Tomcat SingleSignOn 検証

目的

・Tomcat に付属の SingleSignOn 機能を検証する

環境構築

Windows

・インストールパラメータ

項目	内容
Java インストール先	C:\jdk1.5.0_12
tomcat インストール先	D:\tomcat5b
tomcat SHUTDOWN ポート	28005
tomcat HTTP ポート	28080
tomcat AJP13 ポート	28009
ログインユーザー ID	tomcat
ログインパスワード	tomcat
確認用 web アプリケーション 1	http://localhost:28080/servlets-examples/
確認用 web アプリケーション 2	http://localhost:28080/servlets-examples2/
ログイン用フォーム	http://localhost:28080 /servlets-examples/login_form.jsp

Java 確認

・コマンドプロンプトで set コマンドを実行
・JAVA_HOME 環境変数が設定されていることを確認 , 例 : C:\jdk1.5.0_12
・PATH 環境変数に %JAVA_HOME%\bin が含まれることを確認 , 例 : C:\jdk1.5.0_12\bin
・java -version コマンド確認

```
D:\>java -version
java version "1.5.0_12"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.5.0_12-b04)
Java HotSpot(TM) Client VM (build 1.5.0_12-b04, mixed mode, sharing)
```

Tomcat インストール

■ D:\tomcat5b にインストール

```
D:\> dir d:\@user\soft\Java\apache-tomcat-5.5.25.zip
...( 中略 )..
2007/09/25  14:16         6,898,457 apache-tomcat-5.5.25.zip
...( 中略 )..
D:\> unzip -x d:\@user\soft\Java\apache-tomcat-5.5.25.zip
...( 中略 )..
D:\>ren apache-tomcat-5.5.25 tomcat5b
```

tomcat5b 設定

・bin\startup.bat, bin\shutdown.bat に CATALINA_HOME 設定追加

```
D:\> notepad D:\tomcat5b\bin\startup.bat
D:\> notepad D:\tomcat5b\bin\shutdown.bat
```

```
set CATALINA_HOME=D:\tomcat5b
```

・conf\server.xml 編集

```
D:\> cd \tomcat5b\conf
D:\tomcat5b\conf> copy server.xml server.xml.orig
D:\tomcat5b\conf> notepad server.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<Server port="28005" shutdown="SHUTDOWN">
 <GlobalNamingResources>
   <Resource name="UserDatabase" auth="Container"
             type="org.apache.catalina.UserDatabase"
      description="User database that can be updated and saved"
          factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
         pathname="conf/tomcat-users.xml" />
 </GlobalNamingResources>
 <Service name="Catalina">
   <Connector port="28080" maxHttpHeaderSize="8192"
              maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
              enableLookups="false" redirectPort="8443" acceptCount="100"
              connectionTimeout="20000" disableUploadTimeout="true" />
   <Connector port="28009"
              enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />
   <Engine name="Catalina" defaultHost="localhost" jvmRoute="tomcat5b">
     <Realm className="org.apache.catalina.realm.UserDatabaseRealm"
       resourceName="UserDatabase"/>
     <Host name="localhost" appBase="webapps"
      unpackWARs="true" autoDeploy="true"
      xmlValidation="false" xmlNamespaceAware="false">
     </Host>
   </Engine>
 </Service>
</Server>
```

起動

```
D:\tomcat5b\conf> cd \
D:\> \tomcat5b\bin\startup.bat
```

・起動ログ確認

```
2007/09/25 15:25:44 org.apache.catalina.startup.Catalina start
情報 : Server startup in 15141 ms
```

・起動ポート確認

```
D:\>netstat -an | grep LISTENING | grep 280
 TCP    0.0.0.0:28009          0.0.0.0:0              LISTENING
 TCP    0.0.0.0:28080          0.0.0.0:0              LISTENING
 TCP    127.0.0.1:28005        0.0.0.0:0              LISTENING
```

・アプリケーション動作確認 http://localhost:28080/servlets-examples/

停止

```
D:\> \tomcat5b\bin\shutdown.bat
```

Web アプリケーション設定

■必要のない web アプリケーションの削除

・webapps\balancer
・webapps\jsp-examples
・webapps\ROOT
・webapps\tomcat-docs
・webapps\webdav
・conf\Catalina\localhost\manager.xml
・conf\Catalina\localhost\host-manager.xml

Linux

・インストール先 CATALINA_HOME が /usr/local/tomcat5b
・文字コード euc-jp が作業しやすいが、必須でない。UTF-8 がよい。
・その他は修正なし

検証

ログイン

■ conf\tomcat-users.xml 修正

・役割 (role)「tomcat」が存在すること

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

・id/pw=tomcat/tomcat でログインすると役割 (role)「tomcat」を持つように。

```
<user username="tomcat" password="tomcat" roles="tomcat"/>
```

■ webapps\servlets-examples\login_form.jsp 作成

```
<%@page pageEncoding="Windows-31J" contentType="text/html; charset=Windows-31J" %>
<html>
  <head>
    <title>login_form</title>
  </head>
  <body>
    <form method="POST" action="j_security_check">
      <p>id:<input type="text" name="j_username"></p>
      <p>pw:<input type="password" name="j_password"></p>
      <p><input type="submit" value=" ログイン "></p>
    </form>
  </body>
</html>
```

■ webapps\servlets-examples\login_error.jsp 作成

```
<%@page pageEncoding="Windows-31J" contentType="text/html; charset=Windows-31J" %>
<html>
  <head>
```

```
    <title>login_error</title>
  </head>
  <body>
    login error!!
  </body>
</html>
```

■ webapps\servlets-examples\show_user.jsp **作成**

```
<%@page pageEncoding="Windows-31J" contentType="text/html; charset=Windows-31J" %>
<html>
  <head>
    <title>login_success!!</title>
  </head>
  <body>
    login success!!
    <p>request:<%=request%></p>
    <p>request.getRemoteHost(): <%=request.getRemoteHost()%></p>
    <p>request.getContextPath(): <%=request.getContextPath()%></p>
    <p>request.getRemoteUser(): <%=request.getRemoteUser()%></p>
    <p>session.getId(): <%=session.getId()%></p>
    <p><a href="logout.jsp">logout</a></p>
  </body>
</html>
```

■ webapps\servlets-examples\logout.jsp **作成**

```
<%@page pageEncoding="Windows-31J" contentType="text/html; charset=Windows-31J" %>
<html>
  <head>
    <title>logout</title>
  </head>
  <body>
    <% session.invalidate(); %>
    logout!!
    <a href="show_user.jsp"> ユーザー情報表示 ( 要ログイン )</a>
  </body>
</html>
```

■ webapps/servlets-examples/WEB-INF/web.xml **追加設定**

```
<security-constraint>
  <web-resource-collection>
  <web-resource-name>edi</web-resource-name>
  <url-pattern>/*</url-pattern>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>tomcat</role-name>
  </auth-constraint>
</security-constraint>


<login-config>
  <auth-method>FORM</auth-method>
  <form-login-config>
    <form-login-page>/login_form.jsp</form-login-page>
    <form-error-page>/login_error.jsp</form-error-page>
  </form-login-config>
</login-config>


<security-role>
  <role-name>tomcat</role-name>
</security-role>
```

ログアウト

・basic/digest ではログアウトできない。

・form-based では session.invalidate() でログアウトする
・SSL+client 証明書では？

権限の確認

SingleSignOn 確認

・conf/server.xml の <host> に SingleSignOn 設定を追加

```
<Valve className="org.apache.catalina.authenticator.SingleSignOn" />
```

■ SingleSignOn 設定がない場合

1.http://localhost:28080/servlets-examples/show_user.jsp
・ログインが必要
2.http://localhost:28080/servlets-examples/show_user.jsp
・別途ログインが必要

■ SingleSignOn 設定がある場合

1.http://localhost:28080/servlets-examples/show_user.jsp
・ログインが必要
・request.getRemoteUser(): tomcat
・session.getId(): DC8A5622659C179B4E0264507B6BAD7F
2.http://localhost:28080/servlets-examples/show_user.jsp
・ログインの必要なし
・request.getRemoteUser(): tomcat
・session.getId(): 99E4191E17B140C8BDFE2A12CAB94CF5
・Web アプリケーション間での認証の引継ぎが発生している

■セッションタイムアウト時

・片方のアプリケーションでセッションがタイムアウトした場合

JDBCDataSource

今後

既存アプリケーションの再構築

■認証

■共通コードの分離

■個別 Web アプリケーションのプロジェクト分離

・EDI 基盤 (ログイン・ユーザー情報・パスワードリマインダ)
・webedi
・経理
・デジ原
・検品

■新規アプリケーションの構築時の指針作成

・作成方針・利用方針
・レビュー
・管理体制
　・CVS 手順
　・要件定義・開発・テスト・リリース

JDBCStore

・セッションをサーバー間で共有
・Web アプリケーション間では共有できない。
　・web アプリケーションが発行する Cookie は web アプリケーションに限定されている
・SingleSignOn 機能では別の cookie が発行される

参考

■ tomcat-4.0 サーバ設定ドキュメント和訳 / Realm コンポーネント

・http://www.jajakarta.org/tomcat/tomcat3.2-4.0/tomcat-4.0b5/src-ja/catalina/docs/config/realm.html

"" 一旦ユーザーがうまく認証されるならば、HttpServletRequest インタフェースの以下のメソッドは役に立つ値を返すことになります:""getRemoteUser() - 認証されたユーザーのユーザー名を返すことになります。

・tomcat-5.5 ドキュメントでは該当する文書なし。英文でも該当なし。

■ Java Servlet Specification 2.4

・Java サーブレット仕様書 2.4
・http://java.sun.com/products/servlet/download.html より PDF ダウンロード