O que é o SSL?

O SSL é um protocolo criptográfico baseado em cifras assimétricas (chave privada + chave pública), que tem como principal objetivo fornecer a segurança e integridade dos dados transmitidos em redes inseguras, como é o caso da Internet.

Quando um utilizador acede a um site que recorre ao SSL, o servidor envia ao cliente a chave pública deste para que esta possa cifrar a informação que vai ser passada ao servidor. Quando o servidor recebe essa informação, usa a sua chave privada para decifrar a informação transmitida pelo cliente.

Instalar Apache 2

Antes de começar o processo, é fundamental verificar se o sistema operativo está atualizado. Assim sendo vamos executar os comandos:

- Atualizar os repositórios: **apt update**
- Atualizar o sistema operativo: **apt upgrade**

Após isso, vamos seguir os seguintes passos:

Passo 1 – Instalar o servidor apache2 com o comando: **apt install apache2**

Passo 2 – Ativar o serviço e pedir para arrancar sempre com o sistema operativo com os comandos:

systemctl start apache2

systemctl enable apache2

Abrir as portas na firewall http e https

Para abrir as portas na firewall, vamos recorrer à aplicação do ufw (que já vem integrada no sistema operativo) e adicionar as seguintes exceções:

- **Permitir porta 80** → ufw allow 80/tcp
- **Permitir porta 443** → ufw allow 443/tcp

Ou então, opcionalmente, podemos colocar acesso total e de forma mais rápida, com o comando:

ufw allow Apache Full

Habilitar o módulo ssl

Antes de usar qualquer certificado de SSL, é necessário, aticar o **mod_ssl** (que é um módulo do Apache compatível com criptografia SSL).

Habilite o mod_ssl com o comando **a2enmod** com o seguinte comando:

a2enmod ssl

De seguida, reinicie o serviço do apache e 2 verifique se está ativo e sem erros:

- Reiniciar o serviço: **systemctl restart apache2**
- Ver estado do serviço: **systemctl status apache2**

Criar certificados SSL

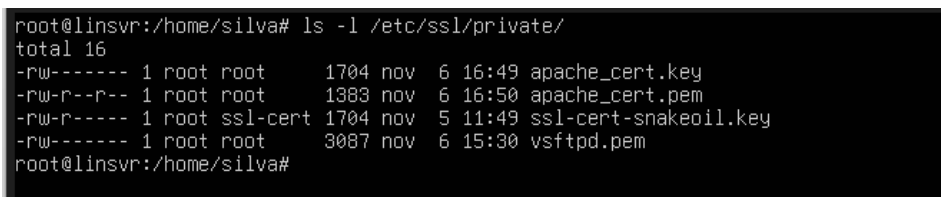
Passo 1 – Vamos gerar o certificado de segurança com a biblioteca openssl. Assim sendo, vamos utilizar o seguinte comando:

openssl req -x509 -nodes -newkey rsa:2048 **-keyout** /etc/ssl/private/nome_chave.key **-out** /etc/ssl/private/nome_certificado.pem -days 365

A seguir vão ser pedidas as seguintes informações de um certificado:



Passo 2 – Confirmar se a chave e o certificado foram bem gerados:



Ficheiro de configurações Apache2

Passo 1 – Quando o apache2 é instalado, os ficheiros de configuração ficam situados no diretório **/etc/apache2**. Se aceder à pasta com o comando cd /etc/apache2 depois pode fazer a listagem da pasta com o comando ls -l para ver o seu conteúdo:

```
root@linsvr:/etc/apache2/sites-available# cd /etc/apache2/
root@linsvr:/etc/apache2# ls -l
total 80
-rw-r--r-- 1 root root  7178 out  8 19:58 apache2.conf
drwxr-xr-x 2 root root  4096 nov  5 11:49 conf-available
drwxr-xr-x 2 root root  4096 nov  5 11:49 conf-enabled
-rw-r--r-- 1 root root  1782 mar 18  2024 envvars
-rw-r--r-- 1 root root 31063 mar 18  2024 magic
drwxr-xr-x 2 root root 12288 nov  5 11:49 mods-available
drwxr-xr-x 2 root root  4096 nov  6 16:44 mods-enabled
-rw-r--r-- 1 root root   274 mar 18  2024 ports.conf
drwxr-xr-x 2 root root  4096 nov  6 17:33 sites-available
drwxr-xr-x 2 root root  4096 nov  6 17:31 sites-enabled
root@linsvr:/etc/apache2#
```

Os projetos dos websites ficam noutro diretorio, mais especificamente, no diretorio **/var/www/html/**:

```
root@linsvr:/etc/apache2# ls -l /var/www/html
total 16
-rw-r--r-- 1 root root 10671 nov  5 11:49 index.html
drwxr-xr-x 3 root root  4096 nov  5 12:00 website
```

Passo 2 – Para proteger o servidor apache2 com o certificado de segurança, vamos fazer os seguintes passos:

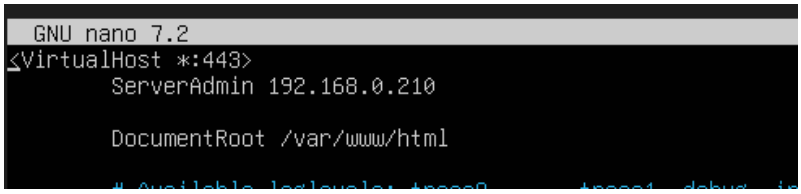
- Garantir que está na pasta das configurações do apache2: **cd /etc/apache2**
- Editar o ficheiro de configuração do apache2 no diretório sites-available. Se já estiver dentro do diretório do apache2 vamos colocar o comando:
  cd sites- available
- Listar o conteúdo da pasta e verificar se tem os ficheiros como na imagem mais abaixo:

```
root@linsvr:/etc/apache2# cd sites-available/
root@linsvr:/etc/apache2/sites-available# ls -l
total 12
-rw-r--r-- 1 root root 1286 mar 18  2024 000-default.conf
-rw-r--r-- 1 root root 4557 nov  6 17:33 default-ssl.conf
root@linsvr:/etc/apache2/sites-available#
```

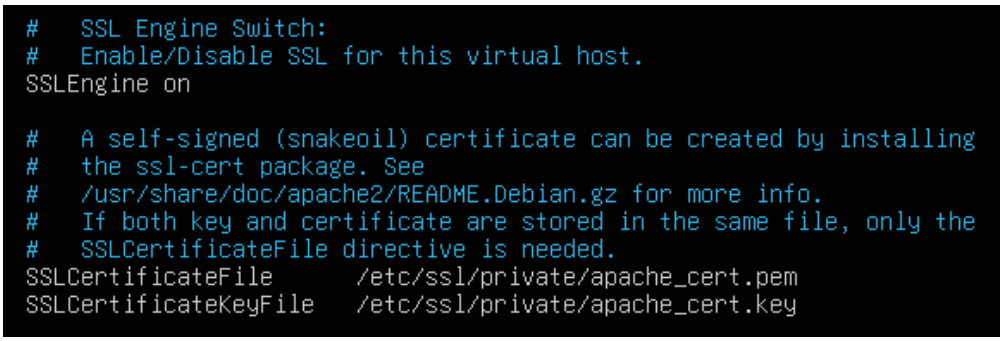
- Editar o ficheiro das configurações com o comando: **nano default-ssl.conf**

Passo 3 – Vamos editar o ficheiro das configurações e fazer os seguintes passos:

- **Abrir o ficheiro das configurações:** nano default-ssl.conf;
- No início do ficheiro, vamos ter duas partes para mudar:
    - **ServerAdmin** → substituir a informação pelo endereço ip do servidor;
    - **DocumentRoot** → indicar que os projetos/websites estão no diretório **/var/www/html** (que já vai dar para os subdomínios a partir desta pasta)



- Mais abaixo, vamos ter de alterar os seguintes dados:
    - Verificar se o motor **SSLEngine** está ativo, ou seja, linha descomentada e com a instrução **on**;
    - Mais abaixo, mudar as localizações da chave privada e certificado para os novos dados gerados aquando criou o certificado:
        - **SSLCertificateFile** → colocar a localização do ficheiro do certificado (pem), que quando gerou o certificado anteriormente e colocou no diretório /etc/ssl/private/apache_cert.pem
        - **SSLCertificateFile** → colocar a localização do ficheiro do certificado (key), que quando gerou o certificado anteriormente e colocou no diretório /etc/ssl/private/apache_cert.key



Muito importante: Grave o ficheiro de configurações (CTRL+S e para sair CTRL+X).

Passo 4 – Em seguida e ainda na pasta das configurações, precisamos habilitar o arquivo de configuração com a ferramenta a2ensite, com o comando:

a2ensite default-ssl.conf

Passo 5 – Fazer o teste à procura de erros de configuração, com o comando:

apache2ctl configtest

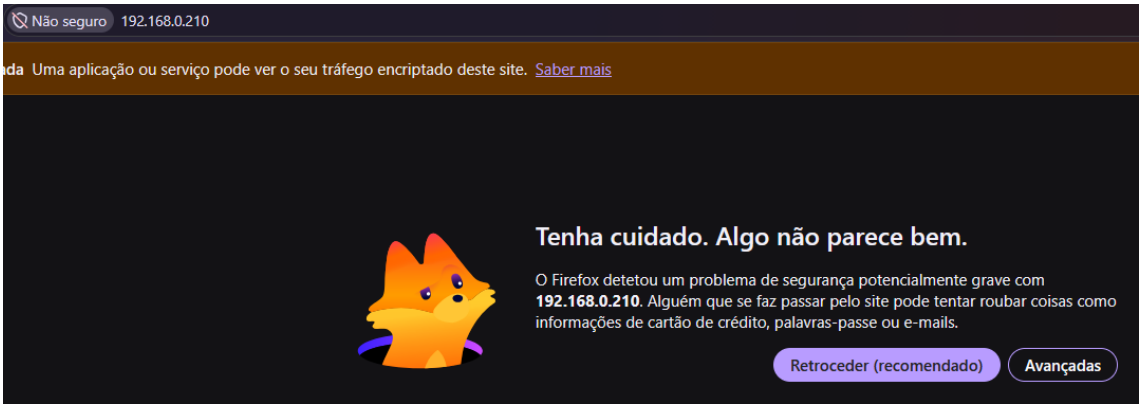
Se aparecer o final a mensagem Syntax OK, significa que está tudo em condições.

Passo 6 – De seguida, reinicie o serviço do apache e 2 verifique se está ativo e sem erros:

- Reiniciar o serviço: **systemctl restart apache2**
- Ver estado do serviço: **systemctl status apache2**

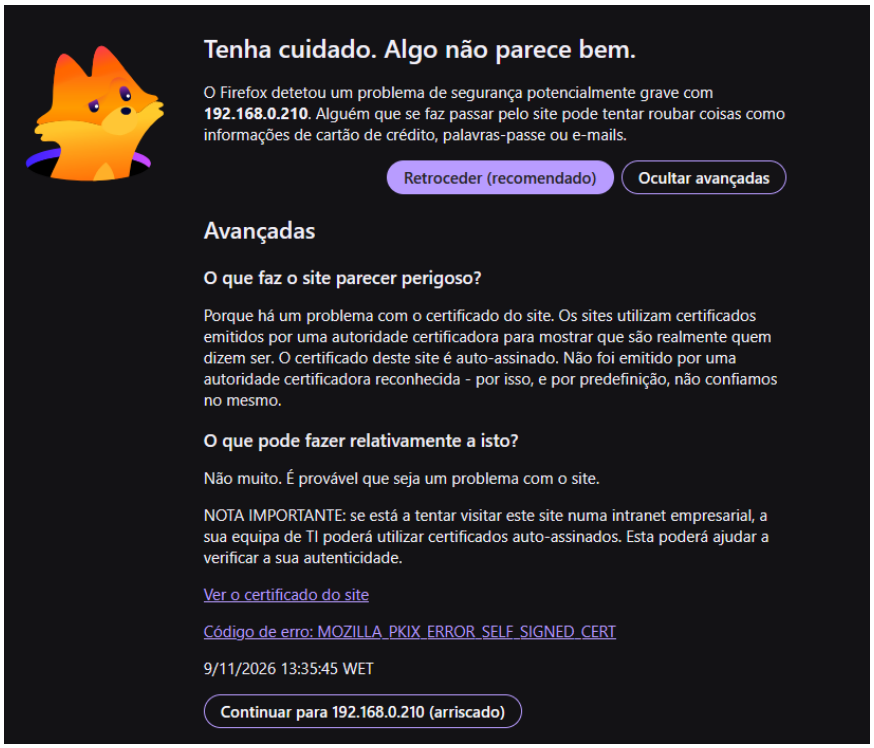
Passo 6 – Fora da máquina virtual, vamos aceder à página do servidor principal (uma vez que ainda não criamos nenhuma pasta para nenhum website.

Como tal, abra um navegador web e digite o ip da máquina do ubuntu server e veja se aparece a seguinte página:

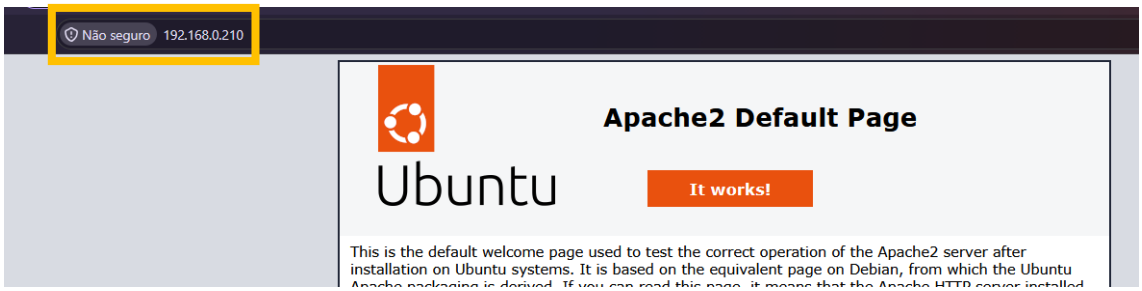


Este erro é normal, pois, como se trata de um certificado auto-assinado irá aparecer um erro! É um alerta do navegador a informar que não pode verificar a identidade do servidor, pois o certificado não é assinado por nenhuma autoridade certificadora conhecida.

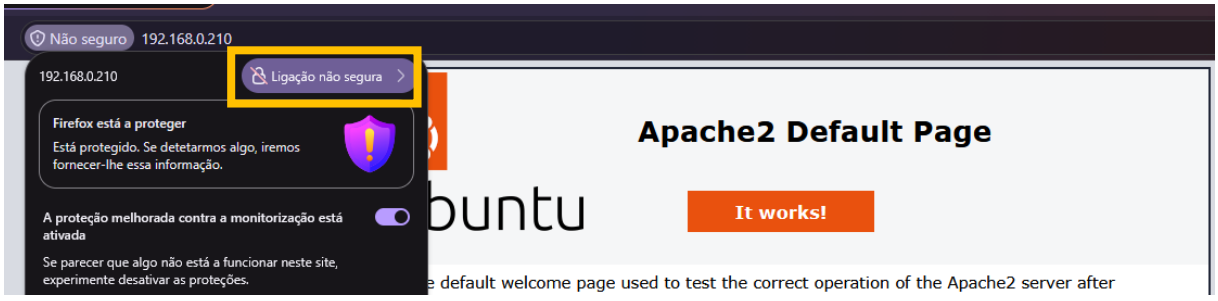
Para continuar, basta clicar no botão Avançado e pedir para continuar:



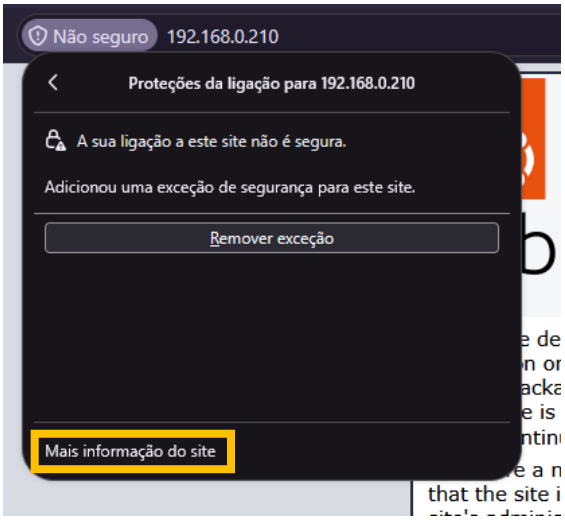
Depois disso, deve entrar na página principal do servidor apache 2:

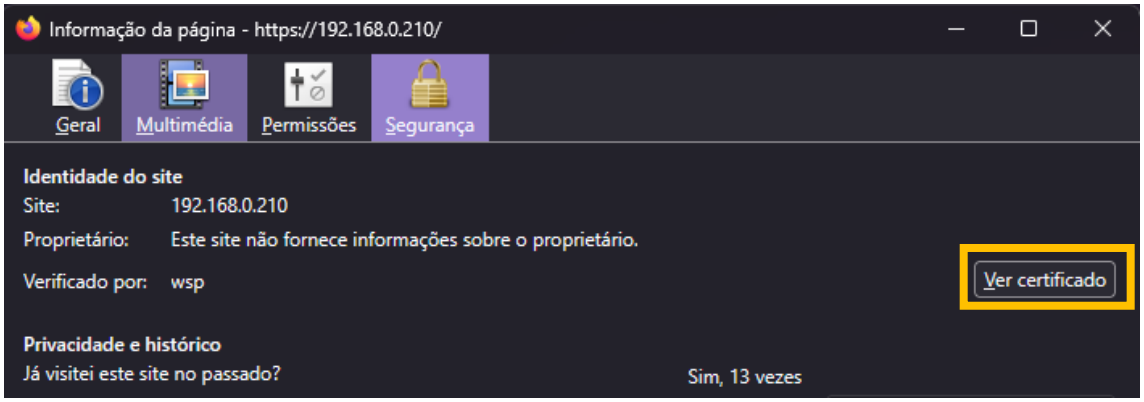


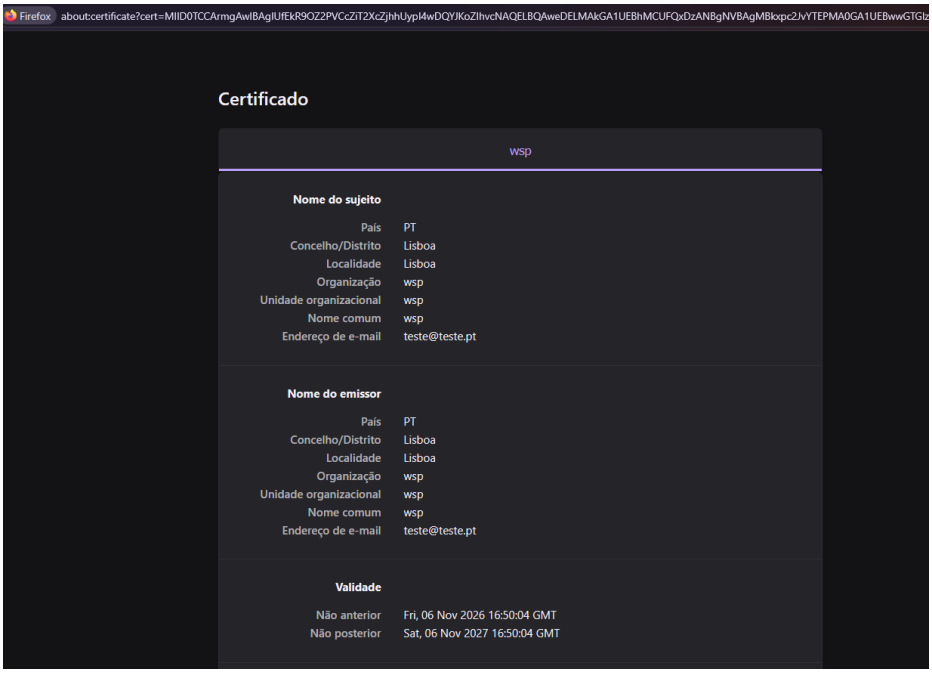
Se reparar com mais pormenor, ao lado do endereço IP que colou no caminho de endereços, temos a mensagem “Não seguro” (mensagem pode variar de navegador para navegador).



Clique na opção Ligação não segura para ver os dados com mais cuidado:


Não seguro
192.168.0.210
Proteções da ligação para 192.168.0.210
A sua ligação a este site não é segura.
Adicionou uma exceção de segurança para este site.
Remover exceção
Mais informação do site


Informação da página - https://192.168.0.210/
Geral
Multimédia
Permissões
Segurança
Identidade do site
Site: 192.168.0.210
Proprietário: Este site não fornece informações sobre o proprietário.
Verificado por: wsp
Ver certificado
Privacidade e histórico
Já visitei este site no passado?
Sim, 13 vezes

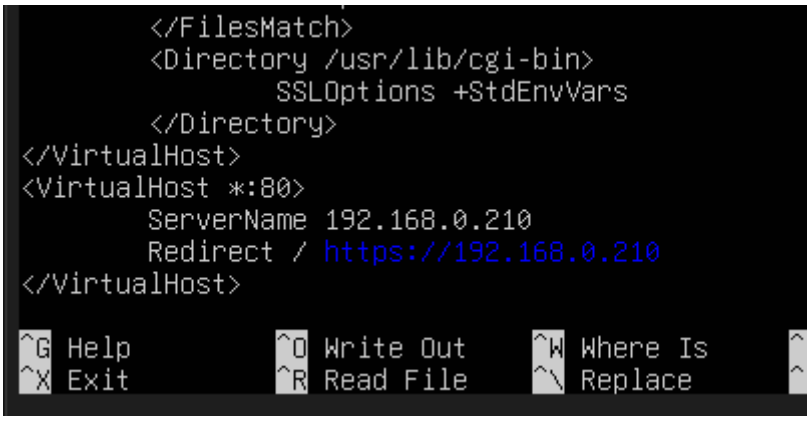

Firefox
about:certificate?cert=MIID0TCCArmgAwIBAgIUfEkR9OZ2PVCcZiT2XcZjhhUypI4wDQYJKoZIhvcNAQELBQAweDELMAkGA1UEBhMCUFQxDzANBgNVBAgMBlxpc2JvYTEPMA0GA1UEBwwGTGlz
Certificado
wsp
Nome do sujeito
País PT
Concelho/Distrito Lisboa
Localidade Lisboa
Organização wsp
Unidade organizacional wsp
Nome comum wsp
Endereço de e-mail teste@teste.pt
Nome do emissor
País PT
Concelho/Distrito Lisboa
Localidade Lisboa
Organização wsp
Unidade organizacional wsp
Nome comum wsp
Endereço de e-mail teste@teste.pt
Validade
Não anterior Fri, 06 Nov 2026 16:50:04 GMT
Não posterior Sat, 06 Nov 2027 16:50:04 GMT

Redirecionar páginas de http e https

Atualmente, nossa configuração irá responder apenas às requisições HTTPS na porta 443. É uma boa prática também responder na porta 80. Vamos configurar o nosso serviço para responder às requisições não criptografadas (porta 80) e redirecioná-las para HTTPS (porta 443).

Passo 1 – Abra o mesmo arquivo de configuração do Apache e vamos fazer os seguintes passos:

- **Abrir o ficheiro das configurações:** nano default-ssl.conf;
- No final do ficheiro que abriu, vamos ao final do mesmo e adicionar o seguinte bloco de informações (basicamente é verificar todos os pedidos que vierem para a porta 80 do servidor, reencaminhar para o https):



- **Muito importante:** No final grave o ficheiro de configurações (CTRL+S e para sair CTRL+X).

Passo 2 – Fazer o teste à procura de erros de configuração, com o comando:

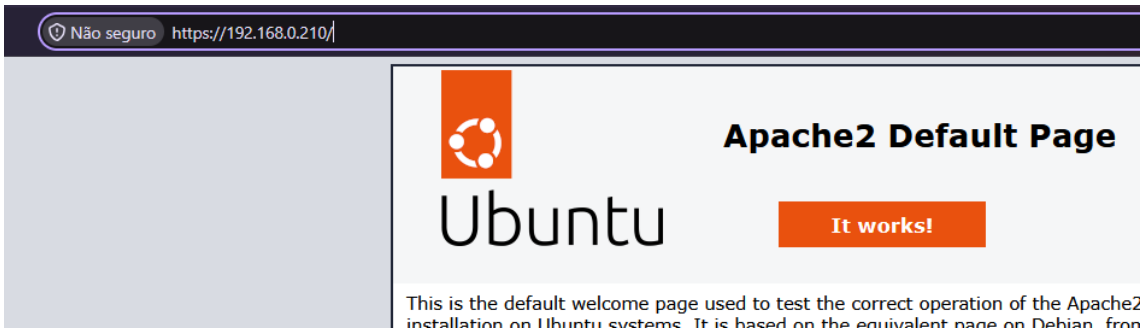
apache2ctl configtest

Se aparecer o final a mensagem Syntax OK, significa que está tudo em condições.

Passo 3 – De seguida, reinicie o serviço do apache e 2 verifique se está ativo e sem erros:

- Reiniciar o serviço: **systemctl restart apache2**
- Ver estado do serviço: **systemctl status apache2**

Passo 4 – Testar abrir novamente a página na máquina física (fora da virtual) e verificar se no caminho o pedido está a ser redirecionado para o https:


Não seguro
https://192.168.0.210/
Ubuntu
Apache2 Default Page
It works!
This is the default welcome page used to test the correct operation of the Apache2