Configuração Servidor Apache com Certificado Auto-Assinado e Autenticaçao *Client-Side*

A distribuição Linux utilizada como referência para os comandos descritos nesse manual é a Ubuntu 16.04.

PREPARANDO O SERVIDOR

1. Atualizando o repositório de pacotes e instalando o apache:

```
# apt-get update
# apt-get upgrade
# apt-get install apache2
```

2. Habilite o SSL no servidor Apache:

```
# cd /etc/apache2/mods-enabled
# ln -s ../mods-available/ssl.* .
# ln -s ../mods-available/socache_* .
# cd /etc/apache2/sites-enabled
# ln -s ../sites-available/default-ssl.conf .
```

3. Crie um diretório que será utilizado como repositório para os certificados e chaves:

```
# mkdir /etc/apache2/certs
# cd /etc/apache2/certs
```

CRIANDO A AUTORIDADE CERTIFICADORA LOCAL

4. Crie a chave da CA e crie o certificado digital da Autoridade Certificadora:

```
# openssl genrsa -des3 -out ca.key 4096
# openssl req -new -x509 -days 365 -key ca.key -out ca.crt
<você será questionado sobre informações relativas a CA>
```

CRIANDO O CERTIFICADO DO SERVIDOR

5. Crie a chave, certificado do servidor. Logo após assine o certificado utilizando a CA criada previamente:

```
# openssl genrsa -des3 -out server.key 4096
# openssl req -new -key server.key -out server.csr
# openssl x509 -req -days 365 -in server.csr -CA ca.crt -CAkey
ca.key -set_serial 01 -out server.crt
<você será questionado sobre informações relativas ao certificado>
```

6. Edite o arquivo /etc/apache2/sites-enabled/default-ssl.conf e adicione/altere o conteúdo abaixo:

SSLCertificateFile	/etc/apache2/certs/server.crt
SSLCertificateKeyFile	/etc/apache2/certs/server.key
SSLCACertificateFile	/etc/apache2/certs/ca.crt

7. Reinicie o serviço do Apache

```
# service apache2 stop
# service apache2 start
```

8. Acesse o servidor utilizando um navegador e verifique se a conexão HTTPS foi estabelecida. Verifique as informações do certificado e certifique-se que são as mesmas que você informou na criação dos certificados do servidor e CA. Para que as mensagens de certificado invalido não mais apareçam, será necessário importar no sistema operacional o certificado (**ca.crt**) da CA e atribui-la com confiável.

CRIANDO O CERTIFICADO DO USUARIO

9. Altere o arquivo de configuração do Apache (/etc/apache2/sites-enabled/default-ssl.conf), adicionando os parâmetros abaixo:

```
SSLVerifyClient require
SSLVerifyDepth  10
```

10. Crie a chave e o certificado do usuário. Em seguida, assine o certificado utilizando a CA previamente criada:

```
# openssl genrsa -des3 -out fulano.key 4096
# openssl req -new -key fulano.key -out fulano.csr
# openssl x509 -req -days 365 -in fulano.csr -CA ca.crt -CAkey
ca.key -set_serial 01 -out fulano.crt
```

11. Converta o certificado digital criado em um formato exportável (P12, PFX ou PEM):

```
# openssl pkcs12 -export -clcerts -in fulano.crt -inkey
fulano.key -out fulano.p12
```

12. Transfira-o para a computador do cliente o arquivo contendo o certificado (**fulano.p12**) e importe o certificado no navegador.

13. Reinicie o serviço do Apache

```
# service apache2 stop
# service apache2 start
```

14. Acesse o servidor utilizando um navegador e verifique se o cliente solicitou a senha do certificado digital ao acessar o servidor.