

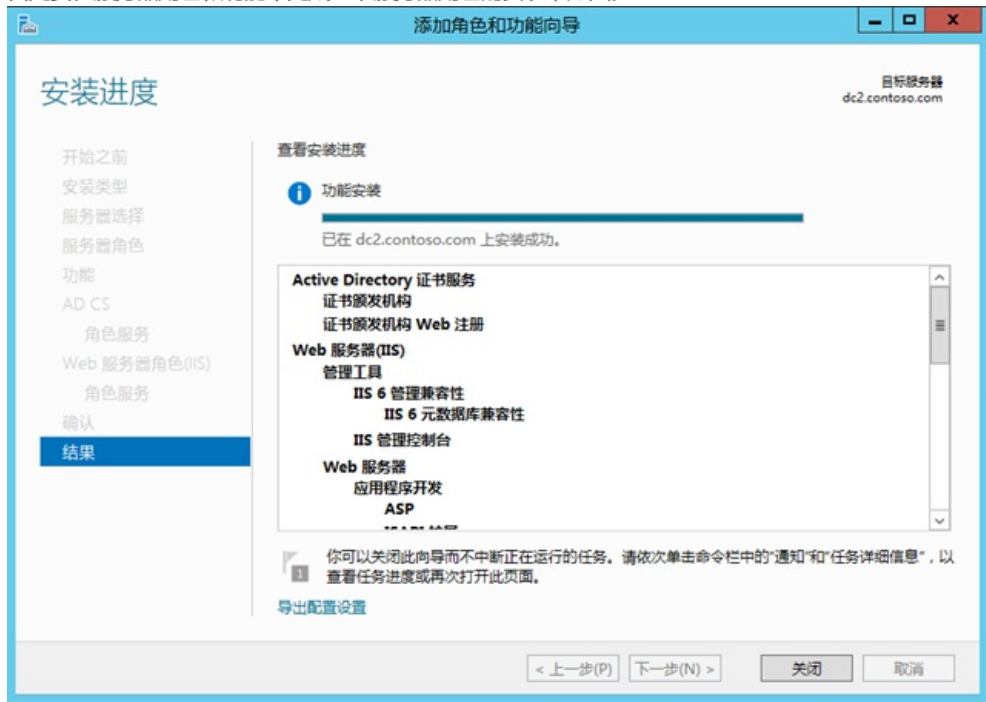
Windows Server 2012 R2工作文件夹④：服务器证书配置

客户端在访问工作文件夹的时候要使用到HTTPS的方式，所以我们需要配置WF.contoso.com这台工作文件夹服务器使用专门的服务器证书，而且要把证书绑定到IIS的HTTPS访问443端口，下面我们来看一下实现的过程。

（一）环境中需要具备一台CA证书颁发服务器

首先我们需要在环境中部署一台CA证书服务器，在我的demo环境中，CA是和DC服务器并置的，我所使用的CA是企业根CA，下面来看看部署CA的关键步骤。

首先要在服务器角色和功能中完成证书服务器角色的安装，如图。



然后进入证书配置向导，继续配置证书服务器。

除了下面图片中的步骤勾选“证书颁发机构”和“证书颁发机构Web注册”以外，其他的步骤全部保持默认即可。如图。



配置完成后，如图所示。



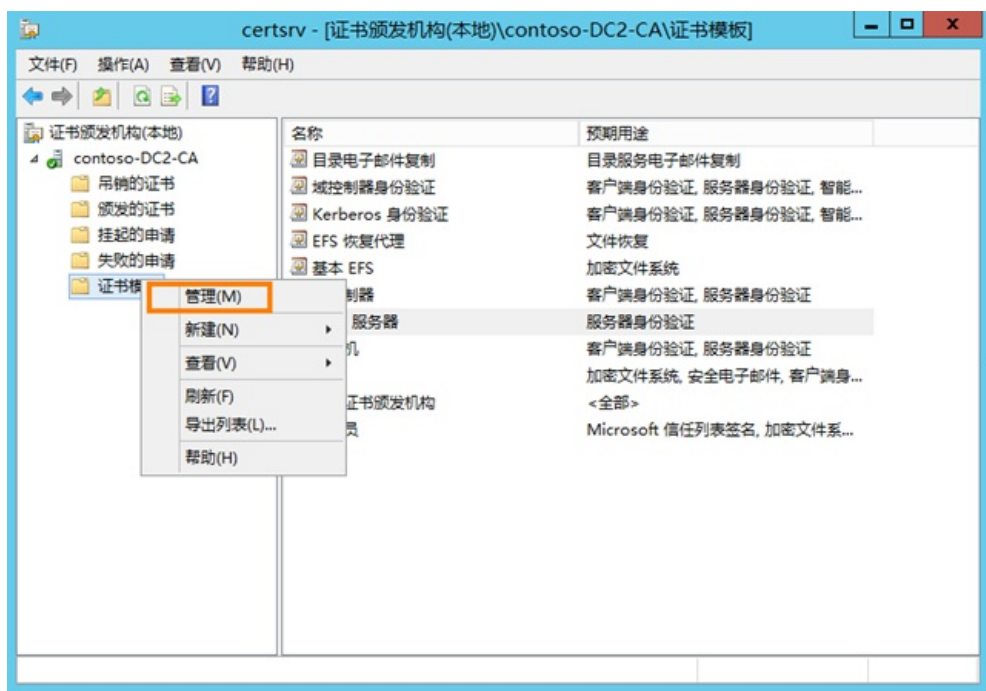
(二) 为工作文件夹服务器所使用的服务器证书新建专用的证书模板，并申请服务器证书

备注：该步骤不是必须的，也可以使用默认的WEB服务器模板

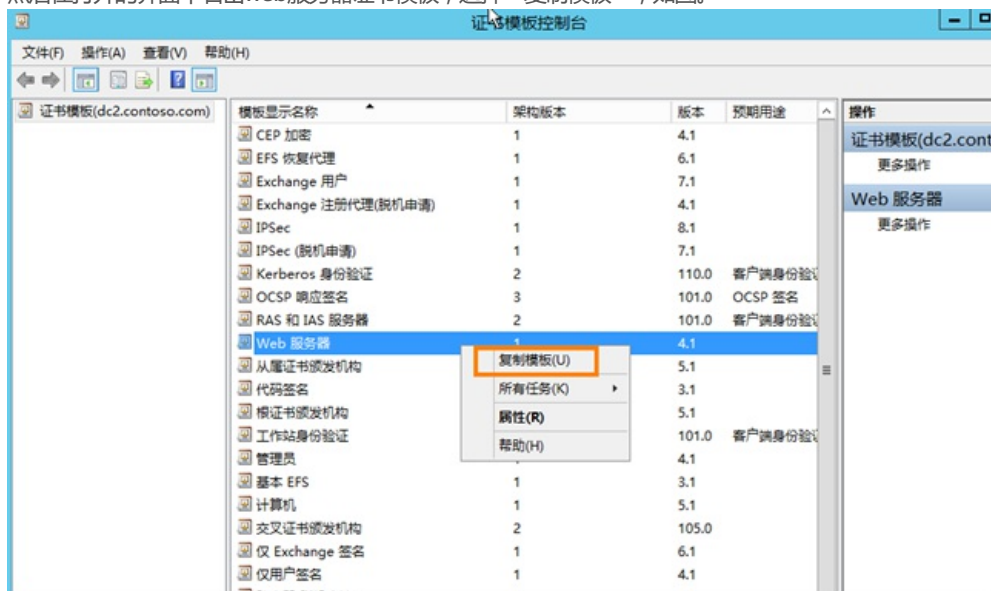
打开CA证书颁发机构管理控制台，如图。



右击证书模板，选择“管理”，如图。



然后在打开的界面中右击web服务器证书模板，选择“复制模板”，如图。



在常规中，为复制后的模板起个名字：工作文件夹。如图。

新模板的属性

X

服务器	发布要求	取代模板	扩展	安全	
兼容性	常规	请求处理	加密	密钥证明	使用者名称

模板显示名称(E):

工作文件夹

模板名(T):

工作文件夹

有效期(V):

2

年

续订期(R):

6

周

☐ 在 Active Directory 中发布证书(P)

☐ 如果 Active Directory 中有一个重复证书，不要自动重新注册(D)

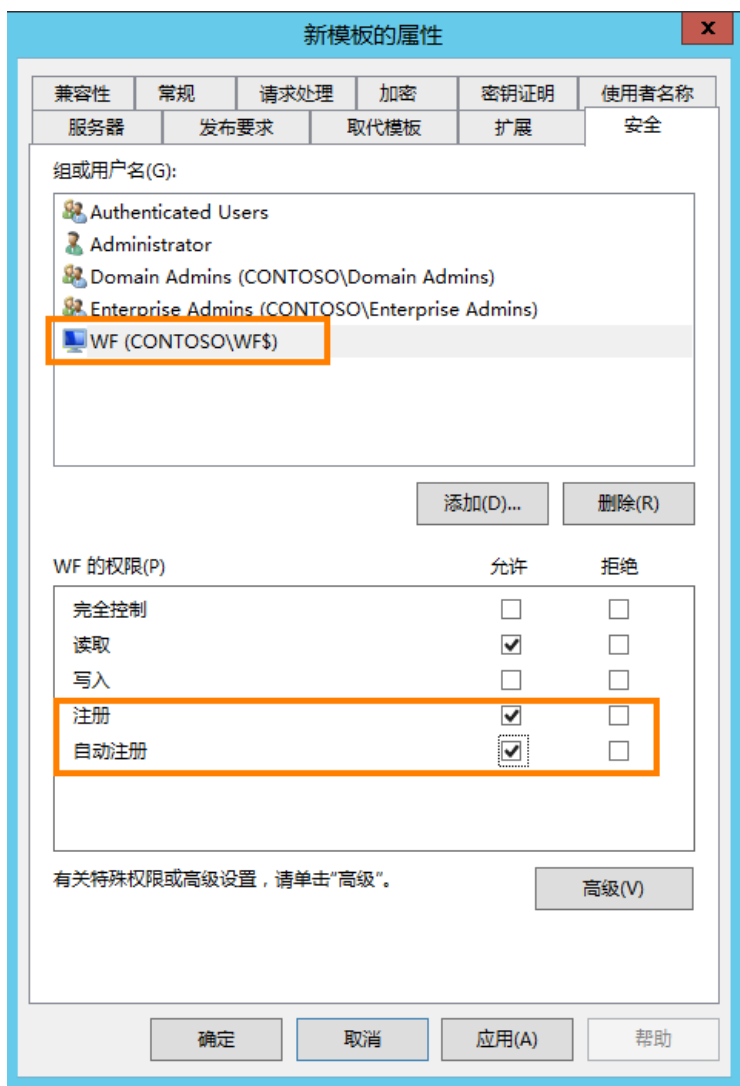
确定

取消

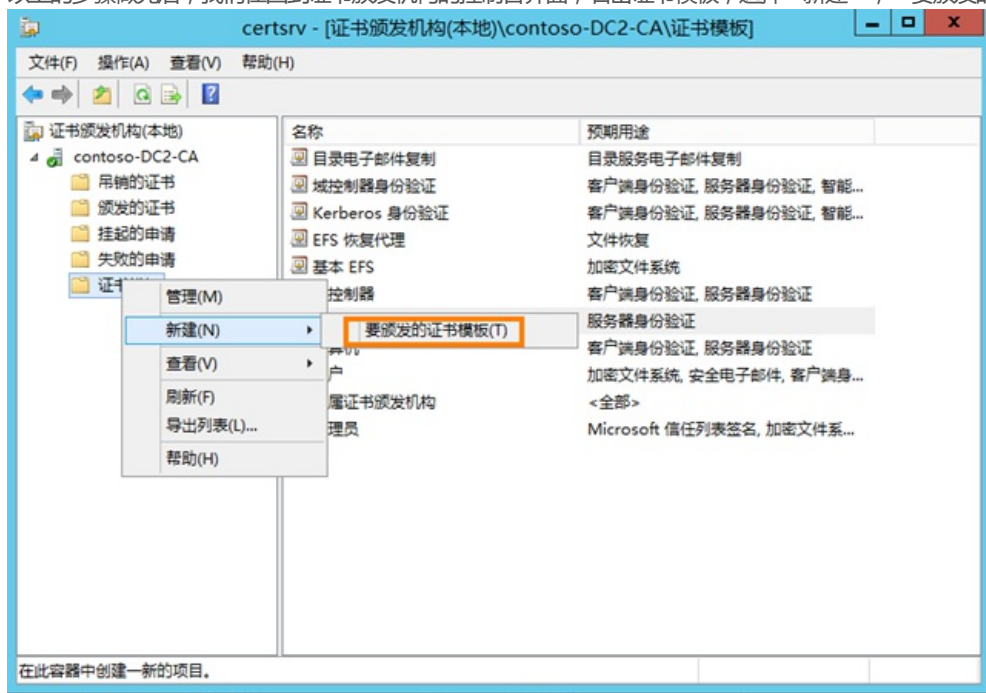
应用(A)

帮助

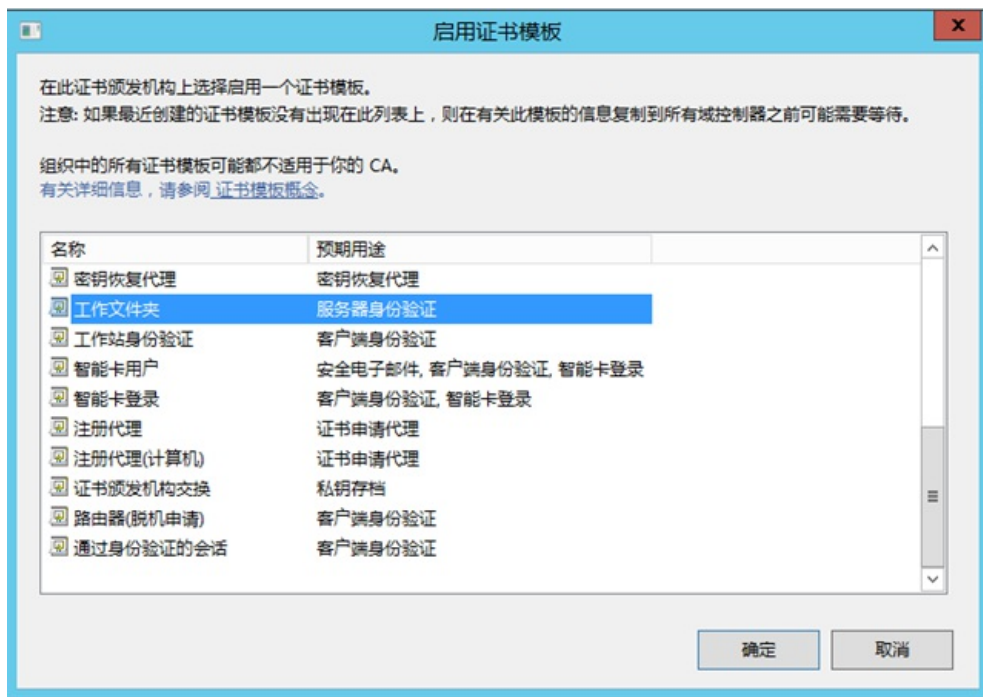
然后在模板属性的安全选项卡，把工作文件夹服务器的计算机名称添加进来，并给予“注册”和“自动注册”的权限。如图。



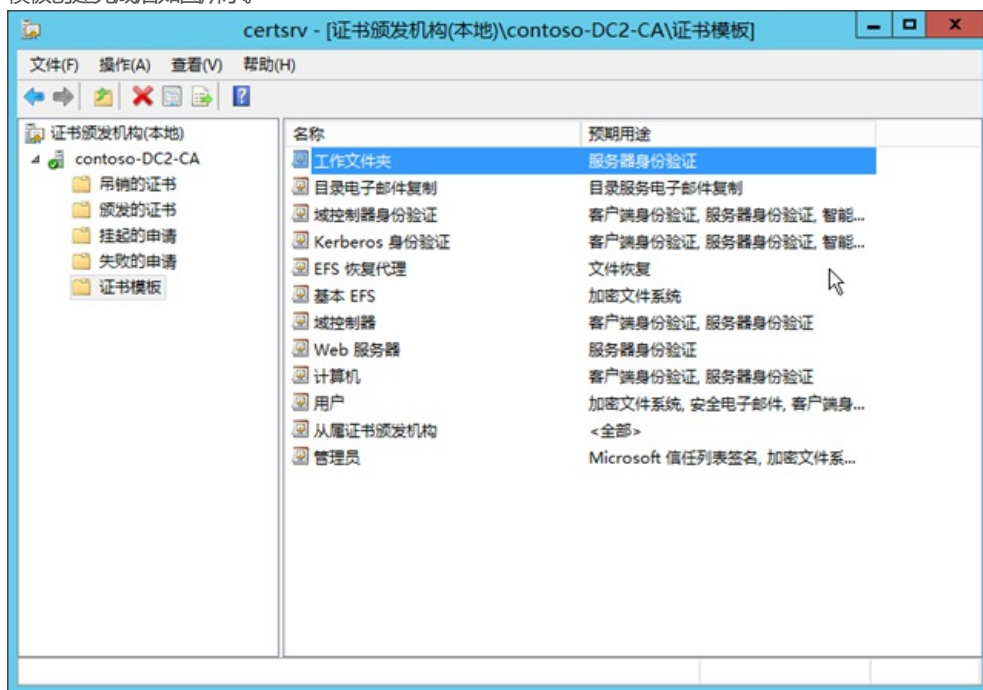
以上的步骤做完后, 我们在回到证书颁发机构的控制台界面, 右击证书模板, 选择“新建”, “要颁发的证书模板”, 如图。



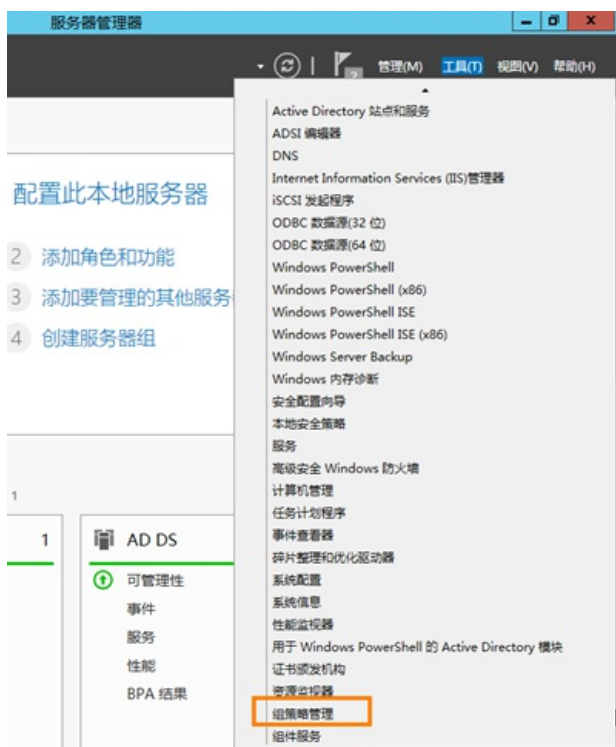
在模板列表中选择我们刚才复制出来的“工作文件夹”模板。如图。



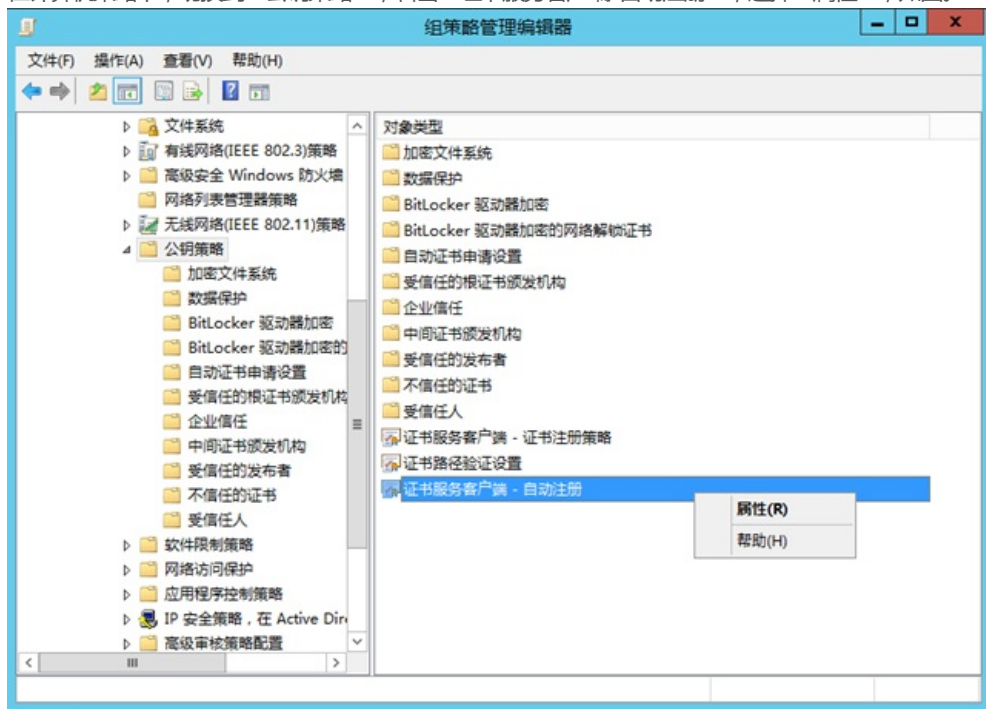
模板创建完成后如图所示。



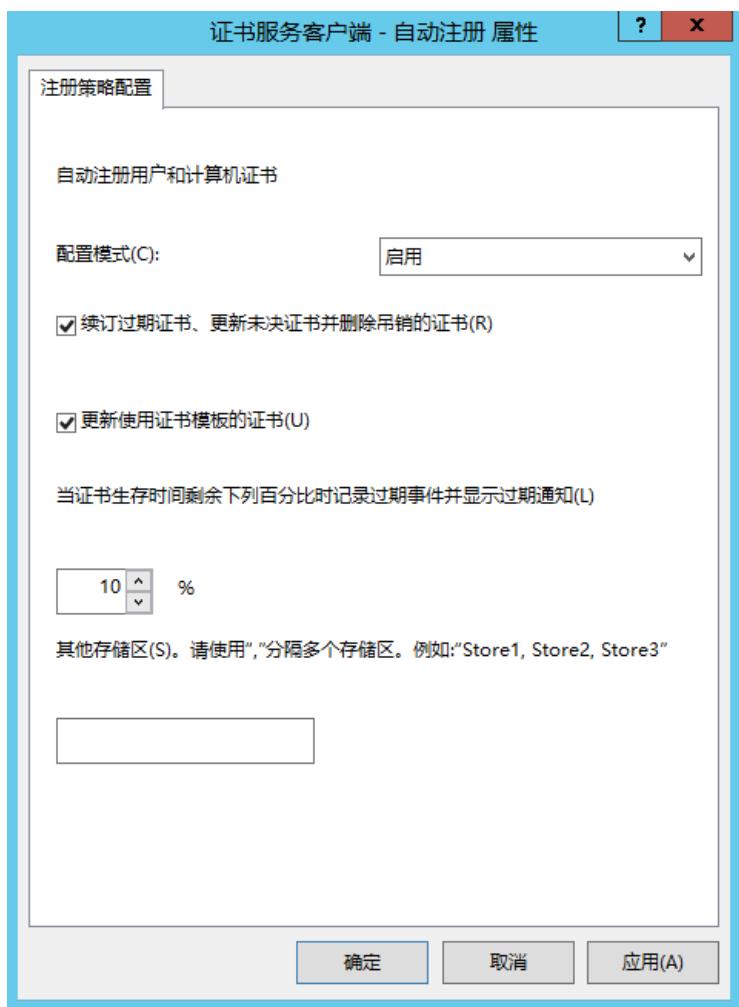
接下来, 我们在通过服务器管理器打开“组策略管理”工具, 来设置证书自动注册的相关策略, 如图。



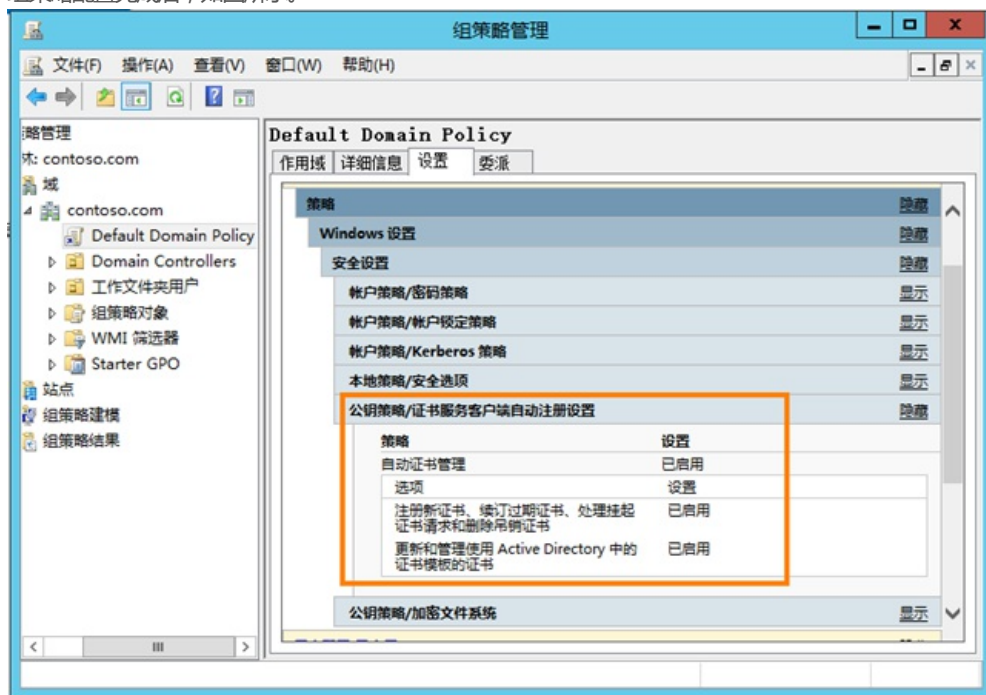
在计算机策略下，切换到“公钥策略”，右击“证书服务客户端-自动注册”，选择“属性”，如图。



在证书客户端自动注册属性中，选择配置模式为已启用，并勾选“续订过期证书、更新未决证书并删除吊销的证书”和“更新使用证书模板的证书”，如图。

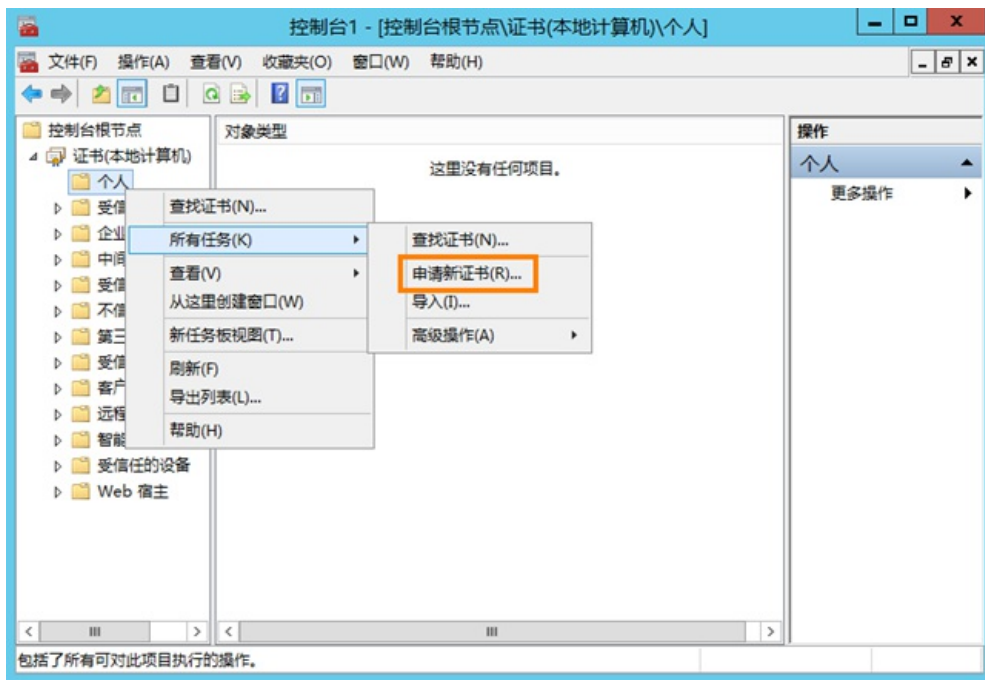


组策略配置完成后，如图所示。



接下来我们手动为WF.contoso.com工作文件夹服务器手动申请服务器证书。

在WF.contoso.com工作文件夹服务器上打开MMC，加载证书单元（本地计算机），在个人中，右击选择“所有任务”，“申请新证书”，如图。

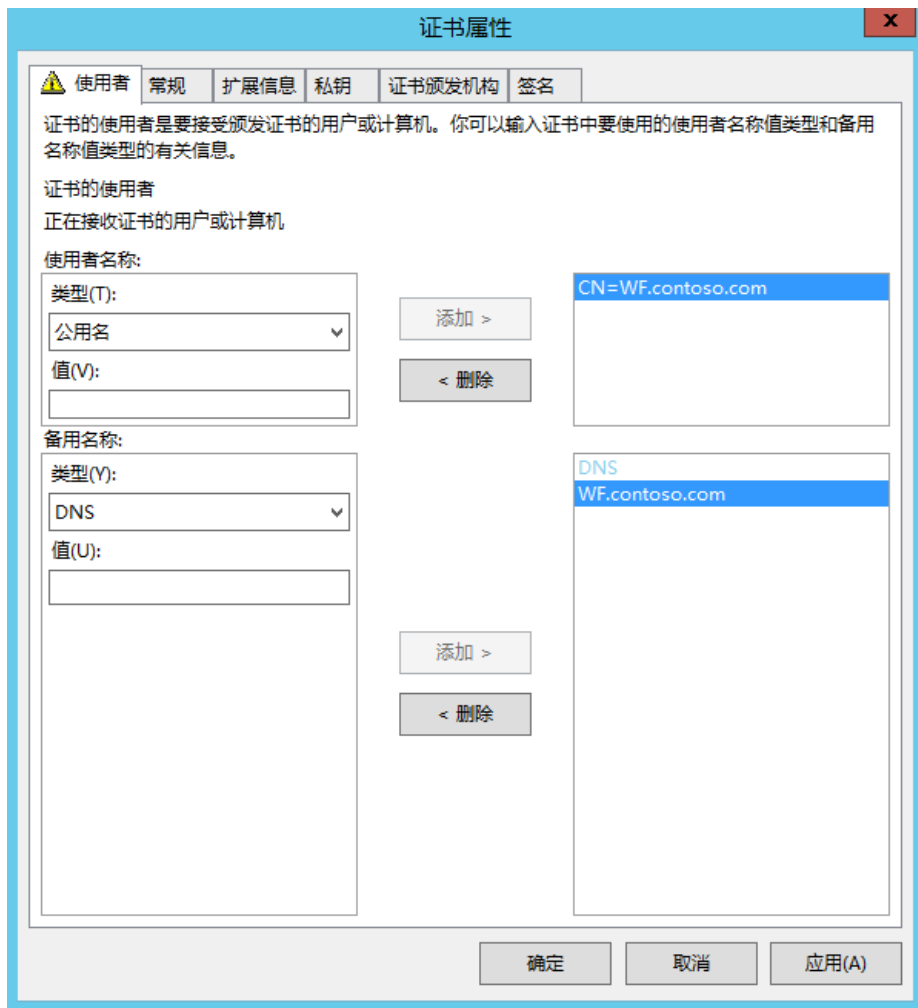


选择“工作文件夹”证书模板，并点击“注册此证书需要详细信息，单击这里以配置设置”进行证书的设置，如图。



这里我配置了一下证书的使用者名称和备用名称。如图。

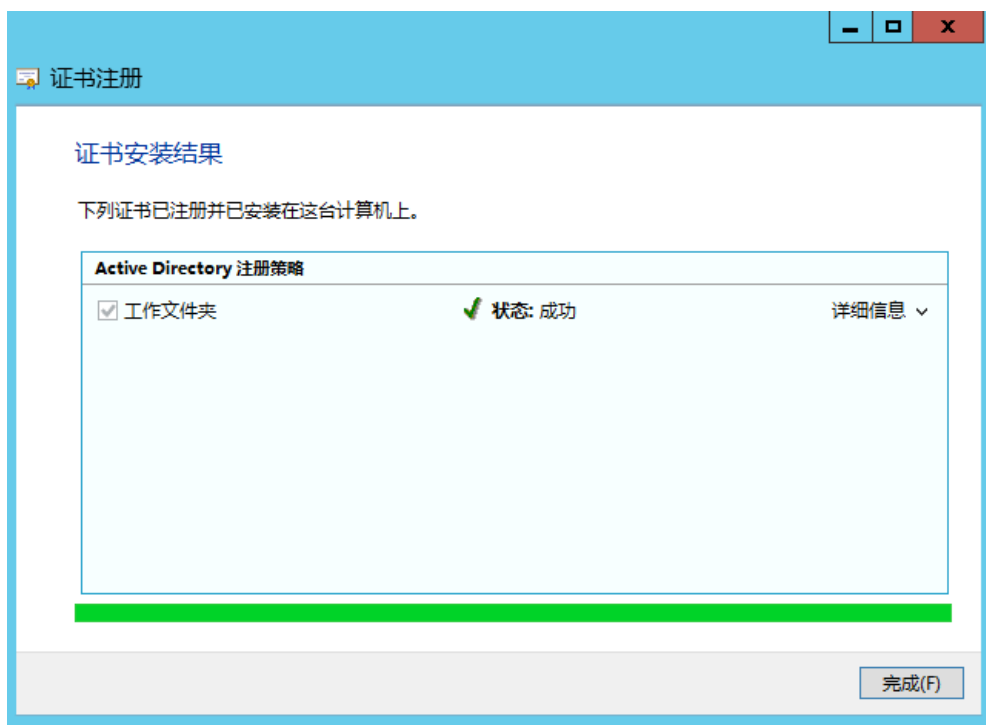
备注：我的环境中只使用了WF.contoso.com。



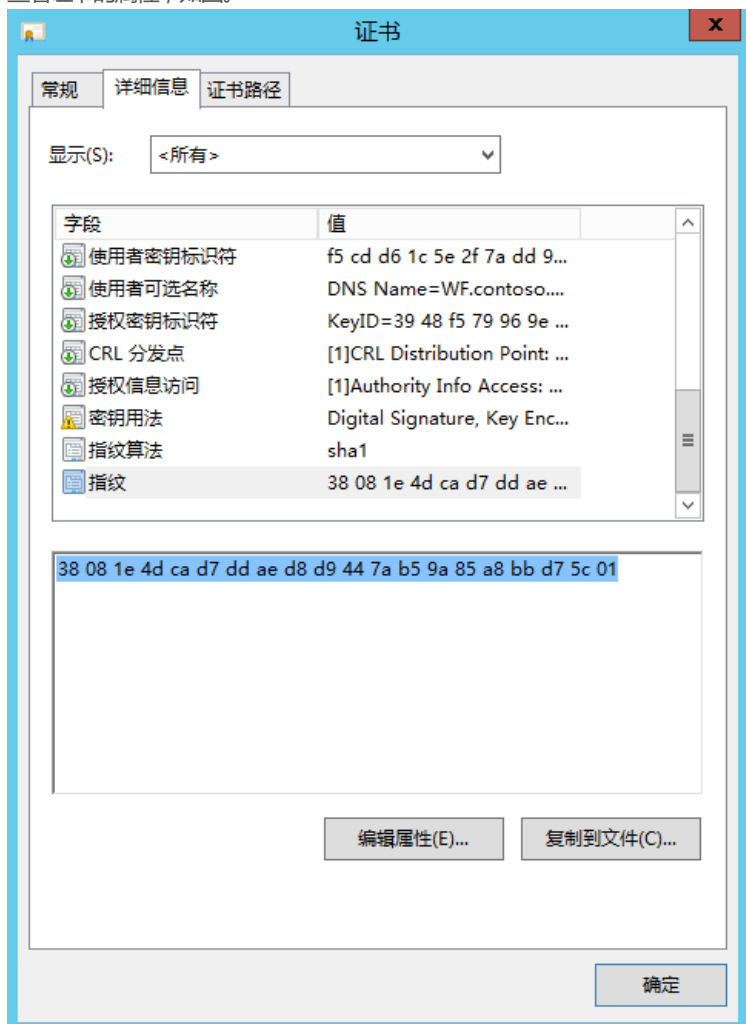
然后回到证书请求界面，点击“注册”，如图。



注册完成后，如图所示。



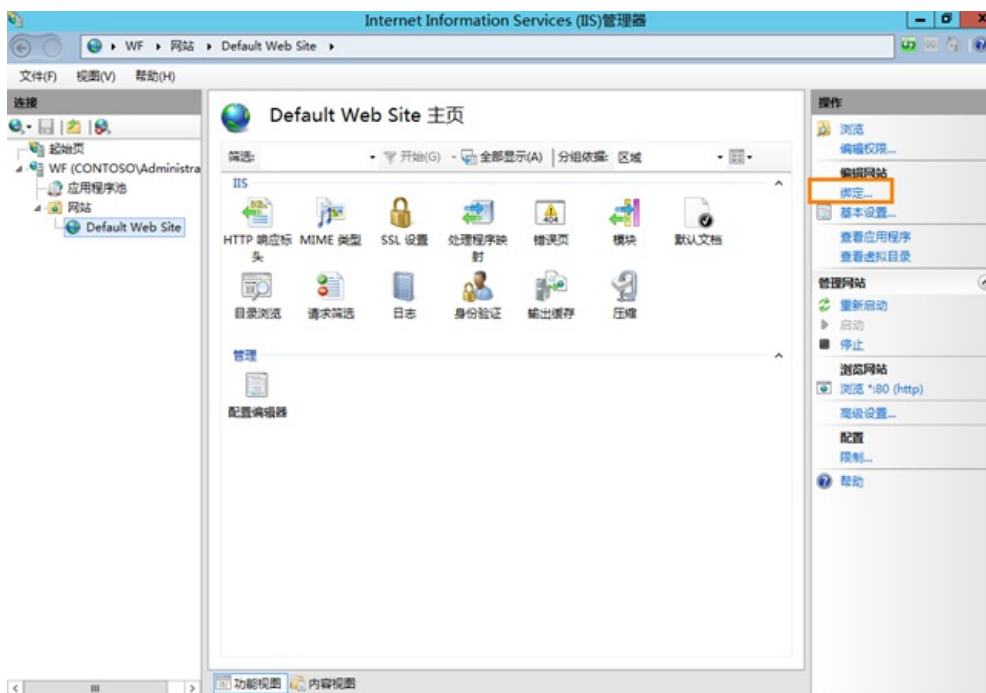
查看证书的属性，如图。



(三) 配置IIS的证书绑定

做完上述操作后，下面我们来将申请到的服务器证书绑定到IIS。

首先打开IIS管理器，在下图的界面中，选择“绑定”，如图。

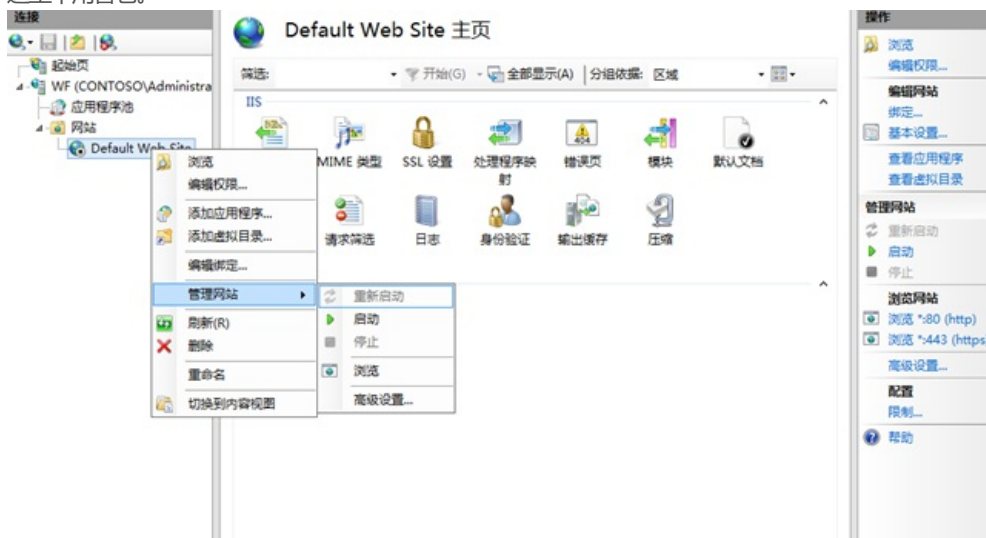


在添加网站绑定界面，选择类型为HTTPS，选择的SSL证书为我们上一个步骤中所申请的服务器证书，如图。



配置完成后，我们会发现默认的IIS站点处于停止状态，这是正常的，我们也不需要没办法启用它，因为默认IIS的端口被工作文件夹占用了。

这里不用管它。



到此为止，证书的新建、配置、申请和绑定都讲完了。接下来我们将继续对工作文件夹服务器进行其他的准备和配置工作，敬请关注。

本文出自“[曾垂鑫的技术专栏](#)”博客，谢绝转载！

