0 软件环境

|  |
| --- |
| jdk 1.6.38  tomcat 7  eclipse Helios  cas-server-3.5.2  cas-client-3.2.1  win7 x64  注意：环境变量设置，及eclipse中jre install 设置  C:\Users\Administrator>echo %JAVA\_HOME%  E:\Program Files\Java\jdk1.6.0\_38  C:\Users\Administrator>echo %CLASSPATH%  .;E:\Program Files\Java\jdk1.6.0\_38\lib\dt.jar; |

1 下载 cas-server cas-client

|  |
| --- |
| 服务端下载地址 : http://downloads.jasig.org/cas-clients/  客户端下载地址 : http://downloads.jasig.org/cas/ |

简化的配置

|  |
| --- |
| #创建目录,进入目录  mkdir /neusoft/keys  #生成证书  keytool -genkey -alias ec -keyalg RSA -keystore ec.keystore  #导出证书  keytool -export -file ec.crt -keystore ec.keystore -storepass Sa\*963.-+ -alias ec  #把证书导入到客户端JDK中  keytool -import -v -trustcacerts -storepass Sa\*963.-+ -alias ec -file ec.crt -keystore "$JAVA\_HOME/jre/lib/security/cacerts"  #异常情况   keytool错误： java.io.IOException: Keystore was tampered with, or password was incorrect  #解决方法是，把%JAVA\_HOME%\lib\security下的cacerts文件备份后删除掉，在执行.  #文件目录没有权限 请切换root用户执行  #配置服务端 修改%TOMCAT\_HOME%\conf\server.xml文件  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"                 maxThreads="150" scheme="https" secure="true"                 clientAuth="false" sslProtocol="TLS"                 keystoreFile="/neusoft/keys/eckey"  <!--在2.1中生成的证书的位置-->                 keystorePass="Sa\*963.-+"/>        <!--在2.1中设置的密码-->  # 启动服务、验证SSL配置是否成功  http://yourhost:8443/cas |

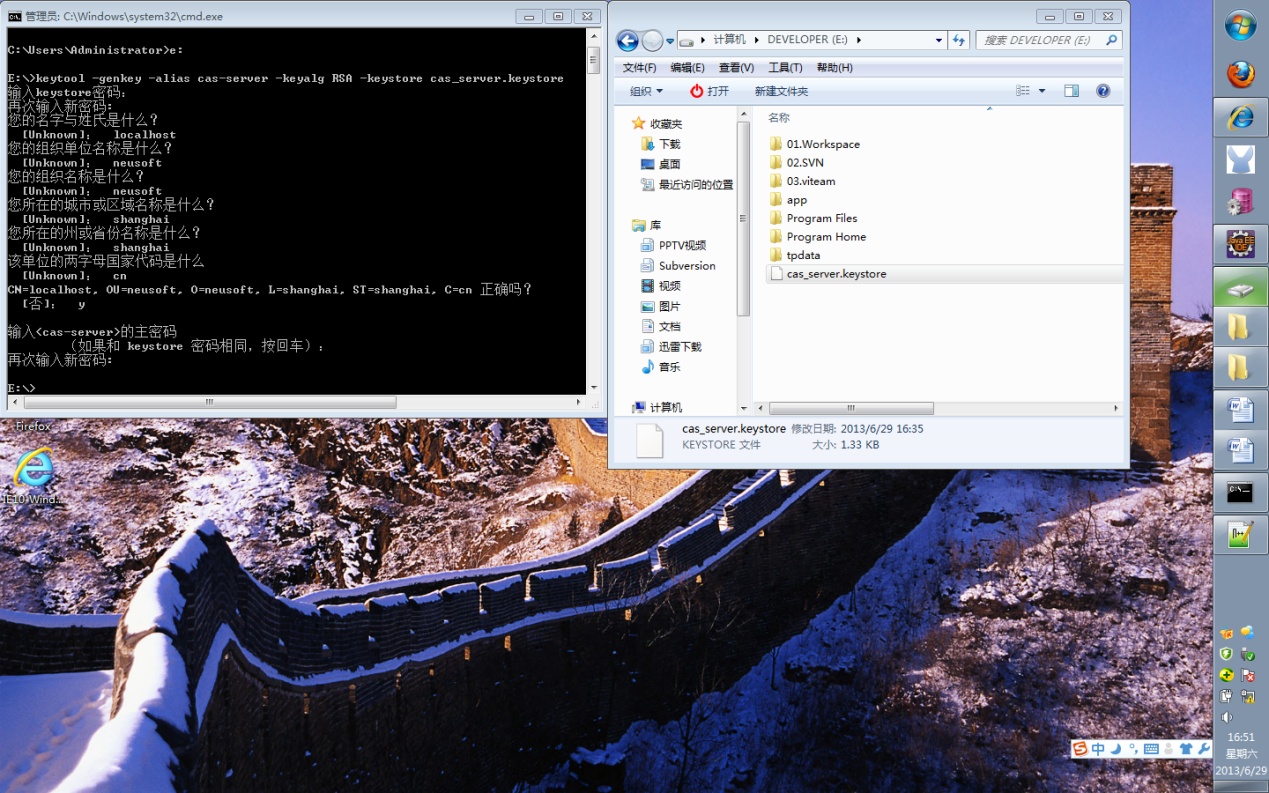
详细配置说明

2 解压：cas-client-3.2.1-release.zip cas-server-3.5.2-release.zip

|  |
| --- |
| 将\cas-server-3.5.2\modules\cas-server-webapp-3.5.2.war 改名为cas.war 放入tomcat webapps目录中发布  为了不改变tomcat原来的文件。我选在eclipse中配置tomcat  1、打开eclipsetomcat配置界面，将tomcat server locations选择为第三项  Server Path设置为：E:\Program Home\tomcat deploy  Deploy path 设置为： webapps  这样就可以在eclipse中配置 tomcat server.xml |

3 使用JDK包中的keytool工具创建证书文件

|  |
| --- |
| 打开cmd 键入E: 进入到E盘,输入下行命令 创建证书  注意： 证书的别名使用 -alias参数设置为：cas-server  E:\>keytool -genkey -alias cas-server -keyalg RSA -keystore cas\_server.keystore  输入keystore密码：123456  再次输入新密码: 123456  您的名字与姓氏是什么？  [Unknown]： localhost 【关键设置 设置域名 其他随便输入】  您的组织单位名称是什么？  [Unknown]： neusoft  您的组织名称是什么？  [Unknown]： neusoft  您所在的城市或区域名称是什么？  [Unknown]： shanghai  您所在的州或省份名称是什么？  [Unknown]： shanghai  该单位的两字母国家代码是什么  [Unknown]： cn  CN=localhost, OU=neusoft, O=neusoft, L=shanghai, ST=shanghai, C=cn 正确吗？  [否]： y  输入<cas-server>的主密码 123456  （如果和 keystore 密码相同，按回车）：  再次输入新密码: 123456  【执行完成后 会在E盘创建证书文件 cas\_server.keystore】 |



4 配置tomcat SSL协议

在tomcat发布文件夹 E:\Program Home\tomcat deploy\ 创建文件夹 keystore 将cas\_server.keystore文件copy到目录中

|  |
| --- |
| 在eclipse server中配置 server.xml , 使tomcat支持SSL协议，将下面的配置考入server.xml文件中。  <Connector port=*"8443"* minSpareThreads=*"5"* maxSpareThreads=*"75"*  enableLookups=*"true"* disableUploadTimeout=*"true"* acceptCount=*"100"*  maxThreads=*"200"* scheme=*"https"* secure=*"true"* SSLEnabled=*"true"*  keystoreFile=*"keystore/cas\_server.keystore"* keystorePass=*"123456"*  clientAuth=*"false"* sslProtocol=*"TLS"* />  注意： keystorePass=”123456” 为创建证书的密码 |

从eclipse启动tomcat 验证 SSL协议 证书是否生效

测试Https。访问https://localhost:8443/，提示有不安全的证书，接受证书 至此SSL协议配置结束。

5 导出导入 密钥文件

打开cmd 进入E:

keystore的默认密码 是changeit

导出密钥文件

|  |
| --- |
| 使用证书cas-server.keystore导出密钥文件 cas\_erver.crt  注意：cas\_server.keystore证书的别名为：cas-server 密码为：123456  keytool -export -file cas\_server.crt -keystore cas\_server.keystore -storepass 123456 -alias cas-server |

将生成的cas\_server.crt导入到jre中

注意： tomcat使用的jre需要设置为%JAVA\_HOME%中的jre

|  |
| --- |
| 打开cmd,运行命令：  "%JAVA\_HOME%/bin/keytool" -import -v -trustcacerts -storepass changeit -alias cas-server -file E:\cas\_server.crt -keystore "%JAVA\_HOME%\jre\lib\security\cacerts"  所有者:CN=localhost, OU=neusoft, O=neusoft, L=shanghai, ST=shanghai, C=cn  签发人:CN=localhost, OU=neusoft, O=neusoft, L=shanghai, ST=shanghai, C=cn  序列号:51ce9c5c  有效期: Sat Jun 29 16:35:40 CST 2013 至Fri Sep 27 16:35:40 CST 2013  证书指纹:  MD5:E6:F7:38:DC:E5:BD:AE:45:51:31:35:22:C9:FD:61:B7  SHA1:30:F4:A2:29:A5:DB:3B:48:3E:28:7A:D0:6D:AD:89:F1:6D:2A:BA:EC  签名算法名称:SHA1withRSA  版本: 3  信任这个认证？ [否]： y  认证已添加至keystore中  [正在存储 E:\Program Files\Java\jdk1.6.0\_38\jre\lib\security\cacerts] |

|  |
| --- |
| 另外在这里我们介绍以下查看证书文件中证书的方法以及删除证书文件中证书的方法 ;  E:>  keytool -delete -alias cas-server -keystore "%JAVA\_HOME%/jre/lib/security/cacerts" -storepass changeit  keytool -delete -alias cas-server -storepass changeit  （注释： 清除系统中可能存在的名字为cas-server 的同名证书）  keytool -list -keystore "%JAVA\_HOME%/jre/lib/security/cacerts" -storepass changeit  查看这书  查看证书文件 :  (1). 查看证书文件 :server.keystore  keytool -list -keystore server.keystore -storepass changeit –alias server  (2). 查看证书文件 :cacerts  keytool -list -keystore cacerts -storepass changeit -alias server  ( 注意不指明别名查看的是证书文件中所有的证书 ; 指明别名 , 只查看别名为该名称的证书 )    删除证书文件中的别名为 seasky 的证书 : ( 删除证书的时候必须指明要删除证书的别名 )  keytool -delete -keystore server.keystore -storepass changeit -alias server  keytool -delete -keystore cacerts -storepass changeit -alias server  显示证书的详细信息 ==== >>> ( 也可以不指明证书别名 )  keytool -list -keystore server.keystore -storepass tiankong –alias server -v |

6 配置客户端 cas-client