ff:ff
    inet 192.168.15.44/24 brd 192.168.15.255 scope global dynamic noprefixroute enp0s3
        valid_lft 13063sec preferred_lft 13063sec
    inet6 2804:431:c7ce:b3b2:5d7e:c265:b74b:9bd7/64 scope global temporary dynamic
        valid_lft 259195sec preferred_lft 84491sec
    inet6 2804:431:c7ce:b3b2:a00:27ff:feb5:ff22/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 259195sec preferred_lft 172795sec
    inet6 fe80::a00:27ff:feb5:ff22/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
rm88574@virtualdebian:/$
```

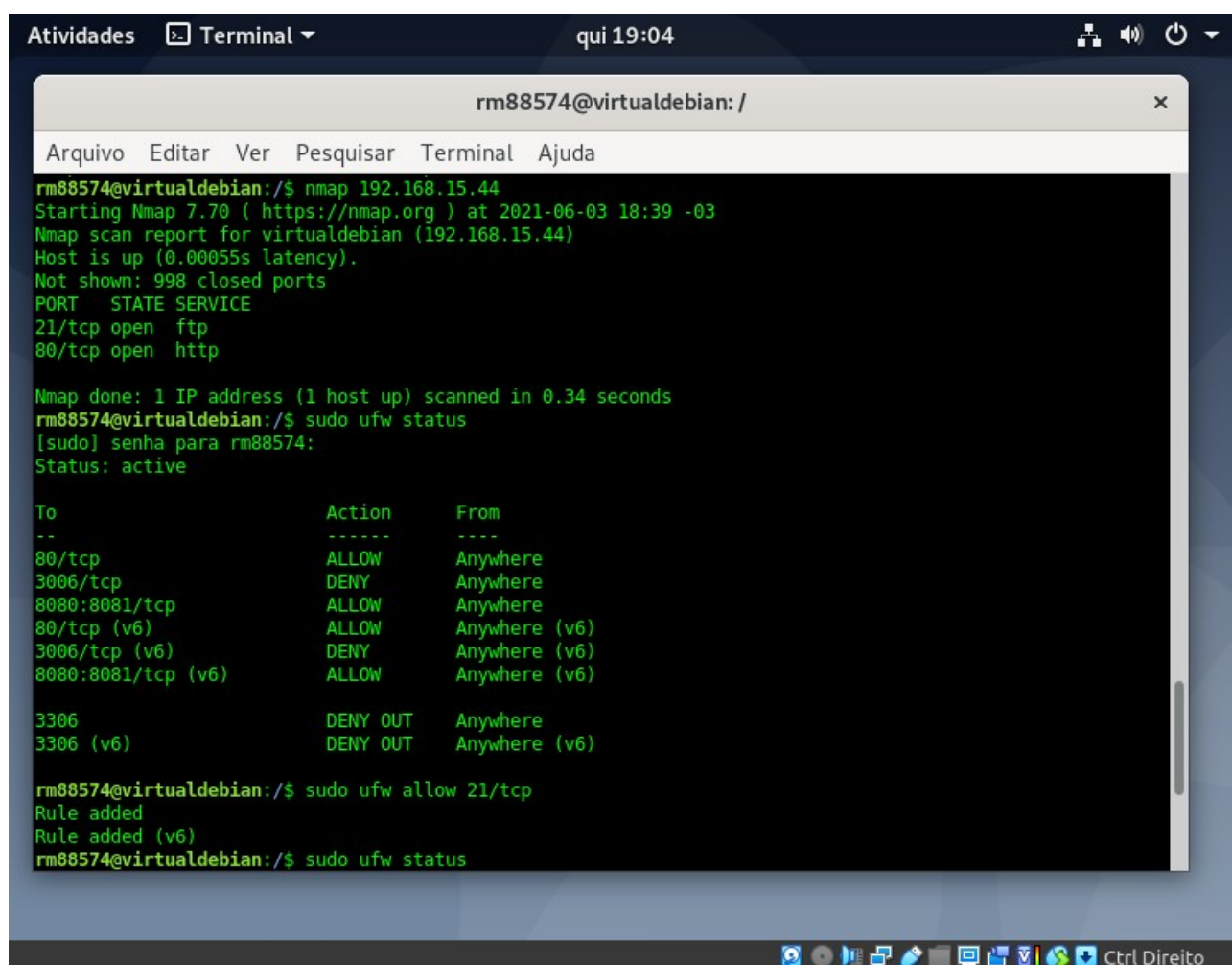
Verificando as portas abertas do servidor da feirinha:

nmap 192.168.15.44

A porta esta aberta, mas precisamos liberar no firewall:

sudo ufw allow 21/tcp

sudo ufw status



The image shows a terminal window titled "rm88574@virtualdebian: /". The terminal output is as follows:

```
rm88574@virtualdebian:/$ nmap 192.168.15.44
Starting Nmap 7.70 ( https://nmap.org ) at 2021-06-03 18:39 -03
Nmap scan report for virtualdebian (192.168.15.44)
Host is up (0.00055s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http

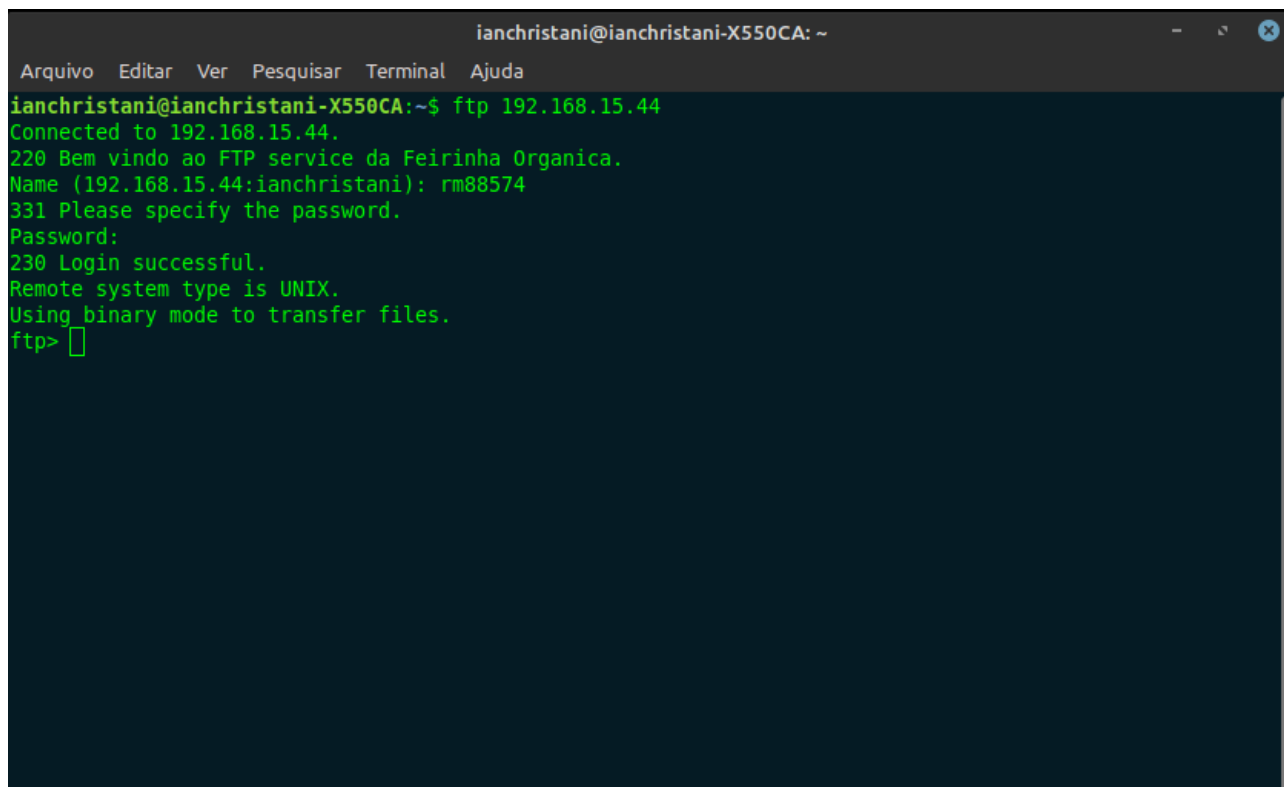
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
rm88574@virtualdebian:/$ sudo ufw status
[sudo] senha para rm88574:
Status: active
```

| To | Action | From |
|--------------------|----------|---------------|
| -- | ----- | ---- |
| 80/tcp | ALLOW | Anywhere |
| 3006/tcp | DENY | Anywhere |
| 8080:8081/tcp | ALLOW | Anywhere |
| 80/tcp (v6) | ALLOW | Anywhere (v6) |
| 3006/tcp (v6) | DENY | Anywhere (v6) |
| 8080:8081/tcp (v6) | ALLOW | Anywhere (v6) |
| 3306 | DENY OUT | Anywhere |
| 3306 (v6) | DENY OUT | Anywhere (v6) |

```
rm88574@virtualdebian:/$ sudo ufw allow 21/tcp
Rule added
Rule added (v6)
rm88574@virtualdebian:/$ sudo ufw status
```

Vamos testar a conexão na maquina hospedeira:

ftp 192.168.15.44



```
ianchristani@ianchristani-X550CA: ~  
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda  
ianchristani@ianchristani-X550CA:~$ ftp 192.168.15.44  
Connected to 192.168.15.44.  
220 Bem vindo ao FTP service da Feirinha Organica.  
Name (192.168.15.44:ianchristani): rm88574  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> 
```

Feito isto, vamos agora instalar o Zabbix Server. De acordo com as boas práticas, vamos criar um diretório temporário para trabalharmos a instalação do aplicativo (dentro do diretório **/tmp**).

Baixando o Zabbix:

```
sudo wget https://repo.zabbix.com/zabbix/4.2/debian/pool/main/z/zabbix-release/zabbix-release\_4.2-2+buster\_all.deb
```

```

rm88574@virtualdebian: /tmp/zabbix
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
rm88574@virtualdebian:/$ ls
bin  dev  home  initrd.img.old  lib32  libx32  media  opt  root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib  lib64  lost+found  mnt  proc  run  srv  tmp  var  vmlinuz.old
rm88574@virtualdebian:/$ cd /tmp
rm88574@virtualdebian:/tmp$ ls
pulse-PKdhtXMmr18n
systemd-private-41a166b843c047e9b0087610a2559a42-apache2.service-1N7STB
systemd-private-41a166b843c047e9b0087610a2559a42-colord.service-LrVNg7
systemd-private-41a166b843c047e9b0087610a2559a42-ModemManager.service-JeKaFz
systemd-private-41a166b843c047e9b0087610a2559a42-rtkit-daemon.service-dwoTGT
systemd-private-41a166b843c047e9b0087610a2559a42-systemd-timesyncd.service-BTGutC
systemd-private-41a166b843c047e9b0087610a2559a42-upower.service-vB1a3R
Temp-69608ddf-76d3-49cf-8531-7f0adf9ba4b8
Temp-7a83369e-29e4-49d7-ab6d-21496002e45f
tracker-extract-files.1000
rm88574@virtualdebian:/tmp$ mkdir zabbix
rm88574@virtualdebian:/tmp$ cd zabbix
rm88574@virtualdebian:/tmp/zabbix$ sudo wget http://repo.zabbix.com/zabbix/4.2/debian/pool/main/z/zabbix-
release/zabbix-release_4.2-2+buster_all.deb
--2021-06-03 19:34:01-- http://repo.zabbix.com/zabbix/4.2/debian/pool/main/z/zabbix-release/zabbix-relea
se_4.2-2+buster_all.deb
Resolvendo repo.zabbix.com (repo.zabbix.com)... 2604:a880:2:d0::2062:d001, 178.128.6.101
Conectando-se a repo.zabbix.com (repo.zabbix.com)|2604:a880:2:d0::2062:d001|:80... conectado.
A requisição HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: 4080 (4,0K) [application/octet-stream]
Salvando em: "zabbix-release_4.2-2+buster_all.deb"

zabbix-release_4.2-2+buste 100%[=====] 3,98K --.-KB/s em 0s
2021-06-03 19:34:01 (20,3 MB/s) - "zabbix-release_4.2-2+buster_all.deb" salvo [4080/4080]
rm88574@virtualdebian:/tmp/zabbix$

```

Descompactando o Zabbix:

```
sudo dpkg -i zabbix-release_4.2-2+buster_all.deb
```

Instalando o Zabbix:

```
sudo apt update
```

```
sudo apt install zabbix-server-mysql zabbix-frontend-php
```

```

Atividades Terminal ▼ qui 19:42
rm88574@virtualdebian: /tmp/zabbix
Arquivo Editar Ver Pesquisar Terminal Ajuda
rm88574@virtualdebian:/tmp/zabbix$ sudo apt install zabbix-server-mysql zabbix-frontend-php
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
The following additional packages will be installed:
  fping libodbc1 libopenipmi0 php-bcmath php-ldap php7.3-bcmath php7.3-ldap snmpd ttf-dejavu-core
Pacotes sugeridos:
  libmyodbc odbc-postgresql tdsodbc unixodbc-bin snmpttrapd
Os NOVOS pacotes a seguir serão instalados:
  fping libodbc1 libopenipmi0 php-bcmath php-ldap php7.3-bcmath php7.3-ldap snmpd ttf-dejavu-core
  zabbix-frontend-php zabbix-server-mysql
0 pacotes atualizados, 11 pacotes novos instalados, 0 a serem removidos e 1 não atualizados.
É preciso baixar 5.789 kB de arquivos.
Depois desta operação, 25,6 MB adicionais de espaço em disco serão usados.
Você quer continuar? [S/n] s
Obter:1 http://deb.debian.org/debian buster/main amd64 libodbc1 amd64 2.3.6-0.1 [223 kB]
Obter:2 http://deb.debian.org/debian buster/main amd64 libopenipmi0 amd64 2.0.25-2.1 [540 kB]
Obter:3 http://deb.debian.org/debian buster/main amd64 fping amd64 4.2-1 [37,7 kB]
Obter:4 http://deb.debian.org/debian buster/main amd64 php7.3-bcmath amd64 7.3.27-1~deb10u1 [15,0 kB]
Obter:5 http://deb.debian.org/debian buster/main amd64 php-bcmath all 2:7.3+69 [5.996 B]
Obter:6 http://deb.debian.org/debian buster/main amd64 php7.3-ldap amd64 7.3.27-1~deb10u1 [29,4 kB]
Obter:7 http://deb.debian.org/debian buster/main amd64 php-ldap all 2:7.3+69 [5.988 B]
Obter:8 http://deb.debian.org/debian buster/main amd64 snmpd amd64 5.7.3+dfsg-5+deb10u2 [56,2 kB]
Obter:9 http://deb.debian.org/debian buster/main amd64 ttf-dejavu-core all 2.37-1 [32,1 kB]
Obter:10 http://repo.zabbix.com/zabbix/4.2/debian buster/main amd64 zabbix-server-mysql amd64 1:4.2.8-1+buster [2.362 kB]
Obter:11 http://repo.zabbix.com/zabbix/4.2/debian buster/main amd64 zabbix-frontend-php all 1:4.2.8-1+buster [2.482 kB]
Baixados 5.789 kB em 4s (1.647 kB/s)
Pré-configurando pacotes ...
A seleccionar pacote anteriormente não seleccionado libodbc1:amd64.
(Lendo banco de dados ... 135673 ficheiros e directórios actualmente instalados.)

```

Instalando o agente:

sudo apt install zabbix-agent

```

Atividades Terminal ▼ qui 19:44
rm88574@virtualdebian: /tmp/zabbix
Arquivo Editar Ver Pesquisar Terminal Ajuda
update-alternatives: a usar /usr/share/fonts/truetype/dejavu/DejaVuSans.ttf para disponibilizar /usr/share/zabbix/assets/fonts/graphfont.ttf (zabbix-frontend-font) em modo auto
Enabling conf zabbix.
To activate the new configuration, you need to run:
  systemctl reload apache2
A processar 'triggers' para libc-bin (2.28-10) ...
A processar 'triggers' para libapache2-mod-php7.3 (7.3.27-1~deb10u1) ...
A processar 'triggers' para systemd (241-7~deb10u7) ...
A processar 'triggers' para man-db (2.8.5-2) ...
A processar 'triggers' para fontconfig (2.13.1-2) ...
rm88574@virtualdebian:/tmp/zabbix$ sudo apt install zabbix-agent
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
Os NOVOS pacotes a seguir serão instalados:
  zabbix-agent
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos e 1 não atualizados.
É preciso baixar 459 kB de arquivos.
Depois desta operação, 993 kB adicionais de espaço em disco serão usados.
Obter:1 http://repo.zabbix.com/zabbix/4.2/debian buster/main amd64 zabbix-agent amd64 1:4.2.8-1+buster [459 kB]
Baixados 459 kB em 2s (209 kB/s)
A seleccionar pacote anteriormente não seleccionado zabbix-agent.
(Lendo banco de dados ... 136867 ficheiros e directórios actualmente instalados.)
A preparar para desempacotar .../zabbix-agent_1%3a4.2.8-1+buster_amd64.deb ...
A descompactar zabbix-agent (1:4.2.8-1+buster) ...
Configurando zabbix-agent (1:4.2.8-1+buster) ...
A processar 'triggers' para man-db (2.8.5-2) ...
A processar 'triggers' para systemd (241-7~deb10u7) ...
rm88574@virtualdebian:/tmp/zabbix$

```

Configurando o banco de dados para o uso do Zabbix:

mysql -u root -p

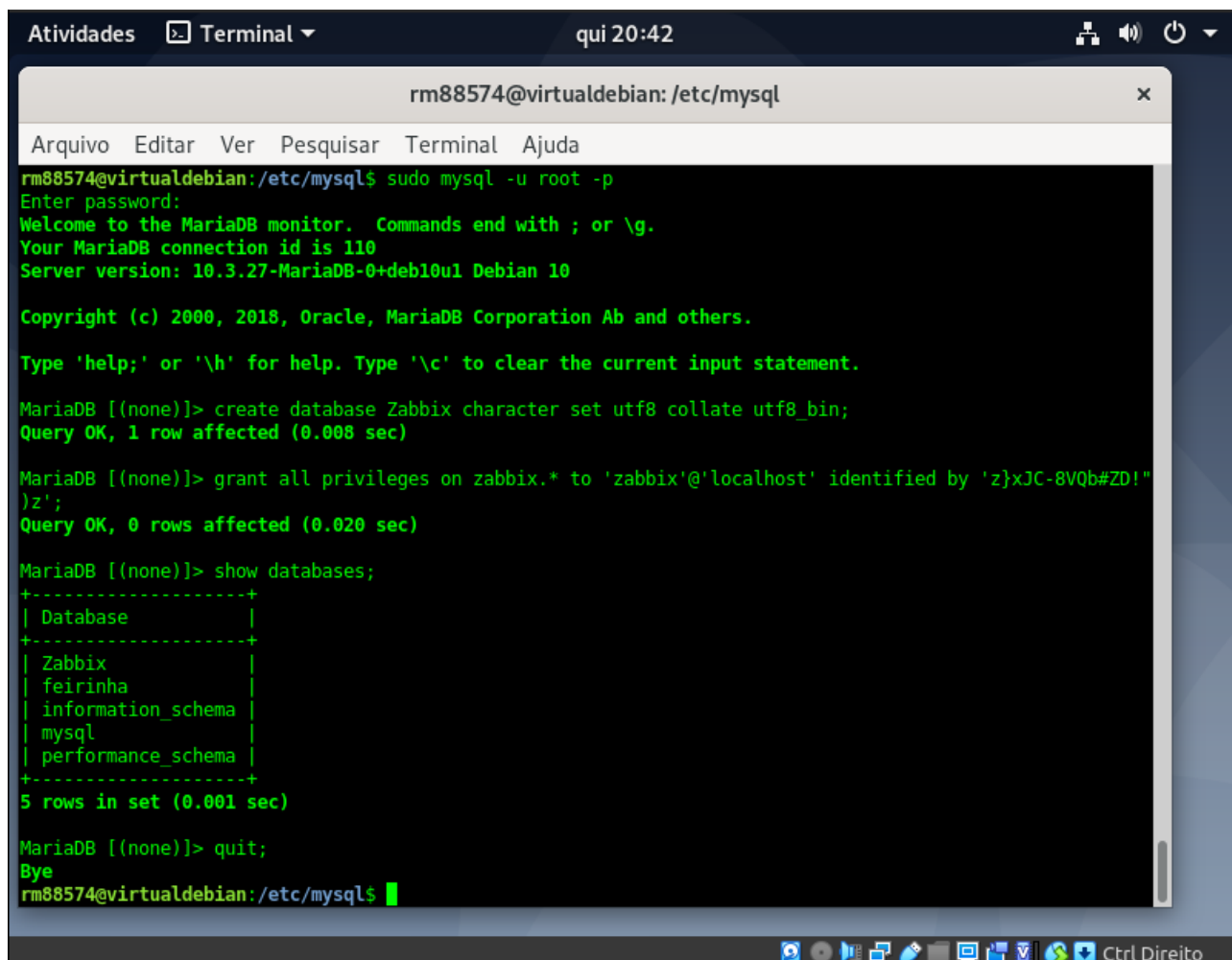
senha: \$i09A04n78_oKaI

create database Zabbix character set utf8 collate utf8_bin;

grant all privileges on Zabbix.* to 'zabbix'@'localhost' identified by 'z}xJC-8VQb#ZD!")z';

Vamos verificar se houve modificação no mysql no root e no usuário zabbix:

show databases;



The screenshot shows a terminal window titled "rm88574@virtualdebian: /etc/mysql". The terminal displays the following commands and output:

```
rm88574@virtualdebian:/etc/mysql$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 110
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> create database Zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected (0.008 sec)

MariaDB [(none)]> grant all privileges on zabbix.* to 'zabbix'@'localhost' identified by 'z}xJC-8VQb#ZD!'
)z';
Query OK, 0 rows affected (0.020 sec)

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| Zabbix   |
| feirinha |
| information_schema |
| mysql    |
| performance_schema |
+-----+
5 rows in set (0.001 sec)

MariaDB [(none)]> quit;
Bye
rm88574@virtualdebian:/etc/mysql$
```

The terminal window has a menu bar with "Arquivo", "Editar", "Ver", "Pesquisar", "Terminal", and "Ajuda". The system clock shows "qui 20:42". The bottom status bar includes system icons and the text "Ctrl Direito".

```
m88574@virtualdebian:~$ mysql -u zabbix -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 57
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| Zabbix   |
| information_schema |
+-----+
2 rows in set (0.001 sec)

MariaDB [(none)]> 
```

Importando os dados iniciais:

```
sudo zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -u zabbix -p Zabbix
```

Configurando o PHP para o Zabbix:

alterando o time zone do arquivo de configuração do apache:

```
sudo nano /etc/zabbix/apache.conf
```

```

rm88574@virtualdebian: ~
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
GNU nano 3.2 /etc/zabbix/apache.conf Modificado

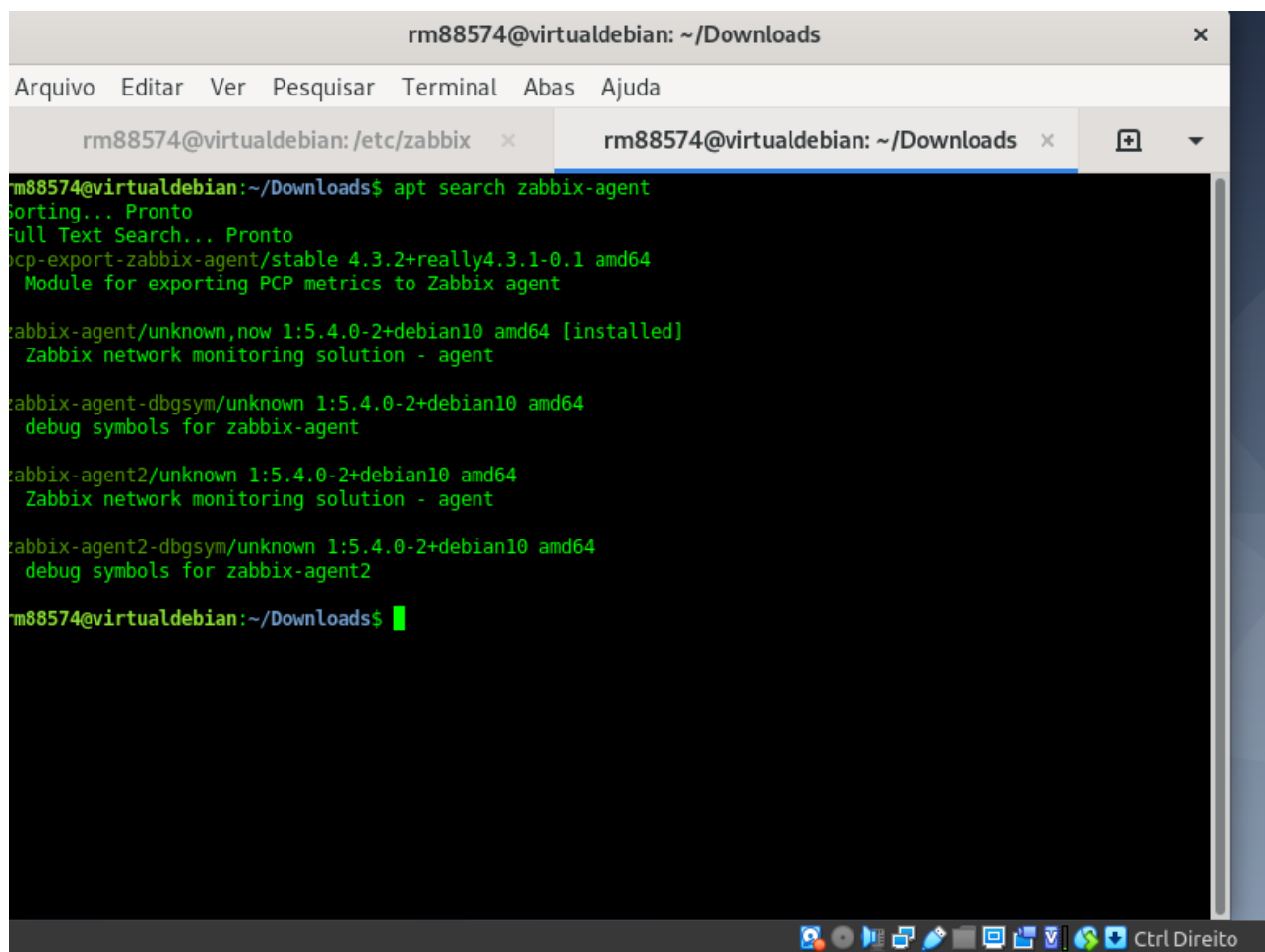
    php_value post_max_size 16M
    php_value upload_max_filesize 2M
    php_value max_input_time 300
    php_value max_input_vars 10000
    php_value always_populate_raw_post_data -1
    # php_value date.timezone Europe/Riga
</IfModule>
<IfModule mod_php7.c>
    php_value max_execution_time 300
    php_value memory_limit 128M
    php_value post_max_size 16M
    php_value upload_max_filesize 2M
    php_value max_input_time 300
    php_value max_input_vars 10000
    php_value always_populate_raw_post_data -1
    php_value date.timezone America/Sao_Paulo
</IfModule>
</Directory>
<Directory "/usr/share/zabbix/conf">
    Order deny,allow
    Deny from all
    <files *.php>
        Order deny,allow
        Deny from all
    </files>
</Directory>

^G Ajuda      ^O Gravar     ^W Onde está? ^K Recort txt  ^J Justificar ^C Pos atual  M-U Desfazer
^X Sair       ^R Ler o arq ^_ Substituir ^U Colar txt  ^I Verf0rtog ^_ Ir p/ linha M-E Refazer

```

Verificando a versão do agente encontra-se instalado:

apt search zabbix-agent



The screenshot shows a terminal window titled 'rm88574@virtualdebian: ~/Downloads'. The terminal output is as follows:

```
rm88574@virtualdebian:~/Downloads$ apt search zabbix-agent
Sorting... Pronto
Full Text Search... Pronto
pcp-export-zabbix-agent/stable 4.3.2+really4.3.1-0.1 amd64
  Module for exporting PCP metrics to Zabbix agent

zabbix-agent/unknown,now 1:5.4.0-2+debian10 amd64 [installed]
  Zabbix network monitoring solution - agent

zabbix-agent-dbgSYM/unknown 1:5.4.0-2+debian10 amd64
  debug symbols for zabbix-agent

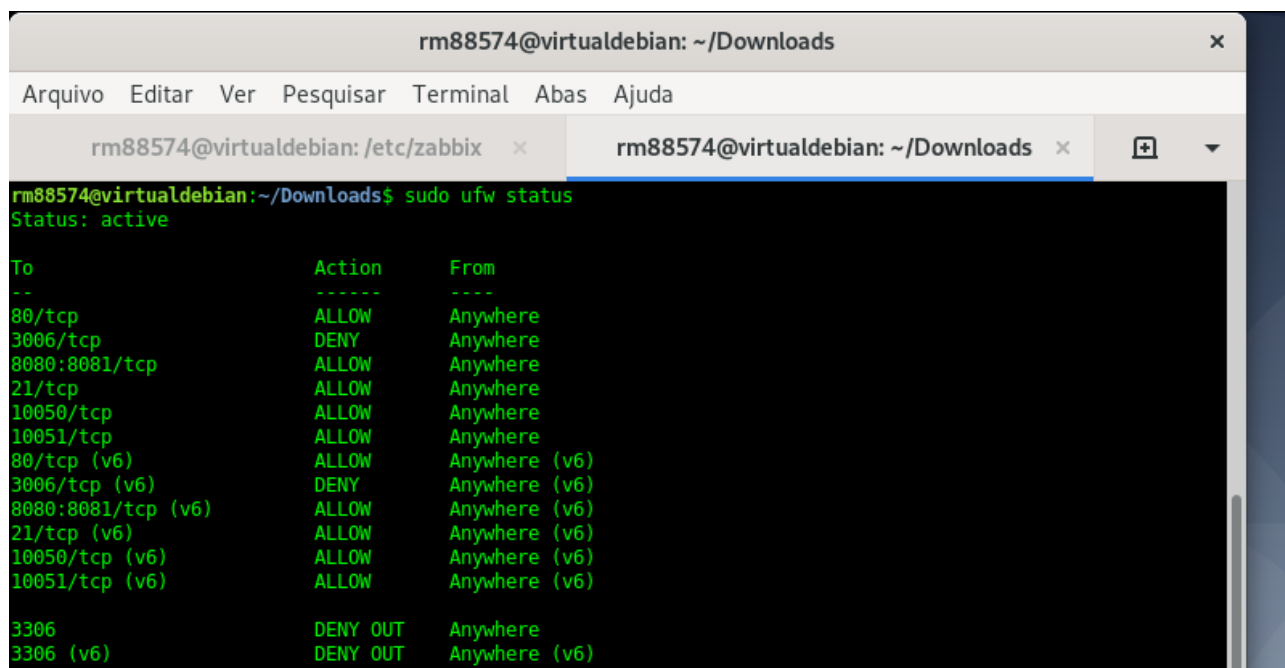
zabbix-agent2/unknown 1:5.4.0-2+debian10 amd64
  Zabbix network monitoring solution - agent

zabbix-agent2-dbgSYM/unknown 1:5.4.0-2+debian10 amd64
  debug symbols for zabbix-agent2

rm88574@virtualdebian:~/Downloads$
```

The terminal window has a menu bar with 'Arquivo', 'Editar', 'Ver', 'Pesquisar', 'Terminal', 'Abas', and 'Ajuda'. The tab bar shows two tabs: 'rm88574@virtualdebian: /etc/zabbix' and 'rm88574@virtualdebian: ~/Downloads'. The status bar at the bottom includes system icons and the text 'Ctrl Direito'.

Feito isto vamos ajustar o firewall:

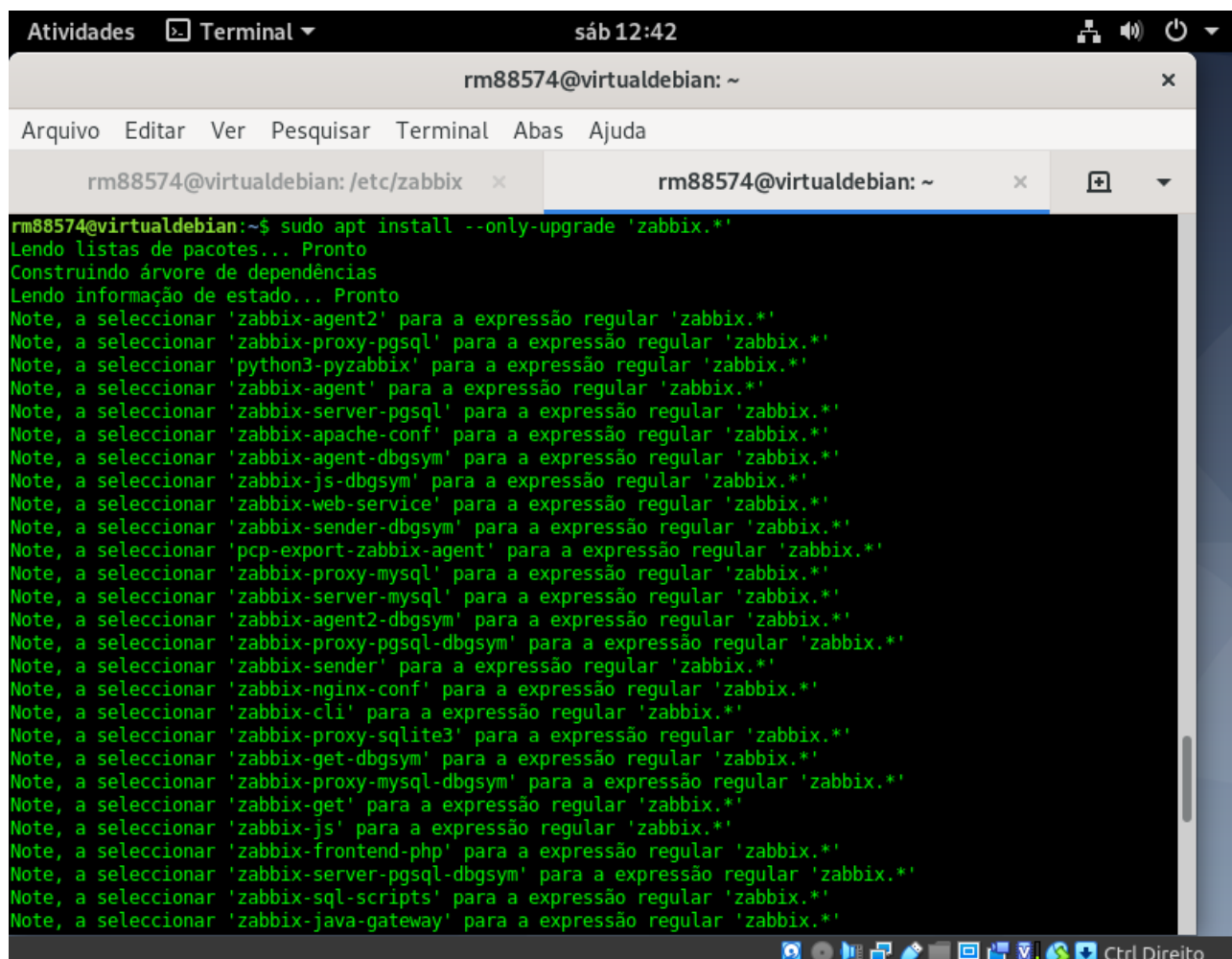


The screenshot shows a terminal window titled "rm88574@virtualdebian: ~/Downloads". The window has a menu bar with "Arquivo", "Editar", "Ver", "Pesquisar", "Terminal", "Abas", and "Ajuda". There are two tabs: "rm88574@virtualdebian: /etc/zabbix" and "rm88574@virtualdebian: ~/Downloads". The terminal content shows the command "sudo ufw status" being executed, resulting in the output "Status: active". Below this, a table of firewall rules is displayed.

| To | Action | From |
|--------------------|----------|---------------|
| 80/tcp | ALLOW | Anywhere |
| 3006/tcp | DENY | Anywhere |
| 8080:8081/tcp | ALLOW | Anywhere |
| 21/tcp | ALLOW | Anywhere |
| 10050/tcp | ALLOW | Anywhere |
| 10051/tcp | ALLOW | Anywhere |
| 80/tcp (v6) | ALLOW | Anywhere (v6) |
| 3006/tcp (v6) | DENY | Anywhere (v6) |
| 8080:8081/tcp (v6) | ALLOW | Anywhere (v6) |
| 21/tcp (v6) | ALLOW | Anywhere (v6) |
| 10050/tcp (v6) | ALLOW | Anywhere (v6) |
| 10051/tcp (v6) | ALLOW | Anywhere (v6) |
| 3306 | DENY OUT | Anywhere |
| 3306 (v6) | DENY OUT | Anywhere (v6) |

Antes de fazermos um teste, vamos garantir a versão mais atual:

```
sudo apt install --only-upgrade 'zabbix.*'
```



The screenshot shows a terminal window titled "Terminal" with the user "rm88574@virtualdebian" and the time "sáb 12:42". The terminal displays the command `sudo apt install --only-upgrade 'zabbix.*'` and its output. The output indicates that the system is upgrading Zabbix packages. It lists several packages that are being upgraded, including `zabbix-agent2`, `zabbix-proxy-pgsql`, `python3-pyzabbix`, `zabbix-agent`, `zabbix-server-pgsql`, `zabbix-apache-conf`, `zabbix-agent-dbg`, `zabbix-js-dbg`, `zabbix-web-service`, `zabbix-sender-dbg`, `pcp-export-zabbix-agent`, `zabbix-proxy-mysql`, `zabbix-server-mysql`, `zabbix-agent2-dbg`, `zabbix-proxy-pgsql-dbg`, `zabbix-sender`, `zabbix-nginx-conf`, `zabbix-cli`, `zabbix-proxy-sqlite3`, `zabbix-get-dbg`, `zabbix-proxy-mysql-dbg`, `zabbix-get`, `zabbix-js`, `zabbix-frontend-php`, `zabbix-server-pgsql-dbg`, `zabbix-sql-scripts`, and `zabbix-java-gateway`. The terminal window has a menu bar with "Arquivo", "Editar", "Ver", "Pesquisar", "Terminal", "Abas", and "Ajuda". The status bar at the bottom shows various system icons and the text "Ctrl Direito".

```
rm88574@virtualdebian:~$ sudo apt install --only-upgrade 'zabbix.*'
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
Note, a seleccionar 'zabbix-agent2' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-proxy-pgsql' para a expressão regular 'zabbix.*'
Note, a seleccionar 'python3-pyzabbix' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-agent' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-server-pgsql' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-apache-conf' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-agent-dbg' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-js-dbg' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-web-service' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-sender-dbg' para a expressão regular 'zabbix.*'
Note, a seleccionar 'pcp-export-zabbix-agent' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-proxy-mysql' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-server-mysql' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-agent2-dbg' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-proxy-pgsql-dbg' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-sender' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-nginx-conf' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-cli' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-proxy-sqlite3' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-get-dbg' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-proxy-mysql-dbg' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-get' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-js' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-frontend-php' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-server-pgsql-dbg' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-sql-scripts' para a expressão regular 'zabbix.*'
Note, a seleccionar 'zabbix-java-gateway' para a expressão regular 'zabbix.*'
```

```
Atividades Terminal sáb 12:44
rm88574@virtualdebian: ~
Arquivo Editar Ver Pesquisar Terminal Abas Ajuda
rm88574@virtualdebian: /etc/zabbix x rm88574@virtualdebian: ~ x
Saltando python3-pyzabbix, não está instalado e só são pedidas actualizações.
Saltando zabbix-cli, não está instalado e só são pedidas actualizações.
zabbix-agent is already the newest version (1:5.4.0-2+debian10).
Saltando zabbix-agent-dbg, não está instalado e só são pedidas actualizações.
Saltando zabbix-agent2, não está instalado e só são pedidas actualizações.
Saltando zabbix-agent2-dbg, não está instalado e só são pedidas actualizações.
zabbix-apache-conf is already the newest version (1:5.4.0-2+debian10).
zabbix-frontend-php is already the newest version (1:5.4.0-2+debian10).
Saltando zabbix-get, não está instalado e só são pedidas actualizações.
Saltando zabbix-get-dbg, não está instalado e só são pedidas actualizações.
Saltando zabbix-java-gateway, não está instalado e só são pedidas actualizações.
Saltando zabbix-js, não está instalado e só são pedidas actualizações.
Saltando zabbix-js-dbg, não está instalado e só são pedidas actualizações.
Saltando zabbix-nginx-conf, não está instalado e só são pedidas actualizações.
Saltando zabbix-proxy-mysql, não está instalado e só são pedidas actualizações.
Saltando zabbix-proxy-mysql-dbg, não está instalado e só são pedidas actualizações.
Saltando zabbix-proxy-pgsql, não está instalado e só são pedidas actualizações.
Saltando zabbix-proxy-pgsql-dbg, não está instalado e só são pedidas actualizações.
Saltando zabbix-proxy-sqlite3, não está instalado e só são pedidas actualizações.
Saltando zabbix-proxy-sqlite3-dbg, não está instalado e só são pedidas actualizações.
zabbix-release is already the newest version (1:5.4-1+debian10).
Saltando zabbix-sender, não está instalado e só são pedidas actualizações.
Saltando zabbix-sender-dbg, não está instalado e só são pedidas actualizações.
zabbix-server-mysql is already the newest version (1:5.4.0-2+debian10).
Saltando zabbix-server-mysql-dbg, não está instalado e só são pedidas actualizações.
Saltando zabbix-server-pgsql, não está instalado e só são pedidas actualizações.
Saltando zabbix-server-pgsql-dbg, não está instalado e só são pedidas actualizações.
zabbix-sql-scripts is already the newest version (1:5.4.0-2+debian10).
Saltando zabbix-web-service, não está instalado e só são pedidas actualizações.
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
rm88574@virtualdebian:~$
```

Para finalizar a instalação do Zabbix e habilitar o monitoramento dos serviços, usaremos a interface web do Zabbix. No navegador entre no **localhost/zabbix**

Atividades Firefox ESR sex 12:46

Instalar plugins < F Feirinha Orgânica Nova aba Nova aba Installation x

localhost/zabbix/setup.php 90%

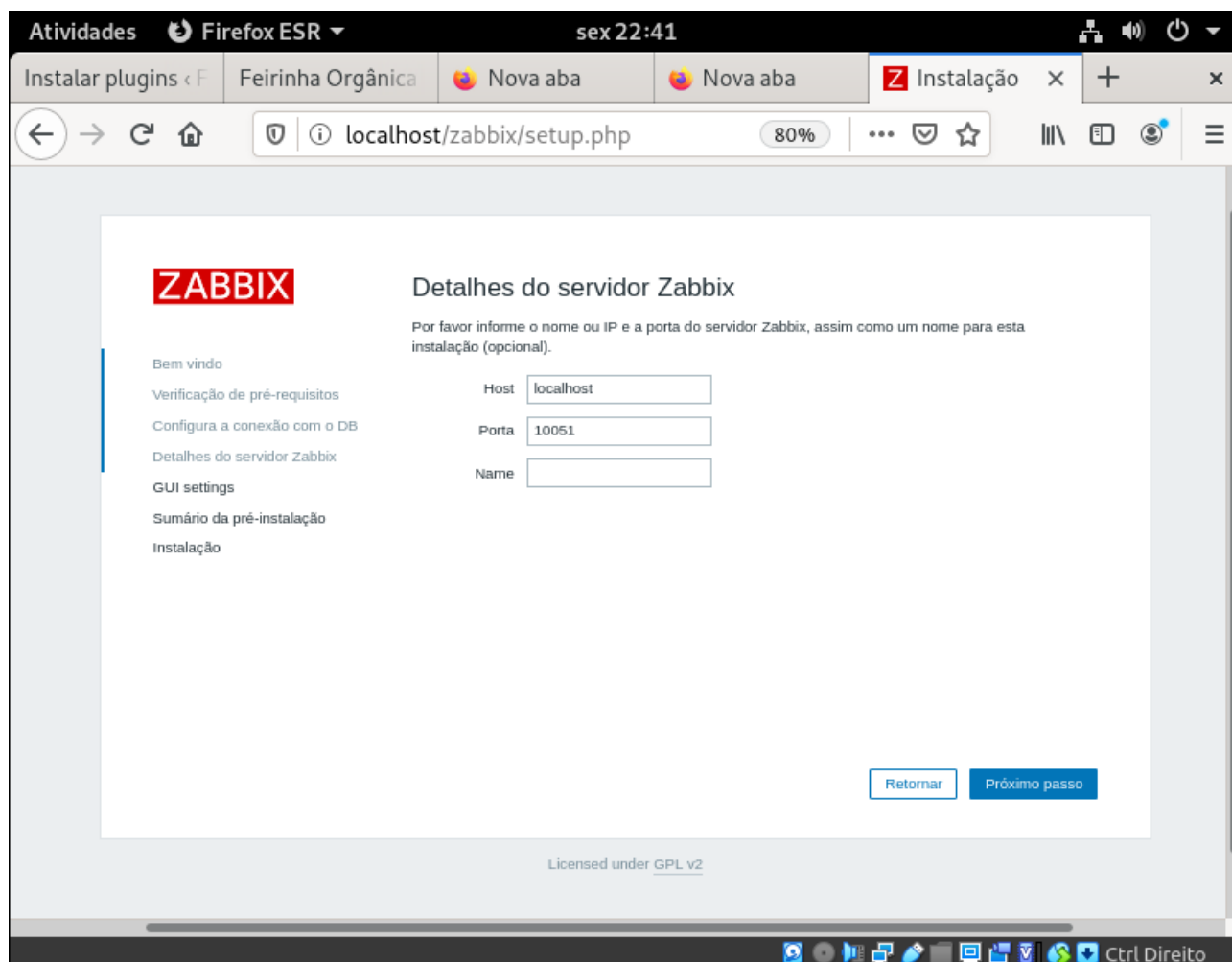
ZABBIX

Check of pre-requisites

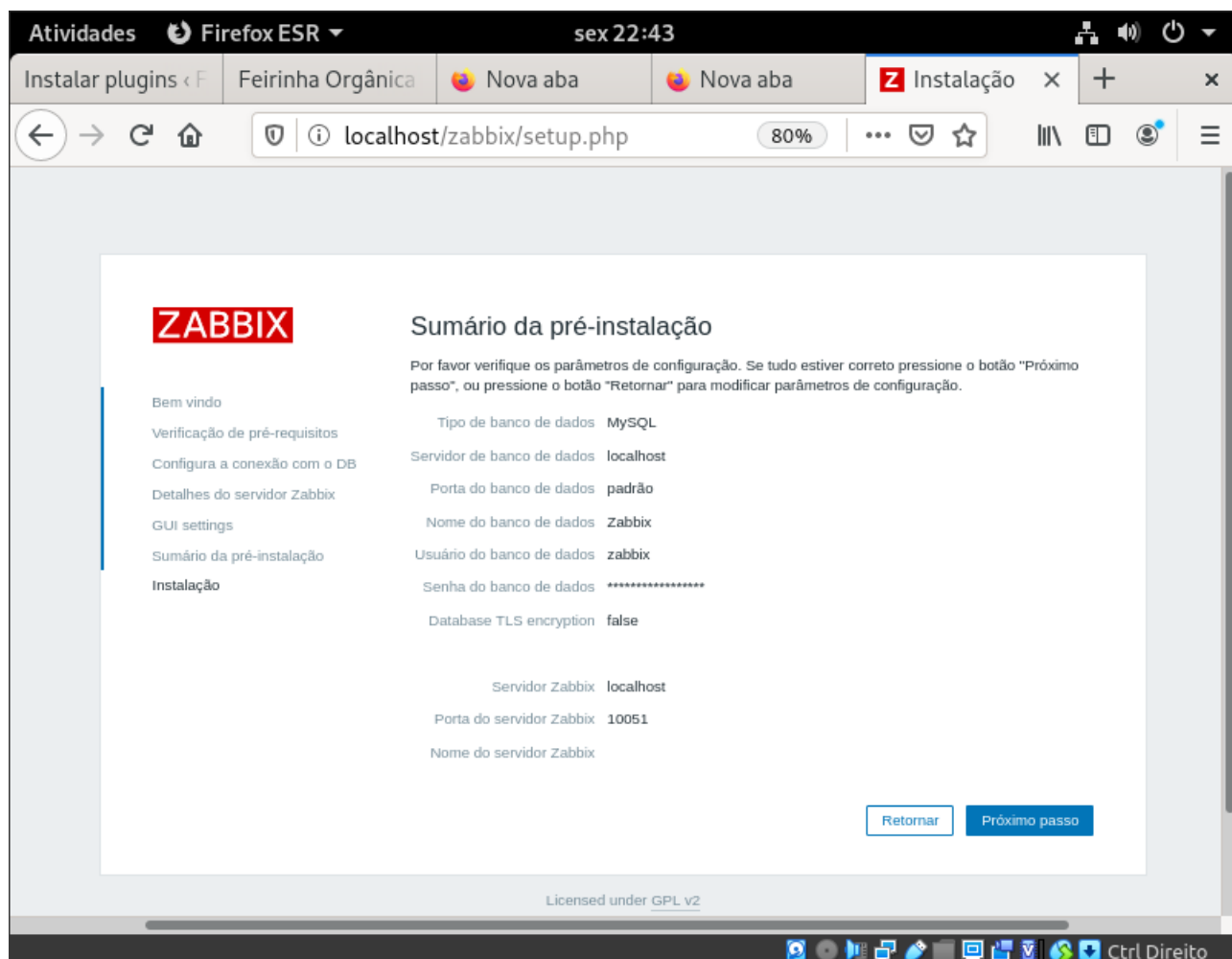
| | Current value | Required | |
|----------------------------------|-------------------|----------|----|
| PHP version | 7.3.27-1~deb10u1 | 5.4.0 | OK |
| PHP option "memory_limit" | 128M | 128M | OK |
| PHP option "post_max_size" | 16M | 16M | OK |
| PHP option "upload_max_filesize" | 2M | 2M | OK |
| PHP option "max_execution_time" | 300 | 300 | OK |
| PHP option "max_input_time" | 300 | 300 | OK |
| PHP option "date.timezone" | America/Sao_Paulo | | OK |
| PHP databases support | MySQL | | OK |
| PHP bcmath | on | | OK |
| PHP mbstring | on | | OK |

Back Next step

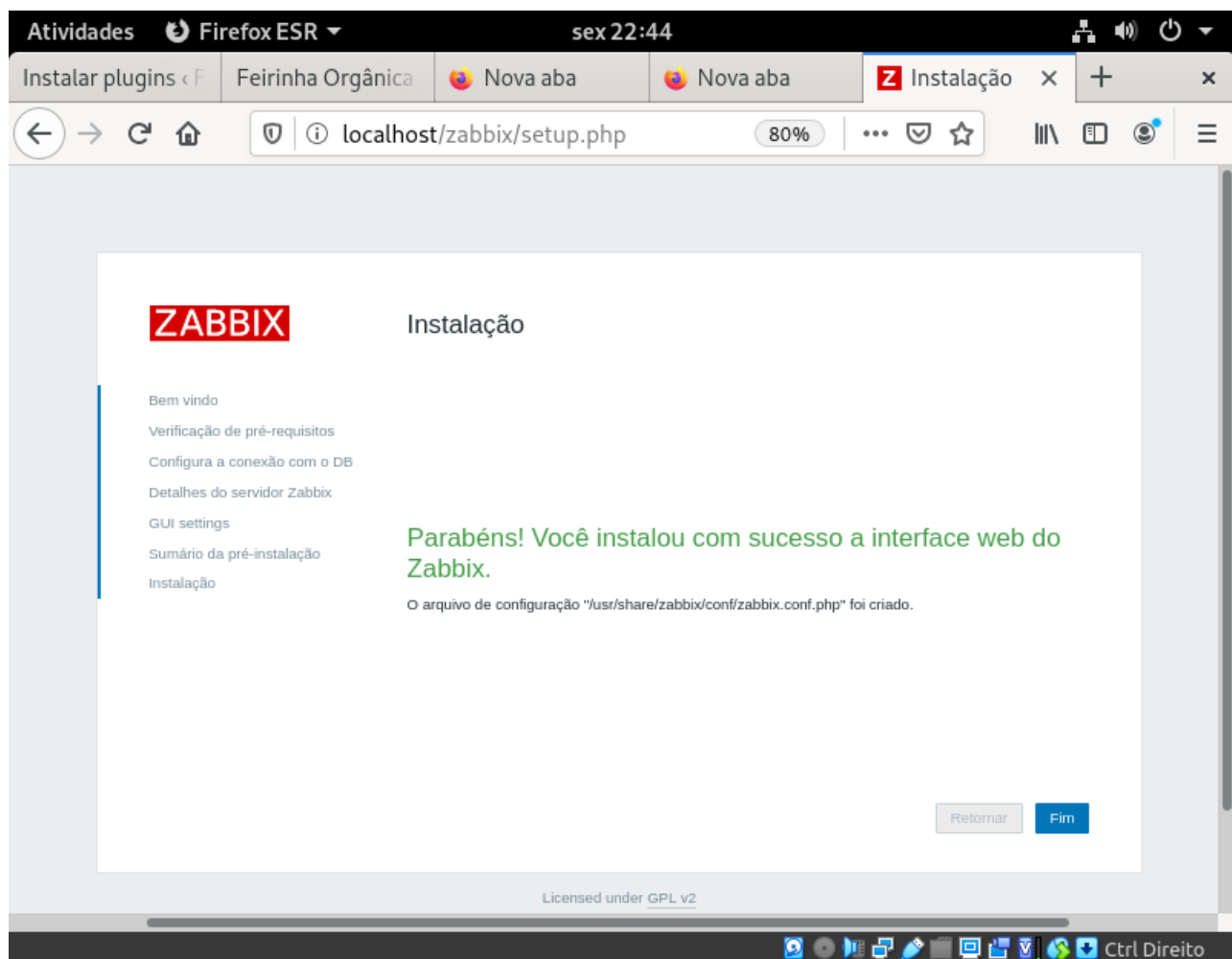
Ctrl Direito



Antes da instalação propriamente dita:



Instalação feita com sucesso:



O acesso aplicativo é feito com usuário padrão **Admin** e a senha é **zabbix**:

The screenshot shows the Zabbix web interface in a Firefox ESR browser window. The browser's address bar displays the URL `localhost/zabbix/zabbix.php?action=dashboard.view#`. The Zabbix dashboard is titled "Global view" and features a left-hand navigation menu with categories like "Monitoramento", "Inventário", "Relatórios", "Configuração", and "Administração". The main content area is divided into several sections:

- Informação do sistema**: A table showing system parameters.
- Incidentes**: A section for viewing incidents, currently showing "Sem dados encontrados."
- Summary Cards**: A series of colored boxes providing quick status updates.

| Parâmetro | Valor | Detalhes |
|---|-------|-----------------|
| Zabbix está rodando | Sim | localhost:10051 |
| Number of hosts (enabled/disabled) | 1 | 1 / 0 |
| Number of templates | 197 | |
| Quantidade de itens (habilitados/desabilitados/não suportados) | 121 | 107 / 0 / 14 |
| Quantidade de triggers (habilitadas/desabilitadas [incidente/ok]) | 55 | 55 / 0 [0 / 55] |
| Número de usuários (online) | 2 | 1 |

| Hora | Informação | Host | Incidente • Severidade | Duração | Reconhecido |
|------------------------|------------|------|------------------------|---------|-------------|
| Sem dados encontrados. | | | | | |

| Disponível | Indisponível | Desastre | Alta | Média | Ate |
|------------|--------------|----------|------|-------|-----|
| 1 | 0 | 0 | 0 | 0 | Ate |

Adicionado o host ao Zabbix:

ZABBIX << Hosts

Todos os hosts / Feirinha Organica Ativo ZBX Itens Triggers Gráficos Regras de descoberta Cenários web

Host Templates IPMI Etiquetas Macros Inventário Criptografia Mapeamento de valor

* Nome do host Feirinha Organica

Nome visível Feirinha Organica

* Grupos Monitoramento geral X Selecionar

Informe aqui o argumento para pesquisa

| Interfaces | Tipo | Endereço IP | Nome DNS | Connectado a | Porta | Padrão |
|------------|------|-------------|----------|--------------|-------|--------|
| Agente | | 127.0.0.1 | | IP | DNS | 10050 |

Adicionar

Descrição

Monitorado por proxy (sem proxy)

Ativo ☒

Atualizar Clonar Clone completo Excluir Cancelar

Agora adicionando os templates:

ZABBIX << Hosts

Todos os hosts / Feirinha Organica Ativo ZBX Itens Triggers Gráficos Regras de descoberta Cenários web

Host Templates 6 IPMI Etiquetas Macros Inventário Criptografia Mapeamento de valor

Associado aos templates Nome Ação

Link new templates

Apache by HTTP X FTP Service X Linux by Zabbix agent X Selecionar

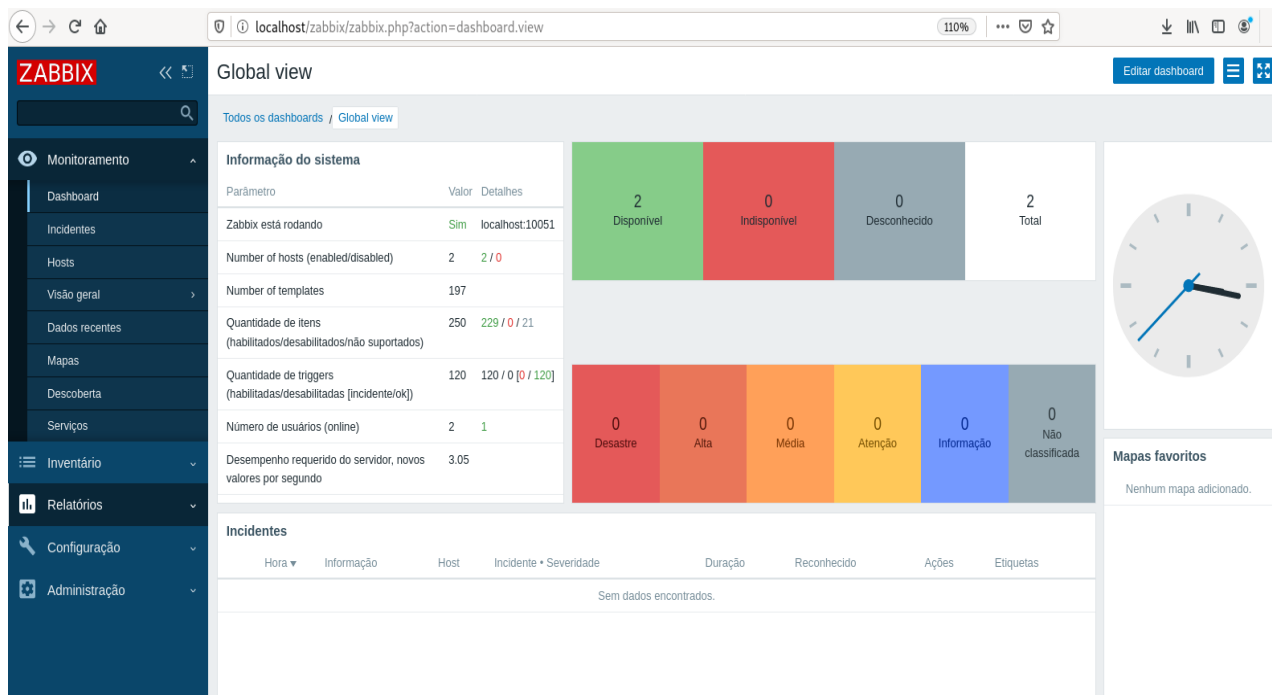
MySQL by Zabbix agent X MySQL by Zabbix agent 2 X Zabbix Server X

Informe aqui o argumento para pesquisa

Atualizar Clonar Clone completo Excluir Cancelar

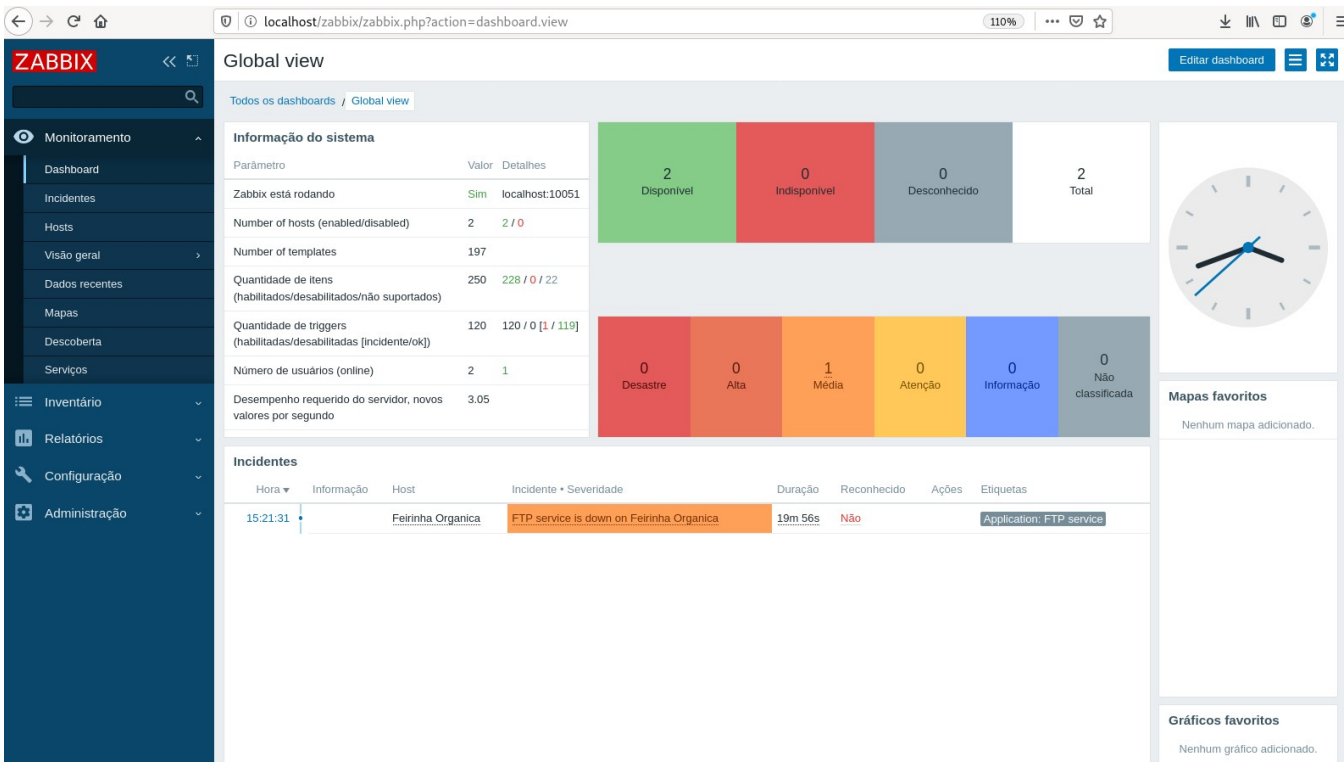
Como não havia o DB MySQL, escolhi 2: MySQL by Zabbix Agent e sua versão mais atual a Agent2.

O Dashboard depois dos templates:



Para finalizar, vamos fazer um teste do monitoramento para ver se esta funcionando. Vamos derrubar o FTP:

systemctl stop vsftpd

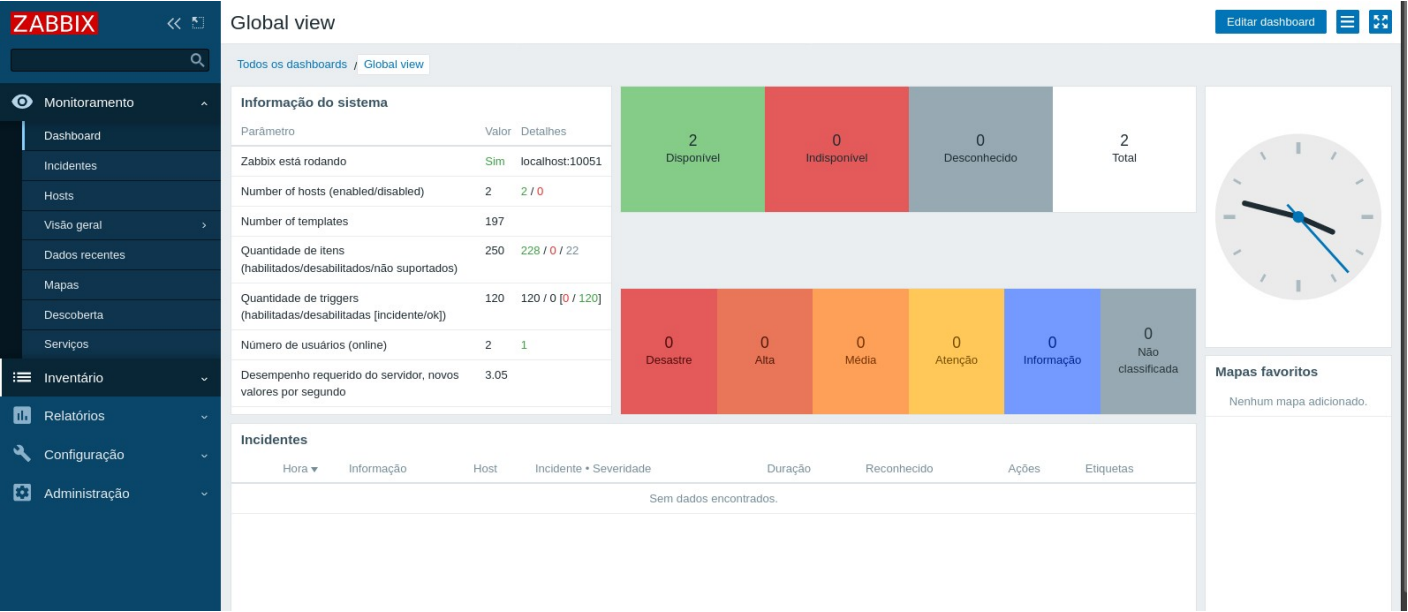


Voltando o serviço:
systemctl start vsftpd

| Hora | Severidade | Hora da recuperação | Status | Informação | Host | Incidente | Duração | Reconhecido | Ações | Etiquetas |
|----------|------------|---------------------|-----------|------------|-------------------|--|---------|-------------|-------|--------------------------|
| 15:21:31 | Média | 15:45:31 | RESOLVIDO | | Feirinha Organica | FTP service is down on Feirinha Organica | 24m | Não | | Application: FTP service |

Exibindo 1 de 1 encontrados

No dashboard:



3 CONCLUSÃO

Com esta atividade pudemos ter a experiência de monitorar um servidor web com um aplicativo fácil de instalar e manipular. Vale ressaltar 2 pontos: primeiramente a importância do monitoramento em tempo real dos serviços; Segundo a satisfação de poder ter feito o processo desde o início até a verificação do funcionamento desse aplicativo. :)

REFERÊNCIAS

Material de estudos do curso de Segurança Cibernética da FIAP – Fase 4 cap 1 ao cap 6;