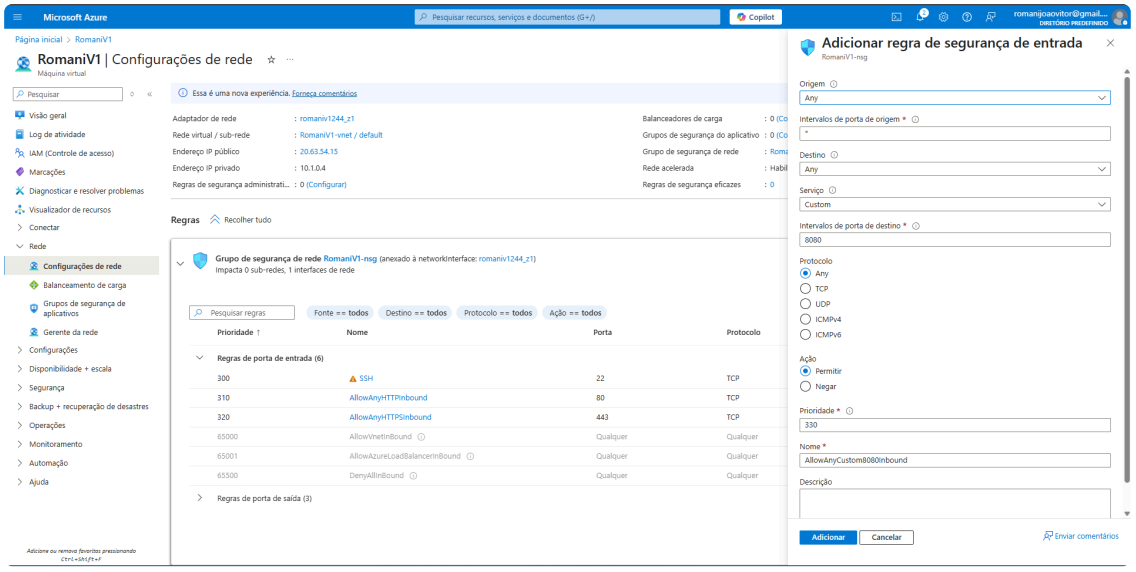
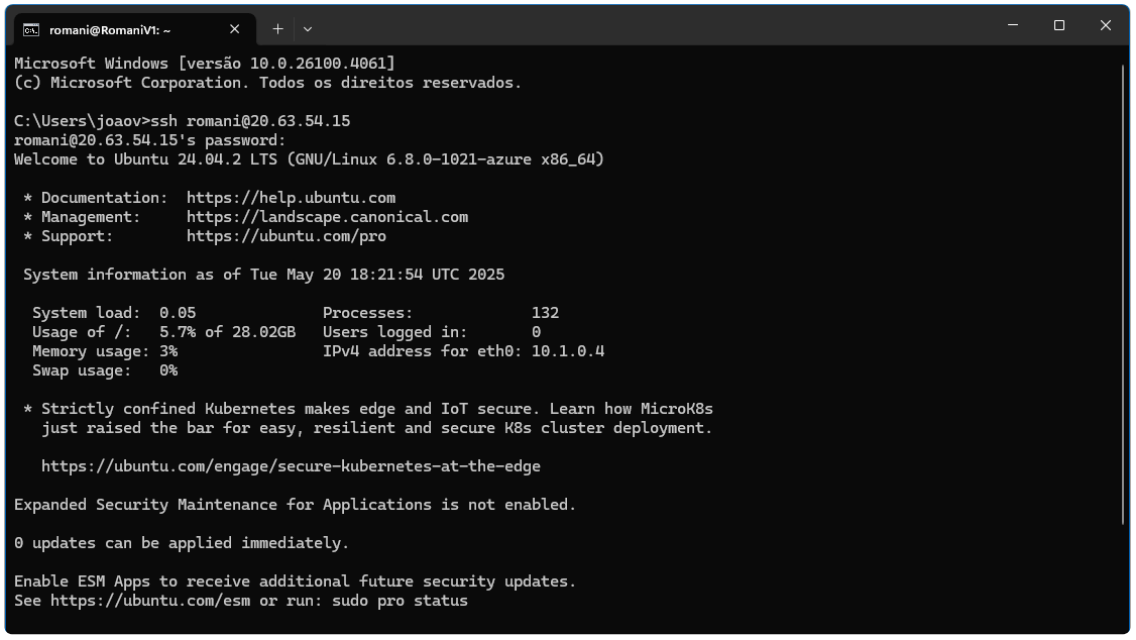
AC-REDES-001 - LAMP

Configuração do Apache para HTTP:

1. O primeiro passo foi **verificar e abrir portas para o HTTP e HTTPS no Network Security Group (NSG) da Azure**:

   1. 

2. Conectar-se a VM:

   1. 

3. Abrindo as portas e ativando o Firewall do Ubuntu - UFW (Uncomplicated Firewall)

1.
```
romani@RomaniV1: ~
romani@RomaniV1:~$ sudo ufw allow ssh
Skipping adding existing rule
Skipping adding existing rule (v6)
romani@RomaniV1:~$ sudo ufw allow http
Skipping adding existing rule
Skipping adding existing rule (v6)
romani@RomaniV1:~$ sudo ufw allow https
Skipping adding existing rule
Skipping adding existing rule (v6)
romani@RomaniV1:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
romani@RomaniV1:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
443                        ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
443 (v6)                   ALLOW IN    Anywhere (v6)

romani@RomaniV1:~$
```

4. Atualização de pacotes da máquina e **Instalação do Apache**

1.
```
romani@RomaniV1:~$ sudo apt update
Hit:1 http://azure.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://azure.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://azure.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:6 http://azure.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
```

2.
```
romani@RomaniV1:~$ sudo apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 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 libapr1t64
  libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 117 not upgraded.
Need to get 2084 kB of archives.
After this operation, 8094 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://azure.archive.ubuntu.com/ubuntu noble-updates/main amd64 libapr1t64 amd64 1.7.2-3.1ubuntu0.1 [108 kB]
Get:2 http://azure.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu7 [91.9 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1.1ubuntu7 [11.2 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-ldap amd64 1.6.3-1.1ubuntu7 [9116 B]
```

5. Ajustando o Firewall para permitir Tráfego Web

1.
```
romani@RomaniV1:~$ sudo ufw app list
Available applications:
  Apache
  Apache Full
  Apache Secure
  OpenSSH
romani@RomaniV1:~$ sudo ufw app info "Apache Full"
Profile: Apache Full
Title: Web Server (HTTP,HTTPS)
Description: Apache v2 is the next generation of the omnipresent Apache web
server.

Ports:
  80,443/tcp
romani@RomaniV1:~$ sudo ufw allow in "Apache Full"
Rule added
Rule added (v6)
romani@RomaniV1:~$
```

6. **Instalação do MySQL** com execução de script de segurança

1.
```
romani@RomaniV1:~$ sudo apt install mysql-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
```

2.
```
romani@RomaniV1: ~

romani@RomaniV1:~$ sudo mysql_secure_installation

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.

VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: no

Skipping password set for root as authentication with auth_socket is used by default.
If you would like to use password authentication instead, this can be done with the "ALTER_USER" command.
See https://dev.mysql.com/doc/refman/8.0/en/alter-user.html#alter-user-password-management for more information.

By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : no

 ... skipping.
```

3.
```
Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : y
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.


Remove test database and access to it? (Press y|Y for Yes, any other key for No) : y
 - Dropping test database...
Success.

 - Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
Success.

All done!
romani@RomaniV1:~$
```

7. **Instalação do PHP** com pacotes auxiliares

1.
```
romani@RomaniV1:~$ sudo apt install php libapache2-mod-php php-mysql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-php8.3 php-common php8.3 php8.3-cli php8.3-common php8.3-mysql
  php8.3-opcache php8.3-readline
Suggested packages:
  php-pear
The following NEW packages will be installed:
  libapache2-mod-php libapache2-mod-php8.3 php php-common php-mysql php8.3
```

8. Fazendo Apache olhar pimeiro para o index.php

1.
```
romani@RomaniV1:~$ sudo nano /etc/apache2/mods-enabled/dir.conf
```

2.
```
romani@RomaniV1: ~
  GNU nano 7.2                    /etc/apache2/mods-enabled/dir.conf
DirectoryIndex index.php index.html index.cgi index.pl index.xhtml index.htm

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

3.
```
romani@RomaniV1:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: ena>
     Active: active (running) since Tue 2025-05-20 19:53:03 UTC; 7min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 11753 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCC>
   Main PID: 11758 (apache2)
      Tasks: 6 (limit: 9457)
     Memory: 12.7M (peak: 12.9M)
        CPU: 62ms
     CGroup: /system.slice/apache2.service
             ├─11758 /usr/sbin/apache2 -k start
             ├─11761 /usr/sbin/apache2 -k start
             ├─11762 /usr/sbin/apache2 -k start
             ├─11763 /usr/sbin/apache2 -k start
             ├─11764 /usr/sbin/apache2 -k start
             └─11765 /usr/sbin/apache2 -k start

May 20 19:53:03 RomaniV1 systemd[1]: Starting apache2.service - The Apache HTTP Se>
May 20 19:53:03 RomaniV1 systemd[1]: Started apache2.service - The Apache HTTP Ser>
lines 1-19/19 (END)
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Tue 2025-05-20 19:53:03 UTC; 7min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 11753 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
```

9. Testando funcionamento do PHP

1.
```
romani@RomaniV1:~$ sudo nano /var/www/html/info.php
```

2.
```
romani@RomaniV1: ~
  GNU nano 7.2                    /var/www/html/info.php
<?php
phpinfo();
?>

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

3.
```
romani@RomaniV1:~$ sudo rm /var/www/html/info.php
```
[1]

Configuração do Apache para HTTPS:

1. **Criando o certificado SSL**

1.
```
romani@RomaniV1:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.k
ey -out /etc/ssl/certs/apache-selfsigned.crt
...+..+.........+.....+.....................+.......+.....+...+....+......+..+.+..+...+.+.....+.................+.....
.+.+...+..+.+........+......+...+........+..+...+.+..+........+........+.......+.......+.........+............+...
```

   1.
      - **openssl**: esta é a ferramenta básica de linha de comando para criação e gerenciamento de certificados OpenSSL, chaves e outros arquivos.
      - **req**: este subcomando especifica que queremos usar o gerenciamento X.509 de solicitação de assinatura de certificado

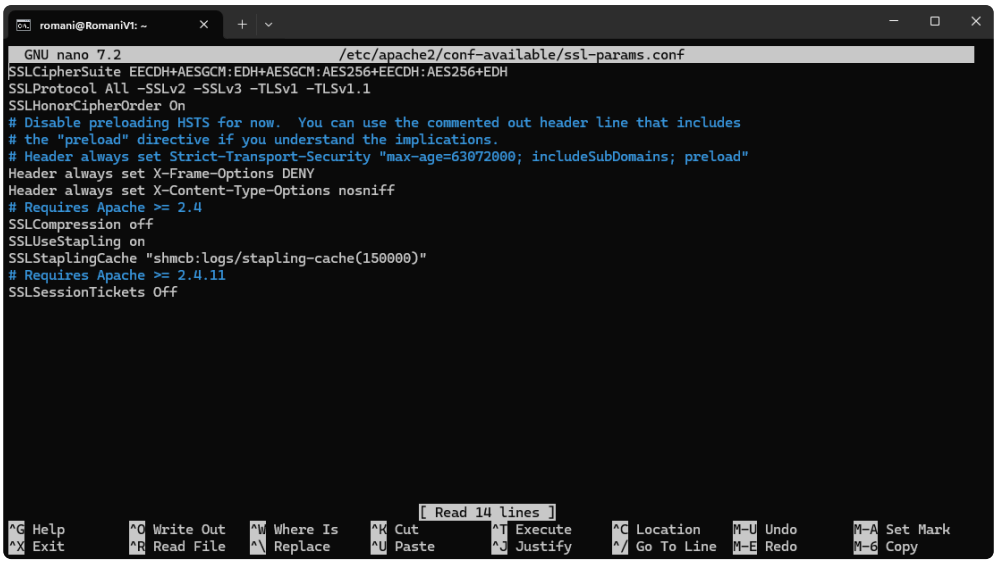
(CSR). O “X.509” é um padrão de infraestrutura de chave pública aderido pelo SSL e o TLS para seu gerenciamento de chaves e certificados. Queremos criar um novo cert X.509, então estamos usando este subcomando.

- **x509**: isso modifica ainda mais o subcomando anterior dizendo ao utilitário que queremos criar um certificado autoassinado em vez de gerar uma solicitação de assinatura de certificado, como normalmente aconteceria.
- **nodes**: isso diz ao OpenSSL para pular a opção de proteger nosso certificado com uma frase secreta. Precisamos que o Apache consiga ler o arquivo, sem a intervenção do usuário, quando o servidor for iniciado. Uma frase secreta impediria que isso acontecesse porque teríamos que digitá-la após cada reinício.
- **days 365**: esta opção define a duração do tempo em que o certificado será considerado válido. Aqui, nós configuramos ela para um ano.
- **newkey rsa:2048**: isso especifica que queremos gerar um novo certificado e uma nova chave ao mesmo tempo. Não criamos a chave necessária para assinar o certificado em um passo anterior, então precisamos criá-la junto com o certificado. A porção `rsa:2048` diz a ele para criar uma chave RSA que seja de 2048 bits.
- **keyout**: esta linha diz ao OpenSSL onde colocar o arquivo gerado de chave privada que estamos criando.
- **out:** isso diz ao OpenSSL onde colocar o certificado que estamos criando.

2.
```
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:Paraná
Locality Name (eg, city) []: Cornélio Procópio
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTFPR
Organizational Unit Name (eg, section) []:UTFPR
Common Name (e.g. server FQDN or YOUR name) []: 20.63.54.15
Email Address []: romani@alunos.utfpr.edu.br
romani@RomaniV1:~$
```

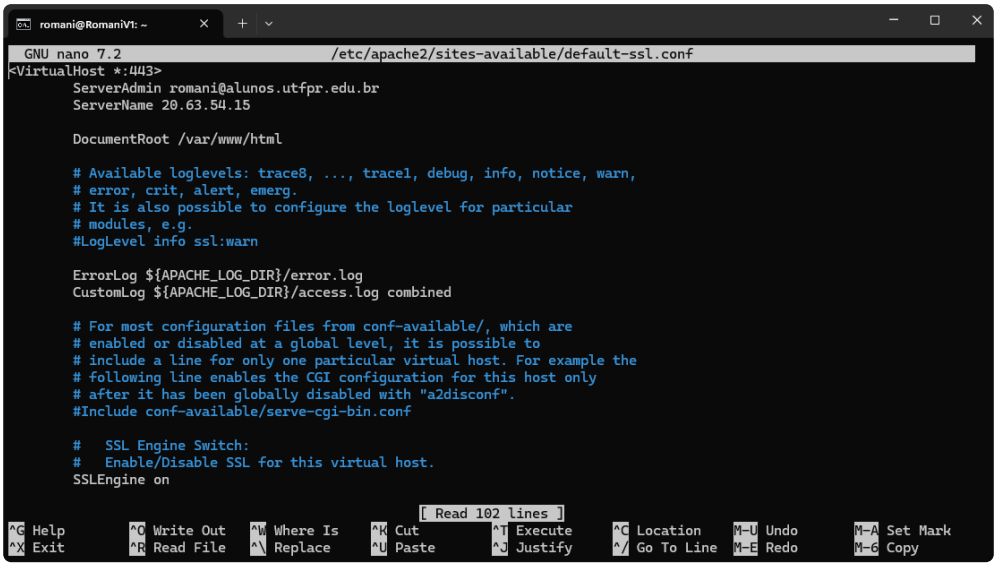
2. **Configurando o Apache para usar o SSL**
   1. Criando um snippet de configuração do Apache com configurações de criptografia robustas

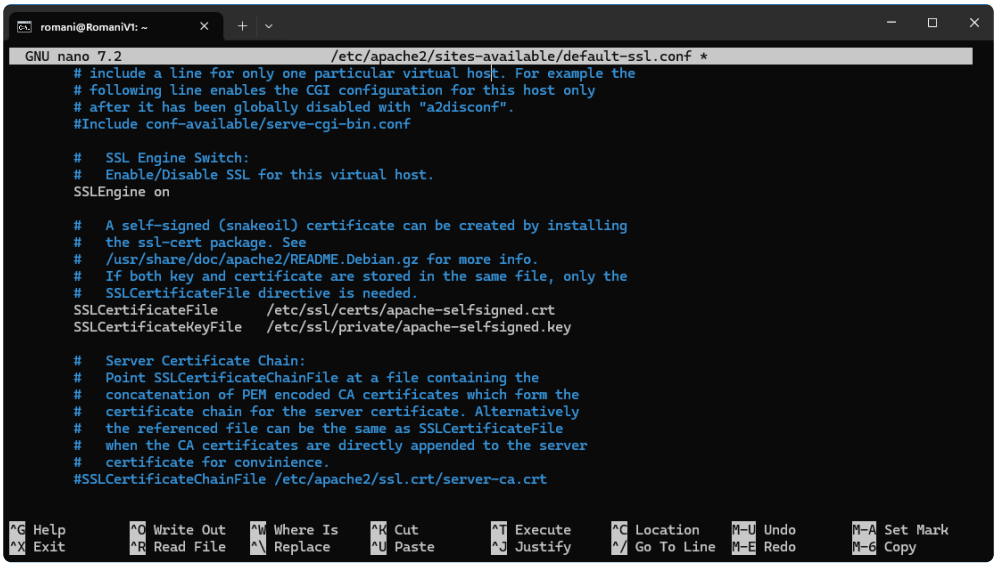
```
romani@RomaniV1:~$ sudo nano /etc/apache2/conf-available/ssl-params.conf
```

1. 

2. Modificando o arquivo padrão de Host Virtual SSL do Apache

```
romani@RomaniV1:~$ sudo nano /etc/apache2/sites-available/default-ssl.conf
```

1. 

2. 

3. Modificando o arquivo de host HTTP para redirecionar para HTTPS

```
romani@RomaniV1:~$ sudo nano /etc/apache2/sites-available/000-default.conf
```

1.
```
romani@RomaniV1: ~
  GNU nano 7.2                    /etc/apache2/sites-available/000-default.conf *
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin romani@alunos.utfpr.edu.br
        DocumentRoot /var/www/html
        Redirect "/" "https://20.63.54.15/"

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
File Name to Write: /etc/apache2/sites-available/000-default.conf
^G Help          M-D DOS Format     M-A Append         M-B Backup File
^C Cancel        M-M Mac Format     M-P Prepend        ^T Browse
```

4. Habilitando as alterações no Apache

```
romani@RomaniV1:~$ sudo a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
romani@RomaniV1:~$ sudo a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
  systemctl restart apache2
romani@RomaniV1:~$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
romani@RomaniV1:~$ sudo a2enconf ssl-params
Enabling conf ssl-params.
To activate the new configuration, you need to run:
  systemctl reload apache2
romani@RomaniV1:~$ sudo apache2ctl configtest
AH00526: Syntax error on line 33 of /etc/apache2/sites-enabled/default-ssl.conf:
SSLCertificateKeyFile: file '/etc/ssl/private/apache-selsigned.key' does not exist or is empty
romani@RomaniV1:~$ sudo nano /etc/apache2/sites-available/default-ssl.conf
romani@RomaniV1:~$ sudo apache2ctl configtest
Syntax OK
romani@RomaniV1:~$ sudo systemctl restart apache2
```

5. Mudando para um redirecionamento permanente

```
romani@RomaniV1:~$ sudo nano /etc/apache2/sites-available/000-default.conf
```

1.
```
romani@RomaniV1: ~
  GNU nano 7.2                    /etc/apache2/sites-available/000-default.conf *
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin romani@alunos.utfpr.edu.br
        DocumentRoot /var/www/html
        Redirect permanent "/" "https://20.63.54.15/"

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
Save modified buffer?
 Y Yes
 N No           ^C Cancel
```

2.
```
romani@RomaniV1:~$ sudo nano /etc/apache2/sites-available/000-default.conf
romani@RomaniV1:~$ sudo apache2ctl configtest
Syntax OK
romani@RomaniV1:~$ sudo systemctl restart apache2
```

Colocando conteúdo no site

```
Windows PowerShell

O Windows PowerShell
Copyright (C) Microsoft Corporation. Todos os direitos reservados.

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

PS C:\Users\joaov> scp C:\Users\joaov\OneDrive\Documentos\UTFPR\3semestre\RedesComputadores\materiais\startbootstrap-age
ncy-gh-pages.zip romani@20.63.54.15:/tmp/
```

```
romani@RomaniV1:~$ cd /tmp
romani@RomaniV1:/tmp$ sudo apt install unzip
```

```
romani@RomaniV1:/tmp$ unzip startbootstrap-agency-gh-pages.zip
Archive:  startbootstrap-agency-gh-pages.zip
db0826e69d91cc131b90fb08deb5151954b700fc
```

```
romani@RomaniV1:/tmp$ sudo mv /tmp/startbootstrap-agency-gh-pages/* /var/www/html/
```

---

1. comando para apagar a página de teste que exibe as informações do servidor ↩