HTTPS证书安装

IOS 7.1版本中，若使用WEB的安装方式，只能使用HTTPS来通讯，因此需要在应用服务器上部署SSL证书。

文档目录：

SSL证书获取

请用户向CA厂商获取证书。

获取证书后，按照以下的说明进行证书部署。

J2EE应用服务器上安装SSL证书

由于tomcat使用ssl配置https时，爆发出了严重安全漏洞，按照apache官方建议，升级tomcat到7.0.85及以后版本，修复安全漏洞。

查看tomcat版本方法：执行<tomcat>/bin/version.sh或version.bat

```
[root@centos7 bin]# ./version.sh
Using CATALINA_BASE:   /home/smartbi/apache-tomcat-7.0.90
Using CATALINA_HOME:   /home/smartbi/apache-tomcat-7.0.90
Using CATALINA_TMPDIR: /home/smartbi/apache-tomcat-7.0.90/temp
Using JRE_HOME:        /home/smartbi/jdk1.8.0_172
Using CLASSPATH:       /home/smartbi/apache-tomcat-7.0.90/bin/bootstrap.jar:/home/smartbi/apache-tomcat-7.0.90/bin/tomcat-juli.jar
Server version: Apache Tomcat/7.0.90
Server built:   Jul 2 2018 17:05:37 UTC
Server number:  7.0.90.0
OS Name:        Linux
OS Version:     3.10.0-693.el7.x86_64
Architecture:   amd64
JVM Version:    1.8.0_172-b11
JVM Vendor:     Oracle Corporation
[root@centos7 bin]#
```

Tomcat下载地址：Tomcat官网

升级Tomcat详情请参见 升级Tomcat。

附录1：TOMCAT服务器证书部署

1. 进入服务器安装目录的conf 子目录，编辑 server.xml文件
2. 修改里面的SSL设置，改法如下：

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
               maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS"
                keystoreFile="xx/xx/xx.keystore"
                keystorePass="xxxx"/>
```

需要注意修改的就是端口号和证书路径，证书密码。
说明：注意防火墙是否禁用端口。

1. 阿里云证书配置tomcat https访问参考如下：

```
      <Connector port="8443" protocol="HTTP/1.1"
                 maxThreads="150"
                 SSLEnabled="true"
                 scheme="https"
                 secure="true"
                 clientAuth="false"
                 keystoreFile="/xxx/xxx/xxx.pfx"
                 keystoreType="PKCS12"
                 keystorePass="xxx"
                 SSLProtocol="TLSv1+TLSv1.1+TLSv1.2"
                 ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256"/>z
```

a. 注：如参考以上配置无法通过https访问，请参考以下修改配置。

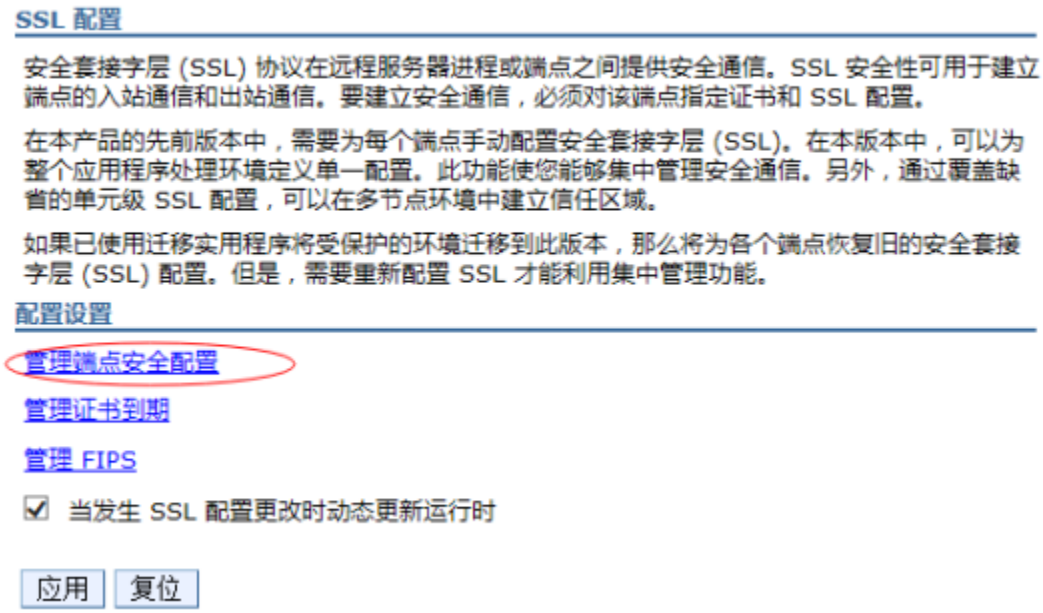
```
      <Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
                 maxThreads="150"
                 SSLEnabled="true"
                 scheme="https"
                 secure="true"
                 clientAuth="false"
                 keystoreFile="/xxx/xxx/xxx.pfx"
                 keystoreType="PKCS12"
                 keystorePass="xxx"
                 ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256"/>
```

附录2：WEBSPHERE服务器证书部署

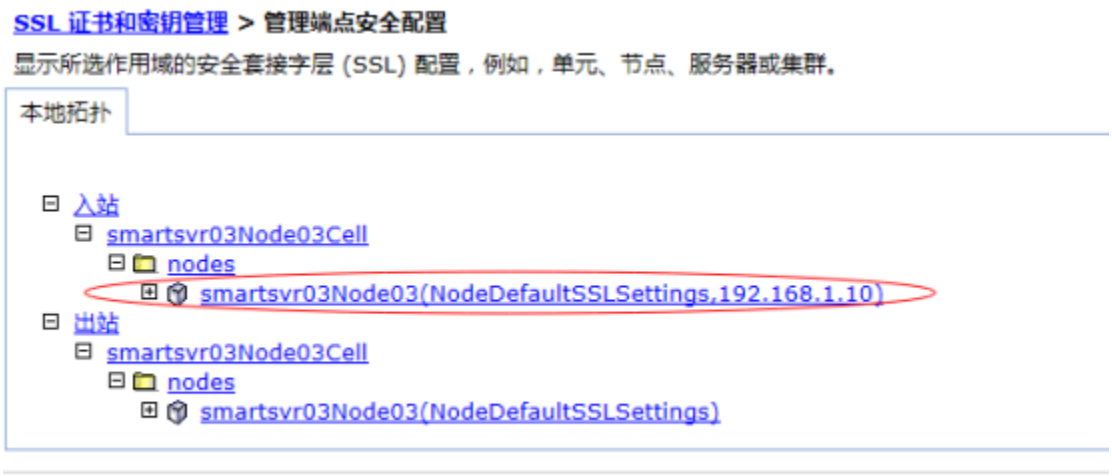
以WAS8.5举例说明

1. 进入服务器管理页面， "安全性"——"SSL证书和密钥管理"

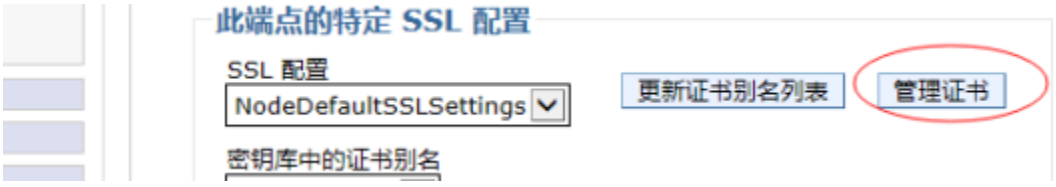
2. 进入"管理端点安全配置"



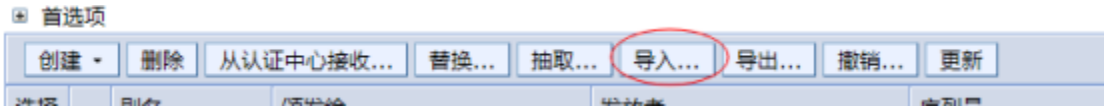
3. 选择对应的服务器或集群的入站设置



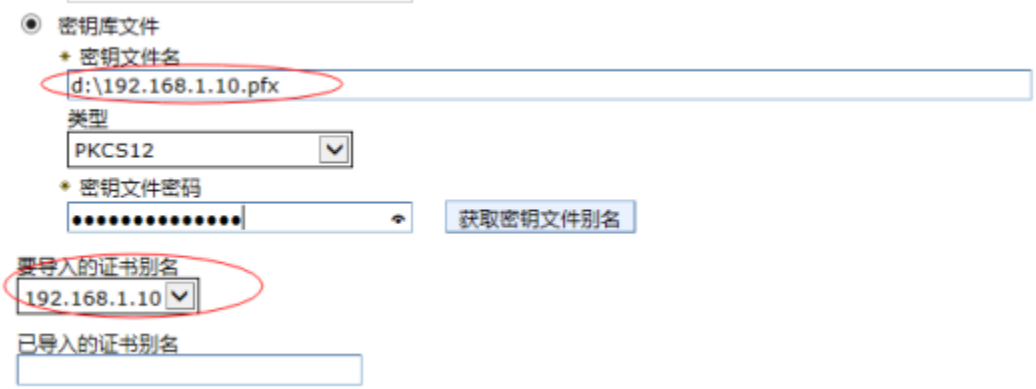
4. 进入管理证书



5. 填写证书存放的路径，导入证书，



注意选择证书别名，选择上面用OpenSSL工具生成的pfx文件，密码默认为：ServerPassword

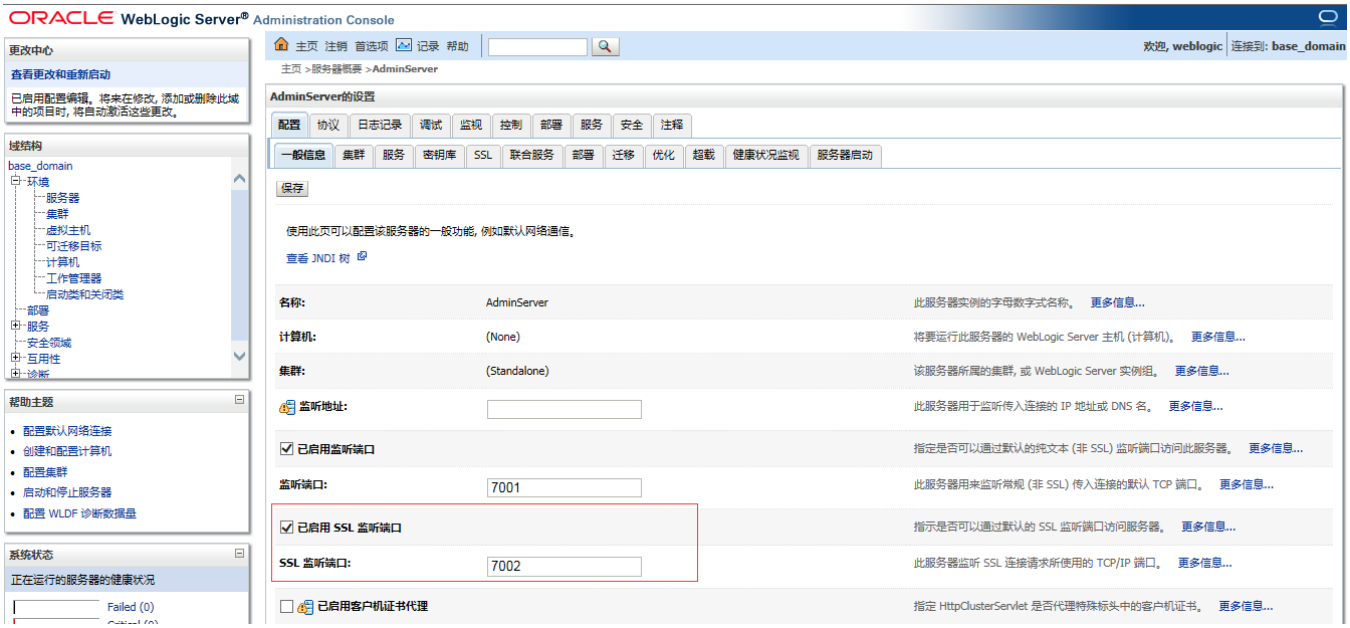


6. 导入后回到上层菜单选择导入的证书别名保存，并重启服务器。

附录3：WEBLOGIC 10/12c服务器证书部署

1、进入服务器管理页面， "环境"——"服务" —“AdminServer”

2、启动SSL端口。

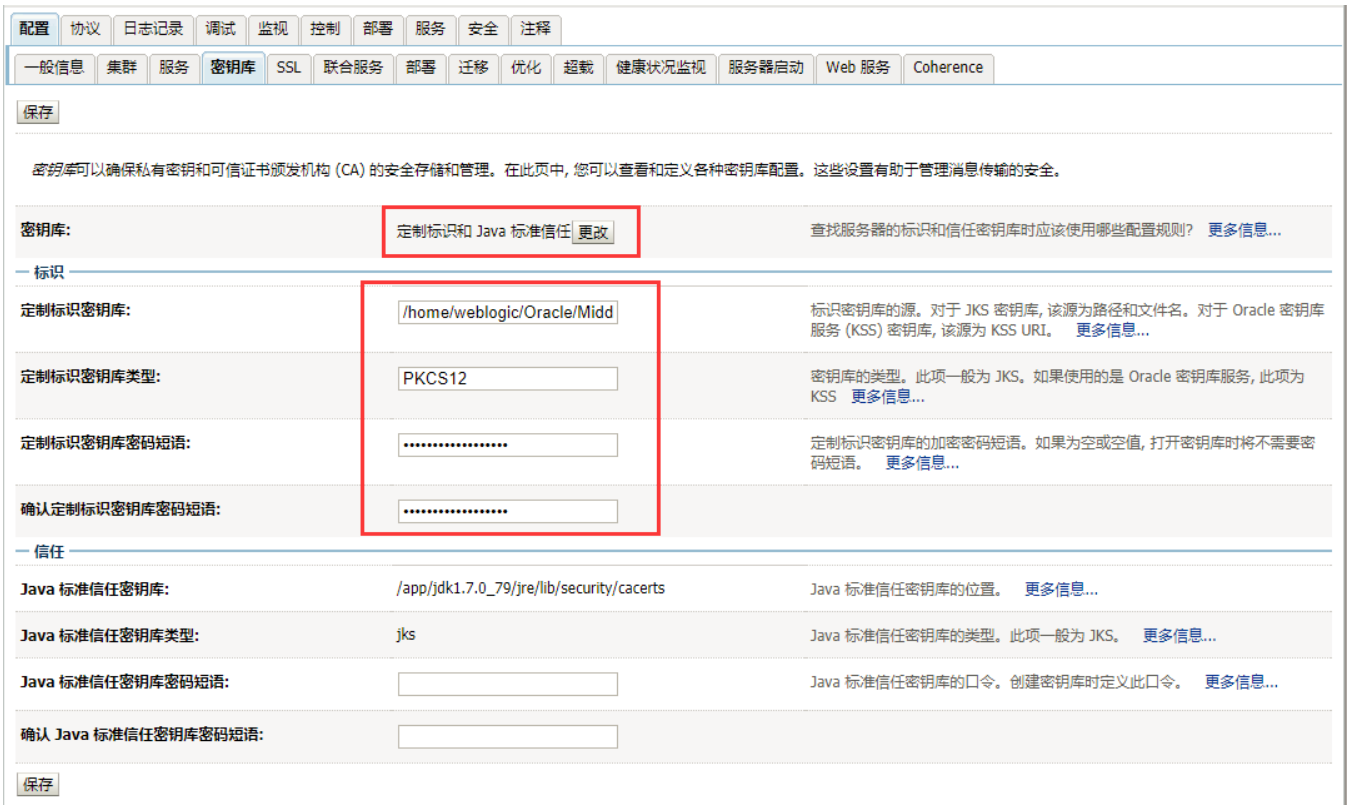


3、进入"密钥库"页面，点击更改按钮，设为为“定制标识和Java标准信任“，设置“密钥库标识“和”密钥库信任“信息。

“密钥库标识“为pfx的路径。

“密钥库类型”为“PKCS12”

“密码”上面用OpenSSL工具生成的pfx文件密码默认为：ServerPassword



3、进入到”SSL“页面，设置“私有密钥别名“和”密码“

附录4：在J2EE服务器上发布APP.WAR

1. 下载app.war，并用winrar软件打开
2. 将新生成的RootCA.cer根证书，替换app.war中的原有证书

3. 修改app.war/index.htm文件中的相关链接，确保它使用HTTPS并且IP或域名与上述生成证书时输入的IP或域名一致

```
d colspan="4" align="left">
  <a href = "http://192.168.1.56:8080/app/RootCer.cer">
     <span class = "btn-text">安装测试证书</span>
  </a>
td>


d style="text-align: center"><strong>iOS</strong></td>
d>标准版<br/>(程序大小3.3M)</td>
d><u><font color="#0066cc"><A href="itms-services:///?action=download-manifest&amp;url=https://192.168.1.56:8080/app
d>适用于iPad/iPhone</td>



d style="text-align: center"><strong>安卓</strong></td>
d>标准版<br/>(程序大小:3.2M)</td>
d><u><font color="#0066cc"><A href="http://192.168.1.56:8080/app/Smartbi.apk">Smartbi apk</a></></font></u></td>
d>适用于安卓系统</td>
```

4. 修改app.war/Smartbi.plist文件中的相关链接，确保它使用HTTPS并且IP或域名与上述生成证书时输入的IP或域名一致

```
<dict>
    <key>assets</key>
    <array>
        <dict>
            <key>kind</key>
            <string>software-package</string>
            <key>url</key>
            <string>https://192.168.1.56:8080/app/Smartbi.ipa</string>
        </dict>
        <dict>
            <key>kind</key>
            <string>display-image</string>
            <key>url</key>
            <string>https://192.168.1.56:8080/app/logo_144.png</string>
        </dict>
    </array>
    <key>metadata</key>
    <dict>
        <key>bundle-identifier</key>
```

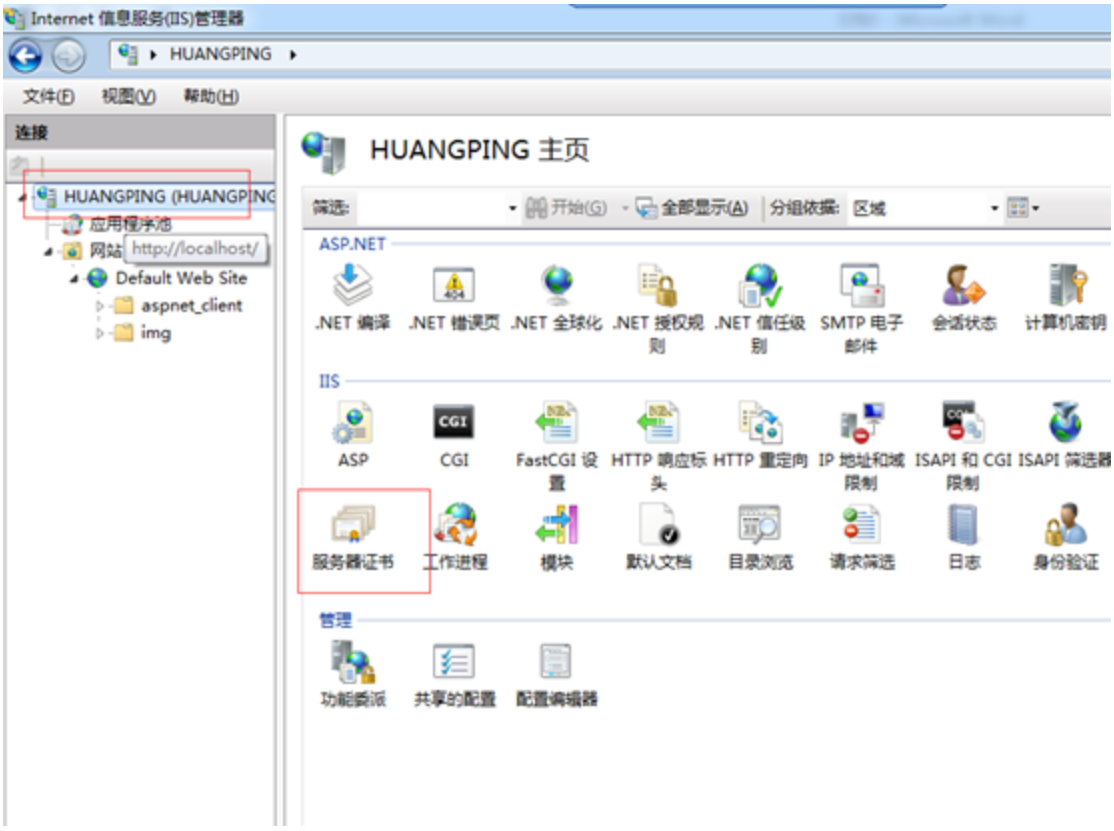
5. 参考smartbi在各应用服务器上的部署方式将修改后的app.war发布到服务器
6. iPad/iPhone中通过Safari访问IPA安装界面并点击该链接安装证书

操作系统	版本名称	下载地址	说明
安装测试证书			
iOS	标准版 (程序大小3.3M)	Smartbi ipa	适用于iPad/iPhone
安卓	标准版 (程序大小:3.2M)	Smartbi apk	适用于安卓系统

7. 点击IPA安装链接进行安装

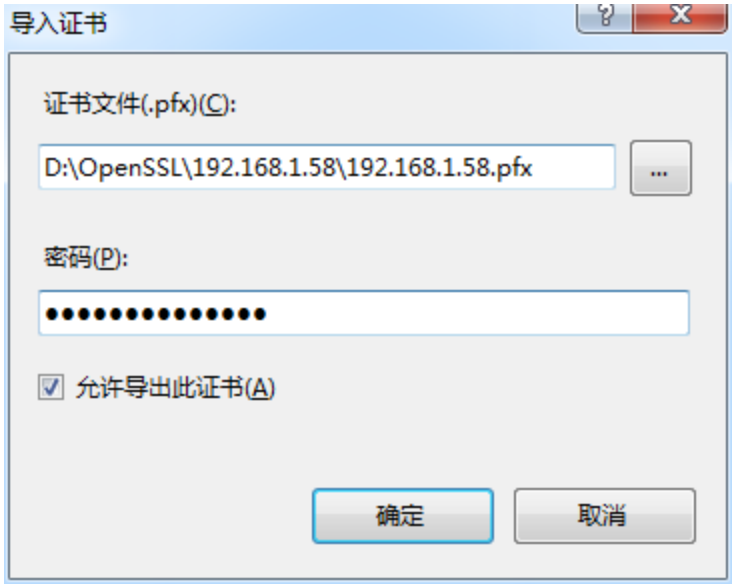
IIS上安装SSL证书及发布ipa

1、打开IIS7，选择根节点，如下

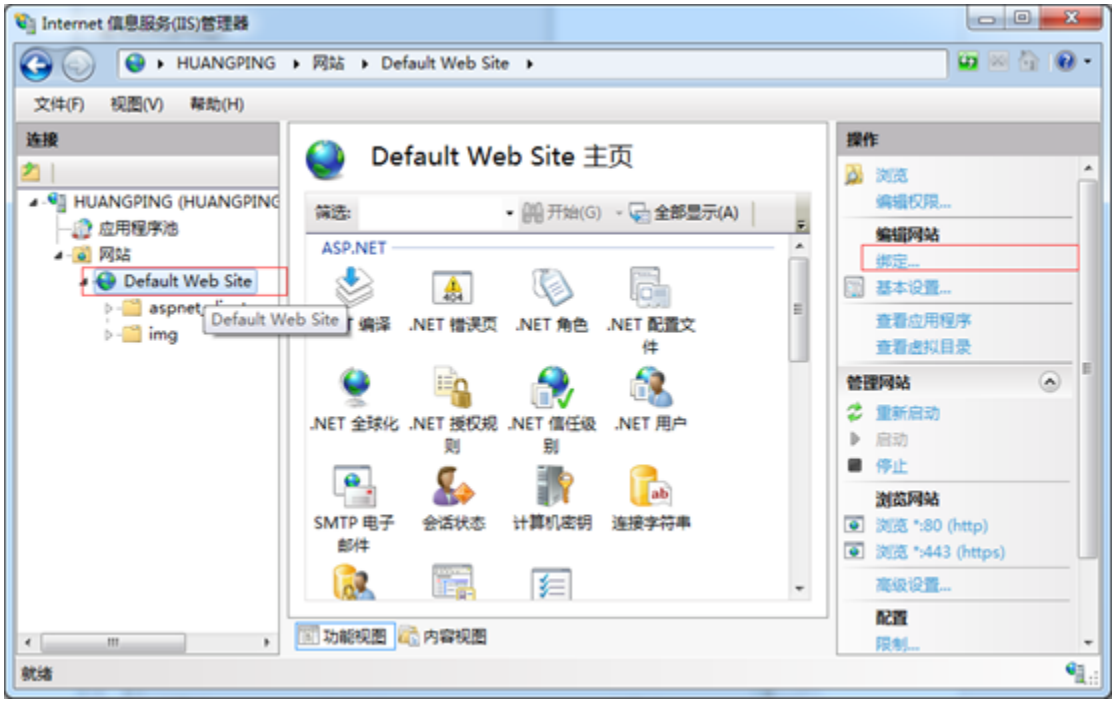


2、接下来可以在右边找到操作栏，选择导入

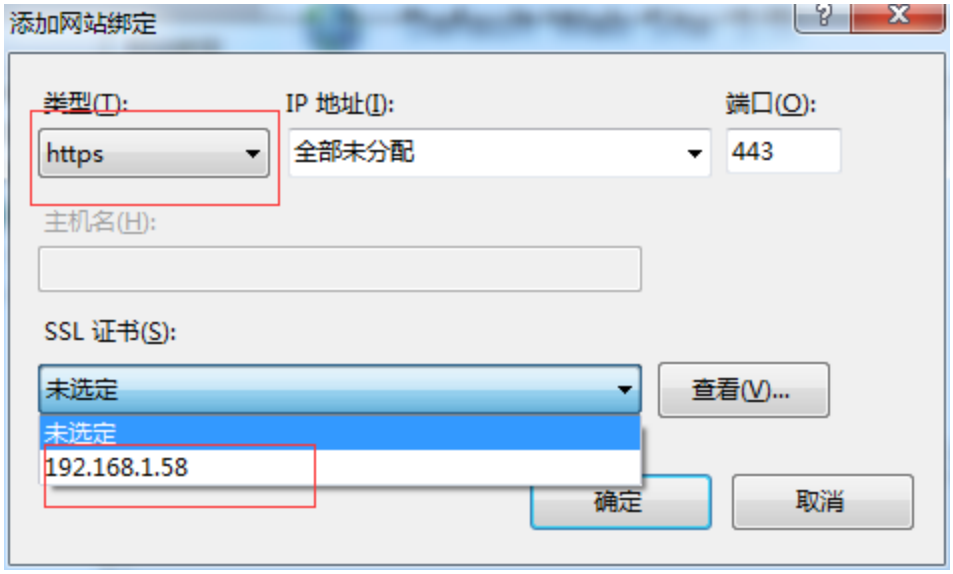
3、选择上面用OpenSSL工具生成的pfx文件，密码默认为：ServerPassword

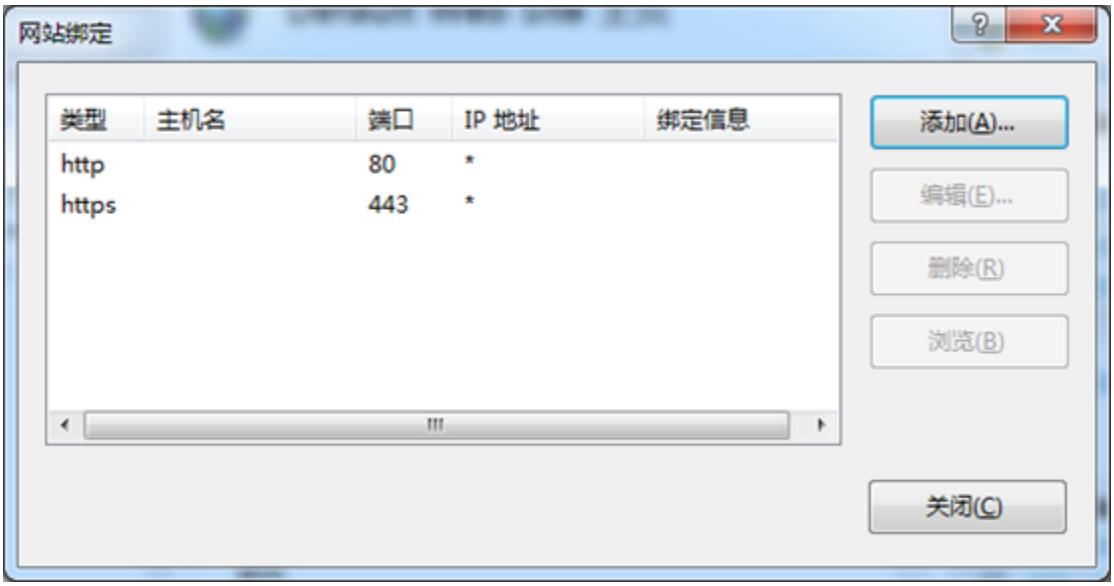


4、选择一个你要启用https的站点，注间是站点不是其中的某个虚拟目录，点击绑定



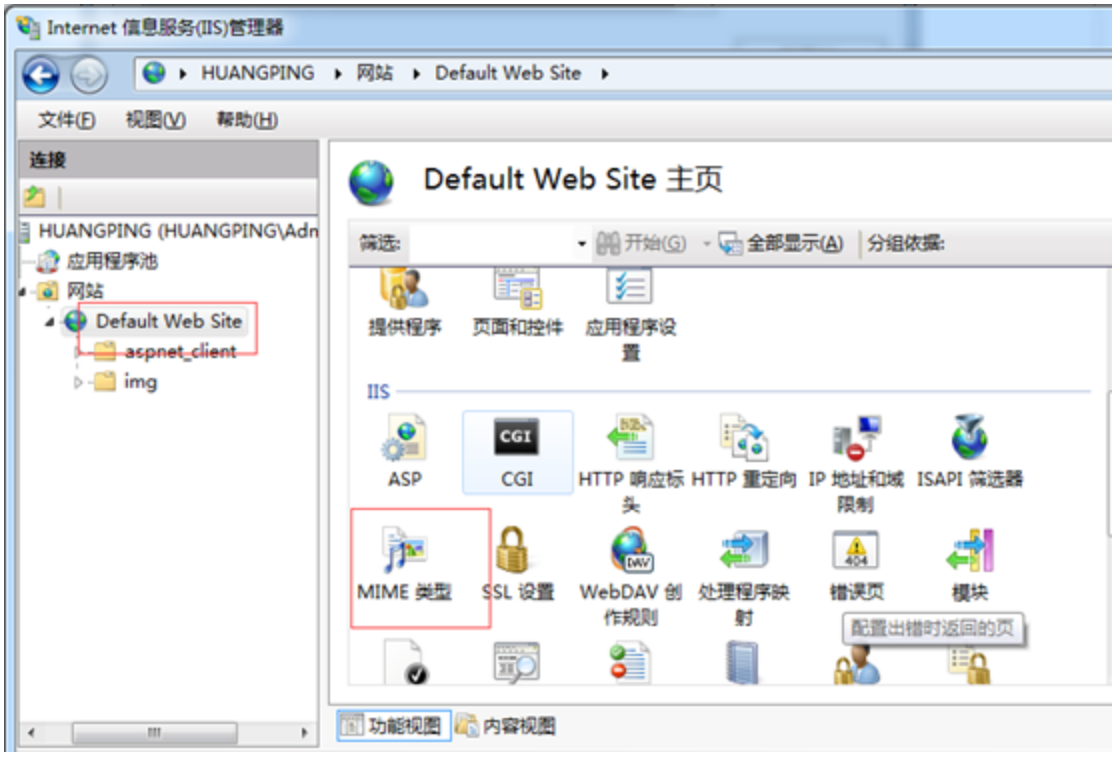
5、点击“添加”，选择“类型”和上面导入的ssl证书，并确定。

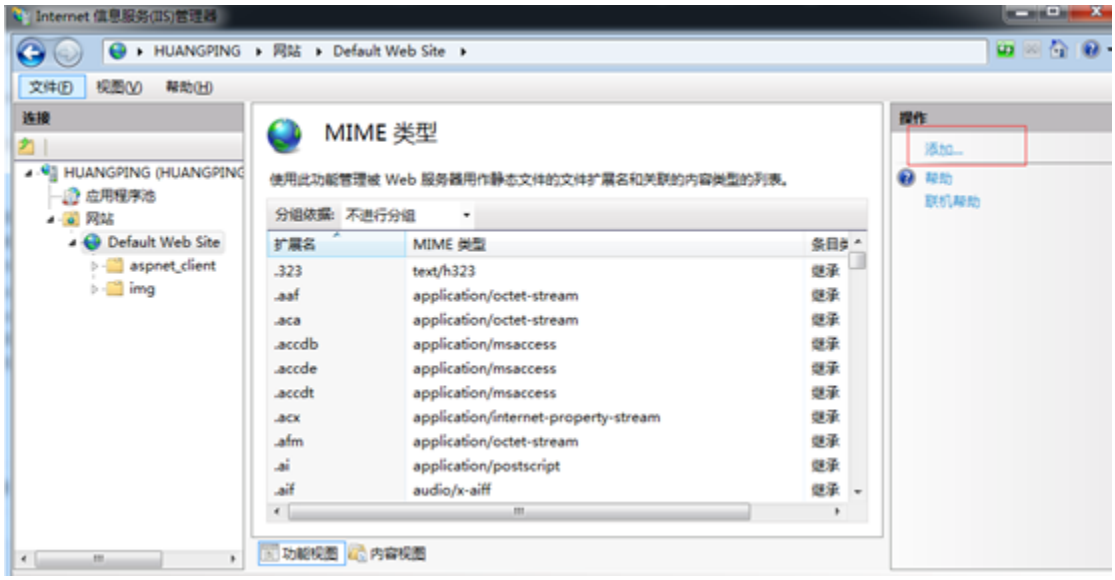


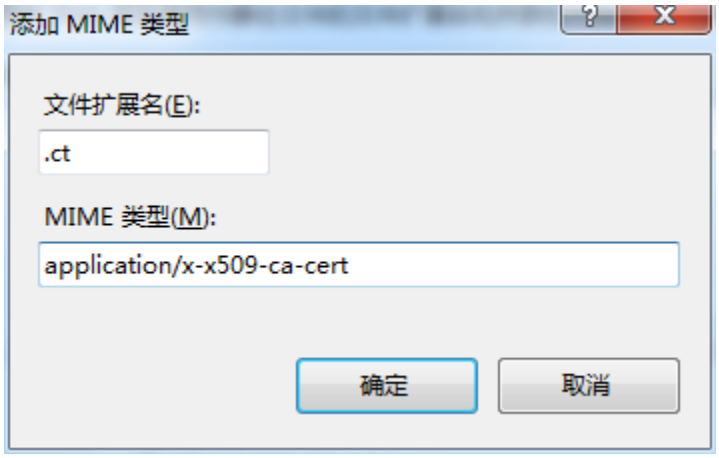


6、点击“MIME类型”， 点击”添加”,添加新的MIME类型。

扩展名	MIME类型
.plist	application/plist
.ipa	application/octet-stream
.mobileprovision	application/octet-stream
.ct	application/x-x509-ca-cert


Internet 信息服务(IIS)管理器
HUANGPING ▸ 网站 ▸ Default Web Site ▸
文件(F) 视图(V) 帮助(H)
连接
HUANGPING (HUANGPING\Adn
应用程序池
网站
Default Web Site
aspnet_client
img
Default Web Site 主页
筛选:
开始(G)
全部显示(A)
分组依据:
提供程序
页面和控件
应用程序设置
IIS
ASP
CGI
HTTP 响应标头
HTTP 重定向
IP 地址和域限制
ISAPI 筛选器
MIME 类型
SSL 设置
WebDAV 创作规则
处理程序映射
错误页
模块
配置出错时返回的页
功能视图
内容视图


Internet 信息服务(IIS)管理器
HUANGPING ▸ 网站 ▸ Default Web Site ▸
文件(F) 视图(V) 帮助(H)
连接
HUANGPING (HUANGPING
应用程序池
网站
Default Web Site
aspnet_client
img
MIME 类型
使用此功能管理被 Web 服务器用作静态文件的文件扩展名和关联的内容类型的列表。
分组依据: 不进行分组
扩展名
MIME 类型
条目
.323 text/h323 继承
.aaf application/octet-stream 继承
.aca application/octet-stream 继承
.accdb application/msaccess 继承
.accde application/msaccess 继承
.accdt application/msaccess 继承
.acx application/internet-property-stream 继承
.afm application/octet-stream 继承
.ai application/postscript 继承
.aif audio/x-aiff 继承
操作
添加...
帮助
联机帮助
功能视图
内容视图


添加 MIME 类型
文件扩展名(E):
.ct
MIME 类型(M):
application/x-x509-ca-cert
确定
取消

7、将OPENSSL中生成的RootCA.cer修改名称为RootCA.ct放到iis目录下

8、将ipa文件放到iis目录下

9、将ipa.rar中的文件放到iis目录下。

修改index.html和app_https.plist文件中的服务器地址

```
</head>
<body>
    <ul class = "download-ul">
        <li>
            <a href = "http://192.168.1.58/RootCer.ct">
            <span class = "btn-text">安装证书</span>
            </a>
        </li>
    </ul>
    <ul class = "download-ul">
        <li>
            <a id = "downloadIOSText" href="itms-services:///?action=download-manifest&url=https://192.168.1.58/app_https.plist">
            <span class = "btn-text">下载APP安装</span>
            </a>
        </li>
    </ul>
</body>
```

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1
<plist version="1.0">
<dict>
    <key>items</key>
    <array>
        <dict>
            <key>assets</key>
            <array>
                <dict>
                    <key>kind</key>
                    <string>software-package</string>
                    <key>url</key>
                    <string>https://192.168.1.58/app_for_iOS.ipa</string>
                </dict>
                <dict>
                    <key>kind</key>
                    <string>display-image</string>
                    <key>url</key>
                    <string>http://192.168.1.58/logo_144.png</string>
                </dict>
            </array>
            <key>metadata</key>
            <dict>
                <key>bundle-identifier</key>
                <string>cn.com.smartbi.SpreadsheetReport</string>
                <key>bundle-version</key>
```

10、将根证书RootCA.cer发送到移动端，下载安装。（若移动端设置有锁屏密码，安装时需要输入锁屏密码）

部署完成后的问题诊断

1. 在手机上无法访问到安装页面
   请检查应用服务器和手机是否在同一个网络环境，并且对应端口没有被防火墙阻止。
2. 安装证书后，点击页面上的链接，提示无法链接服务器
   请确认根证书和app下载链接的的IP或域名是一致的，并且已经替换掉app.war/RootCer.cer。

升级Tomcat

升级Tomcat的方法如下：

1、停止服务

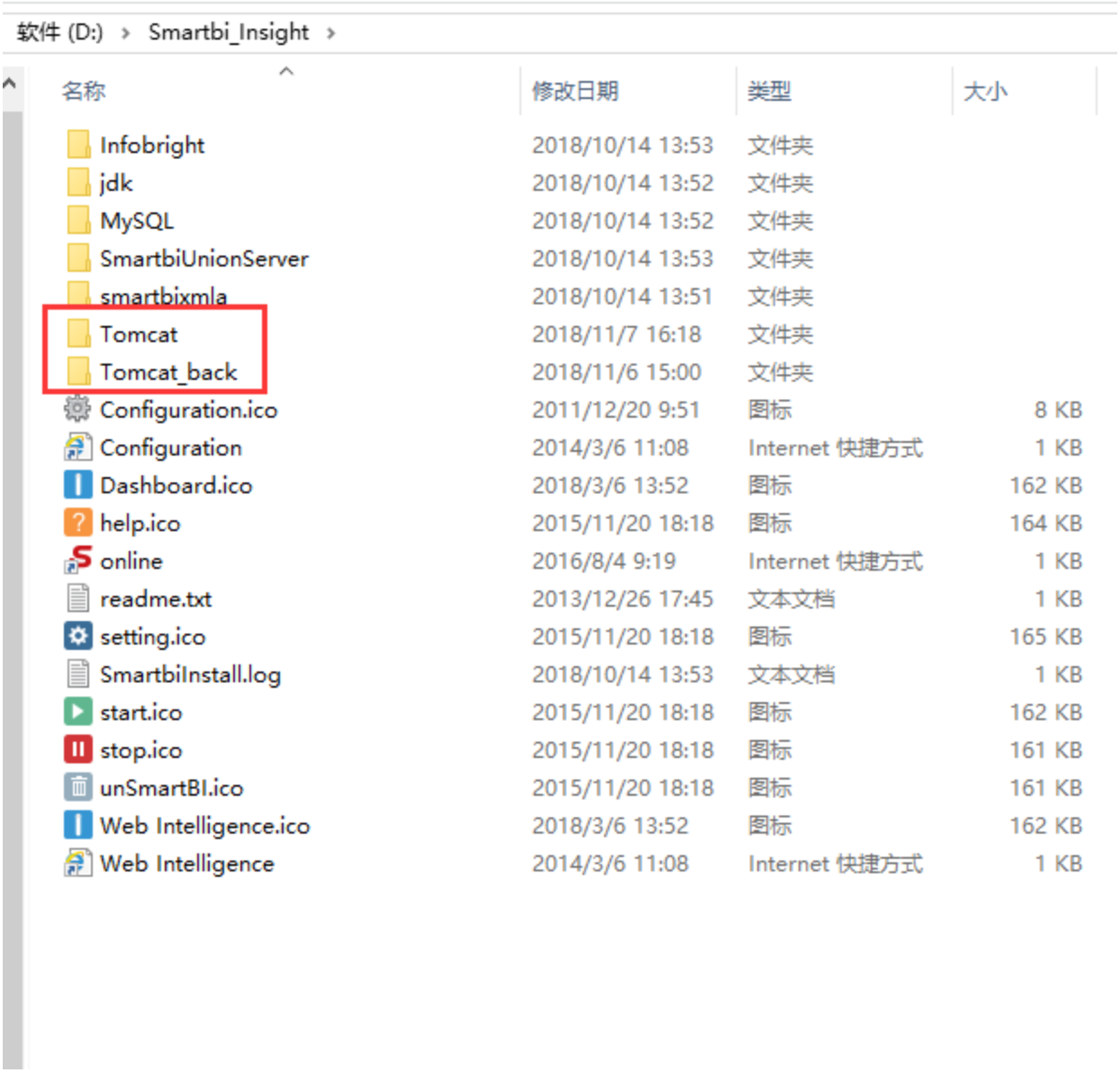
关闭smartbi的cmd窗口或在windows的服务中停止smartbi的服务。

2、修改现有的Tomcat目录

进入安装目录 ， 把Tomcat改名为Tomcat_back

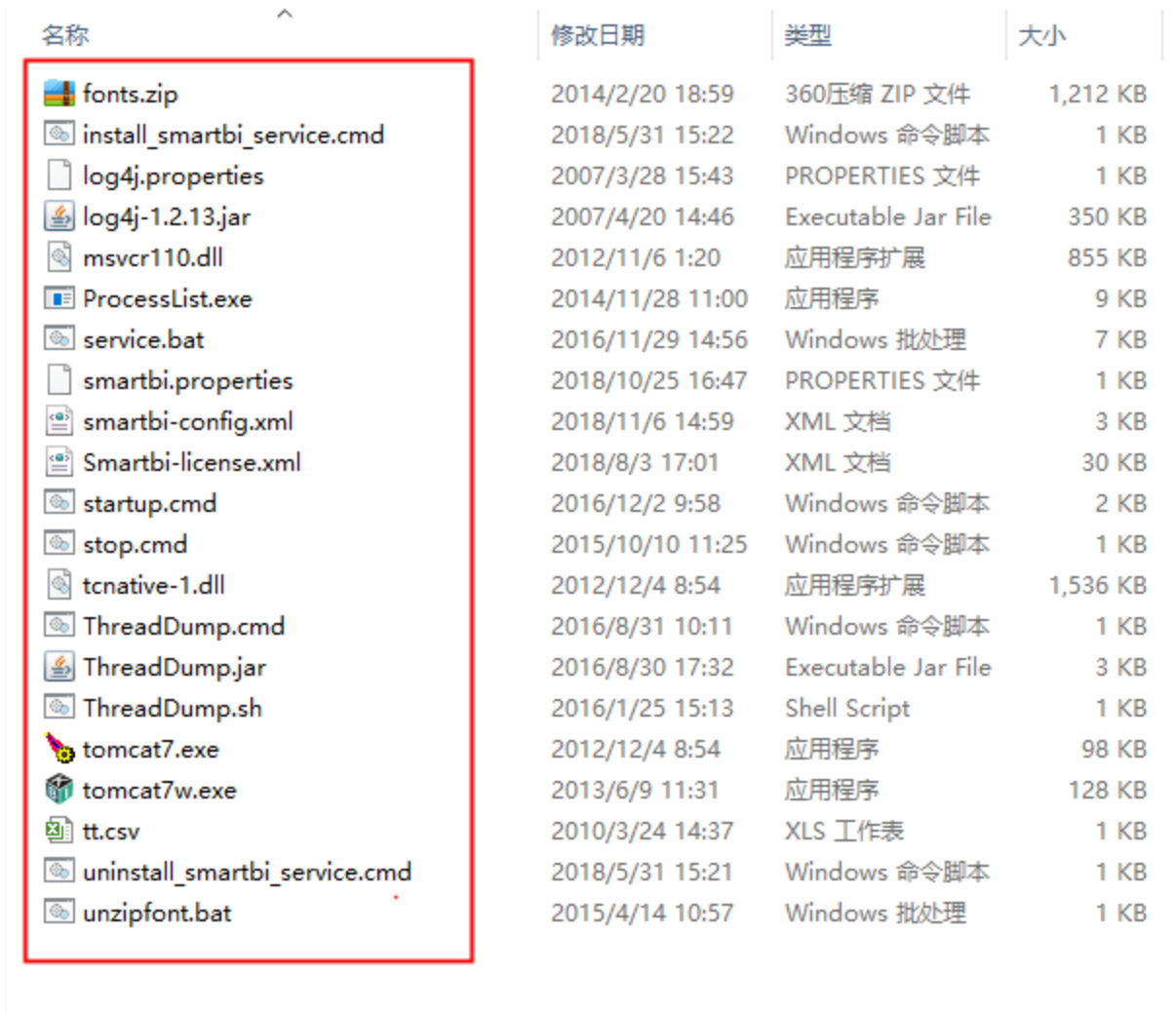
3、复制新的Tomcat

复制新版本Tomcat到安装目录



4、迁移smartbi配置

如下图所示，复制Tomcat_back/bin目录下的红色方框内文件到Tomcat/bin目录下



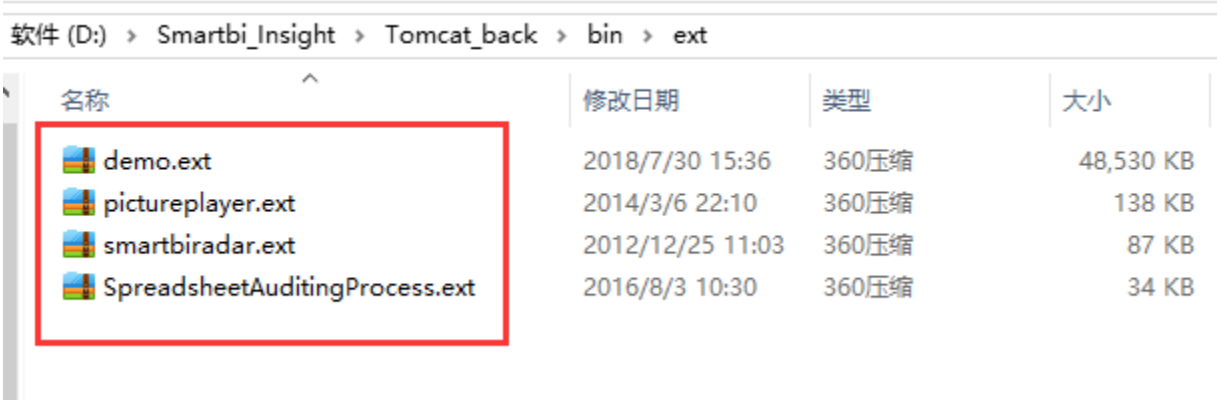
名称	修改日期	类型	大小
fonts.zip	2014/2/20 18:59	360压缩 ZIP 文件	1,212 KB
install_smartbi_service.cmd	2018/5/31 15:22	Windows 命令脚本	1 KB
log4j.properties	2007/3/28 15:43	PROPERTIES 文件	1 KB
log4j-1.2.13.jar	2007/4/20 14:46	Executable Jar File	350 KB
msvcr110.dll	2012/11/6 1:20	应用程序扩展	855 KB
ProcessList.exe	2014/11/28 11:00	应用程序	9 KB
service.bat	2016/11/29 14:56	Windows 批处理	7 KB
smartbi.properties	2018/10/25 16:47	PROPERTIES 文件	1 KB
smartbi-config.xml	2018/11/6 14:59	XML 文档	3 KB
Smartbi-license.xml	2018/8/3 17:01	XML 文档	30 KB
startup.cmd	2016/12/2 9:58	Windows 命令脚本	2 KB
stop.cmd	2015/10/10 11:25	Windows 命令脚本	1 KB
tcnative-1.dll	2012/12/4 8:54	应用程序扩展	1,536 KB
ThreadDump.cmd	2016/8/31 10:11	Windows 命令脚本	1 KB
ThreadDump.jar	2016/8/30 17:32	Executable Jar File	3 KB
ThreadDump.sh	2016/1/25 15:13	Shell Script	1 KB
tomcat7.exe	2012/12/4 8:54	应用程序	98 KB
tomcat7w.exe	2013/6/9 11:31	应用程序	128 KB
tt.csv	2010/3/24 14:37	XLS 工作表	1 KB
uninstall_smartbi_service.cmd	2018/5/31 15:21	Windows 命令脚本	1 KB
unzipfont.bat	2015/4/14 10:57	Windows 批处理	1 KB

注意：windows版本安装包，可能还需要复制tcnative-1.dll替换原来自带的tcnative-1.dll。

如果使用的https加密协议，还需要把对应的证书文件复制到Tomcat/bin目录下。

5、迁移扩展包

如下图所示，复制Tomcat_back/bin/ext目录下的所有ext文件到Tomcat/bin/ext目录下



名称	修改日期	类型	大小
demo.ext	2018/7/30 15:36	360压缩	48,530 KB
pictureplayer.ext	2014/3/6 22:10	360压缩	138 KB
smartbiradar.ext	2012/12/25 11:03	360压缩	87 KB
SpreadsheetAuditingProcess.ext	2016/8/3 10:30	360压缩	34 KB

6、迁移动态链接库

复制Tomcat_back/bin/dynamicLibraryPath的所有文件到Tomcat/bin/dynamicLibraryPath目录下

如果Tomcat_back/bin/dynamicLibraryPath目录为空，则忽略这个步骤

7、迁移smartbi的备份文件

复制Tomcat_back/bin/smartbi_repoBackup的所有文件到Tomcat/bin/smartbi_repoBackup目录下

8、迁移smartbi的war包

复制Tomcat_back/webapps目录下所有文件到Tomcat/webapps目录下