S5800交换机SSL应用举例-HTTPS配置

杨逢君 2010-01-14 发表

S5800交换机SSL应用举例-HTTPS配置

一、 组网需求：

无特殊组网需求，只是通过HTTPS以实现对S5800交换机的Web管理。

二、 组网图：

无特殊组网。

三、 配置步骤：

这里使用微软Windows Server 2003作为证书服务器，S5800通过SCEP（Simple Certificate Enrollment Protocol，简单证书注册协议）申请并获取证书。

3.1 配置证书服务器

本节介绍Windows Server 2003 CA服务的安装与配置，以及SCEP插件的安装与配置，为此，请事先准备好Windows Server 2003系统安装盘，以及SCEP插件（可从微软网站下载，名为cepsetup.exe）。

注意！微软SCEP插件的运行依赖IIS服务，请安装并运行IIS！

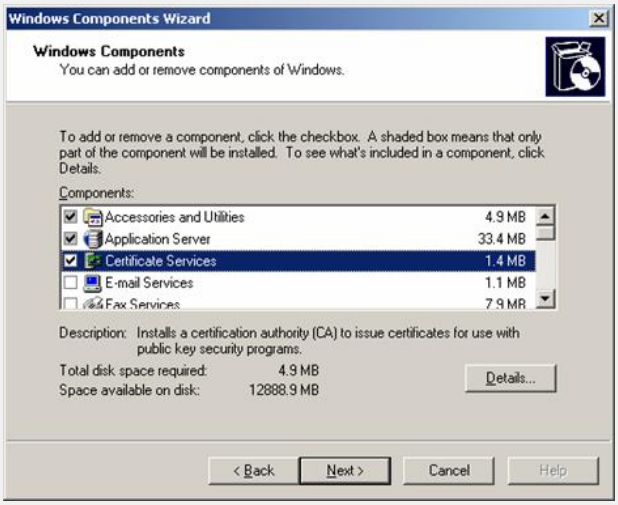
3.1.1 安装与配置Windows Server 2003 CA

1）以管理员身份登录系统。或者，如果您装有 Active Directory，则以域管理员身份登录到系统。

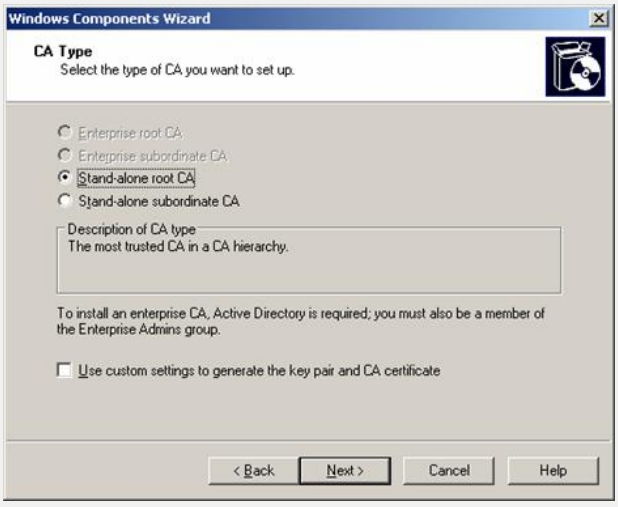
2）单击“开始”，指向“设置”，然后单击“控制面板”。

3）双击“添加/删除程序”并单击“添加/删除 Windows 组件”。

4）在“Windows 组件向导”中，选中“Certificate Services（证书服务）”复选框，如下图所示：



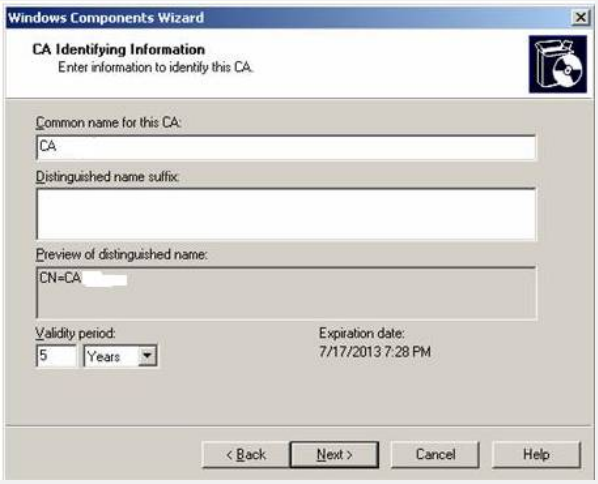
5）单击“Stand-alone root CA（独立根 CA）”。（在没有安装域的情况下，不可选择“Enterprise root CA（企业根CA）”），如下图所示：



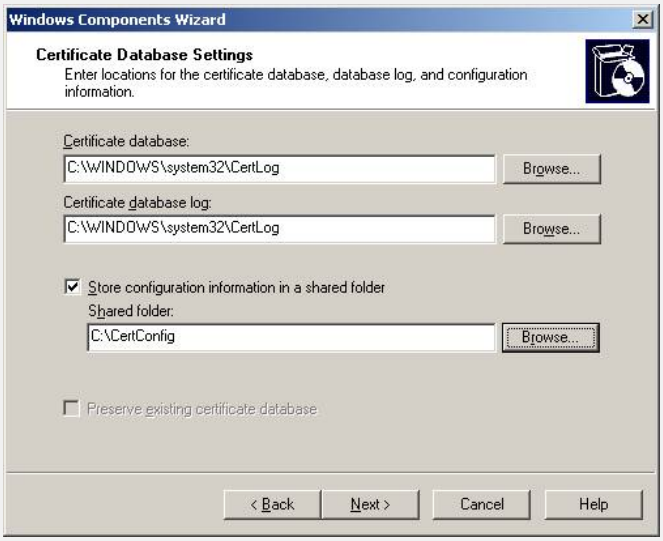
6）键入证书颁发机构的名称和其他必要信息。注意！在 CA 设置完成后这些信息都不能改变，如果要修改只能先删除CA组件再重新安装！

这里取CA CN为CA，如下图所示：

提示：经验证，该名称中可以有空格和点等字符！



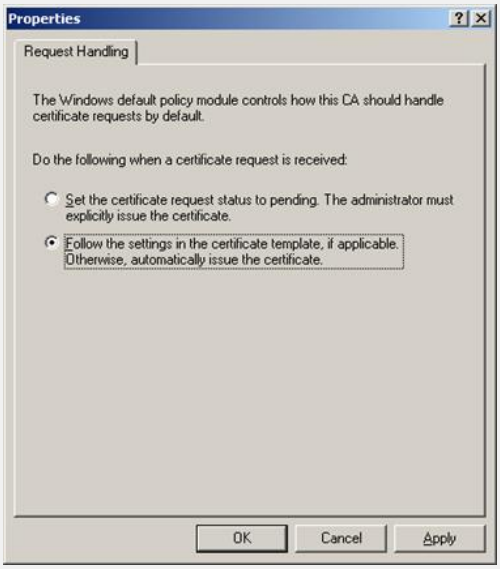
7）指定证书数据库、证书数据库日志和共享文件夹的存储位置，如下图所示：



8) 如果正在运行 WWW 发布服务，则您会遇到一条要求在安装之前停止此项服务的请求信息。单击"确定", 如果出现提示，则键入证书服务安装文件的路径。

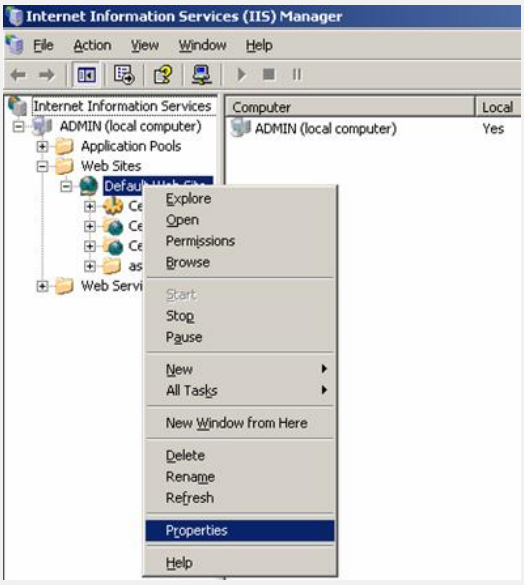
9) 提示组件安装成功。

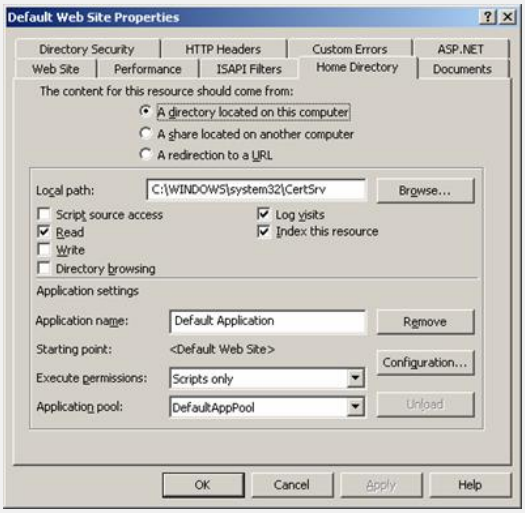
10) 运行CA服务, CA服务默认操作为挂起请求，等待管理员手动颁发证书。为了方便，请按以下三图所示操作（并按提示重启证书服务），让证书服务器自动颁发证书。

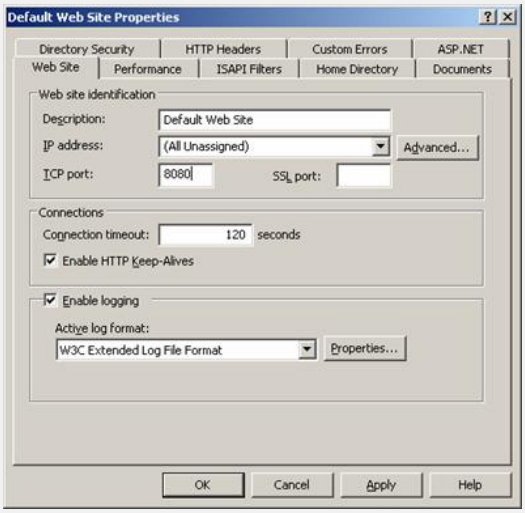


11）（可选）修改IIS服务的属性：

打开[控制面板/管理工具]中的[Internet 信息服务(IIS)管理器]，将[Default Web Site（默认网站）] 属性中“Home Directory（主目录）”的Local path（本地路径）修改为证书服务保存的路径。另外，为了避免与已有的服务冲突，建议修改默认网站的TCP端口号为未使用的端口号，这里取8080。如以下三图所示：







3.1.2　安装与配置SCEP

1）安装下载到本地的SCEP插件（名为cepsetup.exe），如下图所示：

2）选择“Use the local system account（使用本地系统帐号）”，如下图所示：

3）因H3C设备目前尚不支持SCEP Challenge，请一定要去掉下图中“Require SCEP Challenge Phrase to Enroll”选项。

4）为SCEP登记RA（Registration Authority，注册机构）证书：输入RA信息，这里取RA名为RA，如下图所示：

提示：SCEP插件充当RA角色，S5800交换机作为证书申请者，通过SCEP向CA申请证书，因此下文中S5800配置证书申请的注册受理机构时，类型一定要选RA而不是CA！

5）提示SCEP插件安装成功，请记下下图的URL信息，下文中S5800配置注册服务器URL时要与之对应一致。

注意：此处ca实质为host:port，本案例中Windows Server 2003服务器IP为5.5.5.1，因此S5800配置注册服务器URL需为http://5.5.5.1:8080/certsrv/mscep/mscep.dll。

6）查看CA服务，这时应该可以看到有两个证书已颁发给RA（即SCEP插件）。

3.2　配置HTTPS服务器

因证书具有时效性，请事先正确配置S5800时钟与时区！如果全网部署了NTP服务器

，则强烈推荐配置S5800和证书服务器（Windows Server 2003）以及用户的浏览器与NTP服务器同步！

3.2.1　配置PKI并申请证书

1) 配置PKI实体

#配置实体名称为aaa，通用名为S5800。

[S5800] pki entity aaa

[S5800-pki-entity-aaa] common-name S5800

2）配置PKI域

创建并进入PKI域ssl。

[S5800] pki domain ssl

配置可信任的CA名称为RA，与SCEP插件配置中RA名保持一致。

[S5800-pki-domain-ssl] ca identifier RA

#配置注册服务器URL，与SCEP插件配置保持一致。

[S5800-pki-domain-ssl] certificate request url

http://5.5.5.1:8080/certsrv/mscep/mscep.dll

#配置证书申请的注册受理机构类型为RA。

[S5800-pki-domain-ssl] certificate request from ra

#关联PKI实体名aaa。

[S5800-pki-domain-ssl] certificate request entity aaa

3）用RSA算法生成本地密钥对

[S5800] public-key local create rsa

The range of public key size is (512 ~ 2048).

NOTES: If the key modulus is greater than 512,

It will take a few minutes.

Press CTRL+C to abort.

Input the bits of the modulus[default = 1024]:

Generating Keys...

..++++++++.++++++++++

...++..++...++....++...++...++..++...++...++..++...++...++..++...++...++...++..+

+...++...++..++....++..++...++...++..++...++...++...++..++..++...++...++..++..++

...++...++...+++++++++.++++++++++.+

...++..++....++...++..++..++..++...++...++..++...++...++..++...++.+++++++++++++++

+.+++++++

..++...++..++...+++++++++++++++.++++++++++

4）获取CA证书

[S5800] pki retrieval-certificate ca domain ssl

Retrieving CA/RA certificates. Please wait a while.....

The trusted CA's finger print is:

　MD5 fingerprint:9C7A 2FBA 9230 2BF5 F27D 5391 DCF7 9912

　SHA1 fingerprint:189A CC85 F030 F866 51B1 9DD7 6DA9 65BA 5B05 2596

Is the finger print correct?(Y/N):y

Saving CA/RA certificates chain, please wait a moment.....

CA certificates retrieval success.

5）获取本地证书

[S5800] pki request-certificate domain ssl

Certificate is being requested, please wait.....

[S5800]

Enrolling the local certificate,please wait a while.....

Certificate request Successfully!

Saving the local certificate to device.....

Done!

3.2.2　配置SSL服务器端策略

#创建一个名为myssl的SSL服务器端策略。

[S5800] ssl server-policy myssl

#配置SSL服务器端策略使用的PKI域名为ssl。

[S5800-ssl-server-policy-myssl] pki-domain ssl

#（可选）配置服务器端需要验证客户端，这时客户端也需要申请并安装客户端证书。

[S5800-ssl-server-policy-myssl] client-verify enable

3.2.3　配置HTTPS服务

配置指定HTTPS服务器的SSL策略为myssl。

[S5800] ip https ssl-server-policy myssl

使能HTTPS服务。

[S5800] ip https enable

3.2.4　创建Web网管帐号

创建本地帐号以实现Web网管，用户名为abc，密码为123（明文），服务类型一定要指定为telnet，权限级别为3（最高）。

[S5800] local-user abc

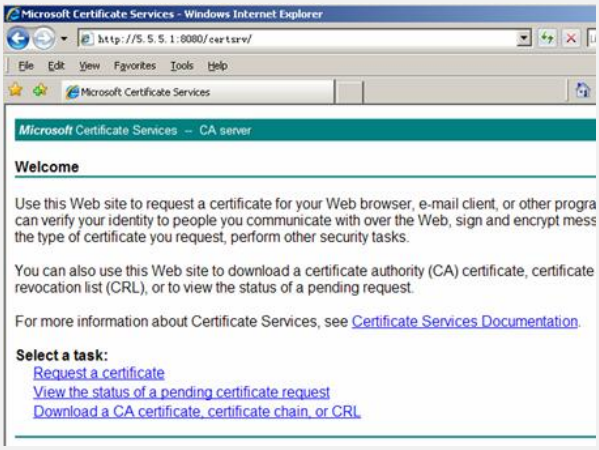
[S5800-luser-abc] password simple 123

[S5800-luser-abc] service-type telnet level 3

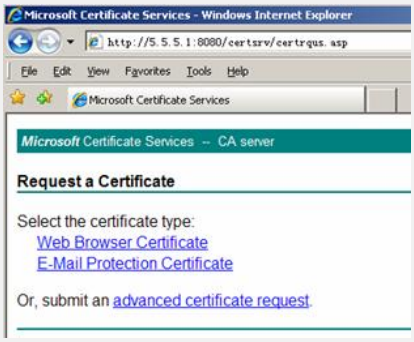
3.3　　配置HTTPS浏览器

本案例中，使用微软IE6作为浏览器。经验证IE7，IE8以及苹果Safari 4也可以配合。至于其它厂家浏览器或不同版本，本人尚未测试。

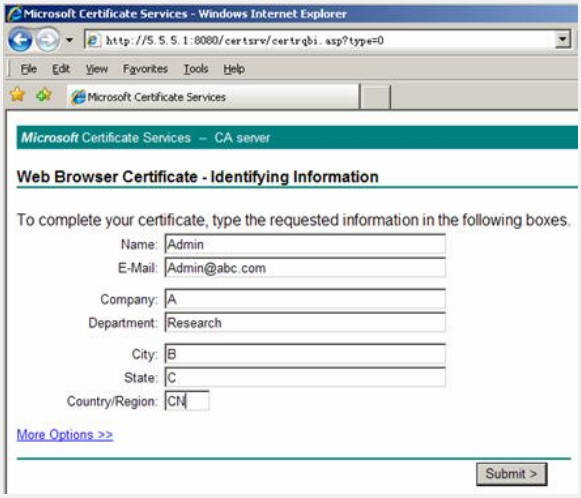
1）运行IE，地址栏输入证书服务器地址为 http://5.5.5.1:8080/certsrv，如下图所示：



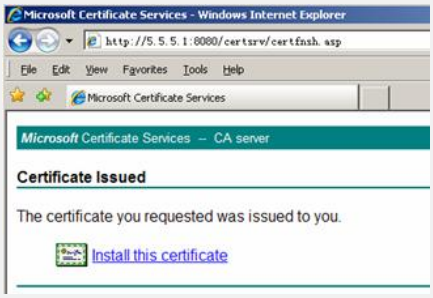
2）选择“Request a certificate”， 接着指定证书类型为“Web Browser Certificate”，如下图所示：



3）输入证书申请者信息，如下图所示：



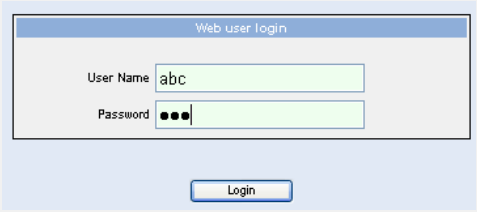
4）当证书申请成功时（Certificate Issued），点击“Install the certificate” 以安装证书。



5）证书安装完毕，可以在浏览器菜单中选Tools（工具） > Internet Options（Internet选项），继而选择 Content （内容）> Certificates（证书）加以查看。

3.4　　验证

1）运行IE，地址栏输入S5800地址为 https://1.1.1.1，应该会弹出web网管登录对话框，输入用户名abc和密码123登录。如下图所示：



四、 配置关键点：

1）因证书具有时效性，证书服务器（Windows Server 2003），HTTPS服务器（S5800交换机）和用户浏览器一定要保持统一时钟，即折合成UTC时间要相同；

2）Windows Server 2003 CA服务配置，推荐使用自动颁发证书策略，缺省为手工审核；

3）SCEP为Cisco提议，目前状态为Internet Draft，而H3C设备尚不支持SCEP Challenge，因此在配置微软SCEP插件时一定要去掉SCEP Challenge选项；

4）S5800通过SCEP申请证书，微软SCEP插件充当RA，因此S5800配置证书申请的注册受理机构类型一定要为RA；

5）因HTTPS服务要涉及H3C设备后台Apache服务器与用户浏览器的相互兼容，请使用H3C验证过的浏览器实施基于HTTPS的Web网管。