Linux: Instalando Apache 2 e SSL no Ubuntu

Como em toda instalação ou configuração no Ubuntu, recomendo atualizar os repositórios do APT e instalar quaisquer atualizações disponíveis.

```
# apt-get update
```

- **apache2** – é servidor web. Veja mais em: http://pt.wikipedia.org/wiki/Servidor_Apache;
- **ssl-cert** – pacote que permite a instalação de outros pacotes que precisam criar certificados SSL. Leia também sobre **OpenSSL**.

Para instalação desse pacotes utilize o comando abaixo:

```
# apt-get install apache2 ssl-cert
```

Habilitando o Suporte ao SSL

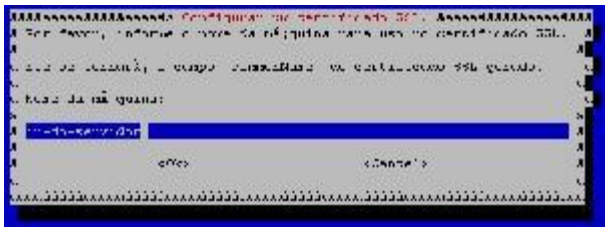
Crie o diretório onde o certificado será criado:

```
# mkdir /etc/apache2/ssl
```

Agora, utilizando o *make-ssl-cert* e o modelo no arquivo *ssleay.cnf* vamos criar o certificado armazenando-o no arquivo *apache.pem*:

```
# make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/apache2/ssl/apache.pem
```

Surgirá uma tela, como a figura abaixo, onde será solicitado o nome do servidor. Eu, particularmente, preencho com o IP, pois meu DNS não está configurado e pretendo acessar o Subversion em outras máquinas.



Criação do certificado SSL. Definindo o nome do servidor.

Vamos definir a permissão ao arquivo.

```
# chmod 660 /etc/apache2/ssl/apache.pem
```

Configurando Apache 2 e habilitando o SSL

Verifique se o Apache 2 para que seja habilitada o suporte a **porta 443**. Para isso visualize o arquivo *ports.conf* no diretório do Apache 2:

```
# vi /etc/apache2/ports.conf
```

Seu arquivo deverá estar como mostro abaixo:

```
NameVirtualHost *:80 Listen
80

<IfModule mod_ssl.c>
# SSL name based virtual hosts are not yet supported, therefore no
```

```
# NameVirtualHost statement here
Listen 443
</IfModule>
```

Para habilitar o módulo de suporte ao SSL no Apache 2 é necessário utilizar o script **a2enmod**. O *a2enmod* criará um link simbólico no diretório */etc/apache2/mod-enabled*. Para desabilitar um módulo utilize o script *a2dismod*. A linha de comando é:

```
# a2enmod ssl
```

O último passo da configuração do Apache 2, para o perfeito funcionamento do SSL, consiste em editar o arquivo 000-default.conf em */etc/apache2/sites-available*, este arquivo deve conter as configurações para a porta 443, ou seja, a porta ao qual definimos como responsável pelo SSL.

```
# vi /etc/apache2/sites-available/000-default.conf
```

Altere a linha <*VirtualHost *:80*> para **<VirtualHost *:443>** e logo abaixo adicione as linhas:

```
<VirtualHost *:443>
ServerName www.exemplo.com
DocumentRoot /var/www/exemplo

SSLEngine on
ServerSignature On
SSLCertificateFile /etc/apache2/ssl/apache.pem

</VirtualHost>
```

Vamos entender cada uma das três linhas acima:

- **SSLEngine on** – Ativa se definida como "on" a utilização do protocolo SSL/TLS;

- **SeverSignature On** – Ativa ou desativa a exbição da assinatura do servidor, ou seja, a linha que exibe as configurações do Apache. Por exemplo: *Apache/2.2.9 (Ubuntu) DAV/2 SVN/1.5.1 PHP/5.2.6-2ubuntu4.1 with Suhosin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g Server at 192.168.0.30 Port 44*. Na influencia no funcionamento do servidor;
- **SSLCertificateFile** – Define o caminho para certificado.

Reinicialize o Apache 2 com o comando:

```
# /etc/init.d/apache2 force-reload
```

Caso ocorra algum erro, então consulte o arquivo de *log* do Apache 2. Este arquivo está localizado em */var/log/apache2/error.log*.

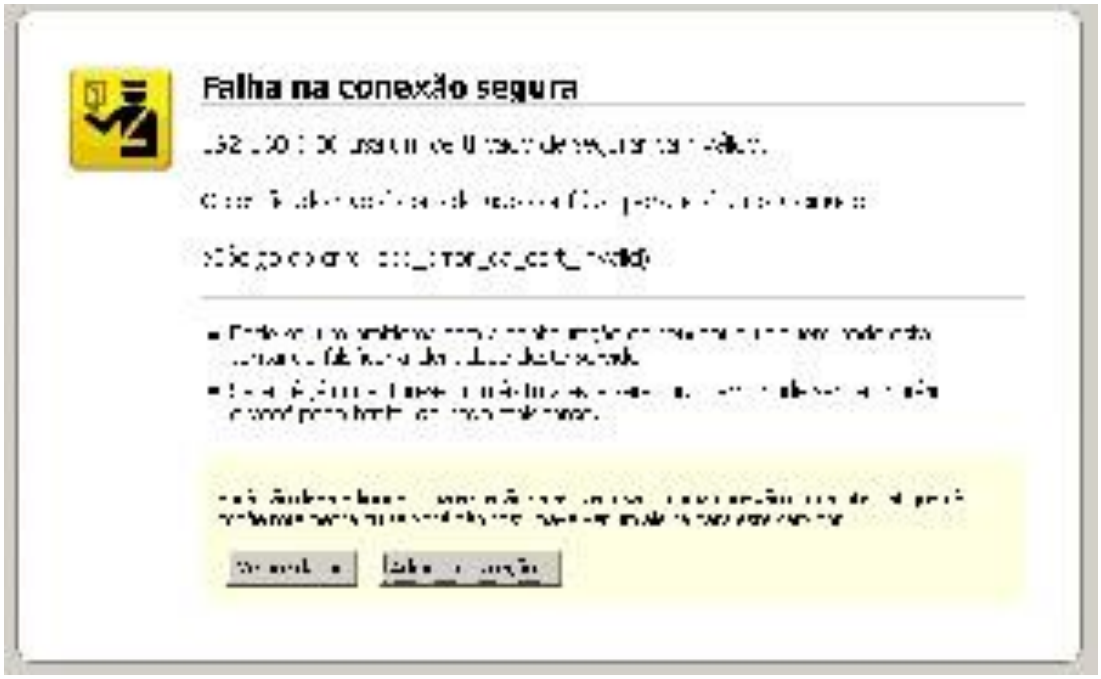
Dica de solução:

```
# openssl req -config /usr/share/ssl-cert/ssleay.cnf -new -x509 -days 1460 nodes
-out /etc/apache2/ssl/apache.pem -keyout /etc/apache2/ssl/apache.pem
```

Teste seu servidor, digitando no navegador o endereço IP precedido por *https*, por exemplo: **https://<IP-DO-SERVIDOR/**.

Você poderá ver uma página como a da figura abaixo. Fique tranquilo! **Essa mensagem não reflete um problema em seu servidor.** Na verdade a mensagem é exibida, pois você configurou um certificado próprio (auto-assinado) e não foi emitido por uma autoridade certificadora, como é o caso de sites que utilizam certificado homologado pela *VeriSign*. Apenas clique no link "você pode adicionar uma exceção" e depois no botão "Adicionar exceção…". Aparecerá seu

endereço IP. “Clique em verificar certificado” e logo em seguida, clique no botão “Confirmar exceção de segurança”. Pronto.



Firefox: Falha na conexão segura

Redirecionamento de HHP para HTTPS

Dentro arquivo /etc/apache2/sites-available/000-default.conf inserir:

```
<VirtualHost *:80>
  ServerName www.exemplo.com
  Redirect permanent / https://www.examplo.com
</VirtualHost>
```