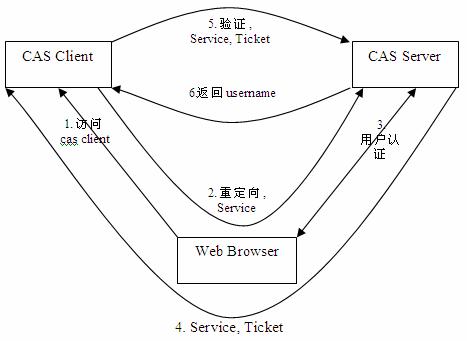
CAS的过程：



WebBrowser:代表客户

CAS Client:代表公司的产品

CAS Server:代表单点登录服务器

1 2 3 4 5 6代表执行的步骤

首先用户访问一个公司产品例如教研平台(CAS Client)，首次访问[1]，没登录，重定向到单点登录服务器进行登录[2]，登录后, CAS Server生成一个Ticket,在服务器上缓存起来，并在客户端生成cookie[3], 转向到教研[4], 教研去服务器上验证[5], 得到用户信息[6]。

由于在服务器端保存了一份Service Ticket(ST), CAS应该实现了跨域，IP的单点登录。

客户端浏览器设置的是 Ticket Granted Cookie（TGC），

CAS Server 的服务器需要支持 SSL 协议

打开客户端client配置web.xml中，关于服务器有2个地方配置，同时对应的产品的名称也有两份。在此，大胆推测，对错先不管：

CAS-Authentication-Filter 这个Fillter 是 关于 1 2 3 4 这几步的配置，即关于登录的。

CAS-Validation-Filter这个Fillter 是 关于 5 6 这两步的配置，即关于验证的。

1 2 3 4 与客户有关，5 6 是产品和服务器，是服务器与服务器的关系。

鞍山的服务器有个毛病：不能访问自己的外网地址。如果，1234[CAS-Authentication-Filter]配置外网单点登录地址，56[CAS-Validation-Filter]配置内网单点登录地址，是否就解决了这个问题？？？？ 需要验证下。

是否不用HTTPS(SSL)也可以使用CAS单点登录？修改一下（不一定好使）：

/WEB-INF/deployerConfigContext.xml

找到

<bean class="org.jasig.cas.authentication.handler.support.HttpBasedServiceCredentialsAuthenticationHandler"

p:httpClient-ref="httpClient"/>

修改为：

<bean class="org.jasig.cas.authentication.handler.support.HttpBasedServiceCredentialsAuthenticationHandler"

p:httpClient-ref="httpClient" p:requireSecure="false"/>

增加参数p:requireSecure="false"，是否需要安全验证，即HTTPS，false为不采用,我们目前不采用HTTPS

需要注意：WEB-INF\spring-configuration\ticketGrantingTicketCookieGenerator.xml这个文件中ticketGrantingTicketCookieGenerator这个bean中

参数p:cookieSecure="true"，同理为HTTPS验证相关，TRUE为采用HTTPS验证，与deployerConfigContext.xml的参数保持一致，这里也修改为false了

<bean id="ticketGrantingTicketCookieGenerator" class="org.jasig.cas.web.support.CookieRetrievingCookieGenerator"

p:cookieSecure="false"

p:cookieMaxAge="-1"

p:cookieName="CASTGC"

p:cookiePath="/cas" />

服务器配置修改：

我们用的是usermgr3 需要把服务器的usermgr3/WebContent/WEB-INF/cas.properties修改陈usermgr3：

server.prefix=${server.name}/usermgr3

CAS中几个时间的设置:

**1）TGT时间：**

在ticketExpirationPolicies.xml中，

<bean id="grantingTicketExpirationPolicy" class="org.jasig.cas.ticket.support.TimeoutExpirationPolicy">

<!-- This argument is the time a ticket can exist before its considered expired.  -->

<constructor-arg

index="0"

value="7200000" />

</bean>

这里进行设置的时间是TGT(ticket granting ticket)的时间，如果TGT时间到期，则需要进行重新登录。这里时间单位是毫秒，默认是两小时。

如果进行了rememberMe配置，则是在

<bean id="grantingTicketExpirationPolicy" class="org.jasig.cas.ticket.support.RememberMeDelegatingExpirationPolicy">  
   
 <!-- 一般情况下的 cas session 实效时间 -->  
 <property name="sessionExpirationPolicy">  
 <bean class="org.jasig.cas.ticket.support.TimeoutExpirationPolicy">  
 <constructor-arg index="0" value="60000" />  
 </bean>  
 </property>  
 <!-- 全天免登录 情况下 cas session的实效时间 -->  
 <property name="rememberMeExpirationPolicy">  
 <bean class="org.jasig.cas.ticket.support.TimeoutExpirationPolicy">  
 <constructor-arg index="0" value="1209600000" />  
 </bean>  
 </property>  
</bean>

中的sessionExpirationPolicy进行配置。

**2）rememberMe时间（记住登录状态时间）**

在上面的rememberMeExpirationPolicy中进行配置。时间单位是毫秒。然后在ticketGrantingTicketCookieGenerator.xml中的

<bean id="ticketGrantingTicketCookieGenerator" class="org.jasig.cas.web.support.CookieRetrievingCookieGenerator"  
 p:cookieSecure="false"  
 p:cookieMaxAge="-1"  
 p:cookieName="CASTGC"  
 p:cookiePath="/cas"   
 p:rememberMeMaxAge="1209600"/>

p:rememberMeMaxAge进行配置，两者时间保持一致，注意这里的时间单位是秒。

CAS通过用户名与ip限制密码输入错误次数:

http://blog.csdn.net/laigood12345/article/details/7488697

现在客户端client的配置可以不输入serverName这个配置。没有这个配置，会支持IP或域名或内网或外网访问教研。

现在需要修改client代码：先增加两个方法

提供getUserCounts（），返回用户数量 ，为了比较许可证里面的用户数

提供saveNewBaseUser（user），保存用户

http://www.jarvana.com/jarvana/view/org/jasig/cas/client/cas-client-core/3.2.1/cas-client-core-3.2.1-javadoc.jar!/index.html

CAS 登录处理主要模块(类):   
              a. Credentials  用于存储用户登录认证信息接口。   
                  其默认实现类：org.jasig.cas.authentication.principal.UsernamePasswordCredentials   
  
              b. CentralAuthenticationService 用于生成 ST(Service Ticket) 和  TGT(TicketGrantingTicket)的认证服务类。   
                  其默认实现类： org.jasig.cas.CentralAuthenticationServiceImpl   
  
              c. CookieRetrievingCookieGenerator 用于将TGT添加至Cookie及对Cookie进行管理。