使用HTTPS协议进行Portal认证的典型配置

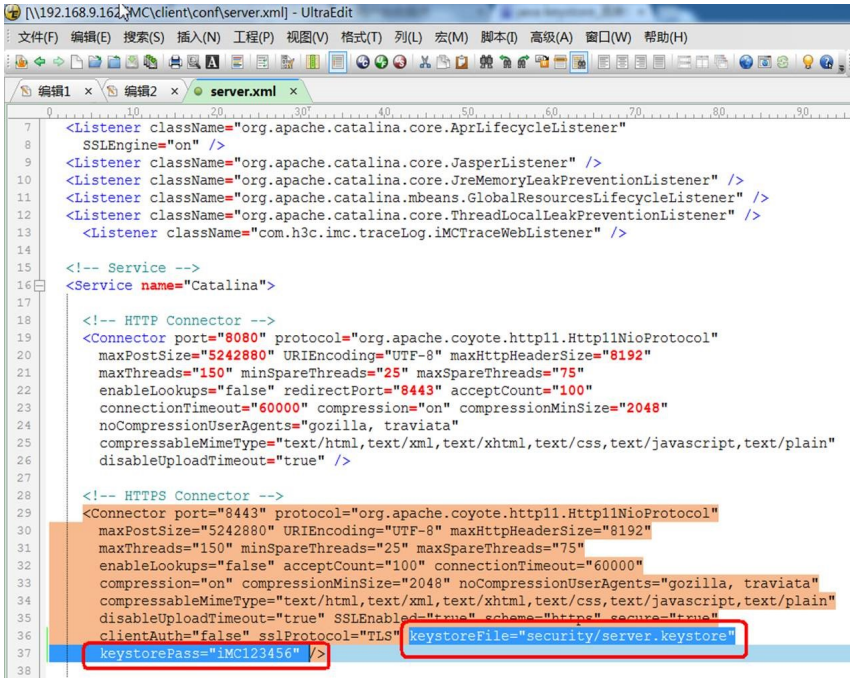
wlan接入 AAA Portal iMC 卞朋朋 2016-12-12 发表

本文档介绍使用HTTPS协议进行Portal认证的典型配置。
本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。
本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。
本文档假设您已了解Portal认证的特性。

普通portal认证组网（图略）。

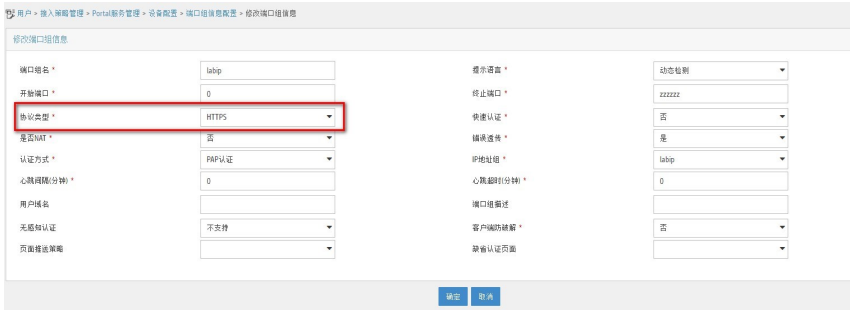
1. 无线portal认证（与http协议的portal认证配置一致，略）。
2. 服务器侧配置（适用于集中式部署，分布式部署请看文章最后注意事项）。

2.1在服务器上，打开监控代理，停止jserver。
2.2将server.keystore文件拷贝到目录\iMC\client\security下，修改文件\iMC\client\conf\server.xml中的内容。如下图红色框内容，其中keystoreFile为文件路径，keystorePass为密码，该keystore文件的密码为iMC123456。



2.3 重新启动jserver。

3. 修改iMC侧配置。将iMC侧端口组信息配置下的协议类型修改为HTTPS。



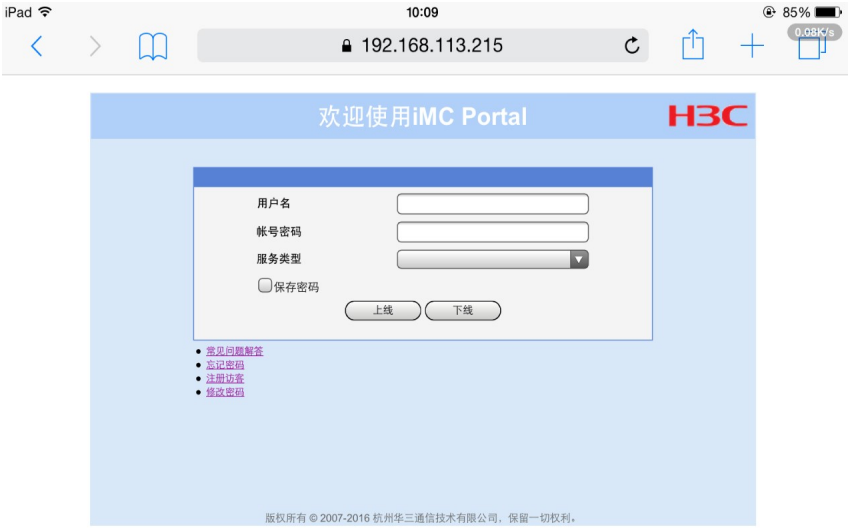
4. 认证过程

4.1 智能终端认证
浏览器首先会提示无法验证服务器信息


iPad
10:08
86%
192.168.113.215
0.12K/s
无法验证服务器身份
“Safari”无法验证“192.168.113.215”的身份。请检查证书的详细资料。
取消
详细信息
继续

选择信任证书之后就可以进行portal认证。

4.2 PC测试



选择继续浏览此网站

1. 在设备上配置portal server的URL时，依旧配置http://ip:port/portal而非HTTPS。
2. 如何获取server.keystore：提供服务器证书/私钥，服务器根证书/私钥，然后由研发进行转换。
3. 如何能够弹出不信任页面：证书是微软受信任的证书机构颁发的才可以。
4. 如果是分布式部署portal server的话，主服务器不需要进行server.keystore的复制以及server.xml的修改，只需要修改从服务器，但要注意，从服务器修改之后，一定要重启一下web server。