通过CAPF在线CA配置自动证书注册和续订

目录

简介

本文档介绍通过适用于Cisco Unified Communications Manager(CUCM)的证书授权代理功能(CAPF)在线功能进行的自动证书注册和续订。

作者：Michael Mendoza，思科TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Unified Communications Manager
- X.509证书
- Windows 服务器
- Windows Active Directory(AD)
- Windows Internet信息服务(IIS)
- NT（新技术）LAN管理器(NTLM)身份验证

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM 版本 12.5.1.10000-22
- Windows Server 2012 R2
- IP电话CP-8865/固件：SIP 12-1-1SR1-4和12-5-1SR2。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档介绍该功能的配置和相关资源，以供进一步研究之用。

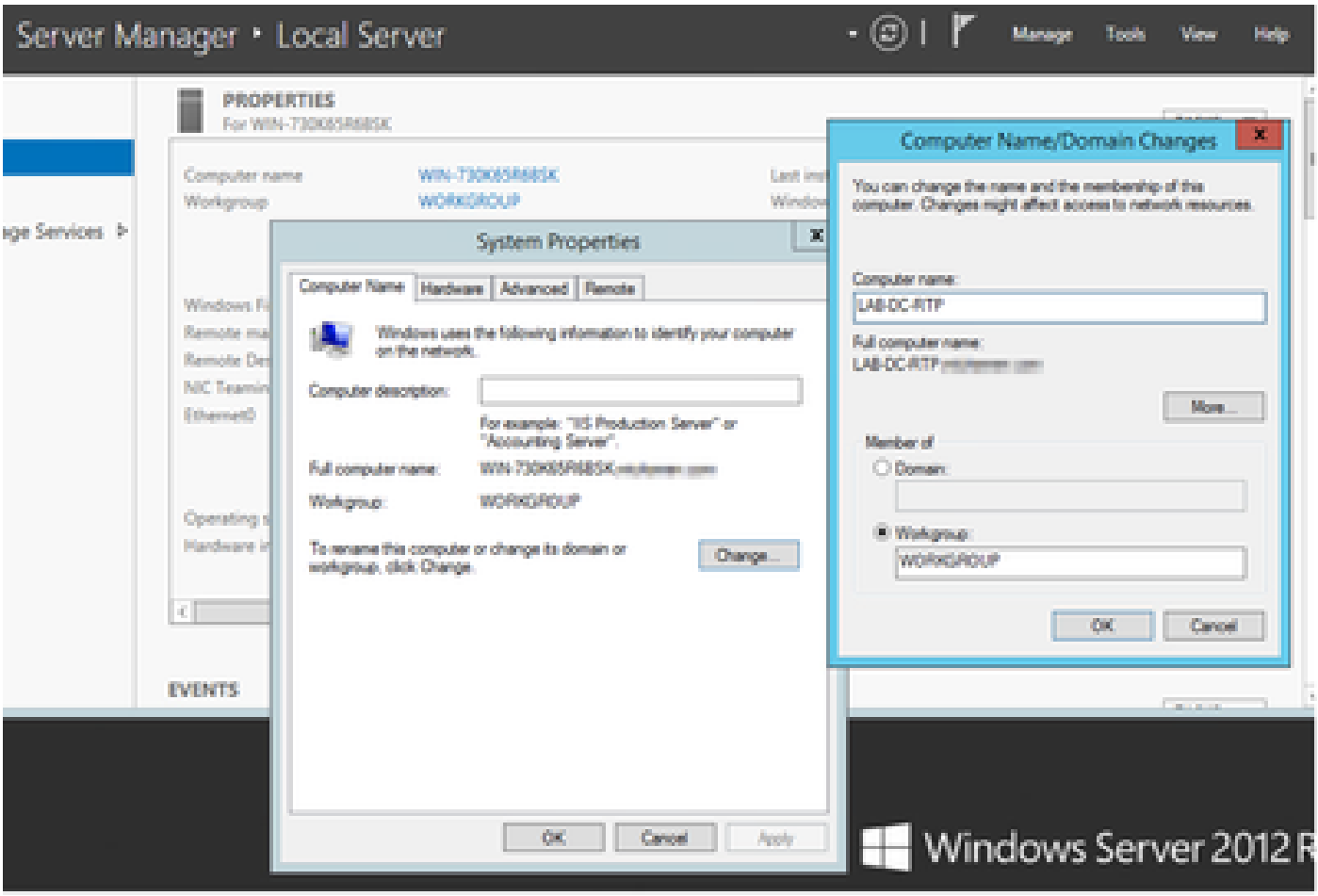
验证服务器时间和日期

确保Windows服务器配置了正确的日期、时间和时区，因为它影响服务器的根CA（证书颁发机构）证书及其颁发的证书的有效时间。

更新服务器计算机名称

默认情况下，服务器的计算机名具有随机名称，例如WIN-730K65R6BSK。启用AD域服务之前需要做的第一件事是，确保在安装结束时将服务器的计算机名称更新为您希望服务器的主机名和根CA颁发者名称的名称；否则，在安装AD服务后需要执行许多额外的步骤来更改此设置。

- 导航到本地服务器，选择计算机名称以打开系统属性
- 选择Change按钮并键入新的计算机名称：



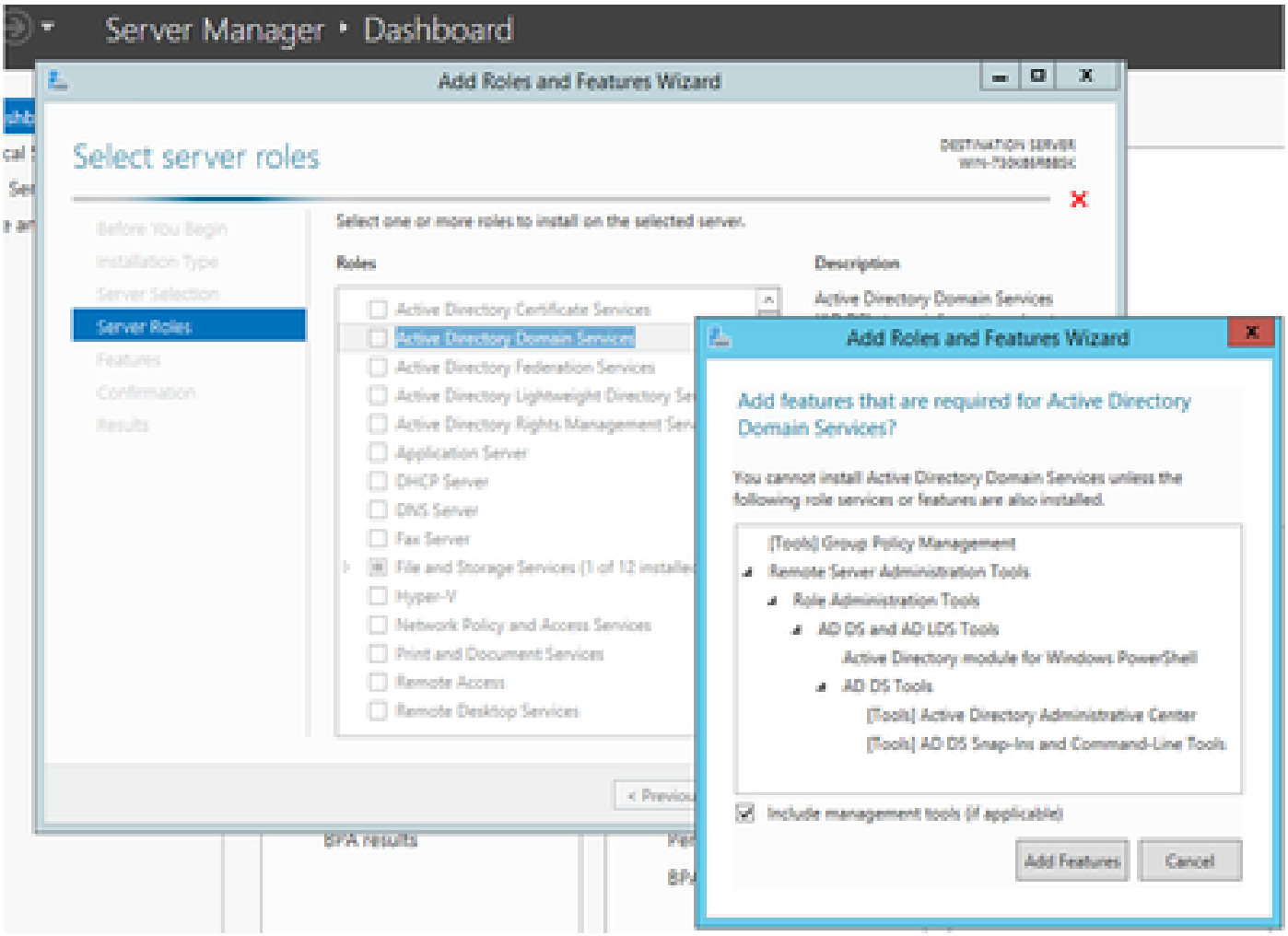
- 重新启动服务器以应用更改

配置

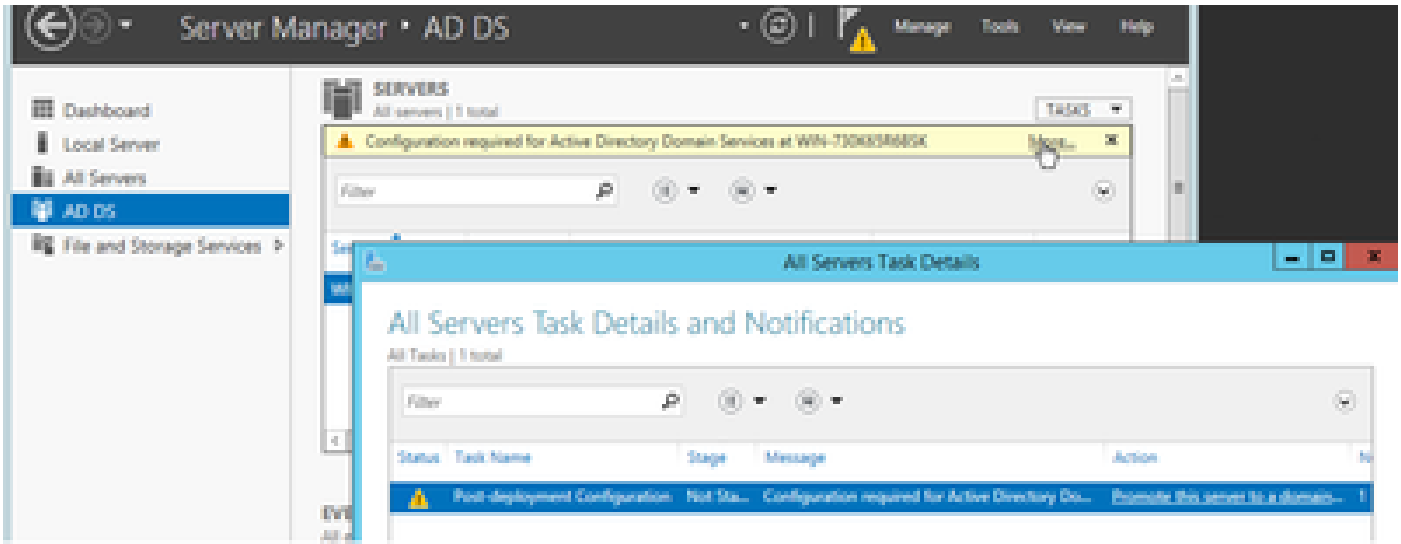
AD服务、用户和证书模板

启用和配置Active Directory服务

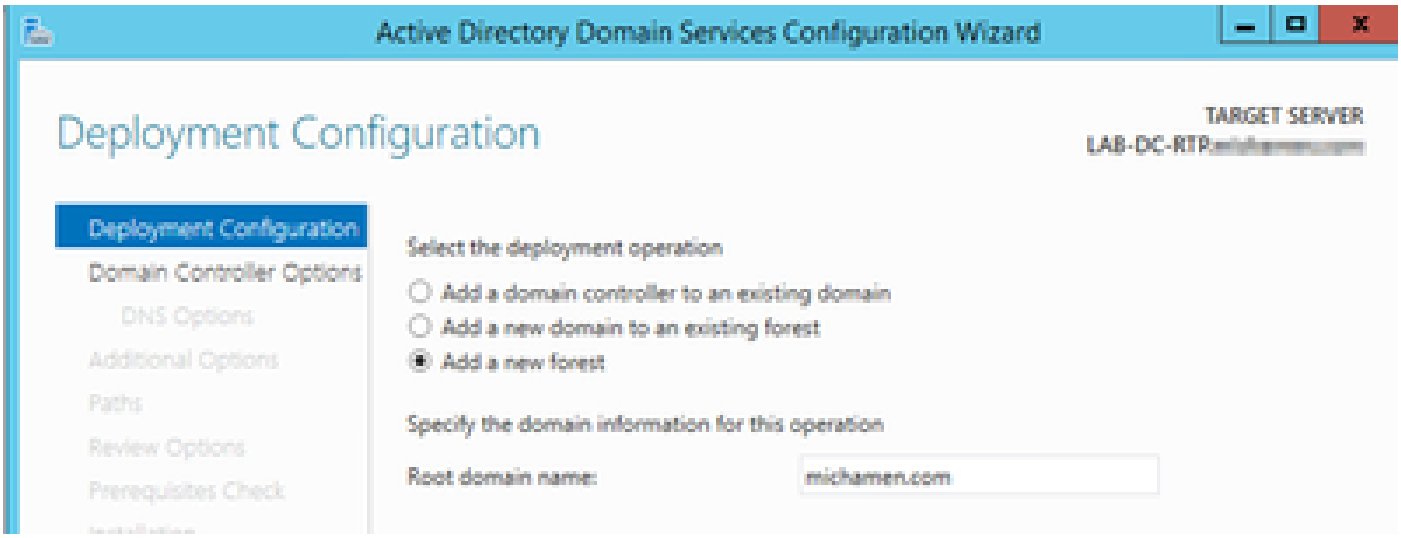
- 在服务器管理器中选择Add Roles and Features选项，选择Role-based or feature-based installation，然后从池中选择服务器（池中必须只有一个），然后选择Active Directory域服务：

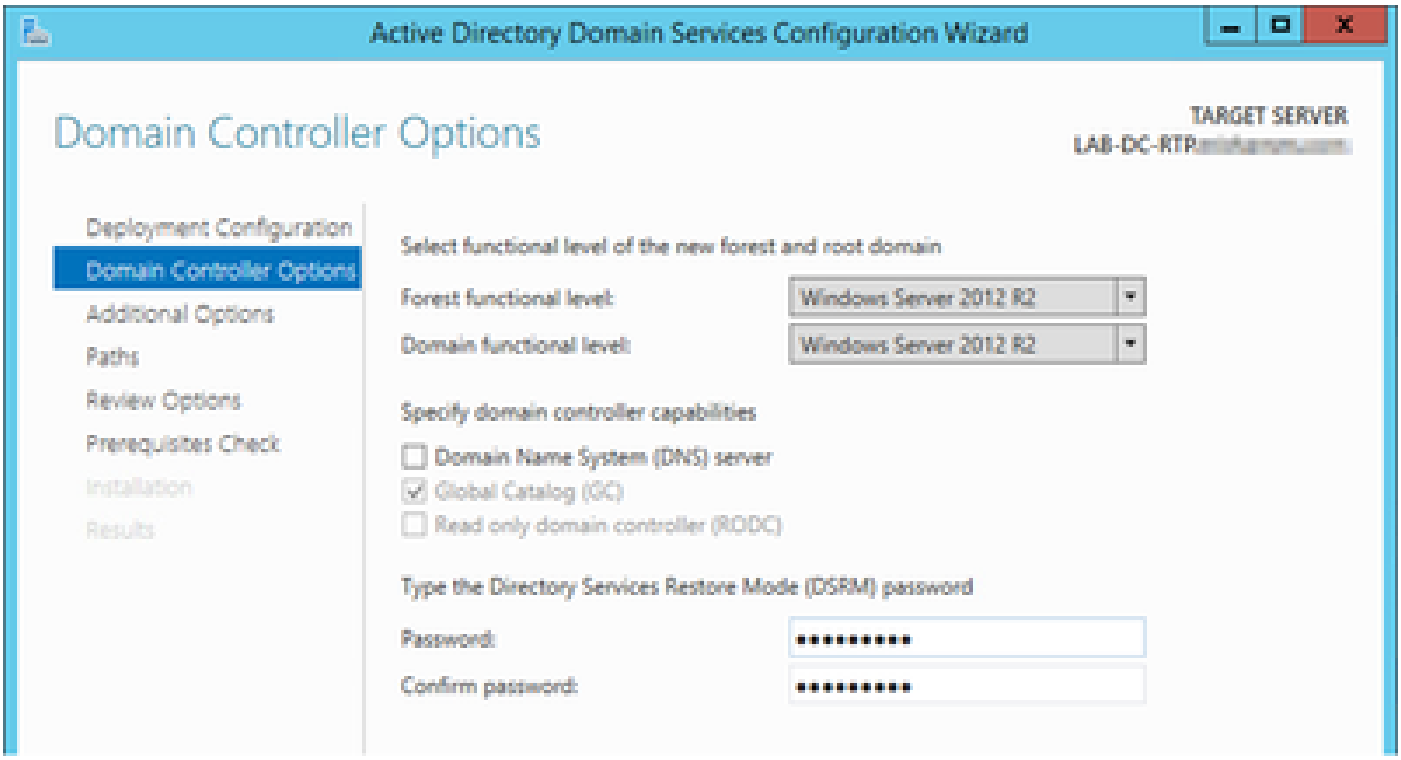


- 继续选择下一步按钮，然后选择安装
- 安装完成后，选择Close按钮
- Server Manager > AD DS下将出现一个警告选项卡，标题为Active Directory域服务所需的配置；选择more链接，然后选择可用操作以启动安装向导：

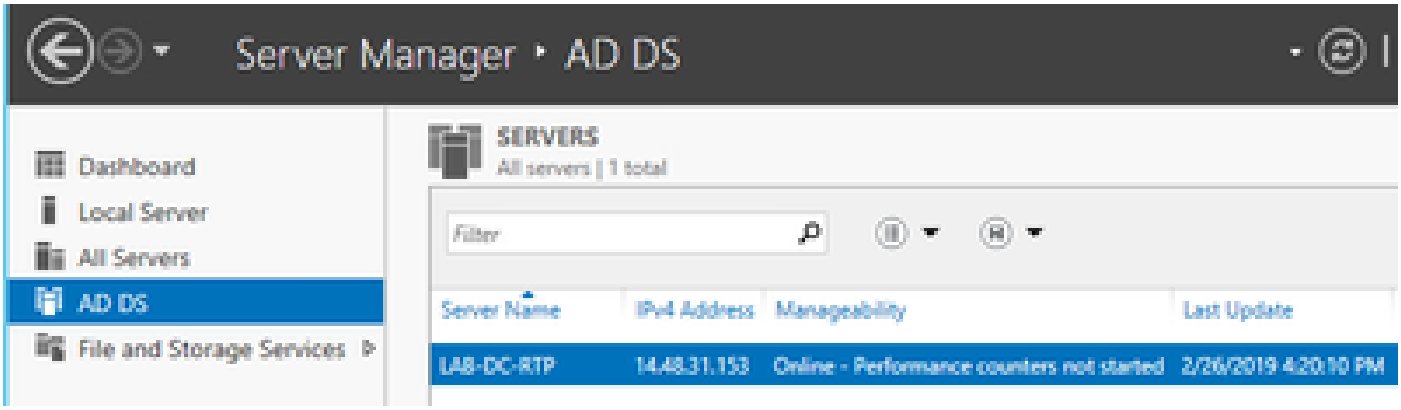


- 按照域设置向导中的提示，使用所需的根域名添加新的林(本实验使用michamen.com),并在可用时取消选中DNS框，定义DSRM密码(本实验使用C1sc0123!):



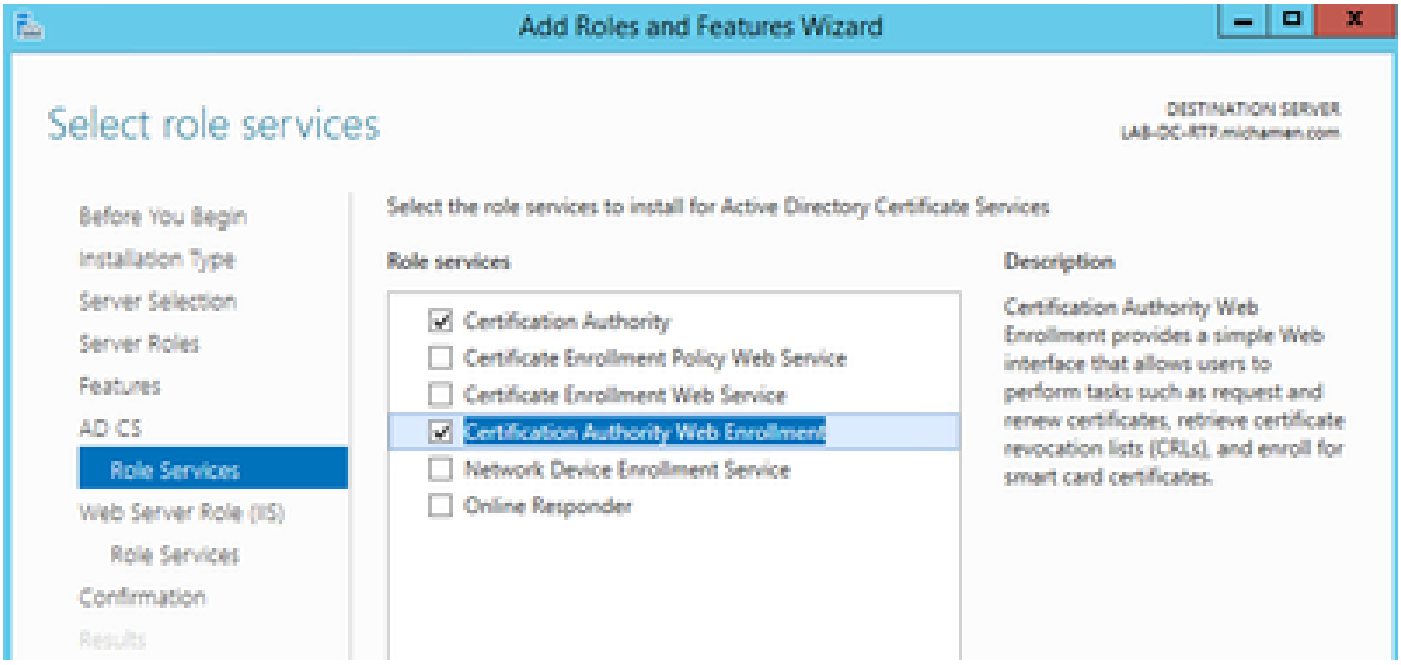


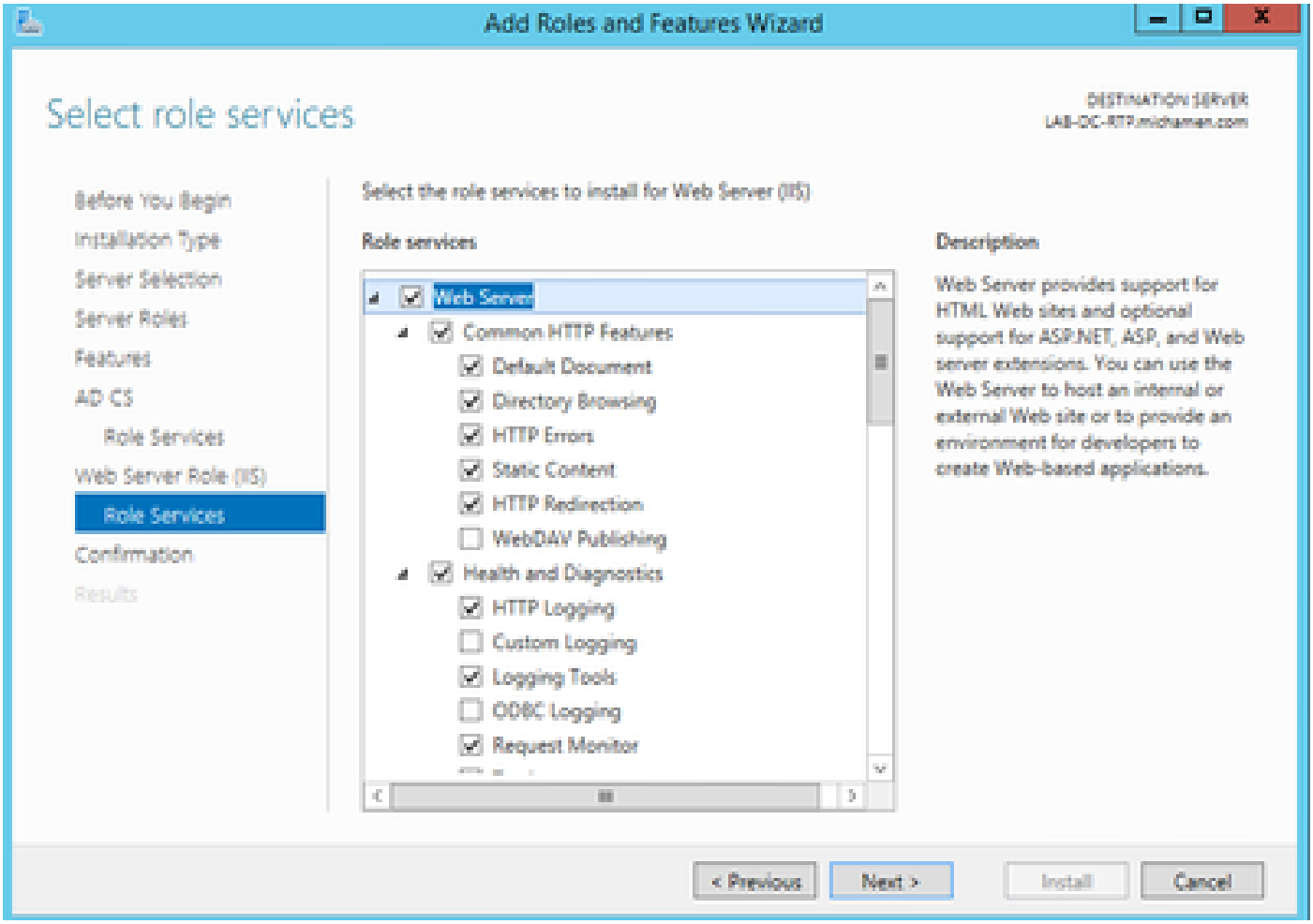
- 需要指定NetBIOS域名(本实验中使用了MICHAMEN1)。
- 按照向导完成操作。然后，服务器重新启动以完成安装。
- 下次登录时需要指定新域名。 例如MICHAMEN1\Administrator。



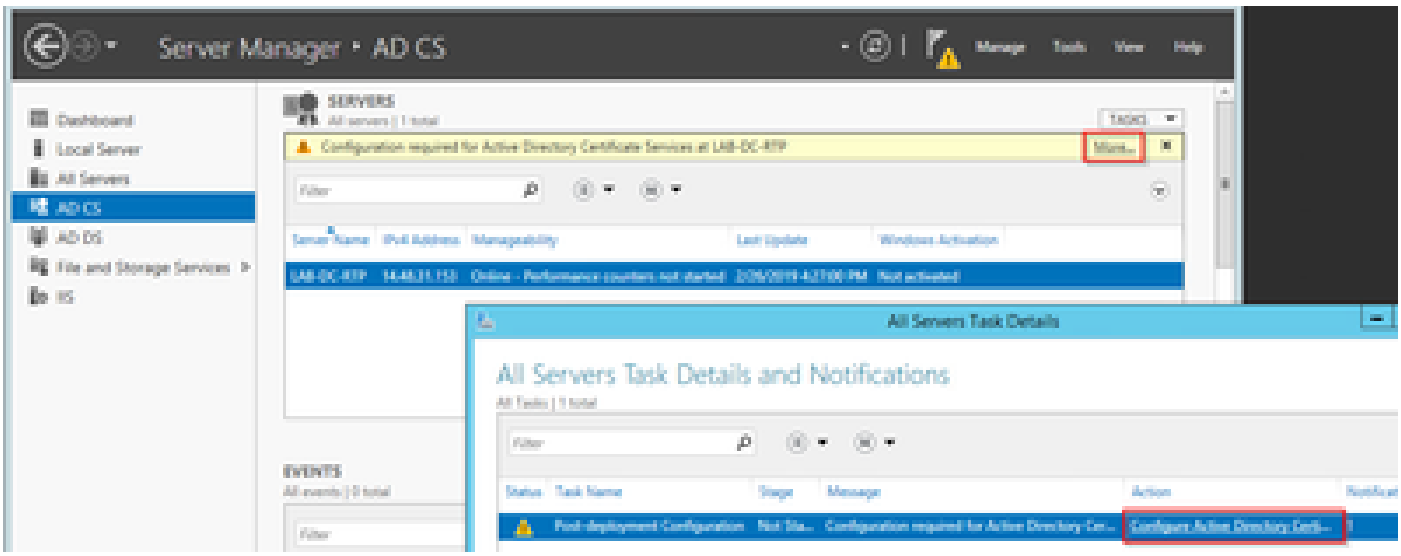
启用和配置证书服务

- 在服务器管理器中，选择Add Roles and Features
- 选择Active Directory证书服务(Active Directory Certificate Services)，然后按照提示添加所需功能（所有可用功能均是从为此实验启用的角色服务中选择的）
- 对于角色服务，请检查证书颁发机构Web注册

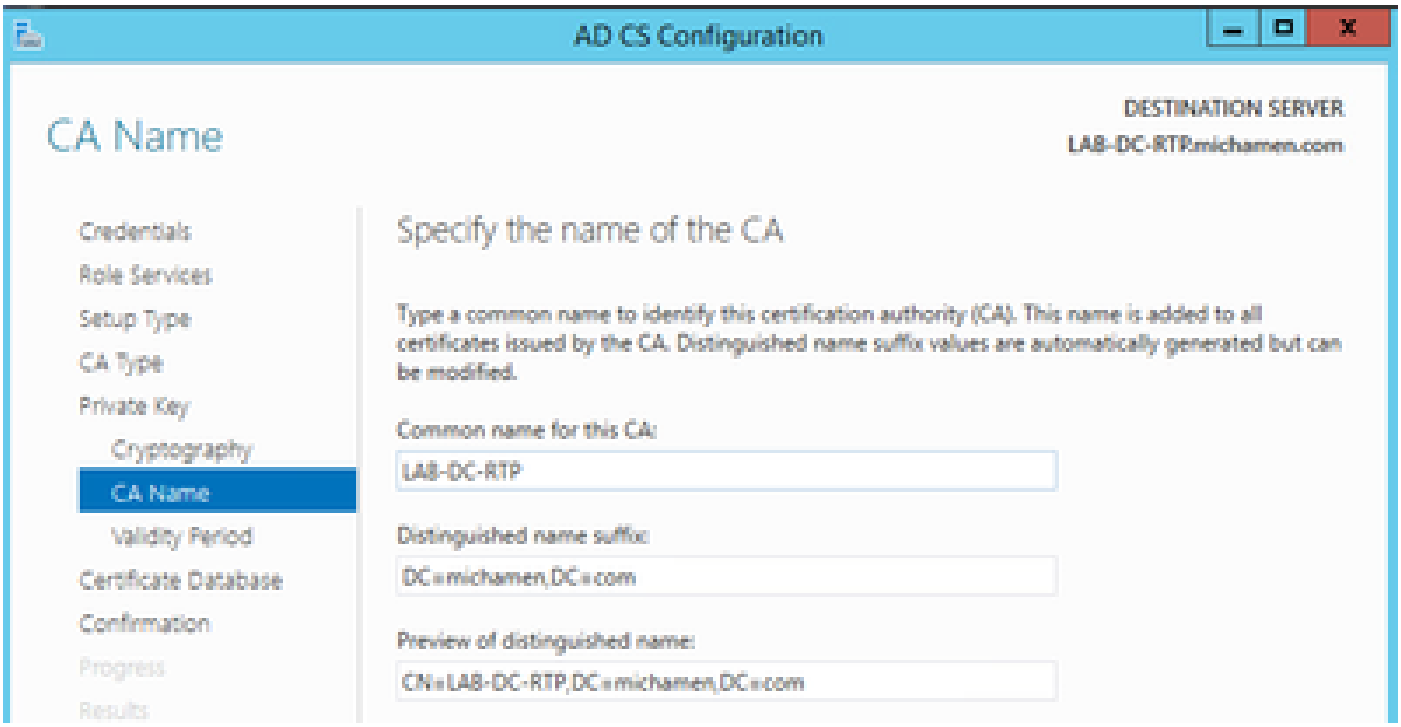




- “服务器管理器”(Server Manager)>“AD DS”下必须出现一个警告选项卡，标题为“Active Directory证书服务所需的配置”(Configuration required for Active Directory Certificate Services)；选择more链接，然后选择可用的操作：



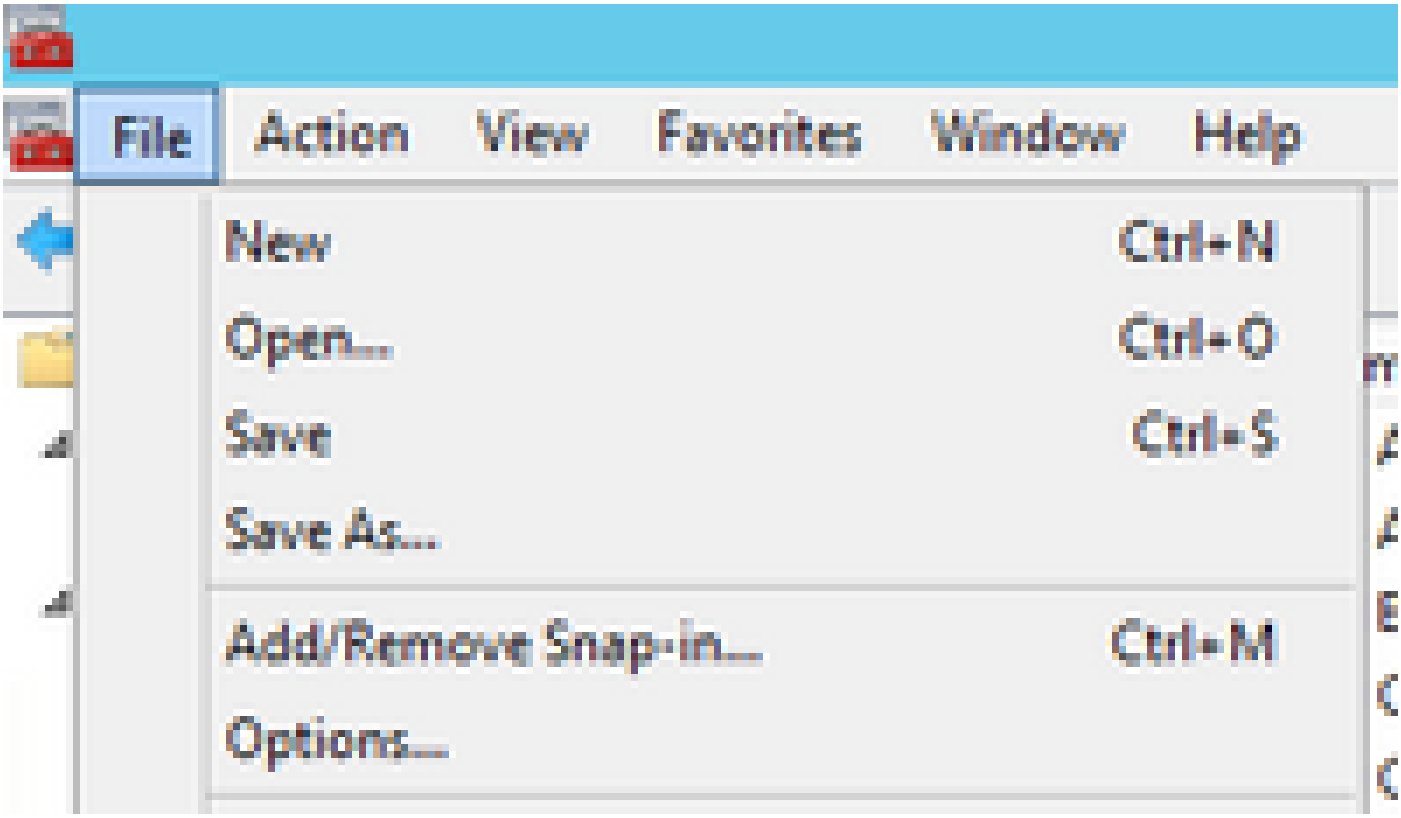
- 在AD-CS安装后配置向导中，浏览以下步骤：
- 选择证书颁发机构和证书颁发机构Web注册角色
- 选择Enterprise CA with options:
- 根 CA
- 创建新的私钥
- 使用私钥 — SHA1的默认设置
- 设置CA的公用名（必须与服务器的主机名匹配）：

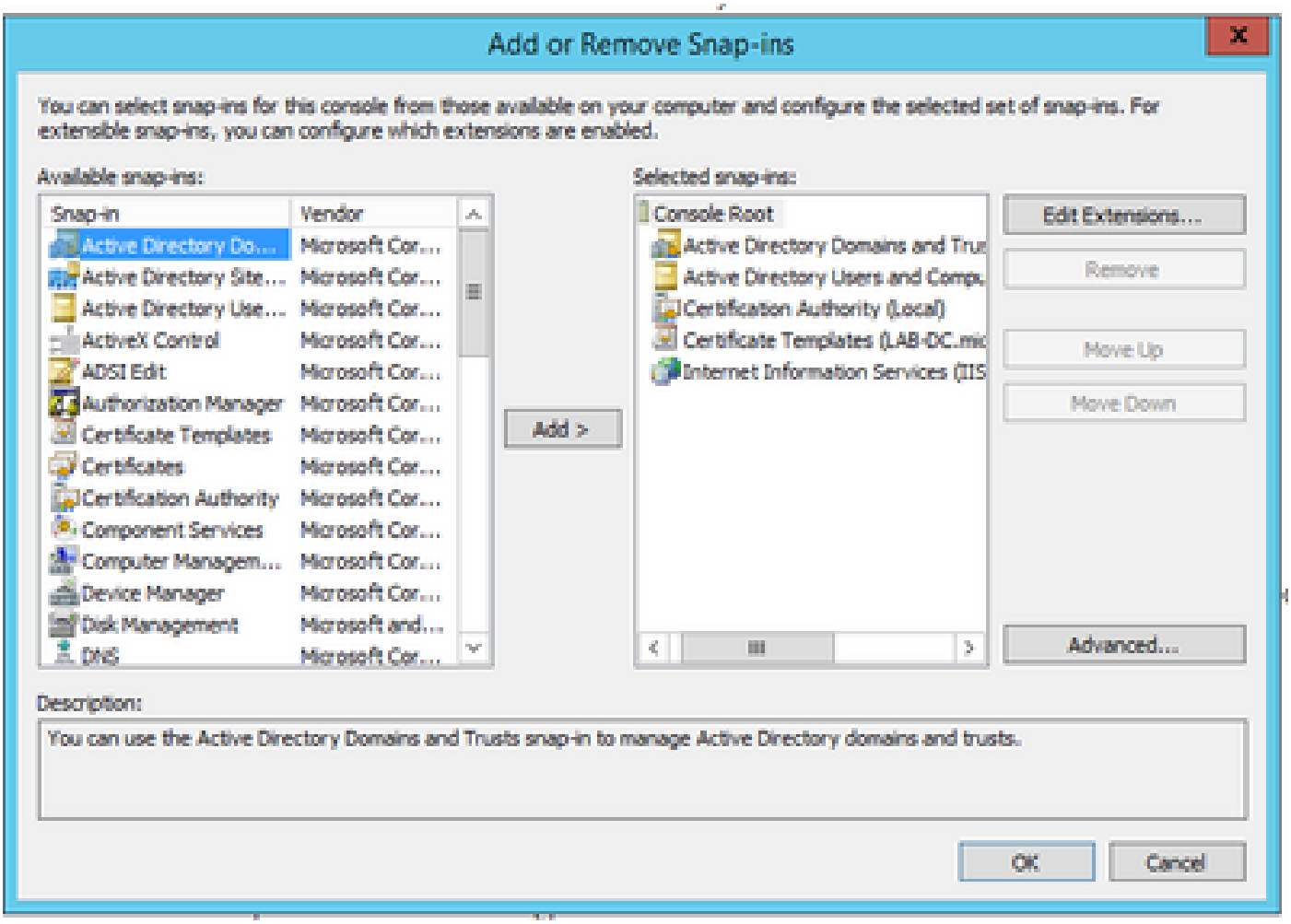


- 将有效期设置为5年（如果需要，还可以设置更多）
- 通过向导的其余部分选择Next按钮

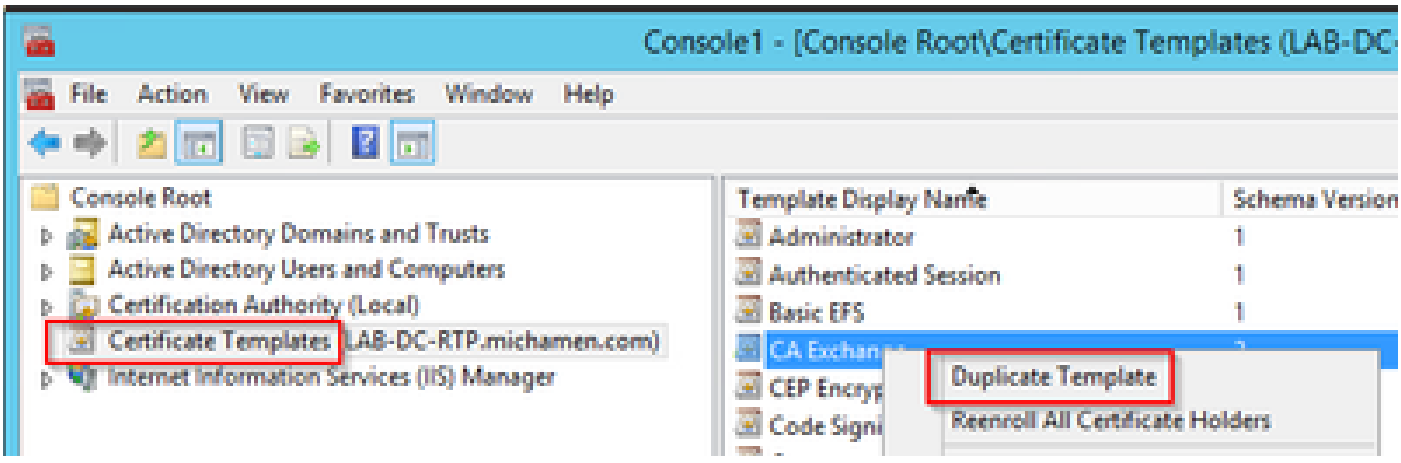
为CiscoRA创建证书模板

- 打开MMC选择Windows开始徽标，然后在“运行”中键入mmc
- 打开MMC窗口并添加以下管理单元（用于配置的不同点），然后选择确定:

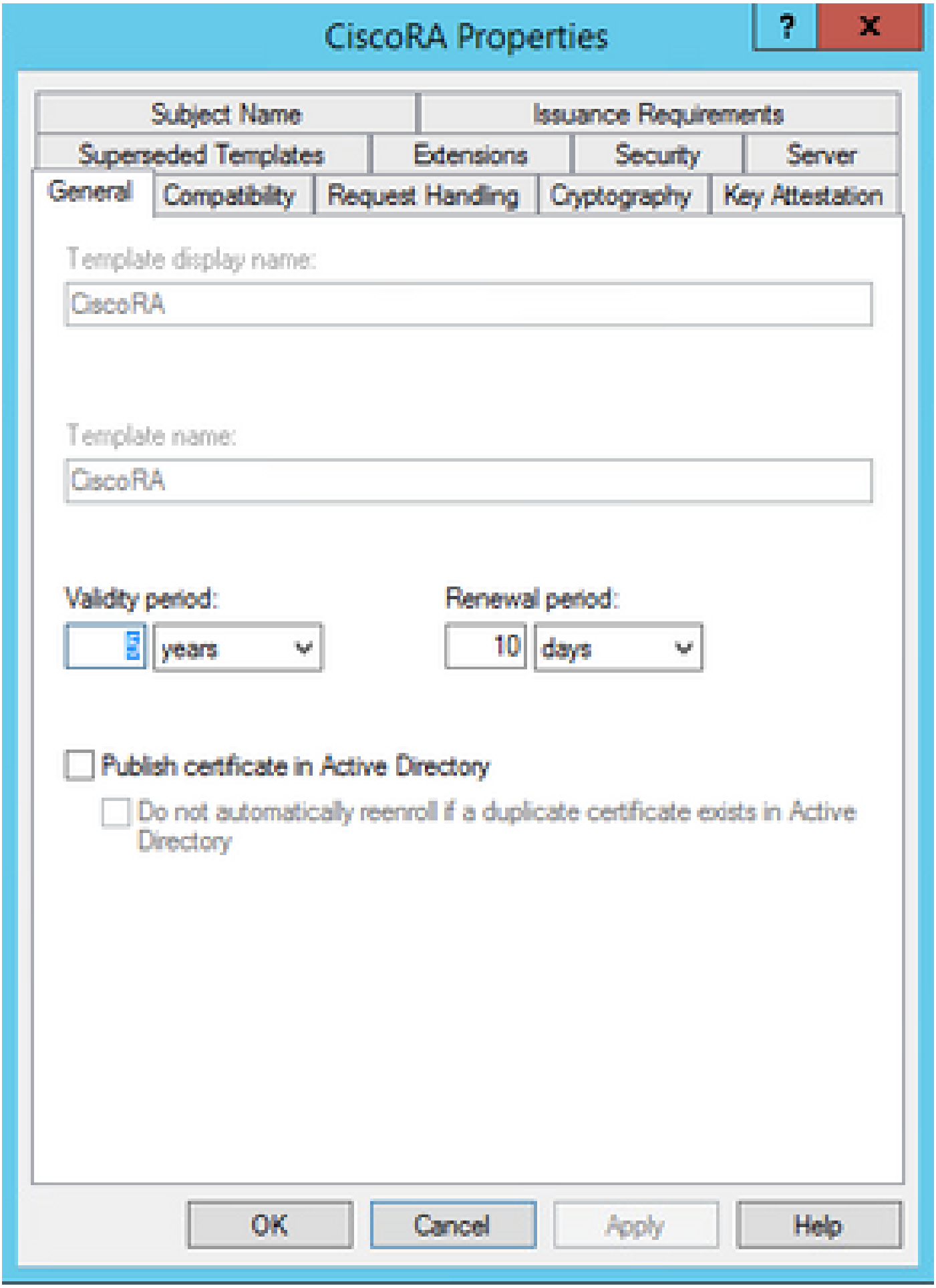




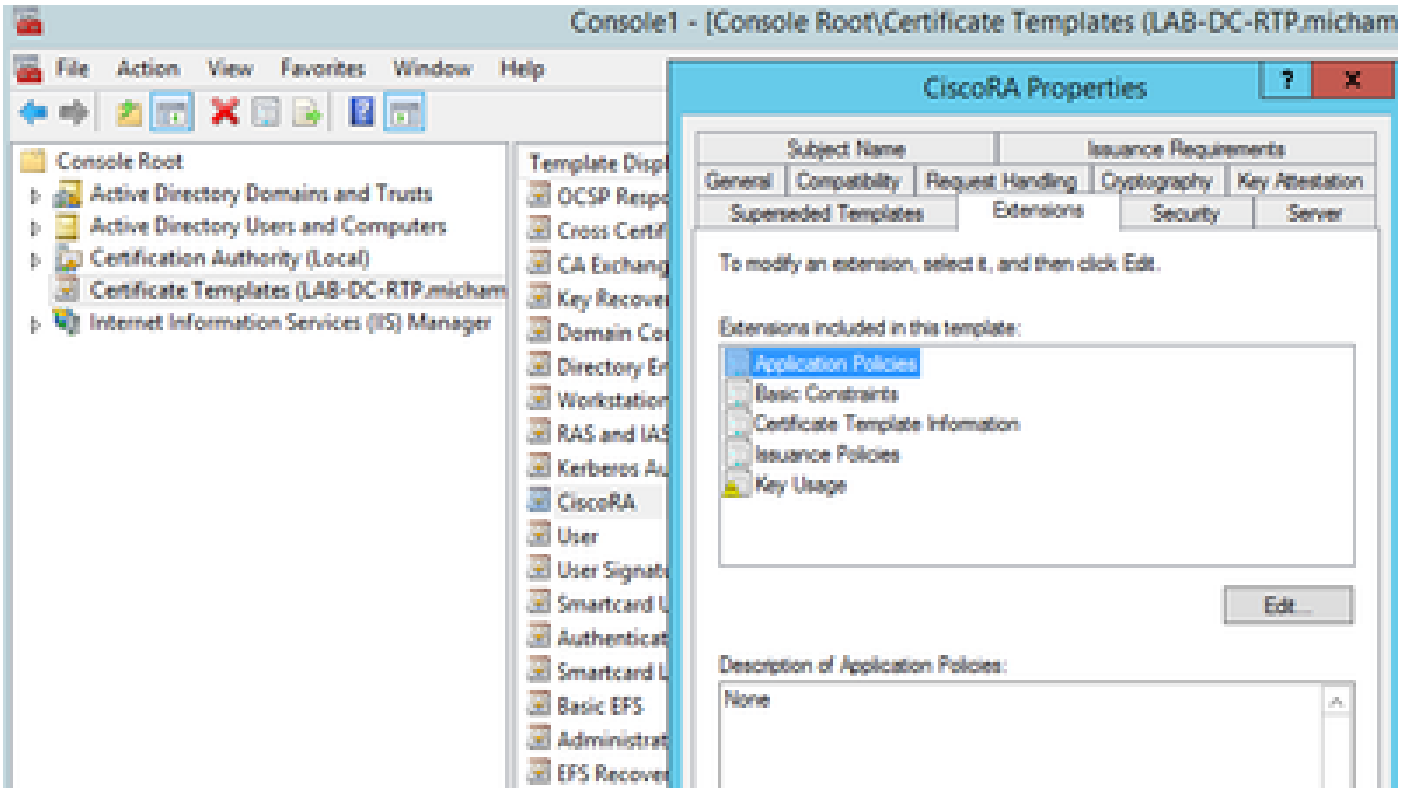
- 选择File > Save，并将此控制台会话保存到桌面以便快速重新访问
- 从管理单元中，选择证书模板
- 创建或克隆模板(最好是“根证书颁发机构”模板，并将其命名为CiscoRA



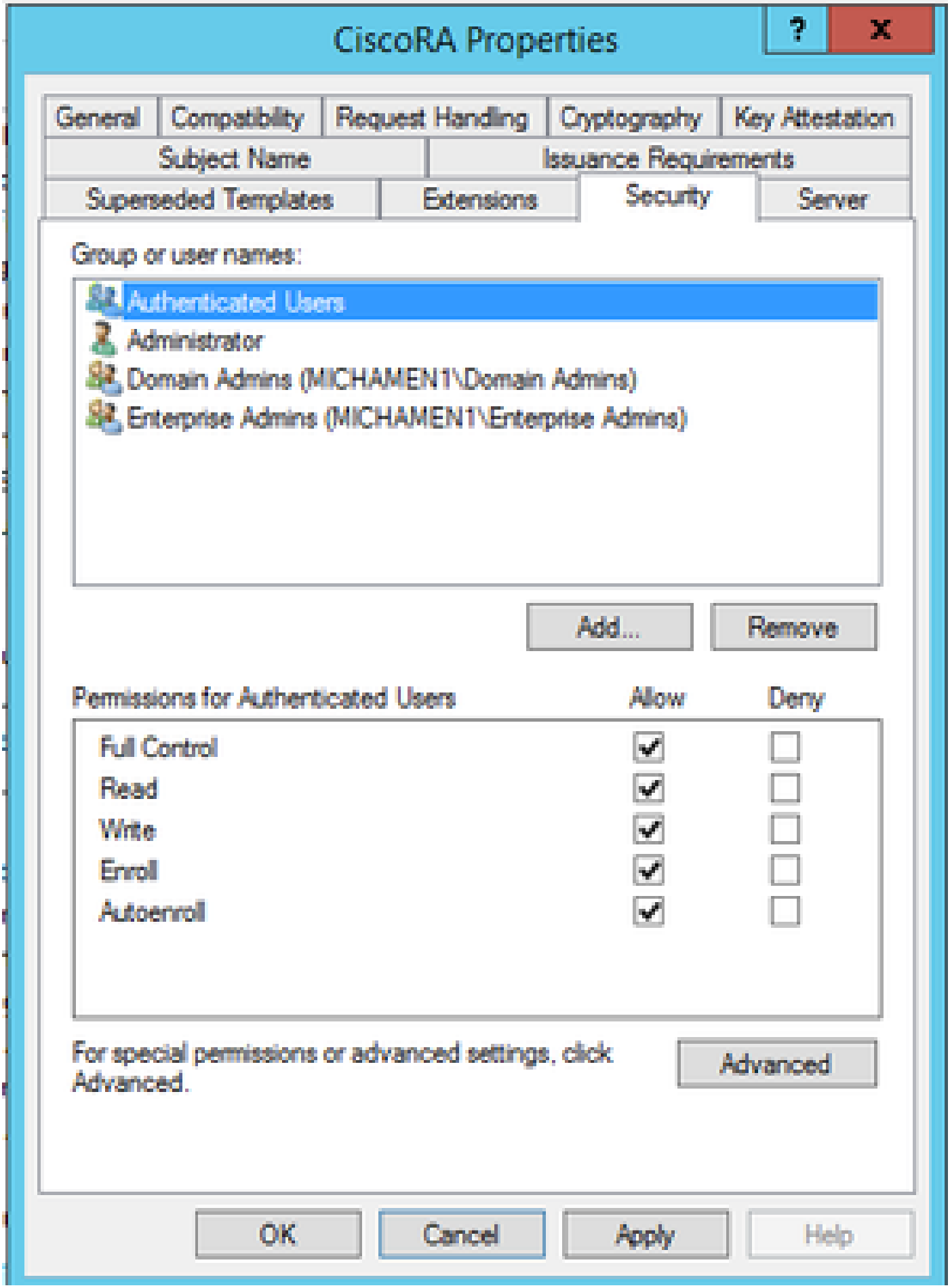
- 修改模板。右键单击它并选择“属性”
- 选择General选项卡，将有效期设置为20年（如果需要，也可以设置其他值）。在此选项卡中，确保模板的“显示名称”和“名称”值匹配


CiscoRA Properties
Subject Name
Issuance Requirements
Superseded Templates
Extensions
Security
Server
General
Compatibility
Request Handling
Cryptography
Key Attestation
Template display name:
CiscoRA
Template name:
CiscoRA
Validity period:
years
Renewal period:
10
days
Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory
OK
Cancel
Apply
Help

- 选择Extensions选项卡，突出显示Application Policies，然后选择Edit

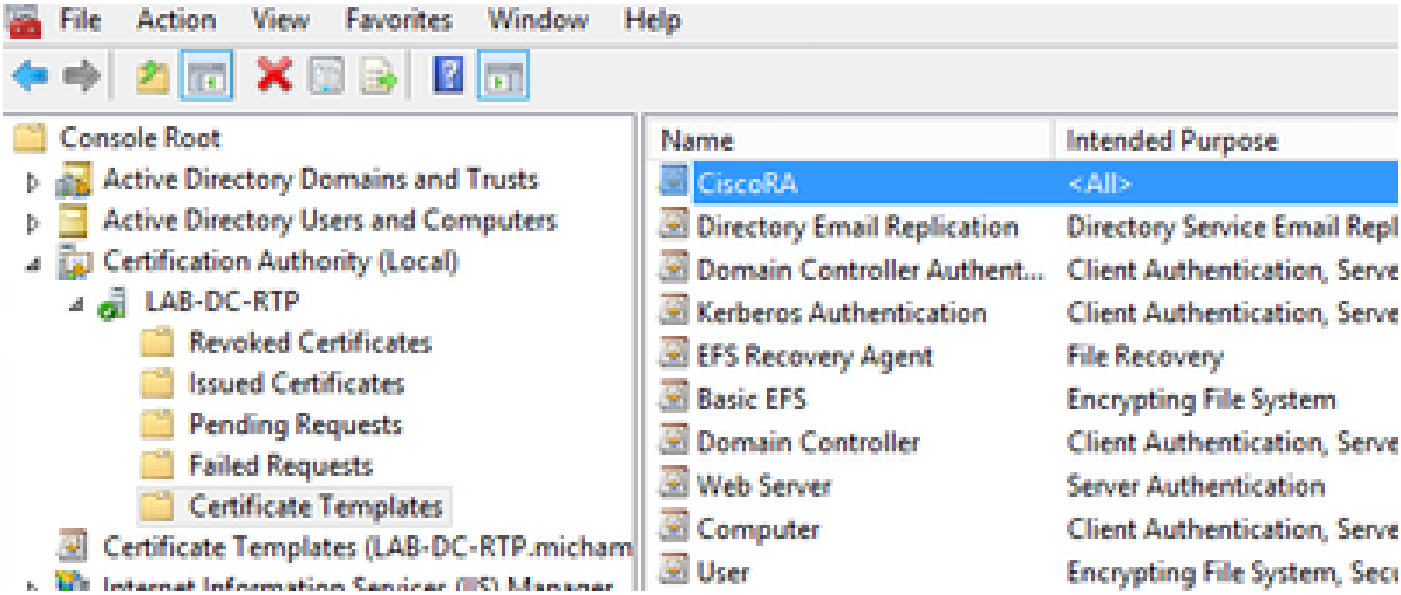


- 删除出现的窗口中显示的所有策略
- 选择Subject Name选项卡，然后选择Supply in Request单选按钮
- 选择Security选项卡并授予显示的所有组/用户名的所有权限


CiscoRA Properties
General
Compatibility
Request Handling
Cryptography
Key Attestation
Subject Name
Issuance Requirements
Superseded Templates
Extensions
Security
Server
Group or user names:
Authenticated Users
Administrator
Domain Admins (MICHAMEN1\Domain Admins)
Enterprise Admins (MICHAMEN1\Enterprise Admins)
Add...
Remove
Permissions for Authenticated Users
Allow
Deny
Full Control
Read
Write
Enroll
Autoenroll
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

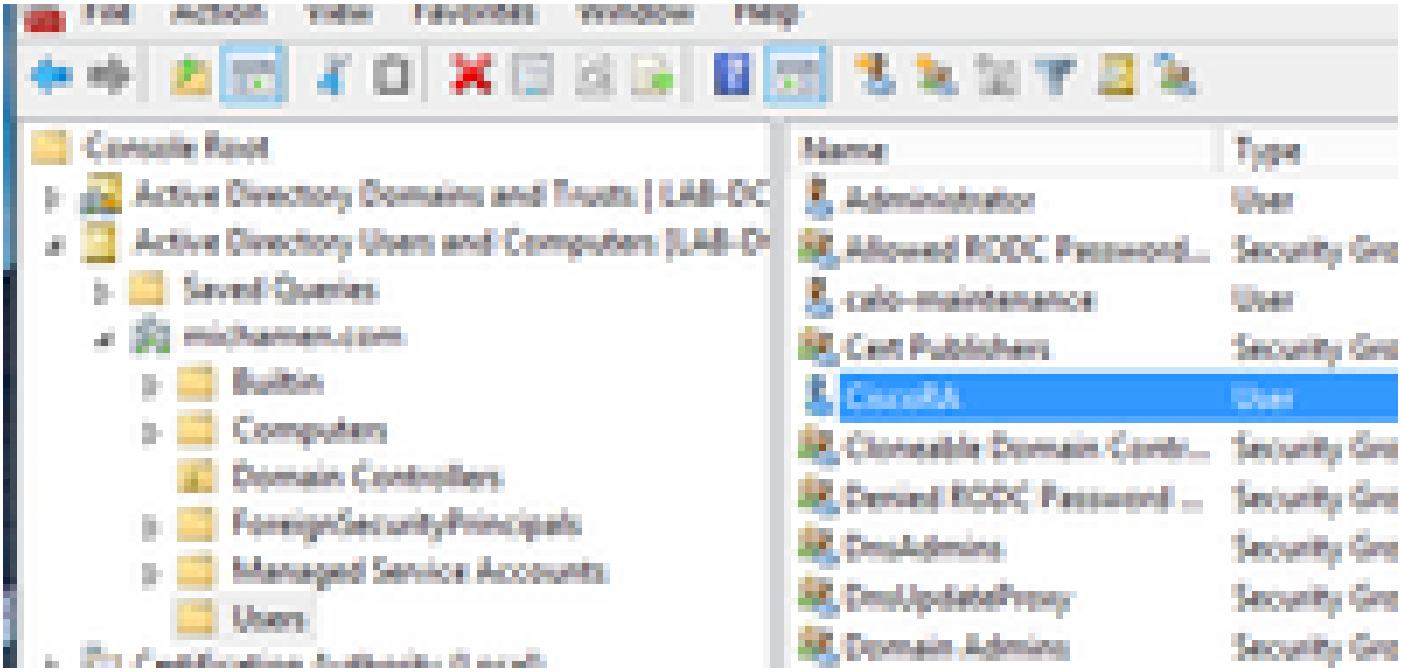
使证书模板可供颁发

- 在MMC管理单元中，选择证书颁发机构并展开文件夹树以查找“证书模板”(Certificate Templates)文件夹
- 在包含“名称”和“目标用途”的框架中的空白处右键单击
- 选择New和Certificate Template to Issue
- 选择新创建和编辑的CiscoRA模板



Active Directory CiscoRA帐户创建

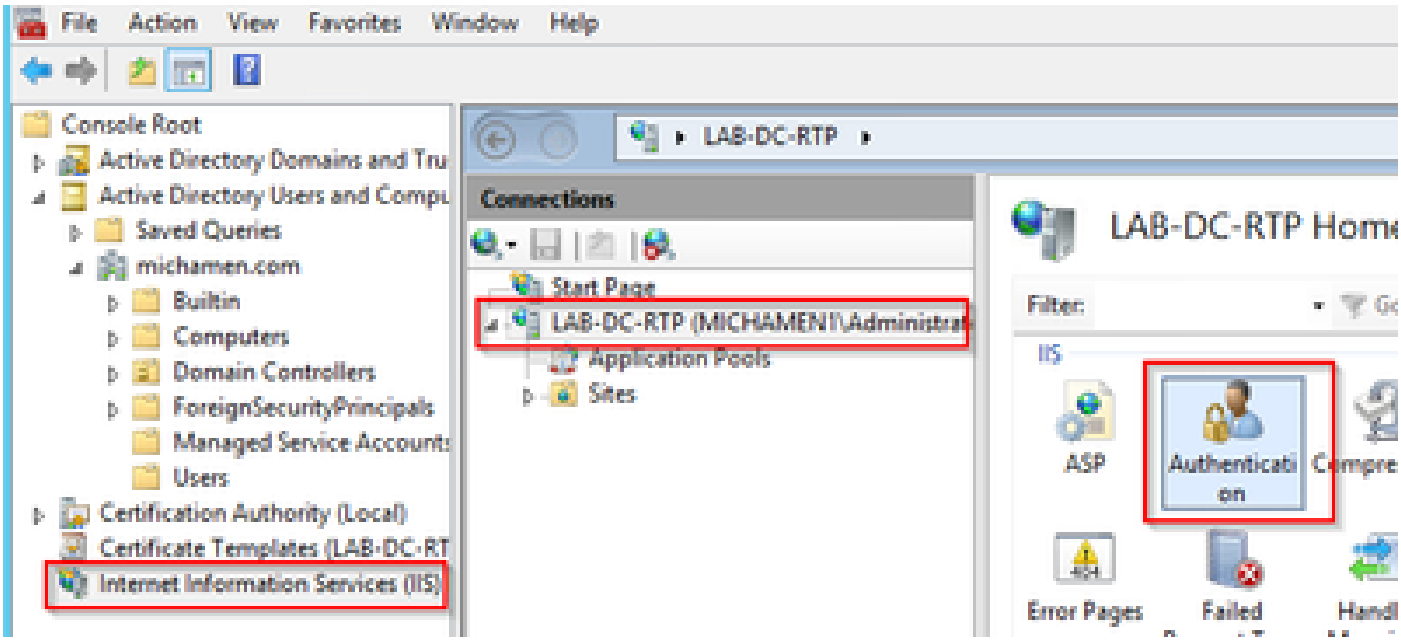
- 导航到MMC管理单元并选择Active Directory用户和计算机
- 在最左窗格中的树中选择Users文件夹
- 在包含“名称”、“类型”和“说明”的框架中的空白处右键单击
- 选择New和User
- 使用用户名/密码(ciscora/Cisco123用于本实验)创建CiscoRA帐户，并在显示密码时选中Password never expires复选框



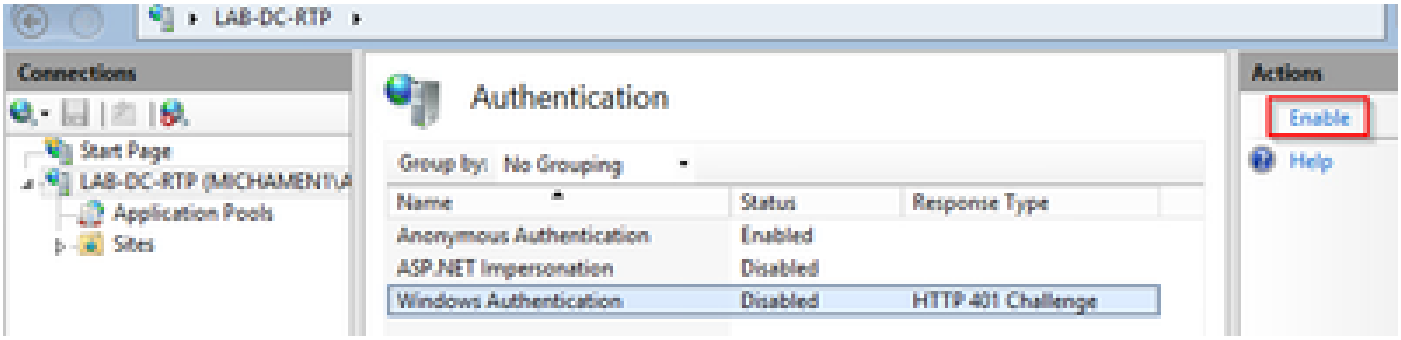
IIS 身份验证和SSL绑定配置

enable NTLM 身份验证

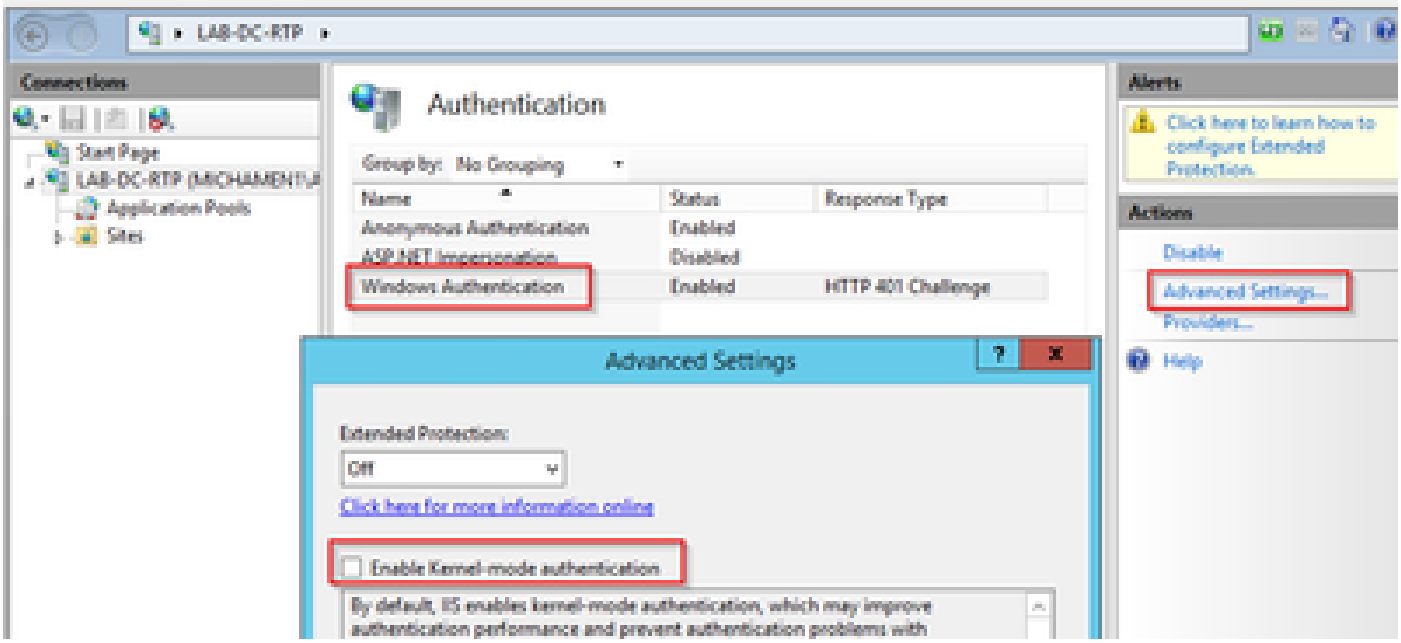
- 导航到MMC管理单元，然后在“Internet信息服务(IIS)管理器”管理单元下选择服务器名称
- 功能列表将显示在下一帧中。双击Authentication功能图标



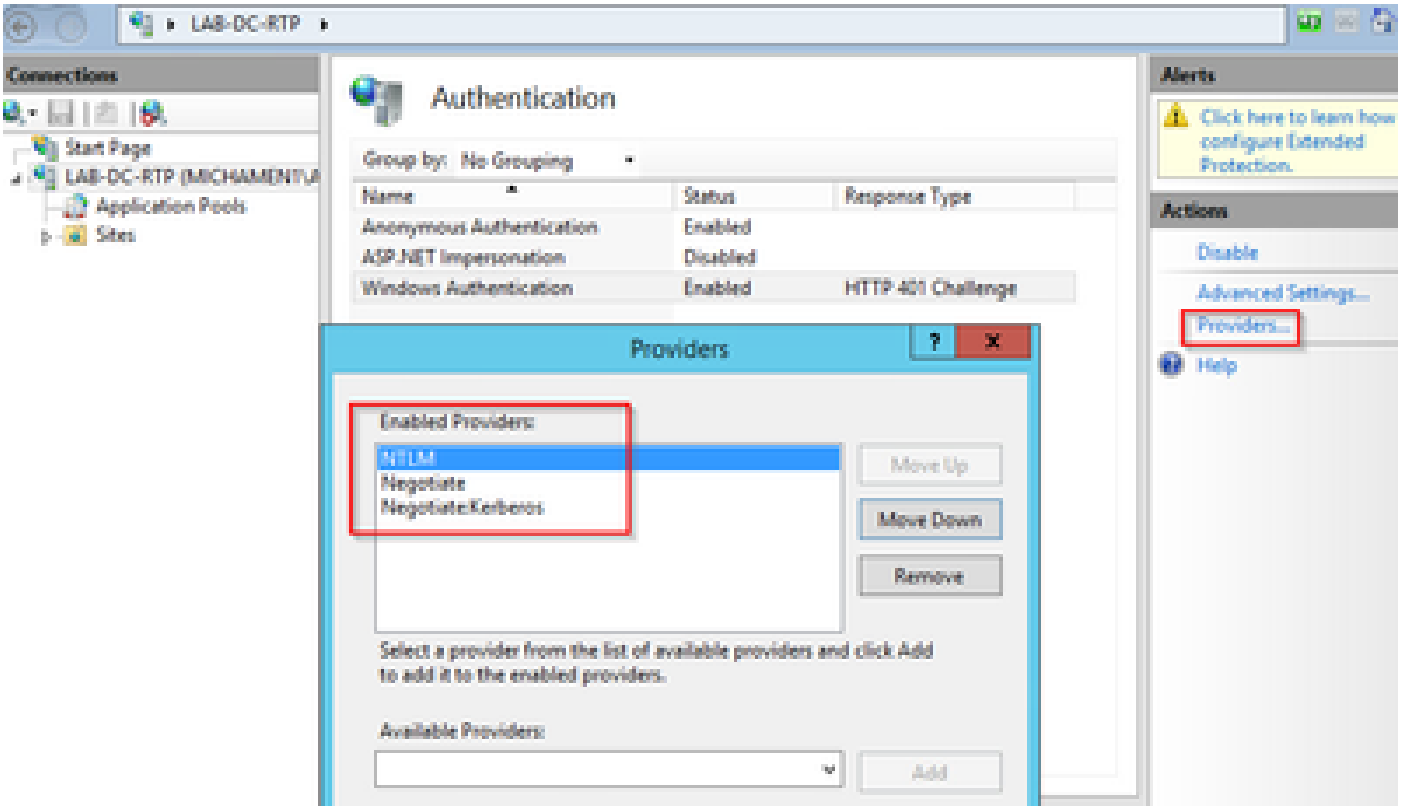
- 突出显示Windows Authentication，然后从Actions帧（右窗格）中选择Enable选项



- 操作窗格显示高级设置选项；选择该选项，并取消选中启用内核模式身份验证



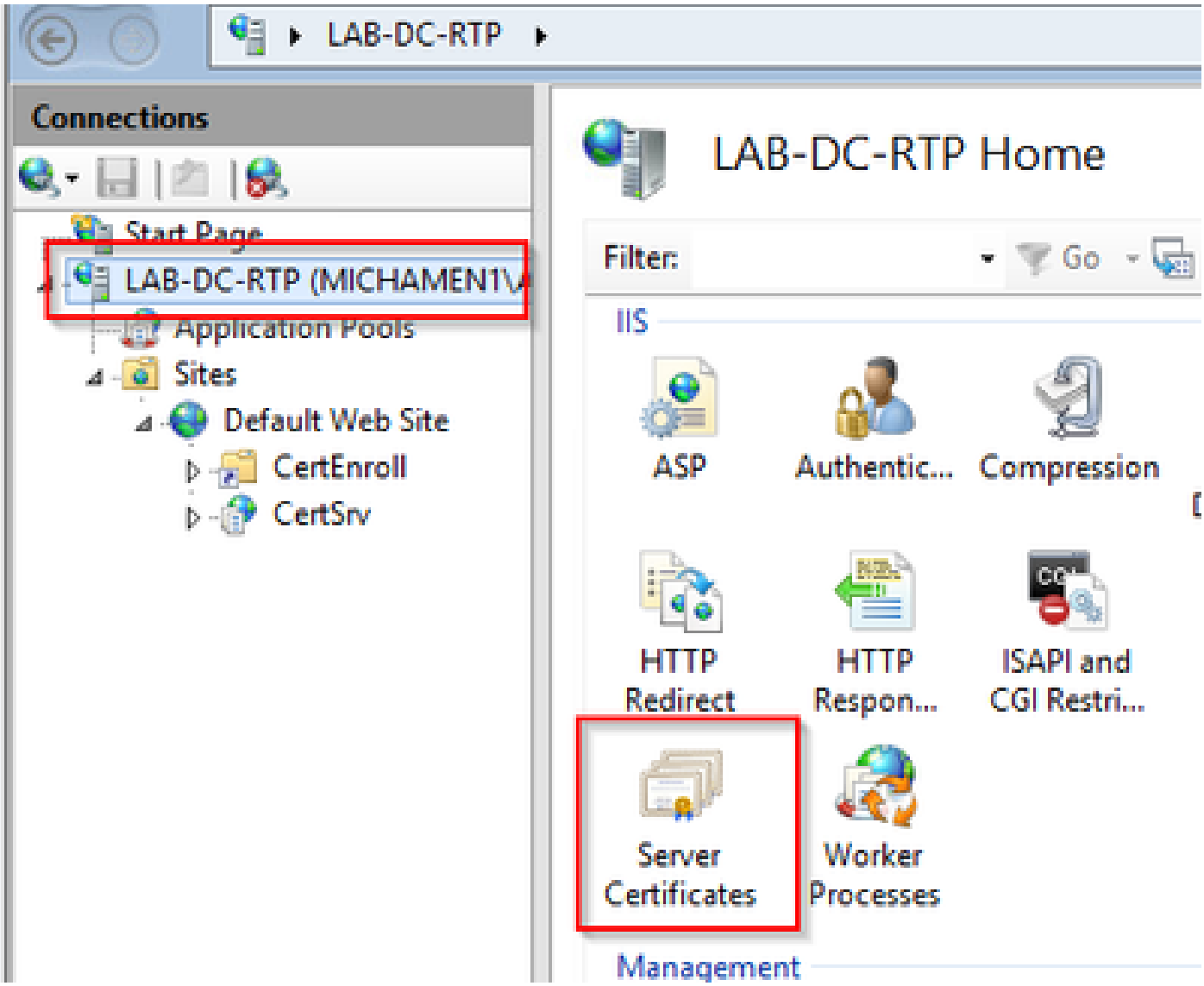
- 选择Providers并按NTML顺序排列，然后选择Negotiate。



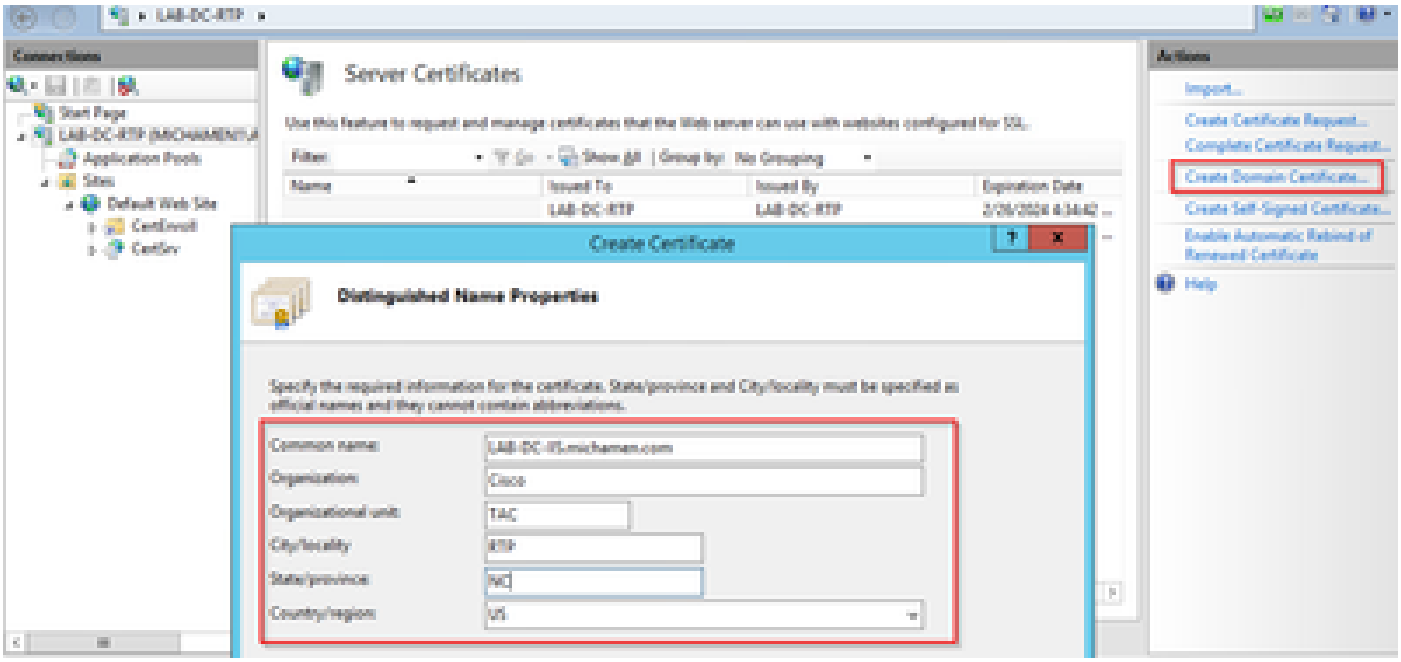
生成Web服务器的身份证书

如果尚未出现这种情况，您需要为Web服务生成证书和身份证书，该证书由CA签名，因为如果Web服务器的证书是自签名，则CiscoRA无法连接到该证书：

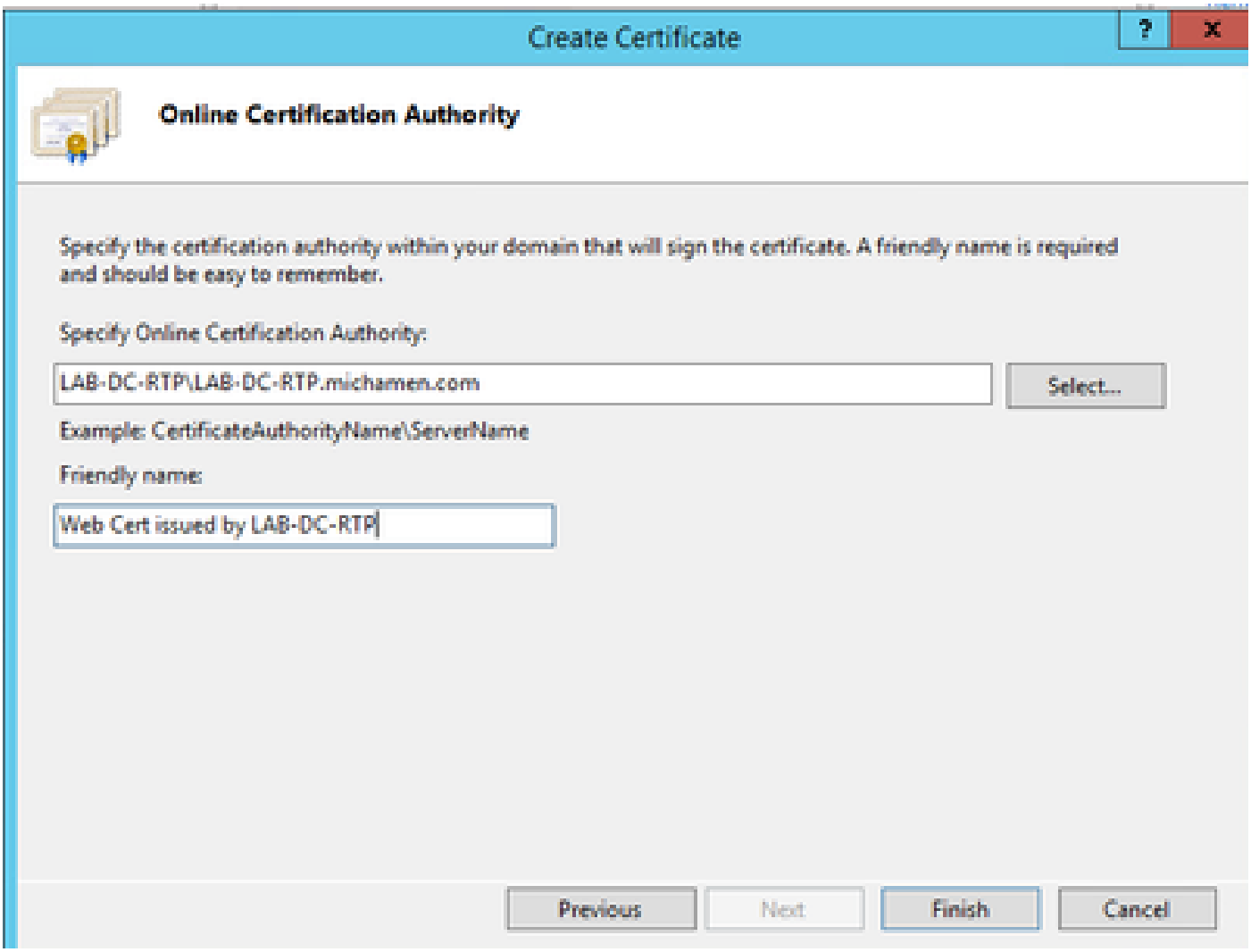
- 从IIS管理单元选择Web服务器，然后双击Server Certificates功能图标：



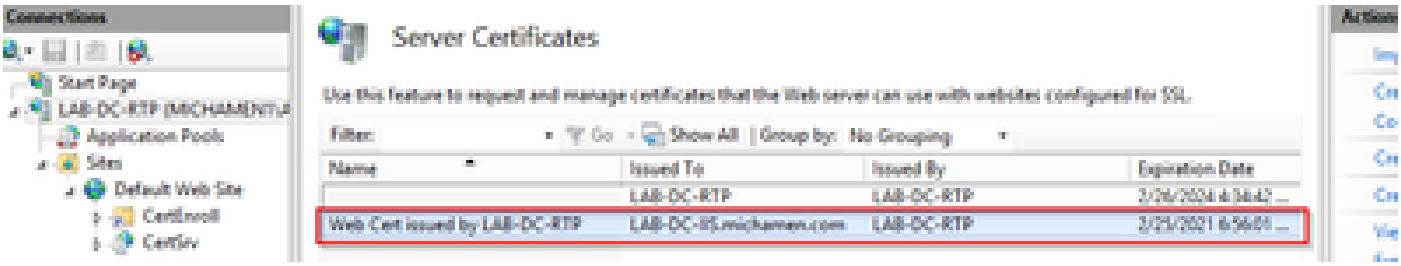
- 默认情况下，您可以看到此处列出的一个证书；即自签名的根CA证书；从操作菜单中选择创建域证书选项。在配置向导中输入值，以创建新证书。确保公用名是可解析的FQDN（完全限定域名），然后选择下一步:



- 选择您的根CA的证书作为颁发者，然后选择Finish:

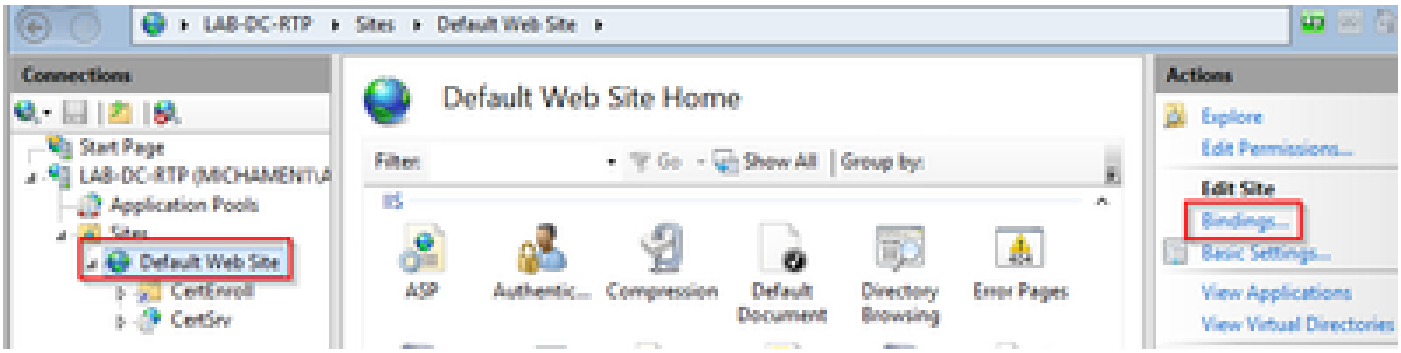


- 您可以看到列出的CA证书和Web服务器的身份证书：

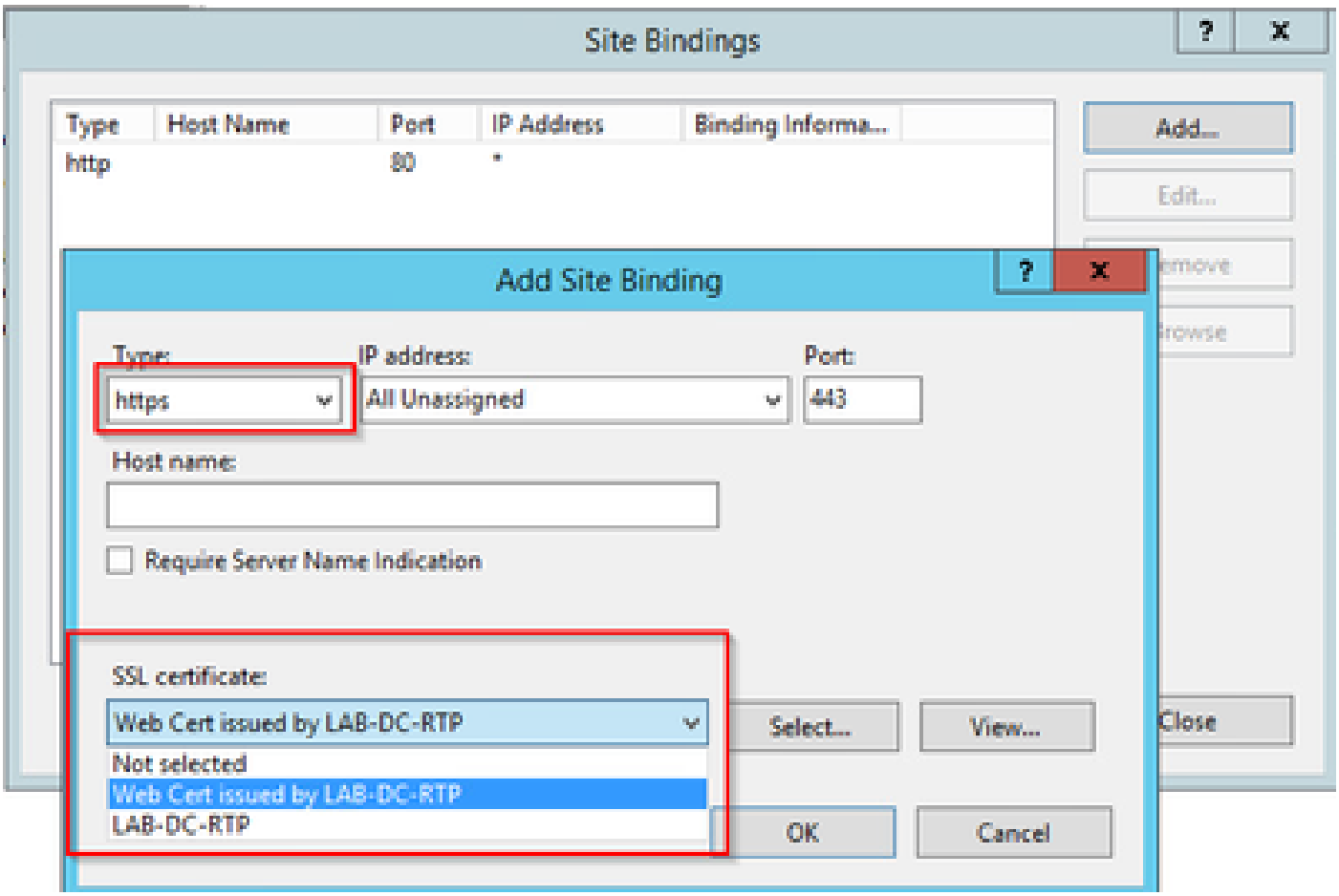


Web服务器SSL绑定

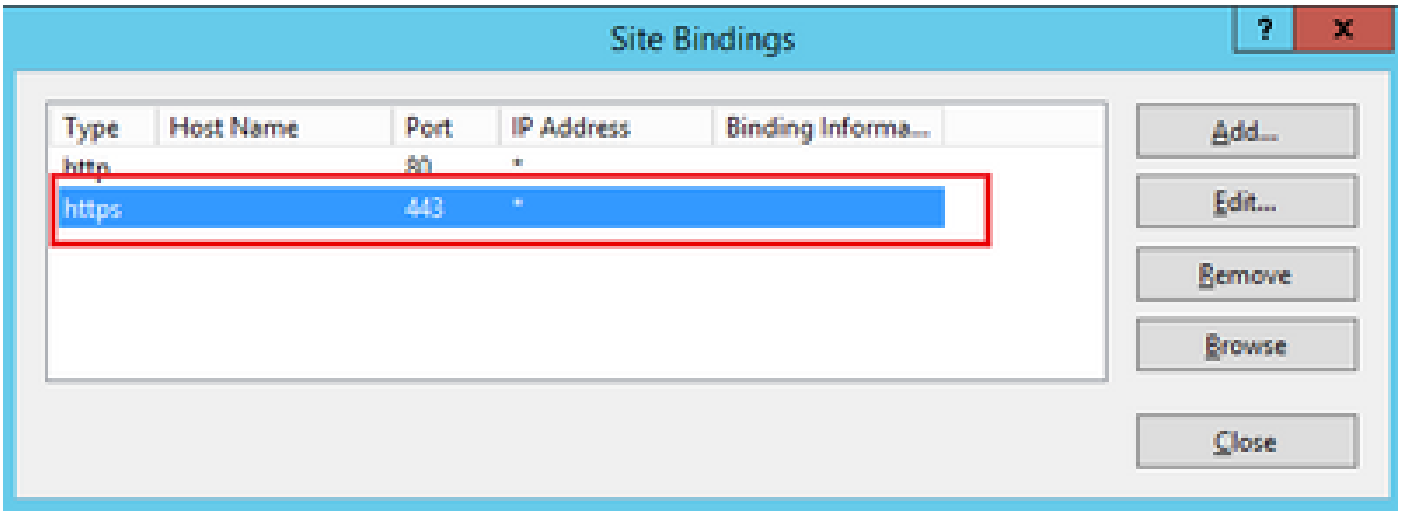
- 在树视图中选择一个站点（您可以使用默认网站或使其更精细到特定站点），然后从“操作”窗格中选择绑定。此时将显示绑定编辑器，通过该编辑器可以创建、编辑和删除网站的绑定。选择Add以将新的SSL绑定添加到站点。

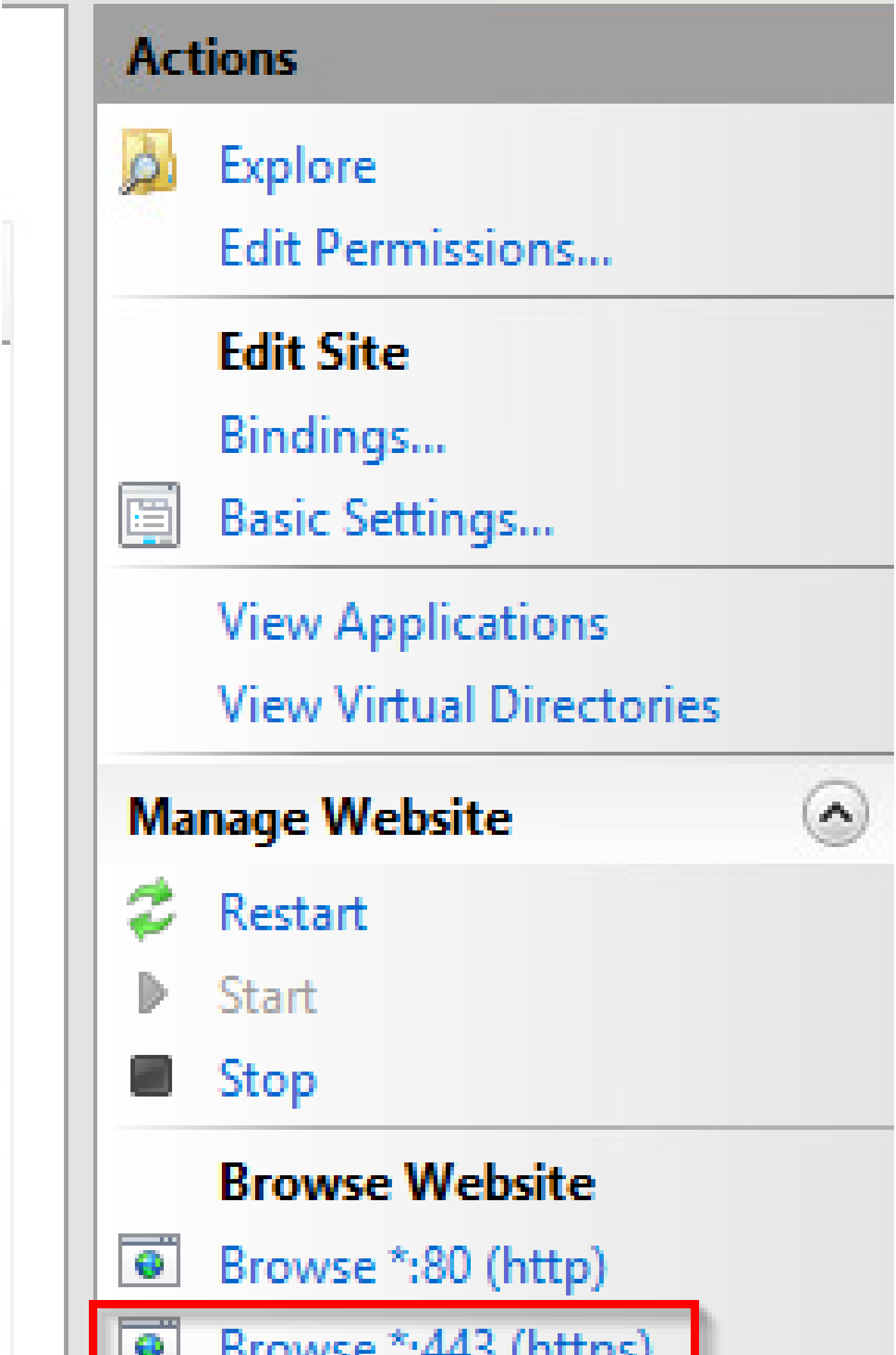


- 新绑定的默认设置为端口80上的HTTP。在类型下拉列表中选择https。从SSL Certificate下拉列表中选择在上一节中创建的自签名证书，然后选择OK。



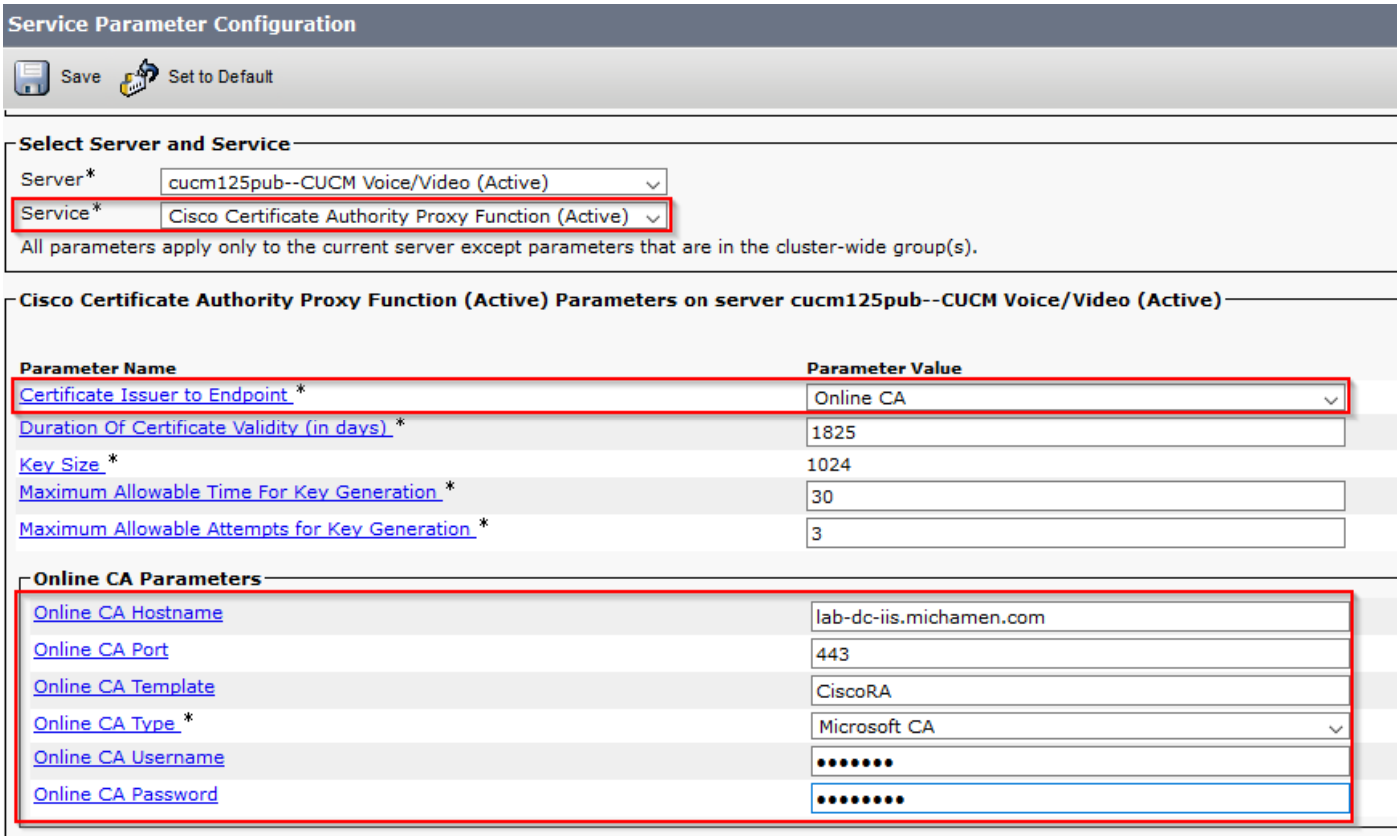
- 现在，您的站点上有新的SSL绑定，剩下的就是从菜单中选择Browse *:443(https)选项验证该绑定是否有效，并确保默认IIS网页使用HTTPS:


Site Bindings
Type
Host Name
Port
IP Address
Binding Informa...
http
80
*
https
443
*
Add...
Edit...
Remove
Browse
Close


Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse *:80 (http)
Browse *:443 (https)

证书也是不错的主意，因为需要为终端启用（或将要启用）安全信令加密；如果集群处于混合模式，则可能需要此证书。

- 导航到System > Service Parameters。在“服务器”字段中选择Unified CM发布服务器，在“服务”字段中选择思科证书颁发机构代理功能
- 将Certificate Issuer to Endpoint的值设置为Online CA，并为Online CA Parameters字段输入值。确保使用Web服务器的FQDN、之前创建的证书模板的名称(CiscoRA)、作为Microsoft CA的CA类型以及使用之前创建的CiscoRA用户帐户的凭据



- 弹出窗口通知您需要重新启动CAPF服务。但首先，通过Cisco Unified Serviceability > Tools > Service Activation激活思科证书注册服务，在Server字段中选择Publisher并选中Cisco Certificate Enrollment Service复选框，然后选择Save按钮：

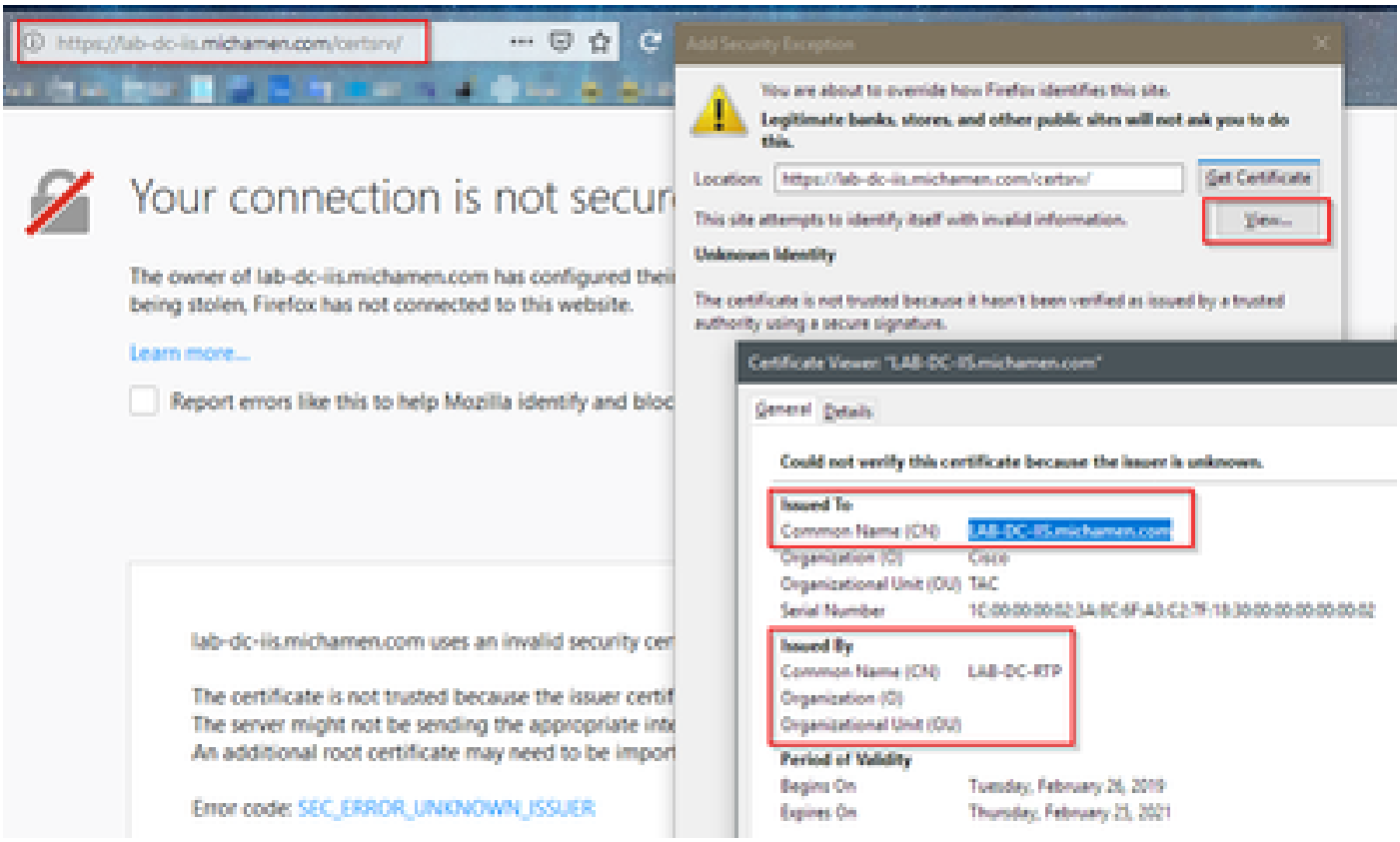
验证

验证IIS证书

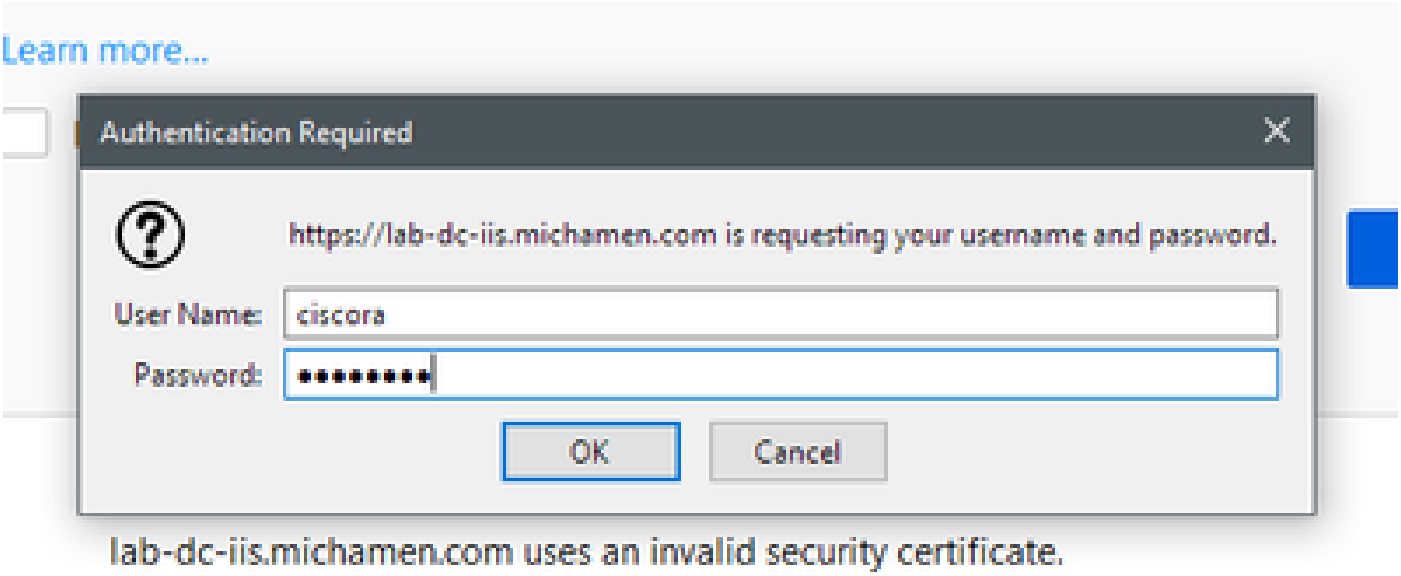
- 从连接到服务器的PC的Web浏览器（最好与CUCM发布服务器位于同一网络）导航至URL:

  https://YOUR_SERVER_FQDN/certsrv/

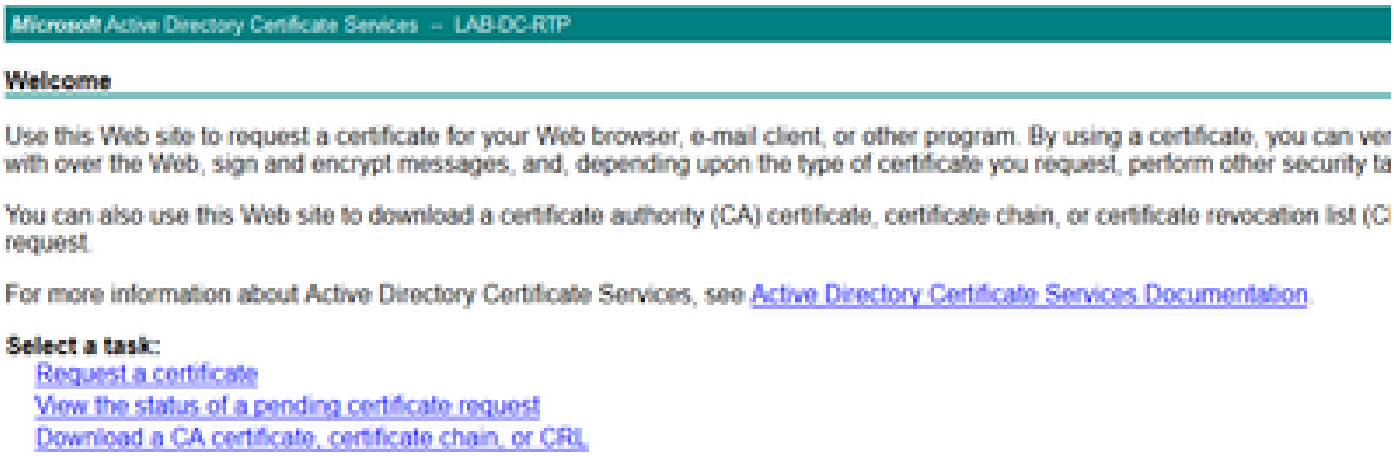
- 显示证书不受信任警报。添加例外并检查证书。确保它与预期的FQDN匹配：



- 接受例外后，您需要进行身份验证；此时，您需要使用之前为CiscoRA帐户配置的凭证：



- 身份验证后，您必须能够看到AD CS（Active Directory证书服务）欢迎页面：



验证CUCM配置

执行通常要遵循的步骤，以便在其中一台电话上安装LSC证书。

步骤1:打开CallManager Administration页面，依次打开Device和Phone

第二步：选择Find按钮以显示电话

第三步：选择要安装LSC的电话

第四步：向下滚动至证书颁发机构代理功能(CAPF)信息

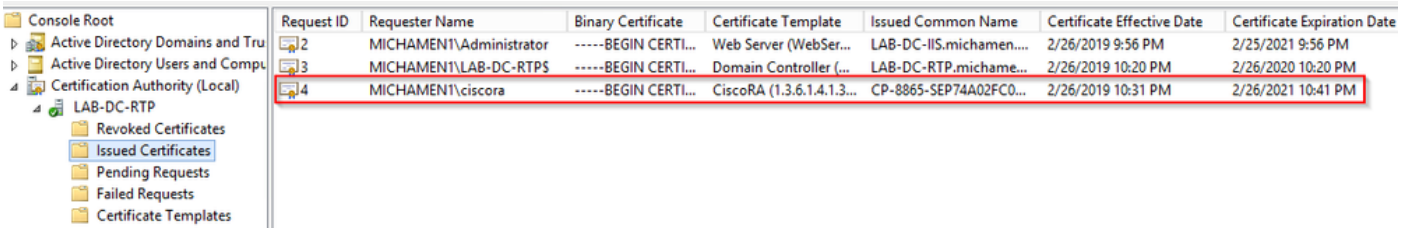
第五步：从Certificate Operation中选择Install/Upgrade。

第六步：选择Authentication Mode。（通过Null字符串可用于测试目的）

步骤 7.滚动到页面顶部，然后为电话选择save，然后选择Apply Config。

步骤 8电话重新启动并重新注册后，使用LSC状态过滤器确认已成功安装LSC。

- 从AD服务器侧打开MMC并展开证书颁发机构管理单元以选择“已颁发的证书”文件夹
- 电话条目显示在摘要视图内，以下是显示的一些详细信息：
  - 请求ID：唯一序列号
  - Requester Name：必须显示已配置的CiscoRA帐户的用户名
  - 证书模板：必须显示所创建的CiscoRA模板的名称
  - 已颁发的公用名：必须显示设备名称附加的电话型号
  - 证书生效日期和证书到期日期



相关链接

- CAPF在线CA故障排除
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。