Como incluir um certificado SSL (HTTPS) no e-SUS APS

Um certificado SSL é um certificado digital que autentica a identidade de um site e permite uma conexão criptografada. SSL significa *Secure Sockets Layer*, um protocolo de segurança que cria um link criptografado entre um servidor web e um navegador web.

Neste artigo, apresentaremos o passo-a-passo para inclusão de um certificado SSL no e-SUS APS (no Linux) e garantir ainda mais segurança no acesso à sua instalação.

Linux

Gerando um certificado SSL

Caso ainda não possua um certificado SSL, mostraremos como obtê-lo usando o Certbot do Let's Encrypt, uma Autoridade Certificadora gratuita, automatizada e aberta, que fornece certificados digitais necessários para habilitar HTTPS em websites.

Caso já possua um certificado SSL, basta pular esta seção e ir para "Instalando o certificado SSL".

Como o PEC vem configurado para o protocolo HTTP na porta 8080 por padrão e o Certbot precisa que o servidor esteja rodando na porta 80 para funcionar, será necessário alterar essa configuração do e-SUS APS. Em /opt/e-SUS/webserver/config, modifique o arquivo **application.properties** para adicionar a seguinte linha:

- **`server.port=80`**

Após a inclusão, é necessário que o serviço do e-SUS APS seja reiniciado:

- **`systemctl stop e-SUS-PEC.service`**
- **`systemctl start e-SUS-PEC.service`**

É preciso ter o ***snapd*** instalado, caso ainda não o possua. Ele vem pré-instalado no Ubuntu 18, 20 e 21, e no Manjaro, dentre outros. Porém, se você utiliza ArchLinux, Debian ou Fedora, por exemplo, será necessário instalá-lo, de acordo com o gerenciador de pacotes da sua distribuição.

Com o *snapd* instalado, execute o comando abaixo:

- **`sudo snap install core`**
- **`sudo snap refresh core`**

Se você tiver algum pacote do Certbot instalado através de um gerenciador de pacotes do sistema (como apt, dnf ou yum), você deve removê-lo antes de prosseguir. O comando exato para fazer isso depende da sua distribuição Linux, mas exemplos comuns são:

- **`sudo apt-get remove certbot`**
- **`sudo dnf remove certbot`**
- **`sudo yum remove certbot`**

Se você já usou o Certbot no passado por meio do script *certbot-auto*, você também deve remover.

Finalmente, instale o Certbot executando o comando abaixo:

- **sudo snap install --classic certbot**

E então rode o comando a seguir para garantir que o Certbot poderá ser executado:

- **sudo ln -s /snap/bin/certbot /usr/bin/certbot**

Por fim, execute-o por meio do comando e preencha as informações solicitadas:

- **sudo certbot certonly --webroot**

obs.:

Caso o comando acima não funcione por pare o serviço do e-SUS.

- **sudo systemctl stop e-SUS-PEC.service**

E, execute o comando e preencha as informações solicitadas:

- **sudo certbot certonly --standalone**

Instalando o certificado SSL

Uma vez que você já possui um certificado SSL, vamos armazená-lo em uma keystore.

E então use o comando abaixo para importar o certificado e criar a keystore, substituindo:

- "fullchain.pem" e “privkey.pem” são os nomes dos certificados que o certbot cria.

- **sudo su**
- **cd /etc/letsencrypt/live/meu.site.com.br**
- **openssl pkcs12 -export -in fullchain.pem -inkey privkey.pem -out esusaps.p12 -name esusaps -CAfile chain.pem -caname esusaps**
- **mv esusaps.p12 /opt/e-SUS/webserver/config**
- **cd /opt/e-SUS/webserver/config**

Agora, é necessário fazer com que o e-SUS APS utilize o certificado salvo na keystore. Em **/opt/e-SUS/webserver/config**, modifique o arquivo **application.properties**, copiando as seguintes propriedades para o final do arquivo:

- **nano application.properties**
  - **server.port=443**
  - **server.ssl.key-store-type=PKCS12**
  - **server.ssl.key-store=config/esusaps.p12**

- **server.ssl.key-store-password=SENHA**
- **server.ssl.key-alias=esusaps**
- **security.require-ssl=true # Sempre deve ser passado verdadeiro para habilitar o uso de SSL.**

O significado de cada propriedade pode ser observado a seguir:

- ***server.port*:** A porta que representa o protocolo HTTPS; utiliza-se como padrão a porta 443. (lembrar que havia alterado para 80)
- ***server.ssl.key-store-type:*** Indica o tipo de Key Store. Caso o tipo seja .p12 (como neste tutorial), é necessário manter esta propriedade e após o = indicar que é PKCS12. Mas, se o tipo for JKS, essa propriedade pode ser omitida.
- ***server.ssl.key-store:*** Este é o caminho relativo ao .jar da aplicação (pec-bundle.jar) de onde se encontra a Key Store. Por exemplo, se a Key Store estiver dentro da pasta config como sugerido nos últimos passos, utilizar: server.ssl.key-store=config/esusaps.p12
- ***server.ssl.key-store-password:*** Senha indicada no momento da criação da Key Store.
- ***server.ssl.key-alias:*** "Apelido" indicado no momento da criação da Key Store "**-name esusaps**".
- ***security.require-ssl:*** Propriedade que indica ao Spring se desejamos fazer uso do protocolo SSL.

Após incluir essas propriedades no arquivo e salvá-lo, é necessário reiniciar o serviço do servidor:

- **systemctl stop e-SUS-PEC.service**
- **systemctl start e-SUS-PEC.service**

Pronto, o certificado SSL já deve ter sido incluído na sua instalação do e-SUS APS! Para confirmar que o processo funcionou, acesse a URL da instalação em seu navegador e procure pelo ícone de cadeado na barra de endereço.

O certificado gerado tem validade de 3 meses, deverá ser renovado para não apresentar erros.

Caso não tenha sido solicitado e-mail ou tenha mudado use:

- **sudo certbot update_account --email seuemail@example.com**

Para testar a renovação automática utilize o comando abaixo:

- **sudo certbot renew --dry-run**

Para forçar o redirecionamento da porta 80 para a 443, será necessário o apache.

- **sudo apt install apache2**

Acessar a pasta de configuração do apache e modificar o arquivos 000-default.conf

- **cd /etc/apache2/sites-avaliable**
- **sudo nano 000-default.conf**

Inserir no arquivo as linhas abaixo

- **ServerName http://seusite.com.br**
- **Redirect / https://seusite.com.br**

Reinicie o serviço do apache para as modificações sejam efetivadas

- **sudo systemctl stop apache2.service**
- **sudo systemctl start apache2.service**

Parte deste tutorial está disponível no site do suporte do laboratório bridge, mas faltam informações que foram supridas nesta versão.

Windows (não recomendado)

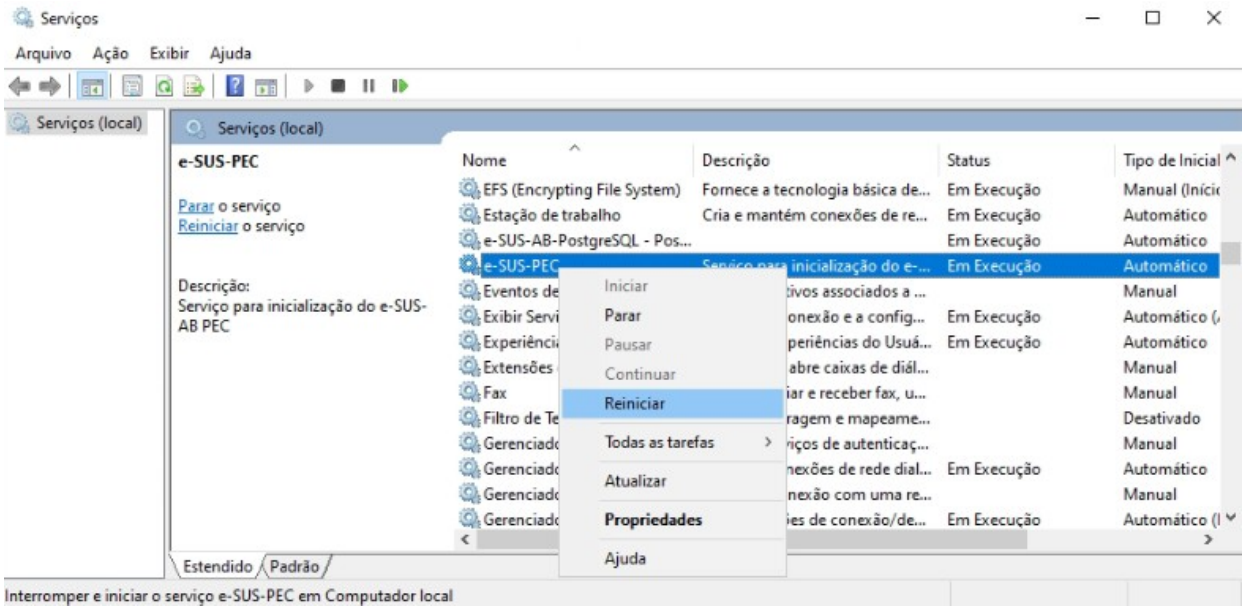
Caso ainda não possua um certificado SSL, mostraremos como obtê-lo usando o Certbot do Let's Encrypt, uma Autoridade Certificadora gratuita, automatizada e aberta, que fornece certificados digitais necessários para habilitar HTTPS em websites.

Caso já possua um certificado SSL, basta pular esta seção e ir para "Instalando o certificado SSL".

Como o PEC vem configurado para o protocolo HTTP na porta 8080 por padrão e o Certbot precisa que o servidor esteja rodando na porta 80 para funcionar, será necessário alterar essa configuração do e-SUS APS. Em c:\Program Files\e-SUS\webserver\config, modifique o arquivo **application.properties** para adicionar a seguinte linha:

- **server.port=80**

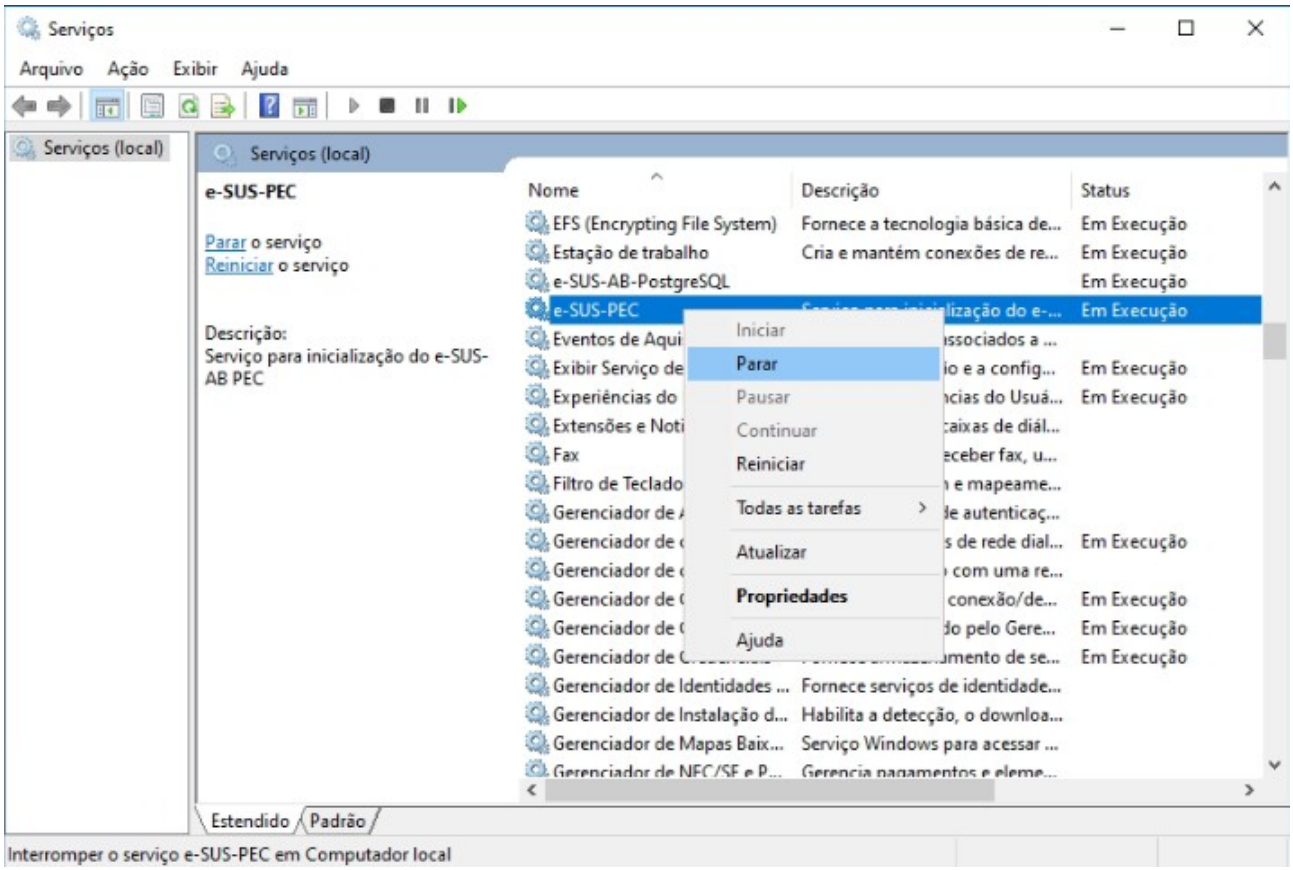
Após a inclusão, é necessário que o serviço do e-SUS APS seja reiniciado:



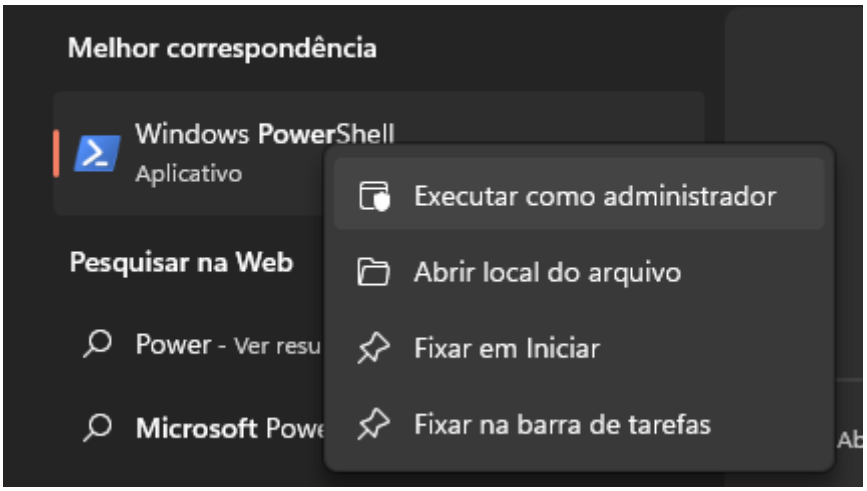
Baixar e instalar o certBot no windows, o instalador está disponível em:

- **`https://github.com/certbot/certbot/releases/latest/download/certbot-beta-installer-win_amd64_signed.exe`**

Para instalação é necessário acesso como administrador

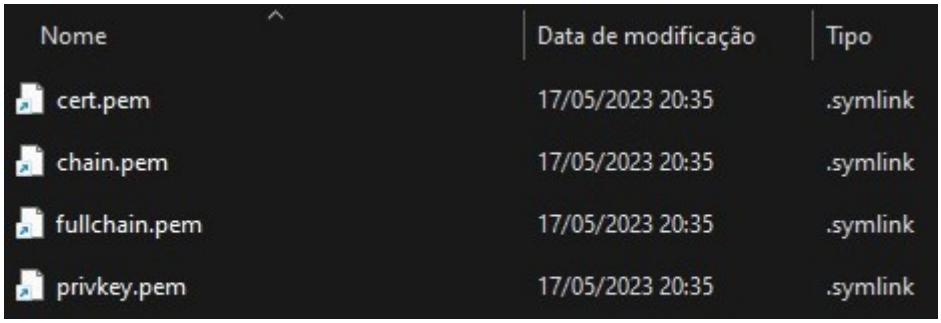


Parar o serviço com esus e abrir um terminal do powershell no modo administrador e executar:




```
c:\certbot certonly --standalone
```

Serão gerados 4 arquivos em C:\certbot\live\nome_do_dominio



Instalando o certificado SSL

Uma vez que você já possui um certificado SSL, vamos armazená-lo em uma keystore.

E então use o comando abaixo para importar o certificado e criar a keystore, substituindo:

- "fullchain.pem" e “privkey.pem” são os nomes dos certificados que o certbot cria.

Ainda com o poweshell aberto, executar

- **`Get-ExecutionPolicy`**
- **`Set-ExecutionPolicy AllSigned`**

Instale o chocoletey

- **`Set-ExecutionPolicy Bypass -Scope Process -Force; [System.Net.ServicePointManager]::SecurityProtocol = [System.Net.ServicePointManager]::SecurityProtocol -bor 3072; iex ((New-Object System.Net.WebClient).DownloadString ('https://community.chocolatey.org/install.ps1'))`**

Instalar o openssl usando o chocolatey

- **`choco install openssl`**

Entre no diretório onde o certbot grava os arquivos e execute os comandos.

- **`cd c:\certbot\live\nome_do_dominio`**
- **`openssl`**
- **`openssl pkcs12 -export -in fullchain.pem -inkey privkey.pem -out esusaps.p12 -name esusaps -CAfile chain.pem -caname esusaps`**
- **`mv esusaps.p12 C:\Program Files\e-SUS\webserver\config`**
- **`cd C:\Program Files\e-SUS\webserver\config`**

Agora, é necessário fazer com que o e-SUS APS utilize o certificado salvo na keystore. Em **`e-SUS\webserver\config`**, modifique o arquivo **`application.properties`**, copiando as seguintes propriedades para o final do arquivo:

- **notepad.exe application.properties**
  - **server.port=443**
  - **server.ssl.key-store-type=PKCS12**
  - **server.ssl.key-store=config/esusaps.p12**
  - **server.ssl.key-store-password=SENHA**
  - **server.ssl.key-alias=esusaps**
  - **security.require-ssl=true # Sempre deve ser passado verdadeiro para habilitar o uso de SSL.**

O significado de cada propriedade pode ser observado a seguir:

- ***server.port*:** A porta que representa o protocolo HTTPS; utiliza-se como padrão a porta 443. (lembrar que havia alterado para 80)
- ***server.ssl.key-store-type:*** Indica o tipo de Key Store. Caso o tipo seja .p12 (como neste tutorial), é necessário manter esta propriedade e após o = indicar que é PKCS12. Mas, se o tipo for JKS, essa propriedade pode ser omitida.
- ***server.ssl.key-store:*** Este é o caminho relativo ao .jar da aplicação (pec-bundle.jar) de onde se encontra a Key Store. Por exemplo, se a Key Store estiver dentro da pasta config como sugerido nos últimos passos, utilizar: server.ssl.key-store=config/esusaps.p12
- ***server.ssl.key-store-password:*** Senha indicada no momento da criação da Key Store.
- ***server.ssl.key-alias:*** "Apelido" indicado no momento da criação da Key Store "**-name esusaps**".
- ***security.require-ssl:*** Propriedade que indica ao Spring se desejamos fazer uso do protocolo SSL.

Após incluir essas propriedades no arquivo e salvá-lo, é necessário reiniciar o serviço do servidor:

Pronto, o certificado SSL já deve ter sido incluído na sua instalação do e-SUS APS! Para confirmar que o processo funcionou, acesse a URL da instalação em seu navegador e procure pelo ícone de cadeado na barra de endereço.

O certificado gerado tem validade de 3 meses, deverá ser renovado para não apresentar erros.

Caso não tenha sido solicitado e-mail ou tenha mudado use:

- **certbot update_account --email seuemail@example.com**

Para testar a renovação automática utilize o comando abaixo:

- **certbot renew --dry-run**