

Configurando Apache com certificados (TLS/SSL)

A título de comentário: vamos utilizar certificados não válidos (nas cadeias oficiais confiáveis dos browsers da Internet), mas segue algumas dicas caso queira utilizá-las em algum momento.

Certificados são, em geral, pagos, e têm uma validade.

Você pode adquirir um certificado da “Comodo CA” para testes, válidos por 90 dias, através do link: <https://www.comodo.com/e-commerce/ssl-certificates/free-ssl-certificate.php>

Ou ainda utilizar certificados como os gerados pela “AC aberta” de uma grupo sem fins lucrativos chamada Let’s Encrypt: <https://letsencrypt.org/>

0. Faça login como usuário administrador do sistema

```
sudo su
# ou
sudo -i
```

1. Agora vamos criar o diretório no qual iremos guardar nossos certificados:

```
mkdir /etc/apache2/ssl/certificados/
```

2. Vamos então entrar no diretório:

```
cd /etc/apache2/ssl/certificados
```

3. Copie os certificados que você recebeu da CA (que gerou o seu certificado, chave privada e também enviou o próprio certificado da CA, o ca.crt)

4. Vamos configurar nosso acesso SSL. Edite o arquivo com o seu editor favorito (no exemplo estamos usando o vim)

```
vim /etc/apache2/sites-enabled/seguranca.conf
```

5. O conteúdo deve ser algo como:

```
<VirtualHost *:443>
  DocumentRoot /var/www/html/
  DirectoryIndex index.php index.htm index.html
  TransferLog /var/log/apache2/access.log
  SSLEngine on
  SSLCertificateKeyFile /etc/apache2/ssl/sua_chave.key
  SSLCertificateFile /etc/apache2/ssl/seu_certificado.crt
  SSLCACertificateFile /etc/apache2/ssl/ca.crt
  ServerSignature off
</VirtualHost>
```

Atenção com os caminhos das linhas que começam com “SSL”

6. Habilite o modulo SSL no Apache

```
a2enmod ssl
```

7. Reinicie o Apache

```
service apache2 restart
```