增加 PostgreSQL 数据源，执行命令：

```
/subsystem=datasources/jdbc-driver=org.postgresql.Driver:add(driver-name=org.postgresql.Driver,driver-module-name=org.postgresql,driver-xa-datasource-class-name=org.postgresql.xa.PGXADataSource)
:reload
```

修复 WSDL 访问位置生成错误，执行命令：

```
/subsystem=webservices:write-attribute(name=wsdl-host, value=jbossws.undefined.host)
:reload
```

如果 HornetQ 启动有问题，使用 JAVA NIO 处理，执行命令：

```
/subsystem=messaging/hornetq-server=default:write-attribute(name=journal-type,value=NIO)
:reload
```

打开日志跟踪，执行命令：

```
/system-property=org.jboss.as.logging.per-deployment:add(value=false)
/subsystem=logging/logger=org.ejbca:add
/subsystem=logging/logger=org.ejbca:write-attribute(name=level, value=DEBUG)
/subsystem=logging/logger=org.cesecore:add
/subsystem=logging/logger=org.cesecore:write-attribute(name=level, value=DEBUG)
```

8. 配置 EJBCA 参数文件

在安装 EJBCA 服务前，需要进行相关参数配置，主要配置文件有 5 个：ejbca.properties、install.properties、cesecore.properties、web.properties、database.properties。

从%EJBCA_HOME%\conf 路径下，分别复制 5 个文件 ejbca.properties.sample、install.properties.sample、cesecore.properties.sample、web.properties.sample、database.properties.sample，并改名为 ejbca.properties、install.properties、cesecore.properties、web.properties、database.properties。

配置文件中对每个配置项都进行了说明，基本上采用缺省配置即可。

（1）配置 ejbca.properties

首先设置应用服务器路径，配置 appserver.home 到%JBOSS_HOME%目录。为了测试方便，打开提示信息，修改 ejbca.productionmode 的值为 false。缺省情况下，禁止通过系统文件修改 EJBCA 的缺省配置。基本 CA 参数配置中，设置密钥库口令，此处采用缺省值“foo123”，其他参数采用缺省值。

（2）配置 install.properties

把 CA 的 DN 名改为 CN=ManagementCA,O=EJBCA,C=CN，其他采用缺省值。

（3）配置 cesecore.properties

设置密钥库口令，此处采用缺省值“foo123”。设置证书最大终止日期 ca.toolateexpiredate 为 2038-01-19 03:14:08+00:00，为缺省值。设置缺省语言为英语，intresources.Preferred language=EN。其他采用缺省值。

（4）配置 web.properties

把 java.trustpassword 值设为 trustpass，把 superadmin.batch 改为 false，把 httpsserver.password 的值改为 serverpass，把 httpsserver.dn 的值改为 CN=${httpsserver. hostname}, O=EJBCA,C=CN，其他保持不变。

（5）配置 database.properties

使用 postgresql 数据库，打开 database.properties 文件，依次设置为：

```
database.name=ejbca
database.url=jdbc:postgresql://127.0.0.1/ejbca
database.driver=org.postgresql.Driver
database.username=postgres
database.password=postgres
database.useSeparateCertificateTable=true
```

9．部署 EJBCA 到 JBoss 应用服务器

启动 JBoss 后，打开命令行窗口，进入%EJBCA_HOME%目录，执行命令“ant deploy”，此命令执行编译和部署 EJBCA 到 JBoss 中。命令执行完成后，系统提示成功。信息如下：

```
BUILD SUCCESSFUL
Total time: 2 minutes 16 seconds
```

执行命令“ant install”，此命令完成 CA 初始化，包括产生所有的证书、密钥，部署数据源、服务，配置 servlet 容器使用的密钥库和信任库文件，最后生成的管理员密钥在%EJBCA_HOME%/p12 目录下。

“ant install”命令只能执行一次，它在数据库中产生了大量信息，再次执行会出错。如果需要重新执行 CA 初始化，在执行“ant install”命令前要删除 ejbca 数据库中的所有表。

10．导入管理员证书

部署完成后，需要把管理员证书导入到浏览器中。在%EJBCA_HOME%/p12 目录下有管理员的 PKCS#12 格式证书密钥文件 superadmin.p12，需要导入到浏览器中。双击 superadmin.p12 文件后，出现“证书导入向导”界面，按照界面提示进行操作即可。其中，在“密码”对话框中，输入私钥保护密码为 ejbca（私钥保护密码为 web.properties 中设置的 superadmin.password 的值，在配置文件中已设置为 ejbca），如图 18-27 所示。

图 18-27　PKCS#12 文件私钥保护密码

11. 修改配置文件后重新部署

如果配置文件有改变，不需要重新安装 EJBCA，只需要执行命令“ant clean deployear”即可完成部署。

18.2.3 申请证书

配置完成后，需要重新启动 JBoss 应用服务器：通过 CTRL+C 终止服务后，重新在命令行窗口执行命令%JBOSS_HOME%\bin\standalone.bat 启动服务。

1. 管理员登录

打开 IE 浏览器，在地址栏输入 https://localhost:8443/ejbca/，出现图 18-28 所示的证书选择界面，选择 SuperAdmin 并单击“确定”按钮。

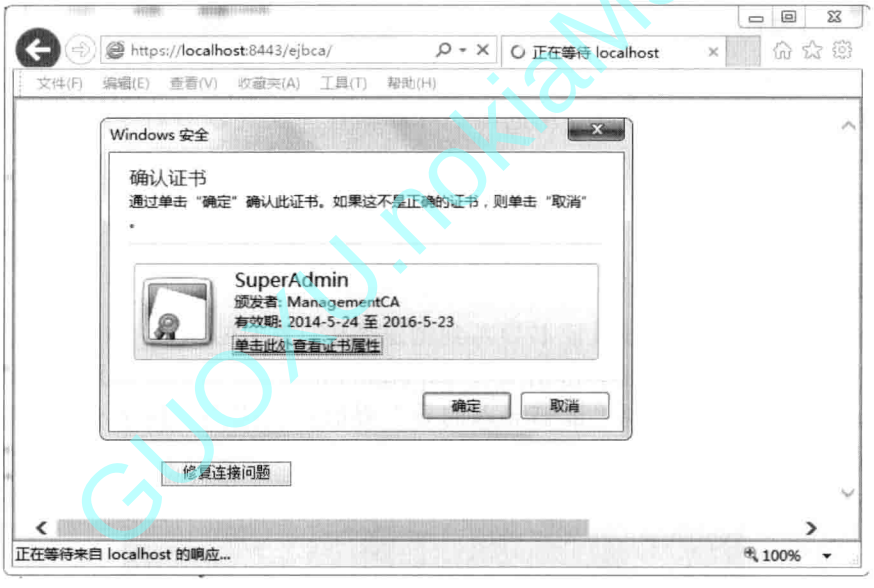

图 18-28 证书登录选择框

由于根 CA 证书没有加入本地信任库，可能会出现“此网址的安全证书有问题”警告窗口，单击“继续浏览此网站”后可进入管理界面，见图 18-29。

2. 导出 CA 证书

在管理界面中单击左侧导航栏“Fetch CA Certificates”，进入如图 18-30 所示界面。

选择“Download to Internet Explorer”后获得 CA 证书文件 ManagementCA.crt。双击该文件，可将该证书导入到本地 Windows 证书库“受信任的根证书颁发机构”中。具体操作步骤请参见 18.1.5 节。

3. 提交申请资料

在管理界面中单击左侧导航栏“Administration”，选择“Add End Entity”进入 EE 注册界面，如图 18-31 所示。

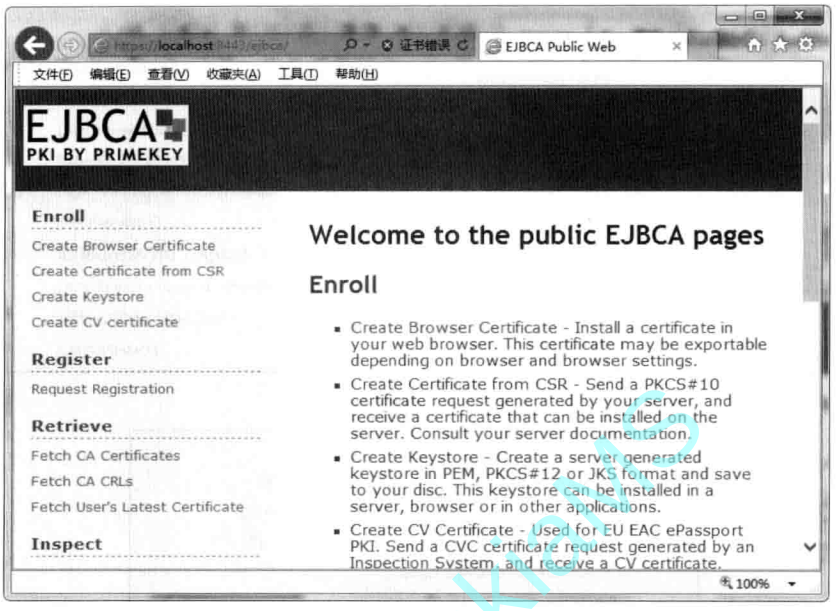

图 18-29　EJBCA 管理界面

图 18-30　导出 CA 证书

为了演示方便，只添加必要的注册信息，包括用户名（ejbcauser-1）、口令（123456）、CN（user-1）、Token（选择 P12 文件）。单击“Add”按钮，提示注册成功，并在底部列出已注册用户，如图 18-32 和图 18-33 所示。

4．下载证书

在管理界面中单击左侧导航栏“Create Browser Certificate”，输入注册时的用户名和密码（分别是 ejbcauser-1 和 123456），如图 18-34 所示。

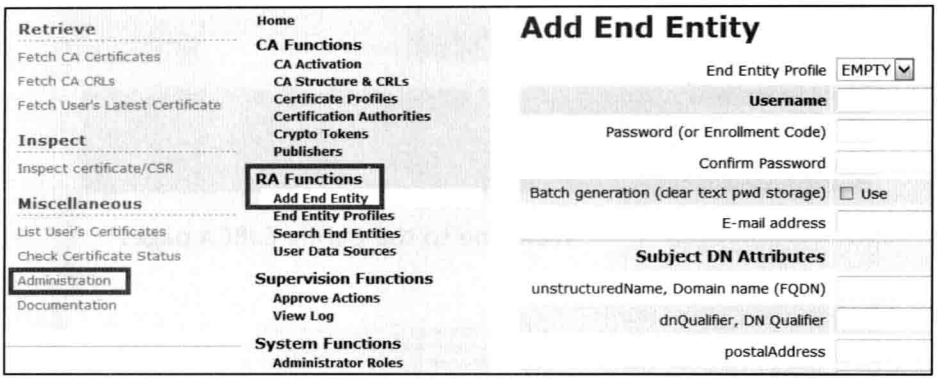

图 18-31　证书申请界面

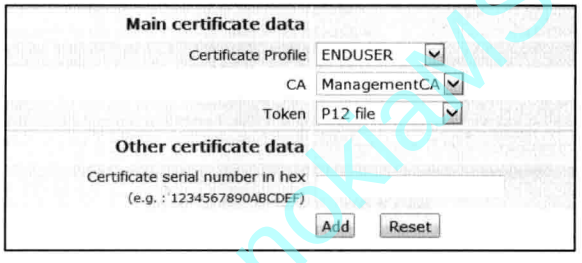

图 18-32　用户注册

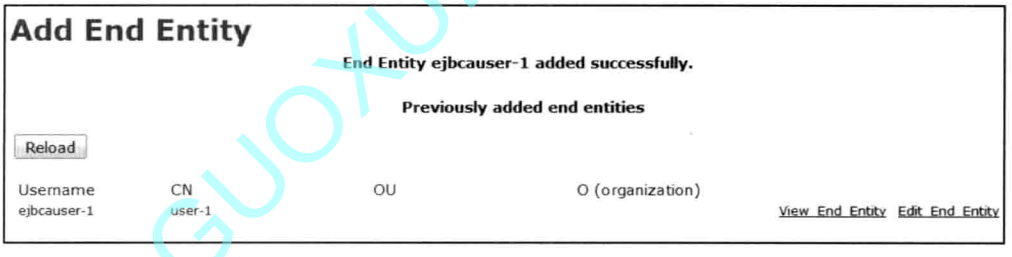

图 18-33　用户注册成功提示

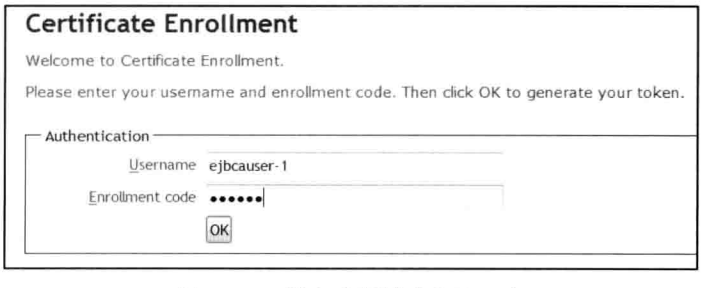

图 18-34　输入注册用户名和口令

单击“OK”按钮后，将出现密钥产生界面，如图 18-35 所示。选择密钥长度 Key length 为 1024 位，单击“Enroll”按钮，出现下载文件提示框，单击“确认”按钮后，等待文件下载完成。下载的文件是 P12 格式，包括证书和私钥，文件保护口令是注册时输入的 123456。

双击下载的 P12 文件，可以将该证书导入到本地 Windows 证书密钥库，与导入管理员证书类似。