Seguridad servidores de aplicaciones I

Índice

1. Seguridade nos servidores de aplicacións

1.1 Introdución

A autenticación é o proceso para verificar que alguén é quen realmente di ser, a autorización, pola súa parte, é o proceso polo que se lle permite facer a alguén autenticado o que solicita.

Para levar a cabo estas tarefas en Tomcat, empréganse os Realms. Un Realm é un arquivo, base de datos ou servizo de directorio que contén unha coleccións de usuarios e contrasinais e roles. Emprégase a clase `org.apache.catalina.Realm` e existen varios tipos de Realms, aínda que nos centraremos en MemoryRealm, no que se accede á información almacenada nun ficheiro (normalmente `tomcat-users.xml`).

A súa localización depende do ámbito do que queiramos que controle a autenticación e autorización:

- Engine. Todo o servidor. Debe estar definida en `server.xml` dentro do elemento `<Engine>`.
- Host. Toda o servidor virtual. Debe estar definida no arquivo de configuración `server.xml` dentro do elemento `<Host>` que se corresponda co sitio virtual ao que queremos que se aplique.
- Context. Unha aplicación concreta. Debe estar definida no ficheiro `context.xml` (en `WebContent/META-INF`) da aplicación correspondente, dentro do elemento `<Context>`.

A información de usuarios e roles está almacenada nun ficheiro que se carga en memoria ao iniciar Tomcat, por defecto, `tomcat-users.xml`.

1.2 Configuración

- Definir o ficheiro (por defecto `tomcat-users.xml`) cos usuario e roles.
  - Definición de roles:

```
<role rolename="nomeDoRol"/>
```

  - Definición de usuarios pertencentes a un rol:

```
<user username="nomeUsuario" password="contrasinal" roles="rol1 rol2..."/>
```

- Configurar o Realm no ámbito que se considere más adecuado:

```
<Context>
  <Realm className="org.apache.catalina.realm.MemoryRealm"/>
</Context>
```

- Protexer o recurso (descritor de despregamento `web.xml` da aplicación).

```
<security-constraint>
```

```
        <web-resource-collection>
            <web-resource-name>ServletPrivado</web-resource-name>
            <url-pattern>/*</url-pattern>
        </web-resource-collection>
        <auth-constraint>
            <role-name>usuariosAutenticados</role-name>
        </auth-constraint>
    </security-constraint>
```

- Configurar o tipo de autenticación (no descritor de despregamento `web.xml` da aplicación).

```
<login-config>
    <auth-method>Basic</auth-method>
    <realm-name>Acceso á información</realm-name>
</login-config>
```

1.3 Autenticación e autorización

Nesta tarefa empregaremos a aplicación calculadora para permitir o acceso unicamente aos usuarios `usuario1` e `usuario2` que pertencen ao rol `usuarioscalculadora`.

Pasos a seguir

- Crearemos os usuarios e rol en Tomcat, engadindo ao ficheiro `tomcat-users.xml` as seguintes liñas:

```
  <role rolename=" usuarioscalculadora"/>
  <user username="usuario1" password="contrasinal" roles=" usuarioscalcu-
ladora "/>
  <user username="usuario2" password="contrasinal" roles=" usuarioscalcu-
ladora "/>
```

- Reiniciamos o servidor Tomcat:

```
sudo service tomcat8 restart
```

- Configuramos o Realm, para elo, dentro deste proxecto, creamos o ficheiro `META-INF/context.xml`, facendo clic dereito sobre `Web Content/META-INF` e escollendo New...→File e escribimos as seguintes liñas:

```
<Context>
  <Realm className="org.apache.catalina.realm.MemoryRealm"/>
</Context>
```

- Protexemos a aplicación co MemoryRealm, empregando autenticación BASIC, para o que editaremos o descritor de despregamento da aplicación web (`web.xml`) engadindo os seguintes elementos como fillos do elemento raíz `<web-app>`.

```
      <security-constraint>
            <web-resource-collection>
                  <web-resource-name>aplicacion Calculadora</web-resource-
name>
                  <url-pattern>/*</url-pattern>
            </web-resource-collection>
            <auth-constraint>
                  <role-name>usuarioscalculadora </role-name>
            </auth-constraint>
      </security-constraint>
      <login-config>
            <auth-method>BASIC</auth-method>
            <realm-name>Acceso a calculadora</realm-name>
      </login-config>
```

- Eliminamos a aplicación do servidor Tomcat (se xa a despregaramos anteriormente), creamos o ficheiro WAR e volvemos despregala empregando o método que nos resulte máis cómodo (Tomcat Managero ou despregamento manual).
- Comprobamos que a configuración foi a adecuada, accedendo desde o navegador da máquina cliente a `http://192.168.0.1:8080/Calculadora`. Comprobamos que é preciso introducir o usuario e contrasinal para acceder á aplicación.