The ESUP authentication layer

The ESUP authentication layer

Introduction

The ESUP authentication layer is a versatile authentication layer, to be accessed by many different clients (web browsers, operating systems, applications...) :

- Web browsers that may support only HTTP scheme (not WebDAV extensions) but redirections and HTTP basic authentication scheme (realms);
- Operating systems and system applications that may be fully WebDAV-compliant but do not implement redirections and/or form completion (and thus can not respond to SSO requests);
- Web applications that may be SSO-compliant but not always.

This versatility is achieved with a highly configurable authentication layer shown in figure 3, made up of an authentication router that chooses between three authentication filters:

- CAS authentication for web browsers and applications,
- LDAP authentication for operating systems,
- Trusted authentication for trusted applications (based on a secret shared between the application and the server).

The selection of a filter is performed by the router, depending on the agent (i.e. the type of the client: browser, application...), its localization (IP address), the target (virtual) server name and the configuration set by the administrators of the server.

Configuration

The router

This is probably the hardest think to configure. The configuration is defined in the **web.xml** file of the application. The different parameters values of the **web.xml** are defined in the **build.properties**.

Let's have a look at the configuration of the web.xml:

```
<filter>
```

General configuration

Filter name and class - you DO NOT have to modify these values

```
<filter-name>authenticationRouter</filter-name>
  <filter-class>org.esupportail.filter.authenticationRouter.AuthenticationRouter</filter-class>
```

Here is the **slide.authenticationRouter.filterList** which determines the filter order. In the example below the router will first try to match the LDAP filter criteria (defined after in the file) then the CAS filter... up to the UNAUTHENTICATED filter.

```
<init-param>
   <param-name>org.esupportail.filter.authenticationRouter.filterList</param-name>
   <param-value>LDAP CAS TRUSTED UNAUTHENTICATED</param-value>
  </init-param>
```

Now you have to configure the **slide.authenticationRouter.defaultAuthenticationFilter** that is the filter used by default if no filter are finally selected by the router (in other words if - for each filter - at least one criterion DOES NOT matches the request).

```
<init-param>
   <param-name>org.esupportail.filter.authenticationRouter.defaultAuthenticationFilter</param-name>
   <param-value>TRUSTED</param-value>
  </init-param>
```

The following parameter is important and will often be let to false. If false, then ONLY ONE filter will be used - the first one matching the request in the **slide.authenticationRouter.filterList**. If true then every filter matching the request will be used.
Imagine for example that the LDAP and TRUSTED criteria match the request, then the request will be first forwarded to the LDAP filter (for an LDAP authentication) and then to the TRUSTED filter (for a TRUSTED authentication) - and in this order !

```
<init-param>
   <param-name>org.esupportail.filter.authenticationRouter.enableCascading</param-name>
   <param-value>false</param-value>
  </init-param>
```

Selection criteria for each authentication filter

The following sections define selection criteria for each filter. There are 4 sections of 5 criteria whose names finish by an authentication filter name (LDAP - CAS - TRUSTED - UNAUTHENTICATED).

```
<!-- LDAP -->
  <init-param>
   <param-name>org.esupportail.filter.authenticationRouter.allowClientIPLDAP</param-name>
   <param-value></param-value>
  </init-param>
  <init-param>
   <param-name>org.esupportail.filter.authenticationRouter.useSecureRequestLDAP</param-name>
   <param-value></param-value>
  </init-param>
  <init-param>
   <param-name>org.esupportail.filter.authenticationRouter.agentLDAP</param-name>
   <param-value></param-value>
  </init-param>
  <init-param>
   <param-name>org.esupportail.filter.authenticationRouter.httpRequestParameterLDAP</param-name>
   <param-value></param-value>
  </init-param>
  <init-param>
   <param-name>org.esupportail.filter.authenticationRouter.destinationHostLDAP</param-name>
   <param-value></param-value>
  </init-param>
```

A filter is selected by the router if each criterion matches the request.

Let's have a look on each criterion in more details.

allowClientIP[FilterName] : if empty then there is no restriction else only requests with one of the given client IP adresses will be forwarded to the filter [FilterName].

```
<!-- TRUSTED -->
 <init-param>
   <param-name>org.esupportail.filter.authenticationRouter.allowClientIPTRUSTED</param-name>
   <param-value>129.20.129.12 129.20.129.13</param-value>
  </init-param>
```

useSecureRequest[FilterName] : if true then only HTTPS requests will be forwarded to the filter [FilterName].

```
<init-param>
   <param-name>org.esupportail.filter.authenticationRouter.useSecureRequestTRUSTED</param-name>
   <param-value>false</param-value>
  </init-param>
```

agent[FilterName] : if empty then there is no restriction else only request with one of the given client agents will be forwarded to the filter [FilterName]. The agent identifies the type of the client - mozilla, DAVFS... - *Regular
expressions are accepted*.

```
<init-param>
   <param-name>org.esupportail.filter.authenticationRouter.agentTRUSTED</param-name>
   <param-value>*mozilla*</param-value>
  </init-param>
```

httpRequestParameter[FilterName] : if empty then there is no restriction else only request with the given parameters will be forwarded to the given filter (here TRUSTED). *Regular expressions are
accepted*.

```
<init-param>
   <param-name>org.esupportail.filter.authenticationRouter.httpRequestParameterTRUSTED</param-name>
   <param-value>auth=trusted authentication=trusted mode*=*secure*</param-value>
  </init-param>
```

destinationHost[FilterName_] : if empty then there is no restriction else only request with the given destination hosts will be forwarded to the given filter (here TRUSTED). *Regular expressions are
accepted*.

```
<init-param>
   <param-name>org.esupportail.filter.authenticationRouter.destinationHostTRUSTED</param-name>
   <param-value>webdav-restricted.univ-rennes1.fr webdav-restricted2.univ-rennes1.fr *.univ-valenciennes.fr<
/param-value>
  </init-param>
```

The LDAP authentication filter

Processes an LDAP authentication.

```
<filter>
```

Filter name and class - you DO NOT have to modify these values

```
<filter-name>LDAP</filter-name>
  <filter-class>org.esupportail.filter.LDAPFilter.LDAPFilter</filter-class>
```

Let the following parameter to true.

```
<init-param>
   <param-name>org.esupportail.filter.LDAPFilter.useAuthenticationRouter</param-name>
   <param-value>true</param-value>
  </init-param>
```

LDAP directory URL's (the alternate URL is optionnal - usefull if the first directory does not work)

```
<init-param>
   <param-name>org.esupportail.filter.LDAPFilter.connectionURL</param-name>
   <param-value>ldap://myLdap.univ.fr:389</param-value>
  </init-param>
  <init-param>
   <param-name>org.esupportail.filter.LDAPFilter.alternateURL</param-name>
   <param-value>ldap://myLdap2.univ.fr:389</param-value>
  </init-param>
```

Bind type = searchbind or fastbind

- searchbind : The filter will first try to find the connected user, using the given **base DN**, **scope** and **filter** - and then will execute a bind request.
- fastbind : The filter will try to bind with the given **pattern**

```
<init-param>
   <param-name>org.esupportail.filter.LDAPFilter.bindType</param-name>
   <param-value>SEARCHBIND</param-value> <!-- FASTBIND -->
  </init-param>
```

fastBindUserPattern : Pattern used to build a DN to bind. The syntax is uniqueAttributeEqualsToLogin={0},baseDN

```
<init-param>
   <param-name>org.esupportail.filter.LDAPFilter.fastBindUserPattern</param-name>
   <param-value>uid=\{0\},ou=people,dc=univ,dc=fr</param-value>
  </init-param>
```

The following attributes are optionnals and specify the credential to connect to the LDAP if needed.

```
<init-param>
<param-name>org.esupportail.filter.LDAPFilter.searchBindConnectionName</param-name>
<param-value>LDAPMaster</param-value>
</init-param>
<init-param>
<param-name>org.esupportail.filter.LDAPFilter.searchBindConnectionPassword</param-name>
<param-value>whatACoolWebDAVServer\!</param-value>
</init-param>
```

The tree last atributes are classical LDAP configuration parameters - you won't have any difficulties to understand them. 😉

```
<init-param>
<param-name>org.esupportail.filter.LDAPFilter.searchBindBaseDN</param-name>
<param-value>ou=people,dc=univ,dc=fr</param-value>
</init-param>
<init-param>
<param-name>org.esupportail.filter.LDAPFilter.searchBindScope</param-name>
<param-value>SUBTREE_SCOPE</param-value> <\!-\- SUBTREE_SCOPE \| ONELEVEL_SCOPE \| OBJECT_SCOPE \-->
</init-param>
<init-param>
<param-name>org.esupportail.filter.LDAPFilter.searchBindFilter</param-name>
<param-value>uid={0}
</param-value>
</init-param>
</filter>
```

The TRUSTED authentication filter

Processes a TRUSTED authentication. The easiest filter to configure.

```
<filter>
```

Filter name and class - you DO NOT have to modify these values

```
<filter-name>TRUSTED</filter-name>
<filter-class>org.esupportail.filter.trustedFilter.TrustedFilter</filter-class>
```

Let the following parameter to true.

```
<init-param>
<param-name>org.esupportail.filter.trustedFilter.useAuthenticationRouter</param-name>
<param-value>true</param-value>
</init-param>
```

Trusted password

```
<init-param>
<param-name>org.esupportail.filter.trustedFilter.trustedPassword</param-name>
<param-value>XXXXXXXXXX</param-value>
</init-param>
```

Optionnal allowed user list - Let it empty for no user restriction.

```
<init-param>
<param-name>org.esupportail.filter.trustedFilter.trustedUsers</param-name>
<param-value>tbellemb:bourges:masterYoda</param-value>
</init-param>
</filter>
```

The UNAUTHENTICATED authentication filter

There is no entry for this filter in the web.xml file because this filter... does not exist !

If the authentication router selects this filter then the request will be directed to a non existing filter - the consequence is that the user name will not be included in the request going to the server.

The SHIB authentication filter (only on the v5.0 and upper)

Processes an Shibboleth authentication.

```
<filter>
```

Filter name and class - you DO NOT have to modify these values

```
<filter-name>SHIB</filter-name>
<filter-class>org.esupportail.filter.shibFilter.ShibFilter</filter-class>
```

Let the following parameter to true.

```
<init-param>
<param-name>org.esupportail.filter.shibFilter.useAuthenticationRouter</param-name>
<param-value>true</param-value>
</init-param>
```

The **slide.shibFilter.localsDomains** attribute is a regular expression which describe de locals domains

```
<init-param>
<param-name>org.esupportail.filter.ShibFilter.localsDomains</param-name>
<param-value>.*@(univ-rennes1\|ensc-rennes\|sciencespo-rennes\|eleves.ensc-rennes\|etudiant.sciencespo-
rennes\|etudiant.univ-rennes1).fr</param-value>
</init-param>
```

The value of the **slide.shibFilter.localsDomainsAttribute** attribute is the attribute name which will pick up the remote user

```
<init-param>
<param-name>org.esupportail.filter.ShibFilter.localsDomainsAttribute</param-name>
<param-value>REMOTE_USER2</param-value>
</init-param>
```

The **slide.shibFilter.remoteUserAttribute** attribute is the name of the attribute which have the value that will be used to define the remote user value

```
<init-param>
<param-name>org.esupportail.filter.ShibFilter.remoteUserAttribute</param-name>
<param-value>REMOTE_USER2</param-value>
</init-param>
```

The **slide.shibFilter.FormatOutOfRemoteUser** attribute is a regular expression which indicate de format of the value to the remote user

```
<init-param>
<param-name>org.esupportail.filter.ShibFilter.FormatOutOfRemoteUser</param-name>
<param-value>(.*)@.*:</param-value>
</init-param>
```

The **slide.shibFilter.RegexpSeparator** attribute is a separator used in the FormatOutOfRemoteUser regular expression

```
<init-param>
<param-name>org.esupportail.filter.ShibFilter.RegexpSeparator</param-name>
<param-value>:</param-value>
</init-param>
```

The *slide.shibFilter.remoteUserAttributeOut
*attribute is the name of the attribute that store the remote user value

```
<init-param>
<param-name>org.esupportail.filter.ShibFilter.remoteUserAttributeOut</param-name>
<param-value>REMOTE_USER</param-value>
</init-param>
```

The parameter **slide.shibFilter.remoteUserAttributeOutSessionOrHeader** allow to choose between the session attributes and the request attributes

```
<init-param>
<param-name>org.esupportail.filter.ShibFilter.remoteUserAttributeOutSessionOrHeader</param-name>
<param-value>session</param-value>
</init-param>
```

The **slide.shibFilter.shibAttributePrefix** attribute is the prefix of the shibboleth attributes

```
<init-param>
<param-name>org.esupportail.filter.ShibFilter.shibAttributePrefix</param-name>
<param-value>Shib</param-value>
</init-param>
```

The following parameter indicate if we put the shibboleth attributes in the session or not

```
<init-param>
<param-name>org.esupportail.filter.ShibFilter.shibAttributesInSession</param-name>
<param-value>true</param-value>
</init-param>
```

The RedirectFilter (only on the v5.1 and upper)

The RedirectFilter is a filter which enable to redirect an url into another.

```
<filter>
```

Filter name and class - you DO NOT have to modify these values

```
<filter-name>REDIRECT</filter-name>
<filter-class>org.esupportail.filter.redirectFilter.RedirectFilter</filter-class>
```

The **slide.redirectFilter.DestinationHostTrigger** attribute is the host name on which the RedirectFilter must be executed

```
<init-param>
<param-name>org.esupportail.filter.redirectFilter.DestinationHostTrigger</param-name>
<param-value>[slide.redirectFilter.DestinationHostTrigger]</param-value>
</init-param>
```

The slide.redirectFilter.DestinationHost attribute is the host name which must used for an indentification

```
<init-param>
<param-name>org.esupportail.filter.redirectFilter.DestinationHost</param-name>
<param-value>[slide.redirectFilter.DestinationHost]</param-value>
</init-param>
```