

Universidade Federal dos Vales do Jequitinhonha e Mucuri



Tutorial Certificação Digital e Chave Pública

Disciplina: SEGURANÇA E AUDITORIA DE SISTEMAS DE INFORMAÇÃO

Discentes: Alex Lopes
 Guilherme Rocha
 José Maria. P
 Luiz Araujo
 Matheus Andrade F de lima

Diamantina, 9 de dezembro de 2020.

Tutoriais para instalação do certificado OpenSSL em ambiente local

Em ambiente Windows:

1) No ambiente Windows é necessário instalar o **xampp**, utilizamos a versão 7.1.10 que inclui a mesma versão do php, esse é o link para instalação:

- https://www.apachefriends.org/pt_br/download.html

2) Depois da instalação, verifique se está tudo funcionando corretamente com o módulo apache verde.

3) Crie um arquivo com o nome de **v3.ext** dentro da pasta **apache** no diretório onde você instalou o **Xampp** (se você não alterou o caminho de instalação, deverá criar esse arquivo dentro de **c:\xampp\apache**).

4) Abra o arquivo do passo 3 e digite os comandos :

1. linha -> `authorityKeyIdentifier=keyid,issuer`
2. linha -> `basicConstraints=CA:FALSE`
3. linha -> `keyUsage = digitalSignature, nonRepudiation,`
4. linha -> `keyEncipherment, dataEncipherment`
5. linha -> `subjectAltName = @alt_names`
6. linha -> `[alt_names]`
7. linha -> `DNS.1 = localhost`

5) Nessa mesma pasta, existe o arquivo **makecert.bat**, é necessário alterá-lo (clique com o **botão direito** em abrir como depois abra com um editor de texto)

6) Troque a linha 9 do arquivo que você abriu no editor de texto por essa nova linha:

9. linha -> `bin\openssl x509 -in server.csr -out server.crt -req -signkey server.key -days 500 -sha256 -extfile v3.ext.txt`

7) Pode **salvar** o arquivo e fechá-lo

8) Clique 2 vezes no arquivo **makecert.bat**.

9) Você informará uma **senha** e deverá gravá-la para não esquecer pois terá que digitar novamente.

10) Em seguida preencha todas as informações que forem solicitadas, a primeira será Country Name: BR.

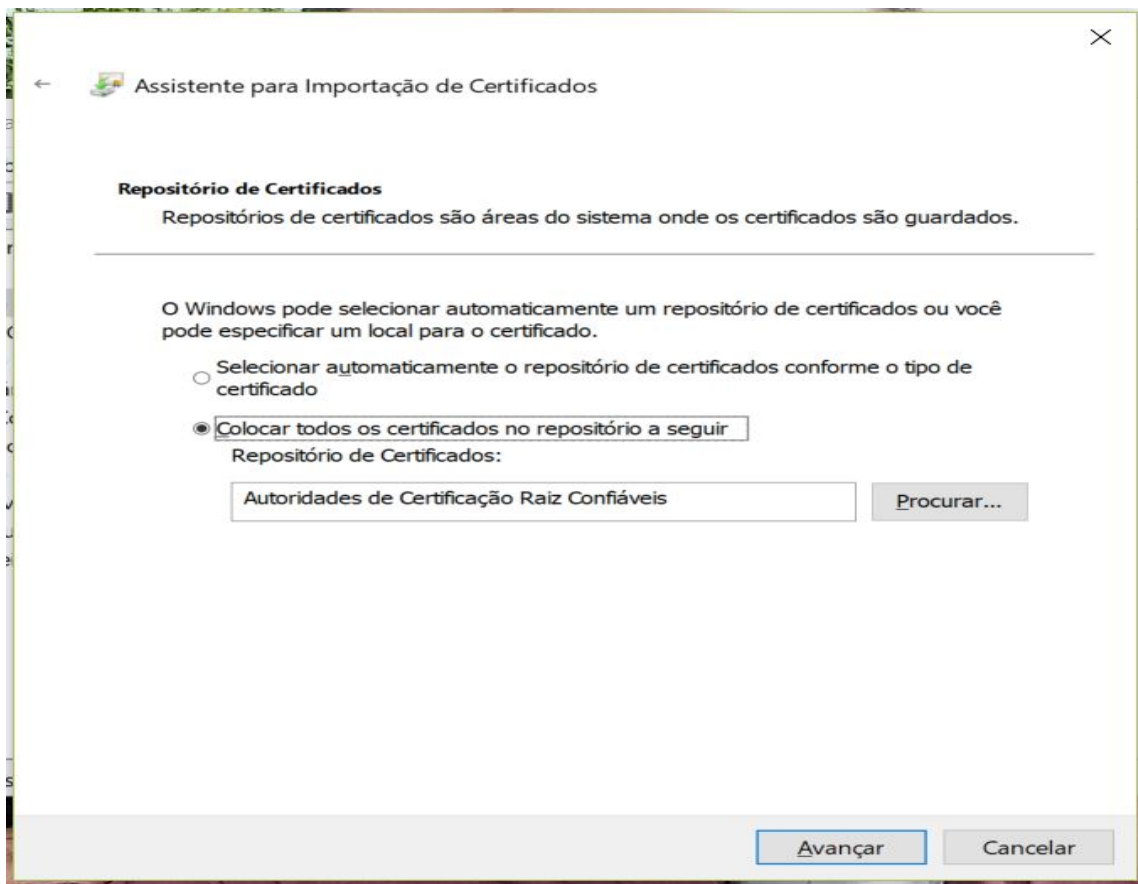
11) É solicitado novamente a **senha** que você criou no passo 9.

12) Aperte a tecla do **Windows + R** e digite **certmgr.msc** e depois clique em **OK**.
(vamos adicionar o novo certificado **SSL** aos certificados confiáveis no Windows e usando o programa **certmgr.msc**)

13) Vá em “**Autoridades de Certificação Raiz Confiáveis**” e veja que na parte direita da janela terá uma aba com o título “**Tipo de Objeto**”. Clique com o botão direito do mouse em **Certificados**, selecione **Todas as tarefas**, e depois clique em **Importar**.

14) Agora abrirá um assistente de importação de certificados, clique em **avancar** e na segunda tela você deverá buscar o local do certificado que foi criado anteriormente.

15) Clique em **Procurar** e selecione o arquivo **server.crt** no caminho **C:\xampp\apache\conf\ssl.crt**. (no caso dentro da pasta apache da sua instalação XAMPP). Clique em **Abrir** e depois clique em **Avançar**.



16) Deixe marcado a opção **padrão**, conforme imagem acima, e clique novamente em **avançar**. Você verá a tela abaixo e pode clicar em **Concluir**.

17) Confirme também o Aviso de Segurança que será mostrado, clicando em **Sim**. E por fim clique em **OK**. Pronto, o certificado SSL para o seu localhost já está configurado.

18) Vá até *localhost*/"Nome do seu sistema" e veja que o certificado foi instalado com sucesso.

19) Para adicionar o certificado HTTPS em somente algumas páginas, crie dois arquivos na pasta raiz do sistema: um chamado "redireciona_https.js" e o outro "redireciona_http.js". No conteúdo do primeiro, insira o código a seguir:

```
if(location.protocol!=='https:'){  
    const httpsURL = 'https://' + location.href.split('/')[1];  
    location.replace(httpsURL)  
}
```

Já no segundo arquivo criado, insira as linhas abaixo:

```
if(location.protocol!=='http:'){  
    const httpURL = 'http://' + location.href.split('/')[1];  
    location.replace(httpURL);  
}
```

20) Feito isso, é só incluir nos arquivos do servidor o arquivo de redirecionamento criado respectivo. O arquivo `redireciona_https` serve para redirecionar páginas HTTP para HTTPS, e o contrário para o outro arquivo.

Em ambiente Linux:

1) Para atualizar os repositórios e o pacote **openssl**, que já é nativo do Linux, execute os seguintes comandos:

```
sudo apt-get update  
sudo apt-get upgrade openssl
```

2) O próximo passo é instalar o **Apache** e ativar seu módulo de **SSL**, para isso, use os comandos abaixo:

```
sudo apt-get install apache2  
sudo a2enmod ssl  
sudo a2ensite default-ssl  
sudo service apache2 reload
```

3) Agora vamos gerar um novo certificado e a chave privada para o mesmo, armazenando-os em um diretório específico:

```
sudo mkdir /etc/apache2/ssl  
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout  
/etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
```

No segundo comando, os parâmetros “**keyout**” e “**out**” se referem ao local de destino da chave e do certificado, respectivamente. O mesmo local criado no comando anterior.

Ao executar o comando anterior, uma série de linhas e, posteriormente, de perguntas será exibida. As perguntas se referem ao país, estado, cidade, organização, setor da organização, nome ou endereço do responsável e seu e-mail. Para responder a elas,

utilize as respostas encontradas na próxima figura (atente-se para alterar as respostas de acordo com suas informações e objetivos):

```
guilherme@guilherme-NE56R:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
Can't load /home/guilherme/.rnd into RNG
140210776814016:error:2406F079:random number generator:RAND_load_file:Cannot open file:../crypto/rand/randfile.c:88:Filename=/home/guilherme/.rnd
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/apache2/ssl/apache.key'
-----
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]:Minas Gerais
Locality Name (eg, city) []:Diamantina
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UFVJM
Organizational Unit Name (eg, section) []:Departamento de Computação
Common Name (e.g. server FQDN or YOUR name) []:localhost
Email Address []:guilherme.rocha@ufvjm.edu.br
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
guilherme@guilherme-NE56R:~$
```

Após isso, altere as permissões do diretório onde os arquivos estão armazenados:

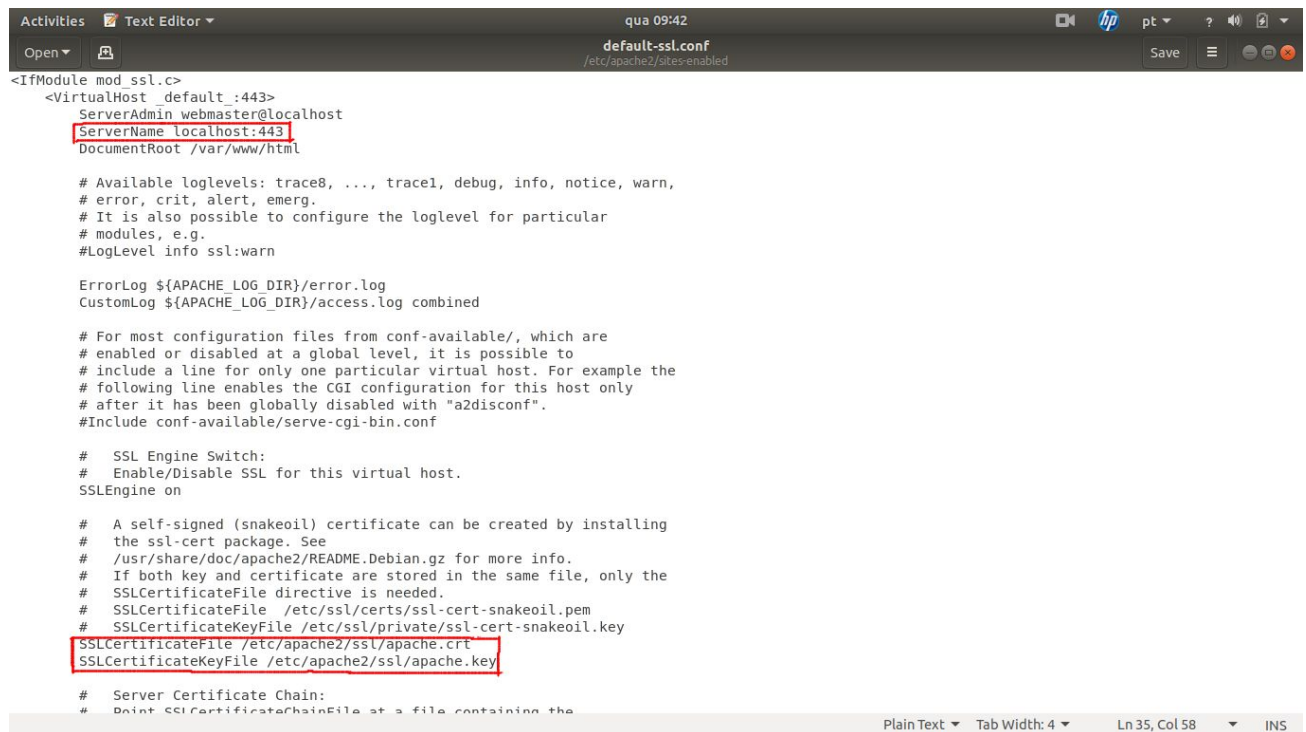
```
sudo chmod 600 /etc/apache2/ssl/*
```

4) Para configurar o **Apache**, abra o arquivo “**default-ssl.conf**” usando o comando abaixo:

```
sudo gedit /etc/apache2/sites-enabled/default-ssl.conf
```

Localize a linha com a expressão “<**VirtualHost _default_:443**>” e insira as seguintes linhas abaixo nos mesmo locais da figura a seguir:

```
ServerName localhost:443
SSLCertificateFile /etc/apache2/ssl/apache.crt
SSLCertificateKeyFile /etc/apache2/ssl/apache.key
```



```
<IfModule mod_ssl.c>
<VirtualHost default :443>
    ServerAdmin webmaster@localhost
    ServerName localhost:443
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf

    #
    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on

    #
    # A self-signed (snakeoil) certificate can be created by installing
    # the ssl-cert package. See
    # /usr/share/doc/apache2/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.
    #
    SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
    #
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
    SSLCertificateFile /etc/apache2/ssl/apache.crt
    SSLCertificateKeyFile /etc/apache2/ssl/apache.key

    #
    # Server Certificate Chain:
    # Print SSLCertificateChainFile at a file containing the
```

Figura 2 -

Reinicie o serviço da Apache:

```
sudo service apache2 reload
```

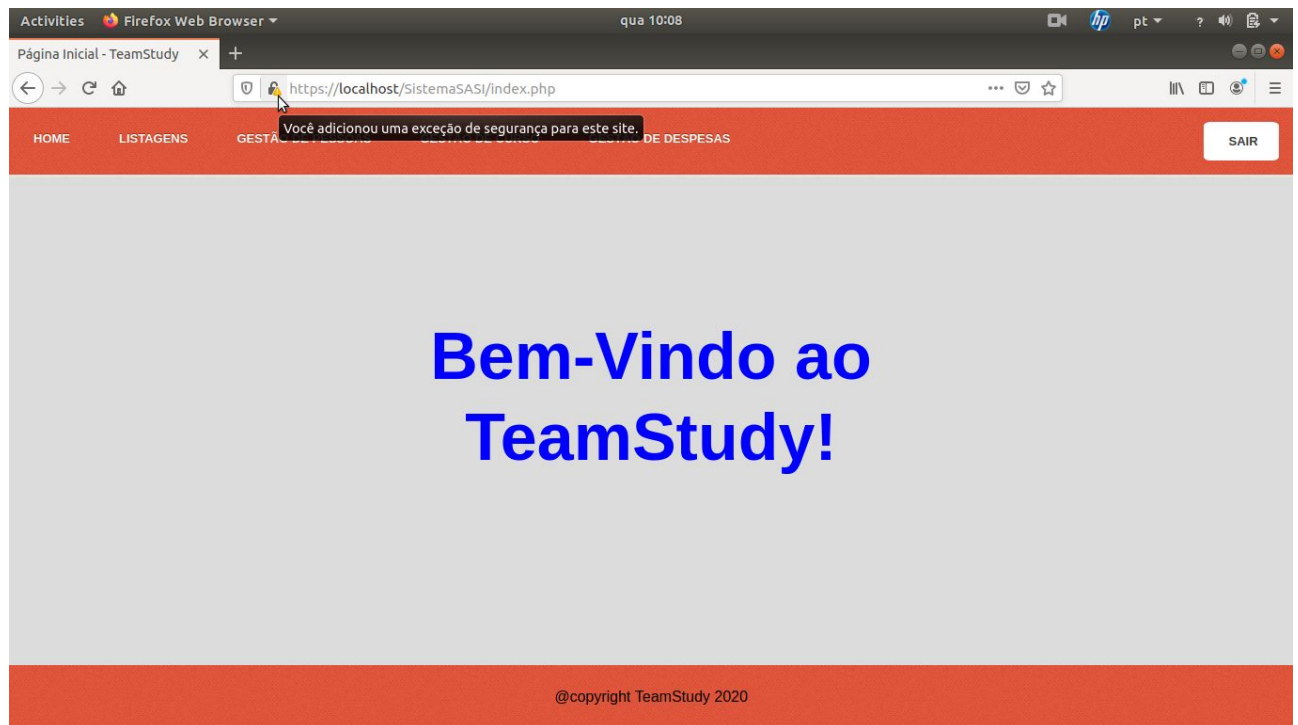
5) Após isso, verifique a conexão do **Apache** com o **SSL** com o comando abaixo:

```
openssl s_client -connect localhost:443
```

Caso encontre as informações abaixo em linhas diferentes no terminal significa que a instalação do certificado **SSL** no **Apache** foi corretamente realizada (as informações entre aspas são variáveis de instalação para instalação e representam um número):

SSL handshake has read “valor que pode variar” bytes and written “valor que pode variar” bytes e SSL-Session:

6) Finalmente, teste o certificado pelo navegador. No caso da figura abaixo, o navegador identificou uma insegurança por ele ser auto-assinado.



7) Para adicionar o certificado HTTPS em somente algumas páginas, crie dois arquivos na pasta raiz do sistema: um chamado “redireciona_https.js” e o outro “redireciona_http.js”. No conteúdo do primeiro, insira o código a seguir:

```
if(location.protocol!=='https:'){  
    const httpsURL = 'https://' + location.href.split('/')[1];  
    location.replace(httpsURL)  
}
```

Já no segundo arquivo criado, insira as linhas abaixo:

```
if(location.protocol!=='http:'){  
    const httpURL = 'http://' + location.href.split('/')[1];  
    location.replace(httpURL);  
}
```

8) Feito isso, é só incluir nos arquivo do servidor o arquivo de redirecionamento criado respectivo. O arquivo redireciona_https serve para redirecionar páginas HTTP para HTTPS, e o contrário para o outro arquivo.

Referências:

1. <https://www.digitalocean.com/community/tutorials/how-to-create-a-ssl-certificate-on-apache-for-debian-8>
2. <https://academiawordpress.com.br/grupos-de-tecnologia-no-telegram-ti-e-mpregos-web-e-mais/>