



# HTTP para HTTPS

Servidor Apache em localhost



# Implementação Inicial

Para nossa implementação, utilizaremos as ferramentas e ambiente em que temos trabalhado até o momento. Existem outras formas de realizar o processo, aquisição e implementação de certificado, etc. O processo que faremos hoje trará uma ideia básica do procedimento geral que será feito em outros ambientes. Utilizaremos:

- Ubuntu (KDE) 18.04
- Web Server Apache (apt install apache2)
- VirtualBox para virtualização do servidor (K)Ubuntu
- Putty para acesso ao servidor (opcional).



# Criação de Chave e Certificado

Utilizando o openssl, criaremos a nossa chave. Ao inserir o comando de criação da chave, será apresentada uma tela pedindo uma senha para a mesma, assim como a inserção dos dados do usuário que constarão em seu certificado.



aecio : sudo — Konsole




Arquivo Editar Exibir Favoritos Configurações Ajuda

```
aecio@aecio-VB:~$ sudo openssl req -x509 -days 365 -newkey rsa:2048 -keyout /home/aecio/localhost.key
[sudo] senha para aecio:
Can't load /home/aecio/.rnd into RNG
140284967600576:error:2406F079:random number generator:RAND_load_file:Cannot open file:./crypto/rand/randfile.c:88:Filename=/home/aecio/.rnd
Generating a RSA private key
.....
+++++
...+++++
writing new private key to '/home/aecio/localhost.key'
Enter PEM pass phrase:
```



aecio : sudo



```
aecio : bash — Konsole
Arquivo  Editar  Exibir  Favoritos  Configurações  Ajuda

aecio@aecio-VB:~$ sudo openssl req -x509 -days 365 -newkey rsa:2048 -keyout /home/aecio/l
ocalhost.key -out /home/aecio/localhost.crt
Can't load /home/aecio/.rnd into RNG
139685971853760:error:2406F079:random number generator:RAND_load_file:Cannot open file:..
/crypto/rand/randfile.c:88:Filename=/home/aecio/.rnd
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/home/aecio/localhost.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:BAHIA
Locality Name (eg, city) []:JACOBINA
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IFBA
Organizational Unit Name (eg, section) []:REDES2
Common Name (e.g. server FQDN or YOUR name) []:localhost
Email Address []:local@localhost.com
aecio@aecio-VB:~$
aecio@aecio-VB:~$
```

aecio : bash



# Configuração do WebServer

Em nosso próximo passo, criaremos um host virtual em nosso web server. Para isso, basta utilizar um editor de texto e inserir o arquivo de configuração conforme as normas do seu webserver no diretório reservado a essa configuração. No apache, o diretório é o `/etc/apache2/sites-available/`. Nesse diretório, insira um arquivo com o nome `https.conf` e as informações a seguir:

Raiz > etc > apache2 > sites-available



000-default.conf



default-ssl.conf



https.conf



aecio : sudo — Konsole

Arquivo

Editar

Exibir

Favoritos

Configurações

Ajuda

GNU nano 2.9.3

/etc/apache2/sites-available/https.conf

```
listen 443
```

```
<VirtualHost *:443>
```

```
    ServerName localhost
```

```
    DocumentRoot /var/www/html
```

```
    SSLEngine on
```

```
    SSLCertificateFile "/home/aecio/localhost.crt"
```

```
    SSLCertificateKeyFile "/home/aecio/localhost.key"
```

```
    <Directory /var/www/html>
```

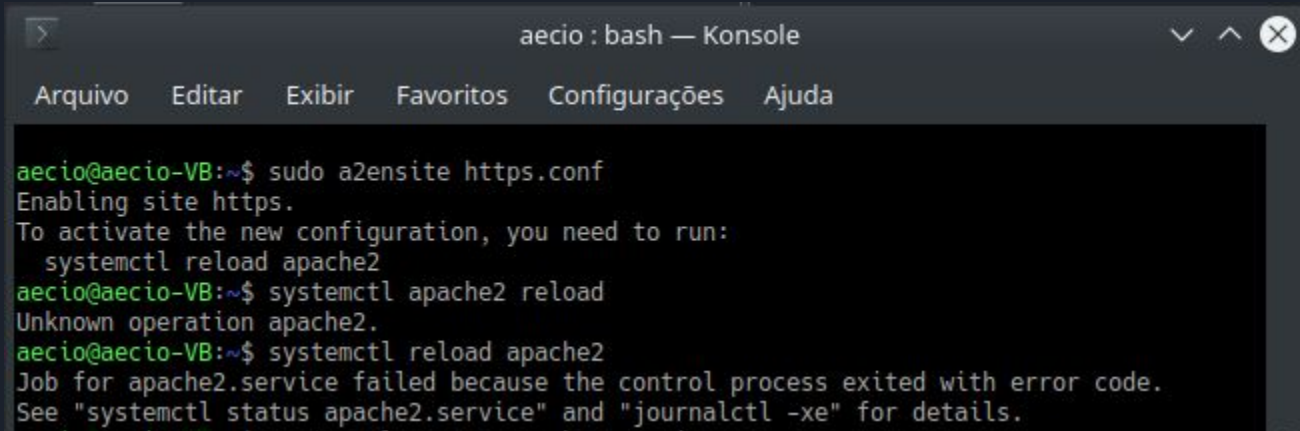
```
        AllowOverride all
```

```
    </Directory>
```

```
</VirtualHost>
```

# Ativação do SSL

Finalmente temos o nosso certificado, chave e o webserver sabendo onde encontrar nossos arquivos. Temos agora que ativar o serviço SSL em nosso servidor. No caso do apache, utilizaremos o comando **sudo a2ensite https.conf** para ativar a encriptação do diretório e em seguida reiniciar o webserver:

A terminal window titled 'aecio : bash — Konsole' with a menu bar containing 'Arquivo', 'Editar', 'Exibir', 'Favoritos', 'Configurações', and 'Ajuda'. The terminal shows the execution of 'sudo a2ensite https.conf', which outputs 'Enabling site https.' and 'To activate the new configuration, you need to run: systemctl reload apache2'. Subsequent attempts to run 'systemctl apache2 reload' and 'systemctl reload apache2' result in errors: 'Unknown operation apache2.' and 'Job for apache2.service failed because the control process exited with error code. See "systemctl status apache2.service" and "journalctl -xe" for details.'

```
aecio@aecio-VB:~$ sudo a2ensite https.conf
Enabling site https.
To activate the new configuration, you need to run:
    systemctl reload apache2
aecio@aecio-VB:~$ systemctl apache2 reload
Unknown operation apache2.
aecio@aecio-VB:~$ systemctl reload apache2
Job for apache2.service failed because the control process exited with error code.
See "systemctl status apache2.service" and "journalctl -xe" for details.
```

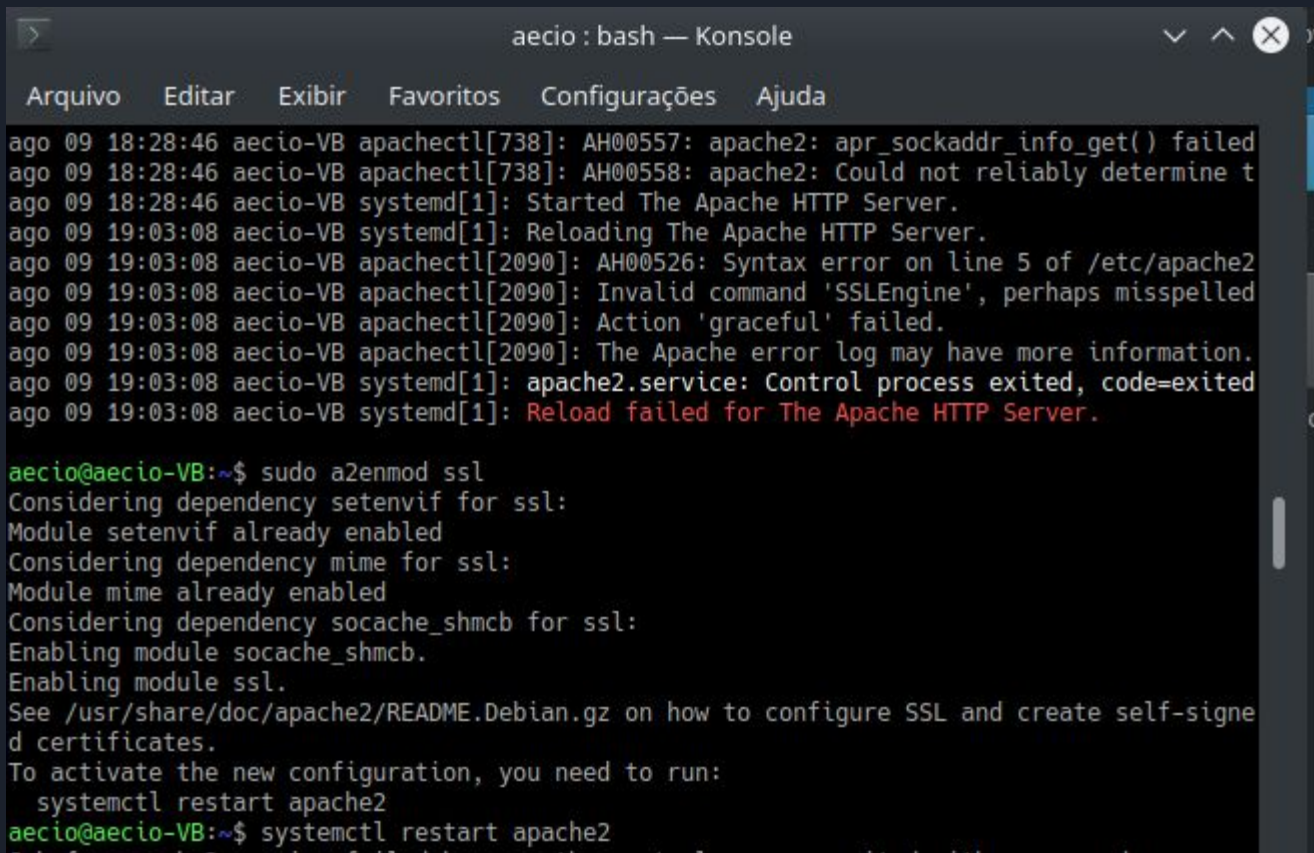




## Porém...

No meu caso, eu tomei um erro nesta operação. O apache me informou em seu log que não é possível ativar encriptação sem antes ativar o SSL (o que significa que ele não vem ativo por padrão) e me orientou no processo de ativação do serviço.

Pode ser necessário rever a configuração das porta no arquivo `/etc/apache2/ports.conf`



```
aecio : bash — Konsole
Arquivo  Editar  Exibir  Favoritos  Configurações  Ajuda

ago 09 18:28:46 aecio-VB apachectl[738]: AH00557: apache2: apr_sockaddr_info_get() failed
ago 09 18:28:46 aecio-VB apachectl[738]: AH00558: apache2: Could not reliably determine t
ago 09 18:28:46 aecio-VB systemd[1]: Started The Apache HTTP Server.
ago 09 19:03:08 aecio-VB systemd[1]: Reloading The Apache HTTP Server.
ago 09 19:03:08 aecio-VB apachectl[2090]: AH00526: Syntax error on line 5 of /etc/apache2
ago 09 19:03:08 aecio-VB apachectl[2090]: Invalid command 'SSLEngine', perhaps misspelled
ago 09 19:03:08 aecio-VB apachectl[2090]: Action 'graceful' failed.
ago 09 19:03:08 aecio-VB apachectl[2090]: The Apache error log may have more information.
ago 09 19:03:08 aecio-VB systemd[1]: apache2.service: Control process exited, code=exited
ago 09 19:03:08 aecio-VB systemd[1]: Reload failed for The Apache HTTP Server.

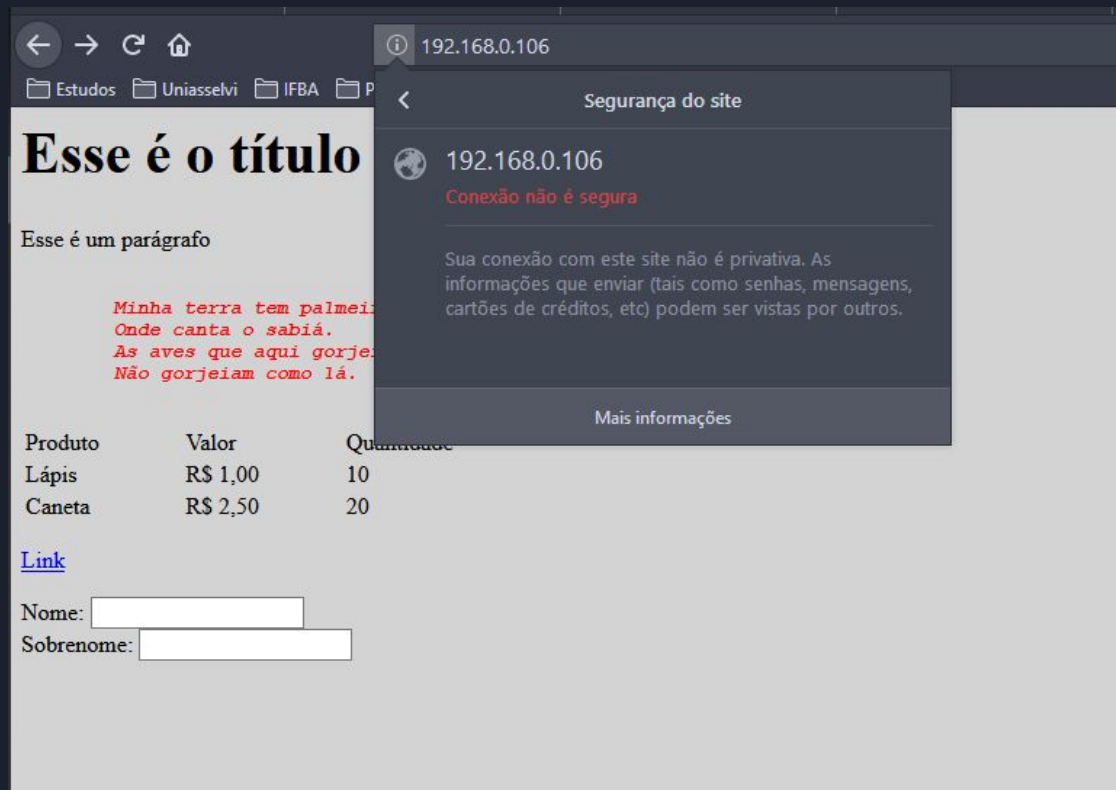
aecio@aecio-VB:~$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signe
d certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
aecio@aecio-VB:~$ systemctl restart apache2
```



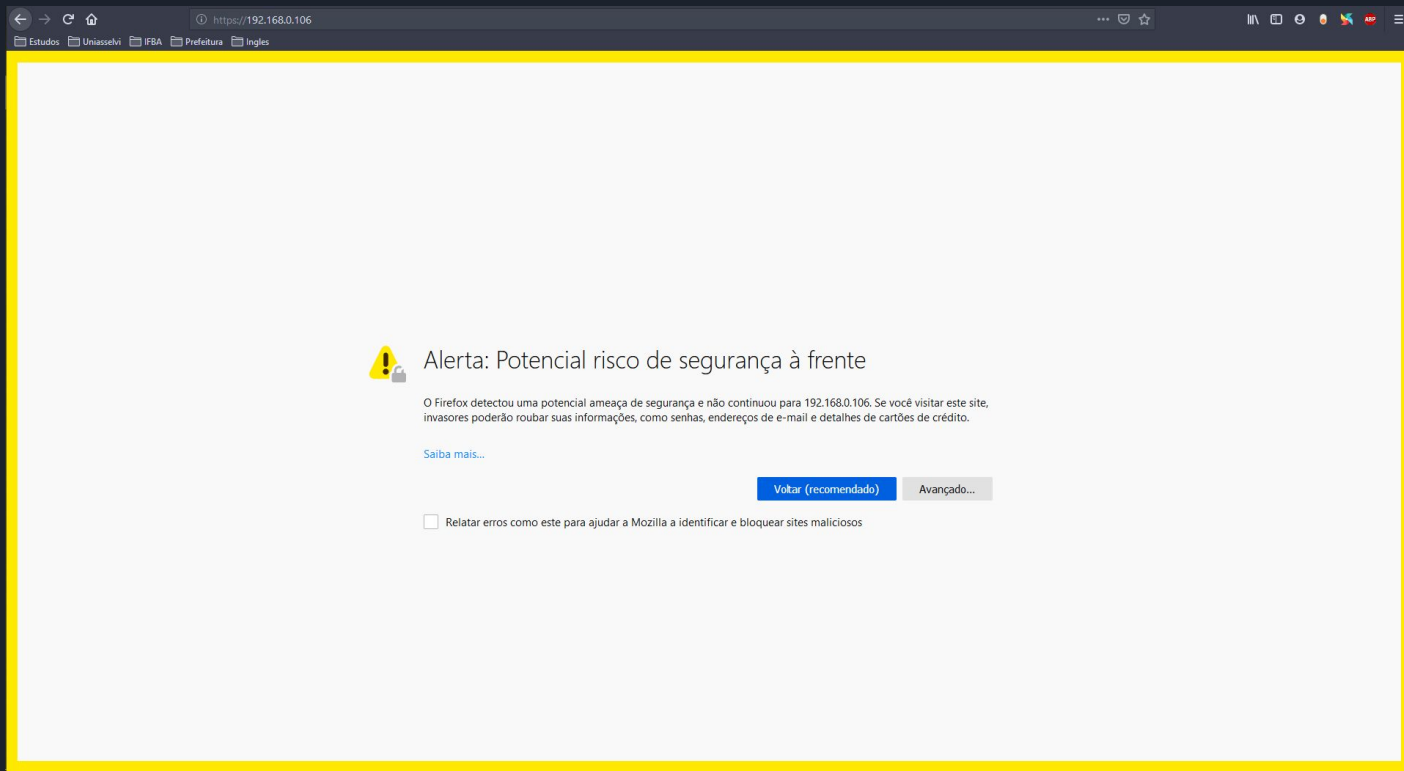
# Conclusão

Com essa última etapa o seu site está com criptografia implementada. Isso significa que um site com criptografia é um site seguro? Não necessariamente. Um site com o protocolo HTTPS traz a segurança de que os pacotes trafegados em rede, se interceptados, não poderão ser lidos. Ainda assim, o site pode ter um site que utiliza criptografia em seus dados pode ser criado para fins ilícitos, tais quais os infinitos sites da deep web. Mas vamos testar a nossa implementação? Primeiro, acesse seu servidor apache pelo protocolo HTTP e sem seguida mude o link para HTTPS e veja o que ocorre.

# Acesso via HTTP



# Acesso via HTTPS





# COMO ASSIM MEU SITE NÃO É SEGURO?

Como eu disse antes, a simples implementação da criptografia não torna o seu site seguro. O que passou a ser seguro é o tráfego de dados entre o cliente e servidor. Se o certificado não for reconhecido pelo navegador como válido, o mesmo exibirá um alerta de acesso a site perigoso. Não se preocupe, você pode fazer seu acesso ao site normalmente confirmando uma exceção.

Sites comprovam sua identidade através de certificados. O Firefox não confia neste site porque ele usa um certificado que não é válido para 192.168.0.106.

Código do erro: [MOZILLA\\_PKIX\\_ERROR\\_SELF\\_SIGNED\\_CERT](#)

[Ver certificado](#)

**Voltar (recomendado)**

Aceitar o risco e continuar



# Fin!

E aqui temos o nosso site, funcionando com o protocolo HTTPS, uma conexão estabelecida com criptografia TLS de última geração, um bela alerta no ícone de conexão segura.

Espero que todo o processo tenha ficado claro. Segue abaixo o link do vídeo com a prática desse processo: [link será inserido mais tarde]

