Configurando HTTPS (SSL) no Tomcat

Este guia detalha como configurar HTTPS usando certificados SSL no seu servidor Tomcat. Lembre-se de substituir os valores de exemplo pelos seus dados reais.

Antes de Começar:

- É necessário ter o Fortes RH implantado. Se ainda não tiver, acesse Instalação do Fortes RH no Windows
- Certifique-se de que seus arquivos de certificado e chave estejam codificados em UTF-8 sem BOM (Byte Order Mark).

Passo 1: Configurar a Porta do Conector

1. Abra o arquivo server.xml. A localização depende do seu sistema operacional:
    - Windows: C:\Program Files\Apache Software Foundation\Tomcat<numero_versão>\conf\server.xml
    - Linux: /opt/shared/tomcat<numero_versão>/conf/server.xml
2. Localize o elemento <Connector>. Adicione ou modifique o atributo redirectPort para 443. Isso redireciona o tráfego HTTP para HTTPS na porta 443. Exemplo:

```java
<Connector port="8080"
           protocol="HTTP/1.1"
           maxPostSize="4194304"
           maxParameterCount="30000"
           connectionTimeout="20000"
           redirectPort="443" />
```

Passo 2: Configurar o Certificado SSL

Escolha **apenas um** dos métodos a seguir (usando um arquivo de certificado PFX ou CRT):

Método A: Usando um Arquivo de Certificado PFX

1. Adicione o seguinte elemento `<Connector>` ao seu arquivo `server.xml`, substituindo os marcadores de posição pelos seus valores:

```java
<Connector port="443"

protocol="org.apache.coyote.http11.Http11NioProtocol"
           maxThreads="200"
           SSLEnabled="true"
           scheme="https"
           secure="true"
           clientAuth="false"
           sslProtocol="TLS"
           keystoreFile=
           "/caminho/para/seu/CertificadoValido.pfx"
           keystorePass="sua_senha" />
```

- Substitua `/caminho/para/seu/CertificadoValido.pfx` pelo caminho real para o seu arquivo PFX.
- Substitua `"sua_senha"` pela senha do seu arquivo PFX.

Método B: Usando um Arquivo de Certificado CRT

1. Adicione o seguinte elemento `<Connector>` ao seu arquivo `server.xml`, substituindo os marcadores de posição pelos seus valores:

```java
<Connector
protocol="org.apache.coyote.http11.Http11AprProtocol"
           port="443"
           maxThreads="200"
           scheme="https"
           secure="true"
           SSLEnabled="true"
           SSLVerifyClient="optional"
           SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
           SSLCertificateFile=
           "/caminho/para/seu/CertificadoValido.crt"
           SSLCertificateKeyFile=
```

```
        "/caminho/para/sua/chaveCertificadoValido.pem"
/>
```

- Substitua `/caminho/para/seu/CertificadoValido.crt` pelo caminho para o seu arquivo de certificado CRT.
- Substitua `/caminho/para/sua/chaveCertificadoValido.pem` pelo caminho para o seu arquivo de chave CRT.

Passo 3: Reinicie o Tomcat

Reinicie o seu servidor Tomcat para aplicar as alterações.

Verificação:

- Acesse seu aplicativo via HTTPS (porta 443): `https://dominio-cliente/fortesrh`
- Se o cliente não utilizar a porta 443, será necessário explicitar a porta no endereço: `https://dominio-cliente:8443/fortesrh`
- A porta HTTP (8080) pode permanecer ativa para fins de integração entre o Fortes RH e o Fortes Pessoal.

Links Úteis:

- Apache Tomcat SSL How-To
- Criando um Certificado PFX/P12 usando OpenSSL
- Configurando Certificado SSL no Tomcat

Lembre-se de manter seus certificados e chaves seguros.