CAS配置

一、去掉安全认证：

1、deployerConfigContext.xml配置，增加p:requireSecure=”false”属性：

|  |
| --- |
| <bean id="proxyAuthenticationHandler"  class="org.jasig.cas.authentication.handler.support.HttpBasedServiceCredentialsAuthenticationHandler" p:httpClient-ref="httpClient" p:requireSecure="false"/> |

2、修改ticketGrantingTicketCookieGenerator.xml配置，

修改参数p:cookieSecure=”false”（关闭https协议）,p:cookieMaxAge=”3600”（cookie生命周期，-1不存储cookie，3600存储1小时）

|  |
| --- |
| <bean id="ticketGrantingTicketCookieGenerator" class="org.jasig.cas.web.support.CookieRetrievingCookieGenerator"        p:cookieSecure="false"        p:cookieMaxAge="3600"        p:cookieName="CASTGC"        p:cookiePath="/cas" /> |

3、修改warnCookieGenerator.xml配置，修改p:cookieSecure=”false”,p:cookieMaxAge=”3600”

|  |
| --- |
| <bean id="warnCookieGenerator" class="org.jasig.cas.web.support.CookieRetrievingCookieGenerator"  p:cookieSecure="false"  p:cookieMaxAge="3600"  p:cookieName="CASPRIVACY"  p:cookiePath="/cas" /> |

二、cas-servlet.xml,单点登出自动跳转页面：,

修改p:followServiceRedirects=”${cas.logout.followServiceRedirects:true}”}

|  |
| --- |
| <bean id="logoutAction" class="org.jasig.cas.web.flow.LogoutAction"  p:servicesManager-ref="servicesManager"  p:followServiceRedirects="${cas.logout.followServiceRedirects:true}"/> |

三、配置数据源deployerConfigContext.xml：

1、添加如下配置

|  |
| --- |
| <bean id="dataSource" class="com.mchange.v2.c3p0.ComboPooledDataSource"  p:driverClass="com.mysql.jdbc.Driver"  p:jdbcUrl="jdbc:mysql://127.0.0.1:3306/pinyougoudb?characterEncoding=utf8"  p:user="root"  p:password="123456" />  <bean id="passwordEncoder"  class="org.jasig.cas.authentication.handler.DefaultPasswordEncoder"  c:encodingAlgorithm="MD5"  p:characterEncoding="UTF-8" />  <bean id="dbAuthHandler"  class="org.jasig.cas.adaptors.jdbc.QueryDatabaseAuthenticationHandler"  p:dataSource-ref="dataSource"  p:sql="select password from tb\_user where username = ?"  p:passwordEncoder-ref="passwordEncoder"/> |

2、修改key-ref改为dbAuthHandler

C:\Users\dell\AppData\Local\Temp\1544420722(1).png

3、引入jar包，放到cas的lib中：

c3p0-\*.jar

cas-server-support-jdbc-\*.jar

mysql-connector-java-\*.jar

四、配置web.xml文件

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?> <web-app xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  xmlns="http://java.sun.com/xml/ns/javaee"  xsi:schemaLocation="http://java.sun.com/xml/ns/javaee http://java.sun.com/xml/ns/javaee/web-app\_2\_5.xsd"  version="2.5">     <!-- ======================== 单点登录开始 ======================== -->   <!-- 用于单点退出，该过滤器用于实现单点登出功能，可选配置 -->   <listener>   <listener-class>org.jasig.cas.client.session.SingleSignOutHttpSessionListener</listener-class>   </listener>     <!-- 该过滤器用于实现单点登出功能，可选配置。 -->   <filter>   <filter-name>CAS Single Sign Out Filter</filter-name>   <filter-class>org.jasig.cas.client.session.SingleSignOutFilter</filter-class>   </filter>   <filter-mapping>   <filter-name>CAS Single Sign Out Filter</filter-name>   <url-pattern>/\*</url-pattern>   </filter-mapping>     <!-- 该过滤器负责用户的认证工作，必须启用它 -->   <filter>   <filter-name>CASFilter</filter-name>   <filter-class>org.jasig.cas.client.authentication.AuthenticationFilter</filter-class>   <init-param>   <param-name>casServerLoginUrl</param-name><!-- CAS服务端登录路径-->  <param-value>http://localhost:8080/cas/login</param-value><!--告诉客户端，服务端的跳转地址-->  <!--这里的server是服务端的IP -->   </init-param>   <init-param>   <param-name>serverName</param-name>   <param-value>http://localhost:9001</param-value><!--当前应用的地址-->  </init-param>   </filter>   <filter-mapping>   <filter-name>CASFilter</filter-name>   <url-pattern>/\*</url-pattern>   </filter-mapping>     <!-- 该过滤器负责对Ticket的校验工作，必须启用它 -->   <filter>   <filter-name>CAS Validation Filter</filter-name>   <filter-class>org.jasig.cas.client.validation.Cas20ProxyReceivingTicketValidationFilter</filter-class>  <init-param>   <param-name>casServerUrlPrefix</param-name>   <param-value>http://localhost:8080/cas</param-value><!--CAS服务端地址，票据校验得知道地址-->  </init-param>   <init-param>   <param-name>serverName</param-name>   <param-value>http://localhost:9001</param-value><!--当前应用的地址-->  </init-param>   </filter>   <filter-mapping>   <filter-name>CAS Validation Filter</filter-name>   <url-pattern>/\*</url-pattern>   </filter-mapping>     <!-- 该过滤器负责实现HttpServletRequest请求的包裹， 比如允许开发者通过HttpServletRequest的getRemoteUser()方法获得SSO登录用户的登录名，可选配置。 -->   <filter>   <filter-name>CAS HttpServletRequest Wrapper Filter</filter-name>   <filter-class>org.jasig.cas.client.util.HttpServletRequestWrapperFilter</filter-class>  </filter>   <filter-mapping>   <filter-name>CAS HttpServletRequest Wrapper Filter</filter-name>   <url-pattern>/\*</url-pattern>   </filter-mapping>     <!-- 该过滤器使得开发者可以通过org.jasig.cas.client.util.AssertionHolder来获取用户的登录名。 比如AssertionHolder.getAssertion().getPrincipal().getName()。 -->   <filter>   <filter-name>CAS Assertion Thread Local Filter</filter-name>   <filter-class>org.jasig.cas.client.util.AssertionThreadLocalFilter</filter-class>   </filter>   <filter-mapping>   <filter-name>CAS Assertion Thread Local Filter</filter-name>   <url-pattern>/\*</url-pattern>   </filter-mapping>     <!-- ======================== 单点登录结束 ======================== -->      </web-app> |

五、登录页面改造：

1、替换登录页面，cas/WEB-INF/view/jsp/default/ui/casLoginView.jsp

2、将登录页面的内容修改成自己需要的东西

3、将css、js等文件粘贴到cas/WEB-INF/

六、修改/WEB-INF/classes/messages\_zh\_CN，

1、增加

authenticationFailure.AccountNotFoundException=\u7528\u6237\u540D\u6216\u5BC6\u7801\u9519\u8BEF.（用户名或密码错误）

authenticationFailure.FailedLoginException=\u7528\u6237\u540D\u6216\u5BC6\u7801\u9519\u8BEF.

2、修改cas-servlet.xml：

p:defaultLocale=”en”改为p:defaultLocale=”zh\_CN”

|  |
| --- |
| <bean id="localeResolver" class="org.springframework.web.servlet.i18n.CookieLocaleResolver" p:defaultLocale="en" /> |