

知 Windows Server 2016操作系统搭建自签名CA证书服务器 (Microsoft Active Directory 证书服务)

证书 漏洞相关 SSL 胡伟 2020-12-10 发表

组网及说明

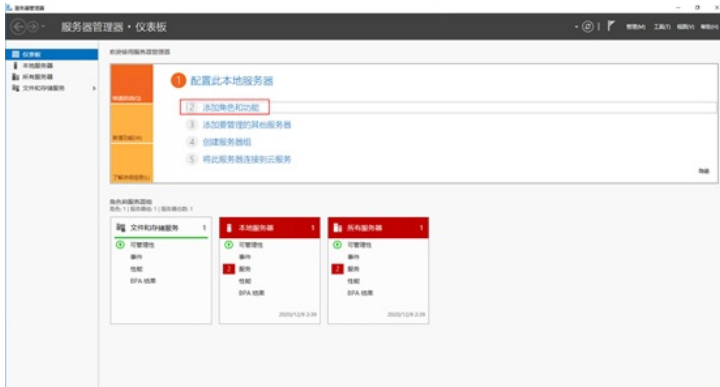
Comware V7安全设备在开启ssl server-policy相关服务时，需要引用PKI的证书服务。
通常我们使用Windows Server 2016进行搭建自签名证书服务器。

Windows Server 2016操作系统安装可参考知了案例

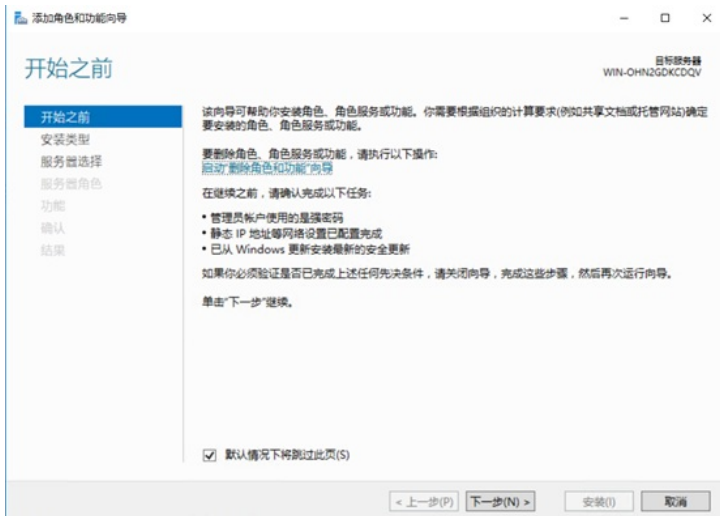
<https://zhiliao.h3c.com/Theme/details/136588>

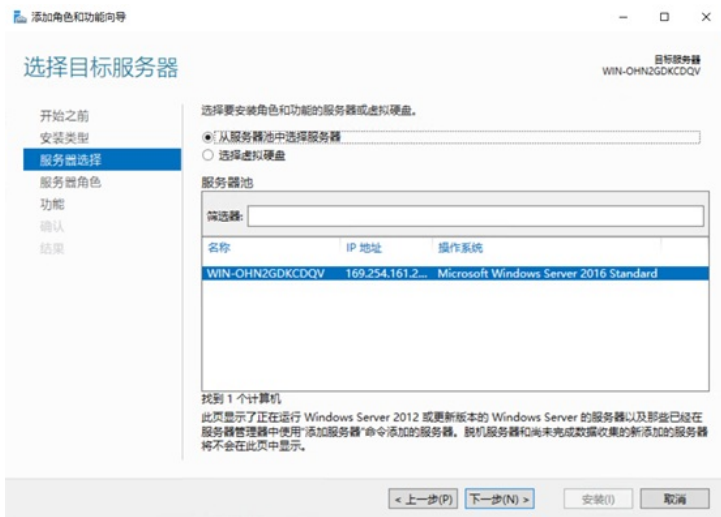
配置步骤

1, 打开服务器管理器，点击【添加角色和功能】。

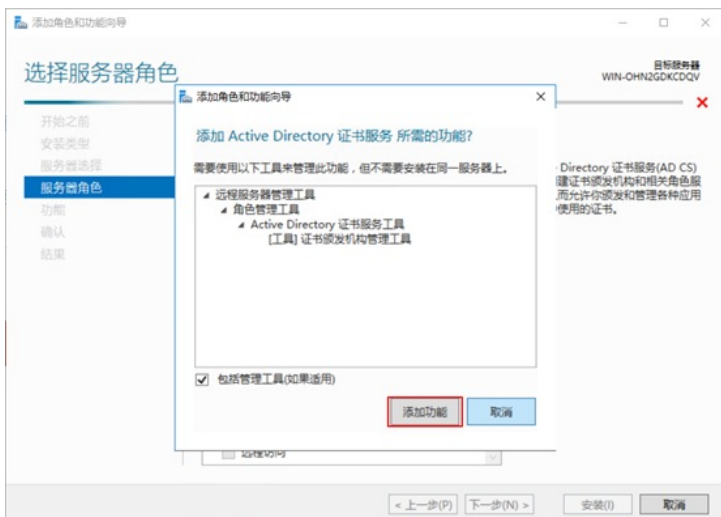
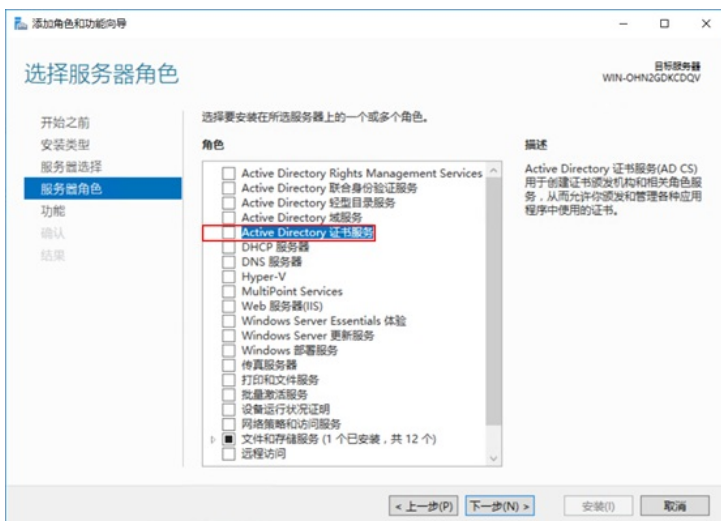


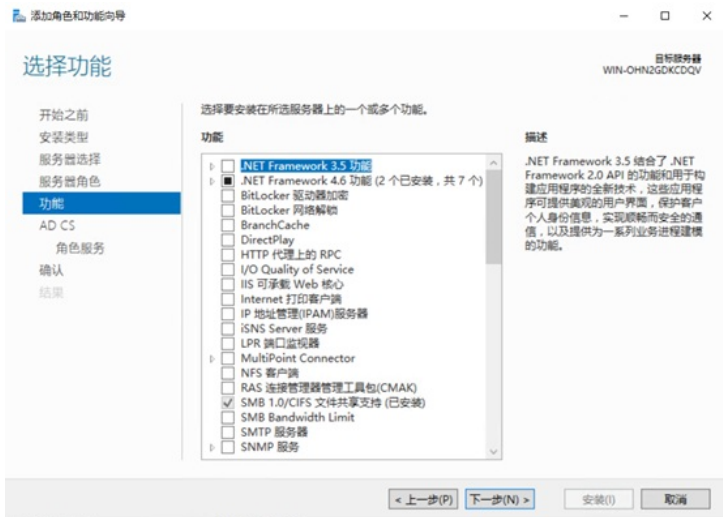
2, 以下步骤缺省点击【下一步】。



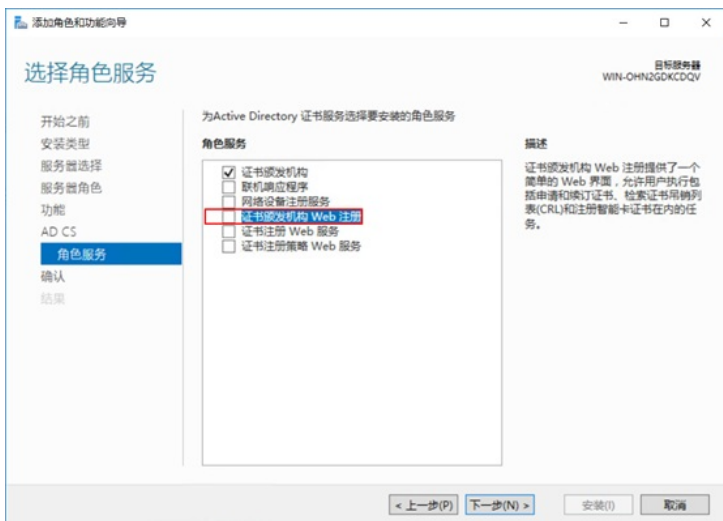


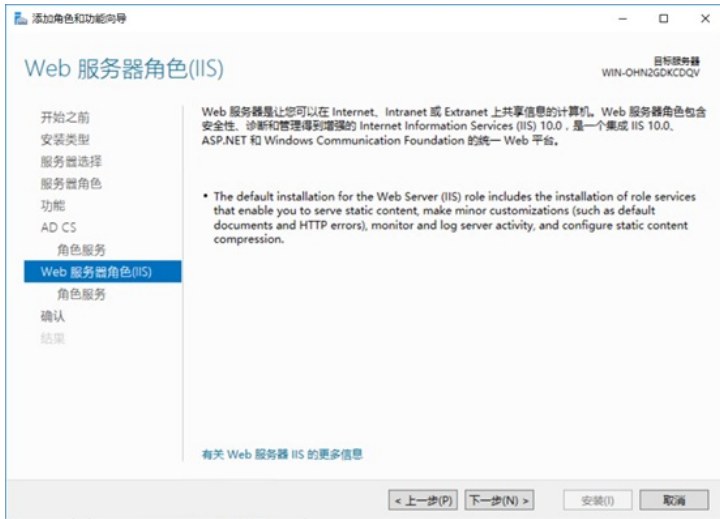
3, 服务器角色需要勾选【Active Directory证书服务】并点击该项自动弹出的【添加功能】, 然后继续点击【下一步】。





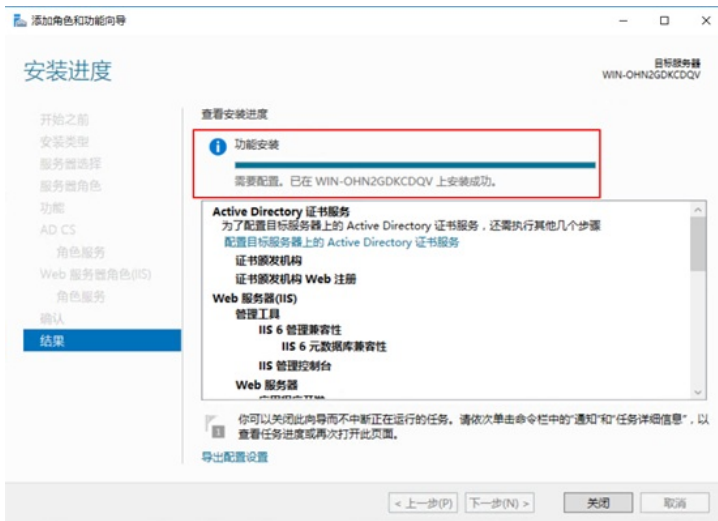
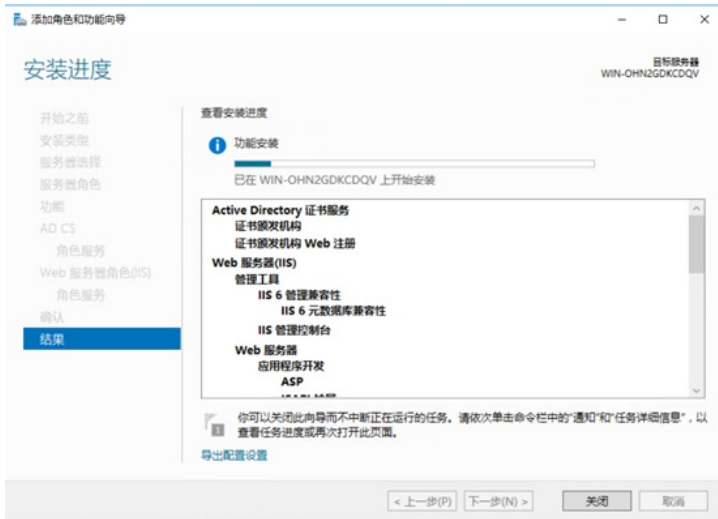
4, 这里再勾选【证书颁发机构Web注册】并点击该项自动弹出的【添加功能】，然后以下步骤缺省点击【下一步】。



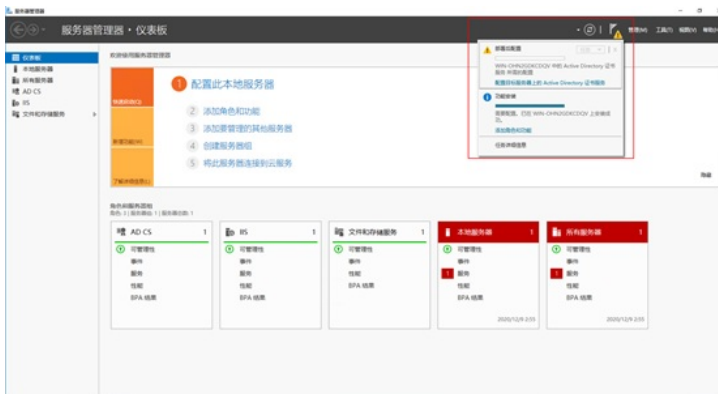


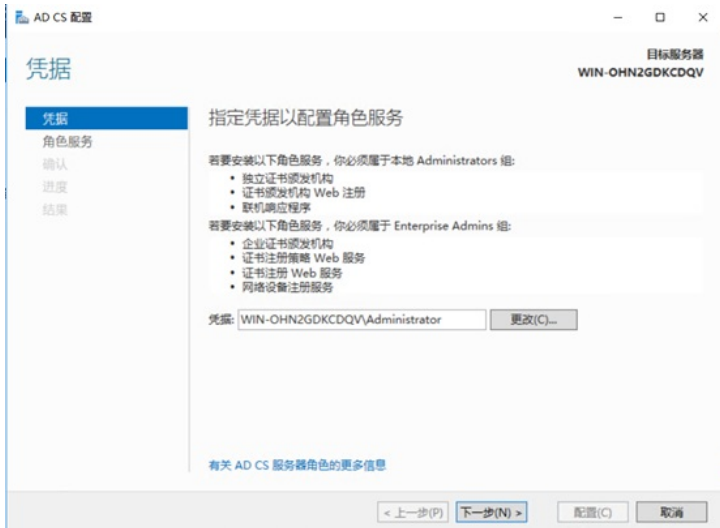
5, 点击【安装】并等待安装完成。





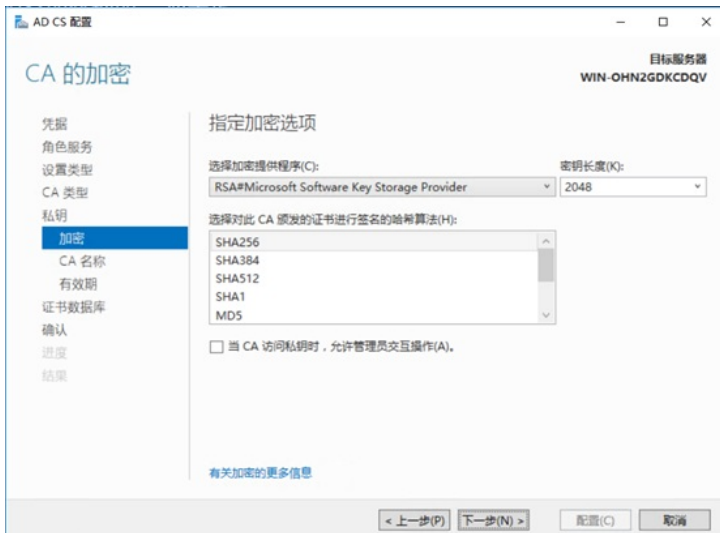
6, 在服务器管理器点击右上角提示, 进行【配置目标服务器上的Active Directory证书服务】, 然后点击【下一步】。





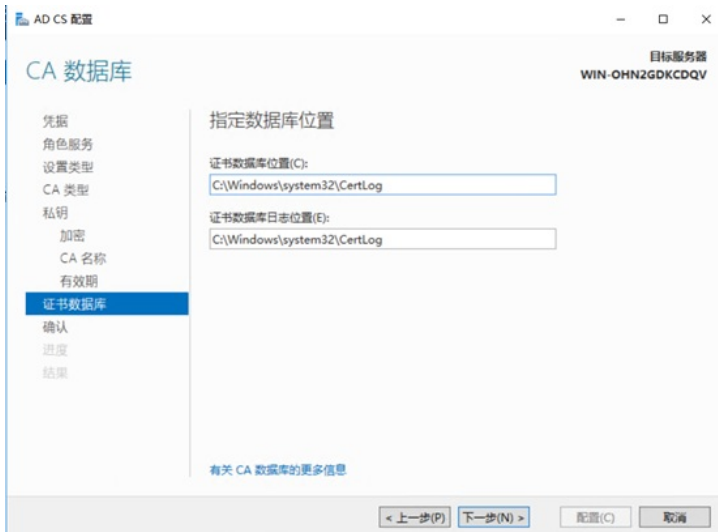
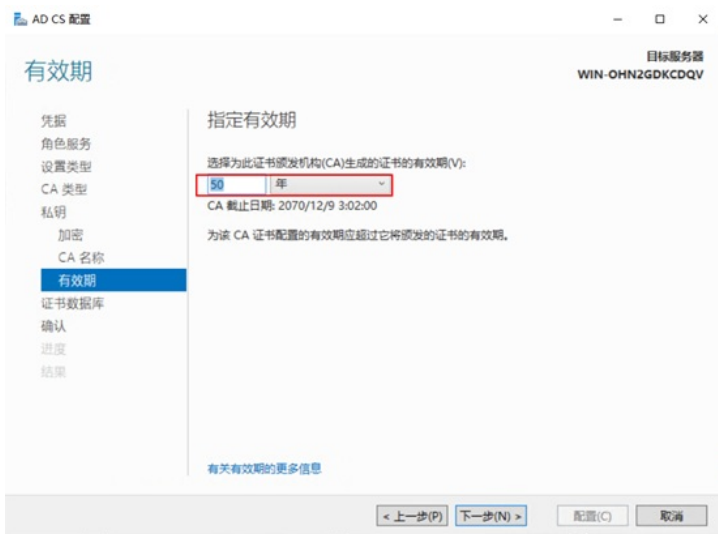
7, 角色服务配置需要将前两个选项【证书颁发机构】和【证书颁发机构Web注册】同时勾选, 然后以下步骤缺省点击【下一步】。

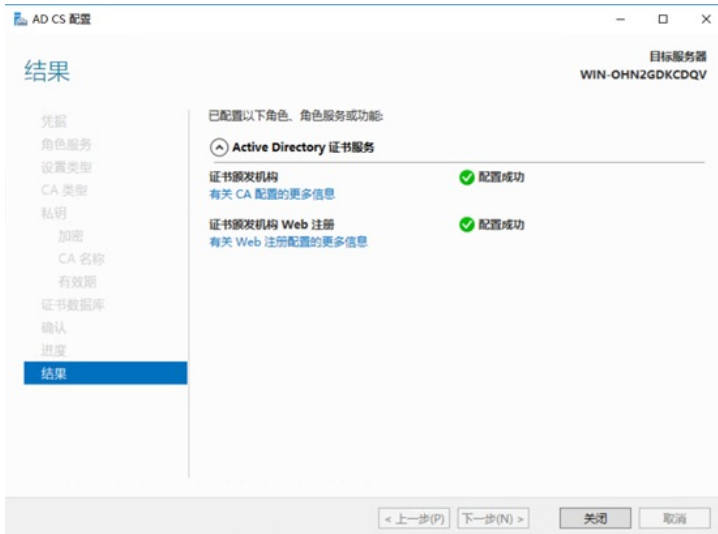
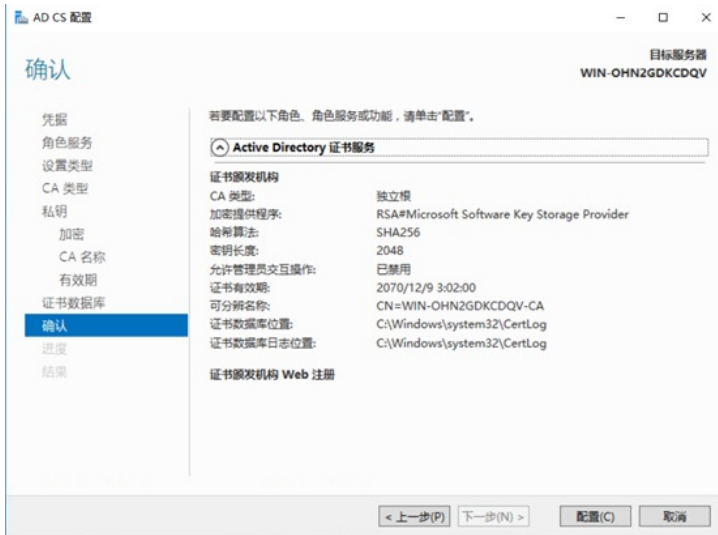






8, 这里证书有效期建议设置为50年, 继续【下一步】直到配置完成。

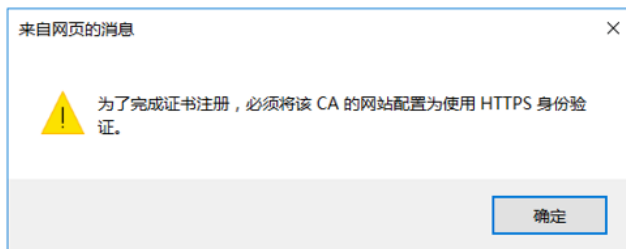




9, 重启操作系统后, 打开系统本地IE浏览器, 输入<http://127.0.0.1/certsrv>, 即可使用证书服务, 当然也可在终端使用IE浏览器访问<http://X.X.X.X/certsrv>来获取证书服务(X.X.X.X为证书服务器的IP地址)。

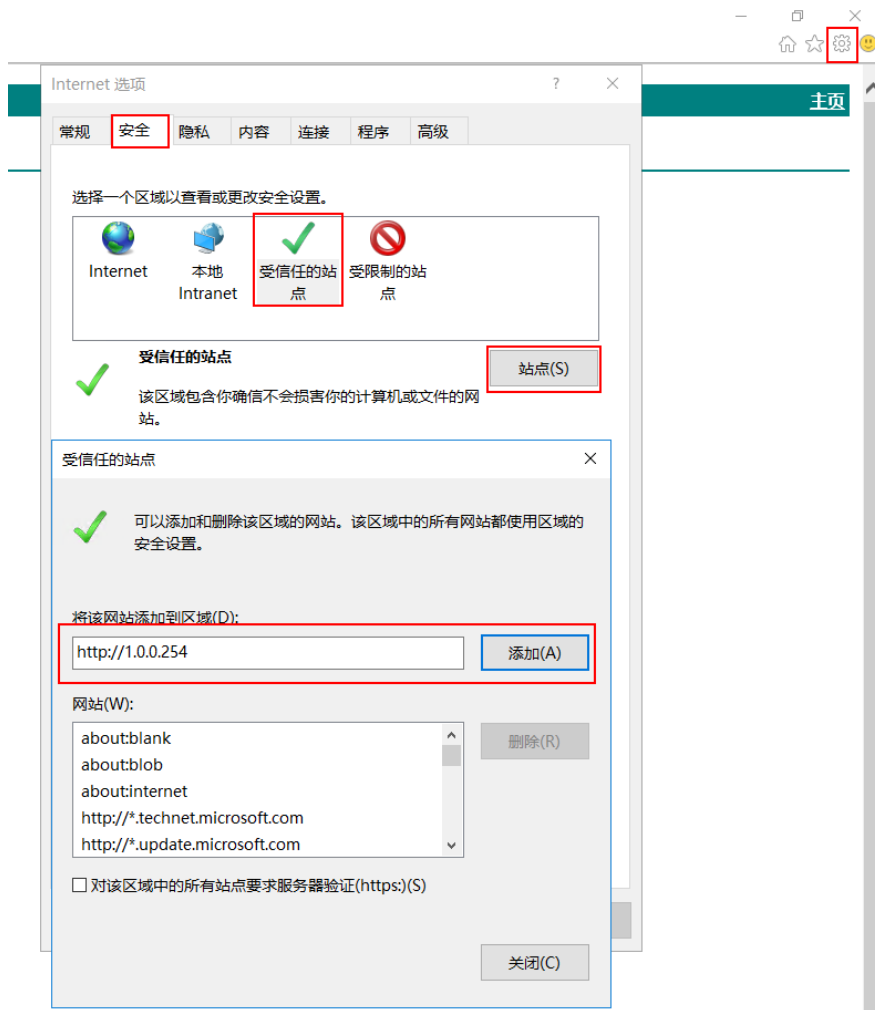


如果申请证书过程中有提示"为了完成证书注册,必须将该CA的网站配置为使用HTTPS身份验证":

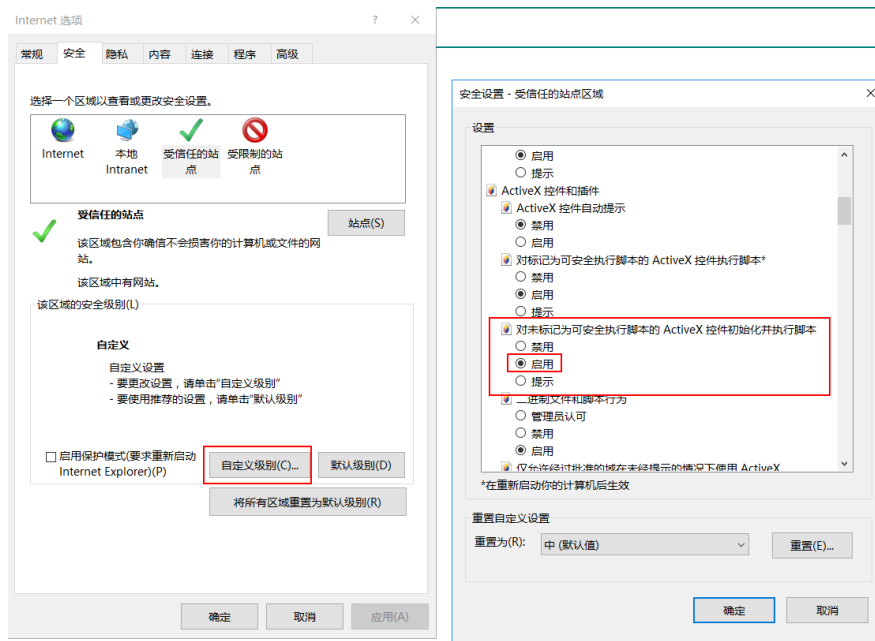


可以对IE浏览器进行如下操作:

首先: 点击【Internet选项】->点击【安全】->点击【受信任的站点】->点击【站点】, 将证书网站地址 (如: http://1.0.0.254) 【添加】到信任站点中, 添加完毕后, 点击【关闭】。



接着: 继续在【受信任的站点】为准点击【自定义级别】, 此时会弹出一个【安全设置】子界面, 拖动滚动条, 找到【对未标记为可安全执行脚本的ActiveX空间初始化并执行脚本】, 将其勾选为【启用】, 之后点击所有【确认】操作, 直到【Internet选项】关闭为止。



10, 在操作系统【Windows管理工具】->【证书颁发机构】组件中可以对证书进行管理。



至此，在Windows Server 2016操作系统中安装自签名CA证书服务器已顺利完成。

配置关键点

无