发布ISE的认证吊销列表在Microsoft CA服务器配置示例

Contents

Introduction

本文描述运行互联网信息服务微软认证授权(CA)服务器的配置(IIS)发布证书撤销列表(CRL)更新。它也解释如何配置思科身份服务引擎(ISE) (版本1.1和以上)检索更新用于证书确认。在证书确认使用可以配置的ISE检索多种CA根证明的Crl。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

本文档中的信息基于以下软件和硬件版本：

- Cisco Identity Services Engine Release 1.1.2.145
- 微软视窗®服务器® 2008 R2

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is

live, make sure that you understand the potential impact of any command.

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Configure

本部分提供有关如何配置本文档所述功能的信息。

Note: 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

配置

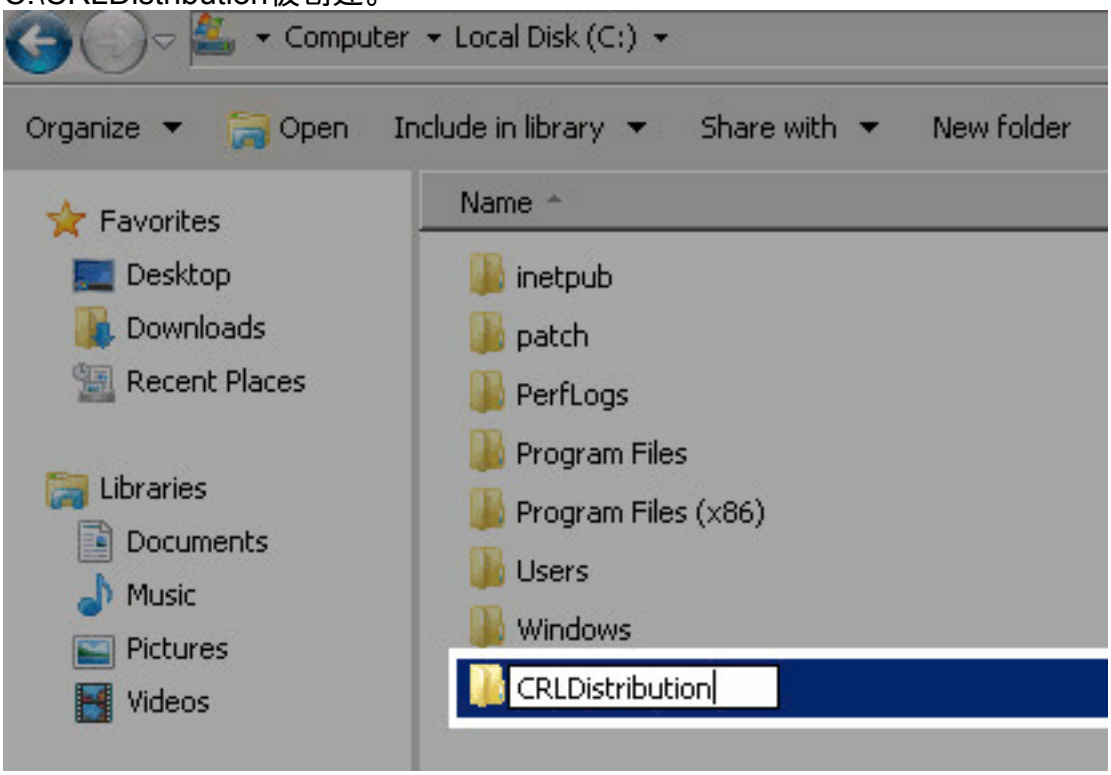
本文档使用以下配置：

- 第1.部分创建并且配置在CA的一个文件夹安置CRL文件
- 第2.部分创建IIS的一个站点显示新的控制分配点
- 第3.部分配置Microsoft CA服务器发布CRL文件到分配点
- 第4.部分验证CRL文件存在并且通过IIS是可访问的
- 第5.部分配置ISE使用新的控制分配点

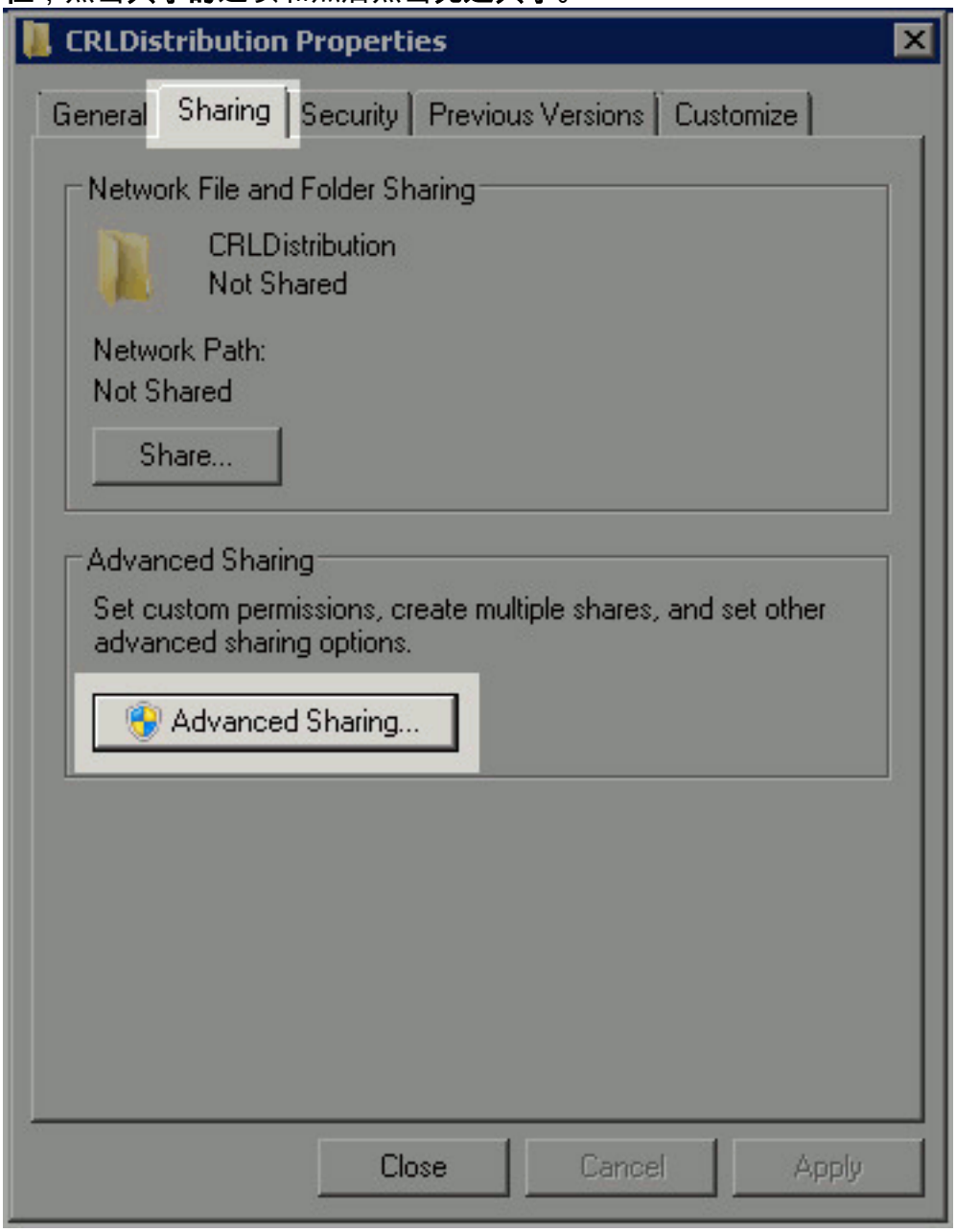
第1.部分创建并且配置在CA的文件夹安置CRL文件

首要任务是配置CA服务器的一个位置存储CRL文件。默认情况下， Microsoft CA服务器发布文件对C:\Windows\system32\CertSrv\CertEnroll\。而不是请使用此系统文件夹，请创建文件的一新文件夹。

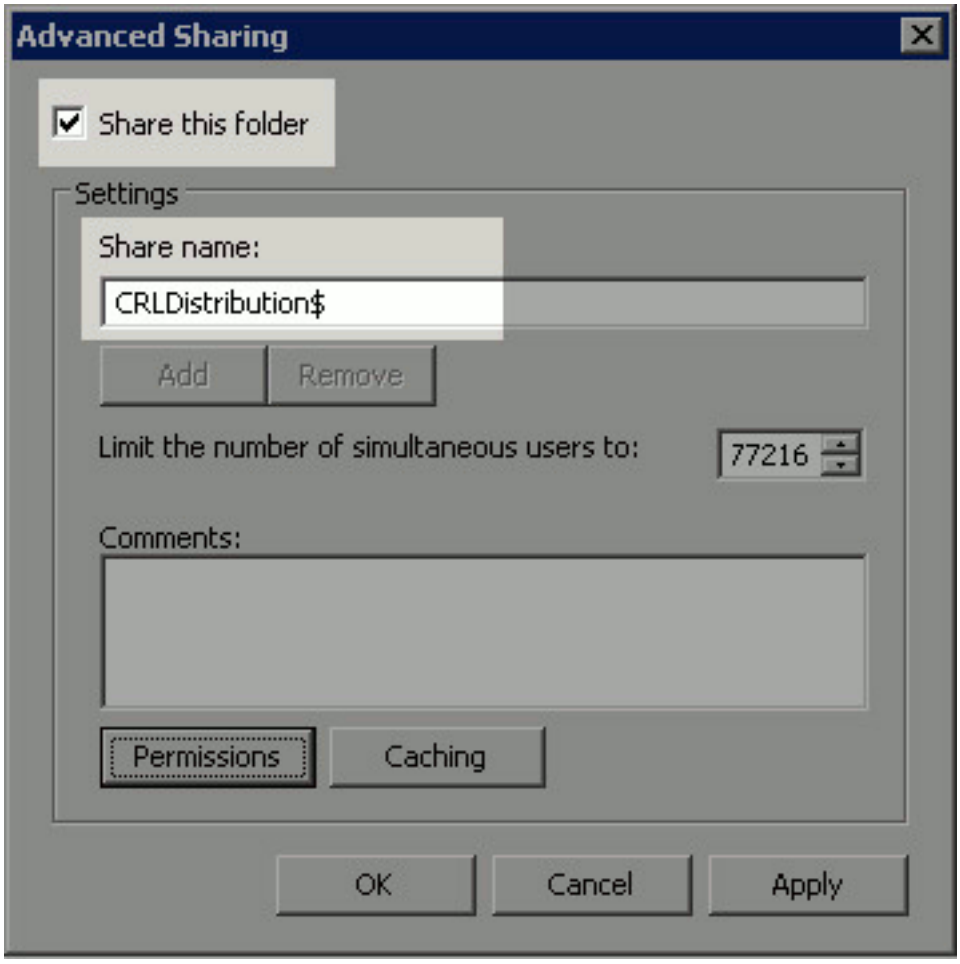
1. 在IIS服务器上，请选择文件系统的一个位置并且创建新文件夹。在本例中，文件夹C:\CRLDistribution被创建。



2. 为了CA能把CRL文件写到新文件夹，共享一定是启用的。用鼠标右键单击新文件夹，选择**属性**，点击**共享的**选项和然后点击**先进共享**。

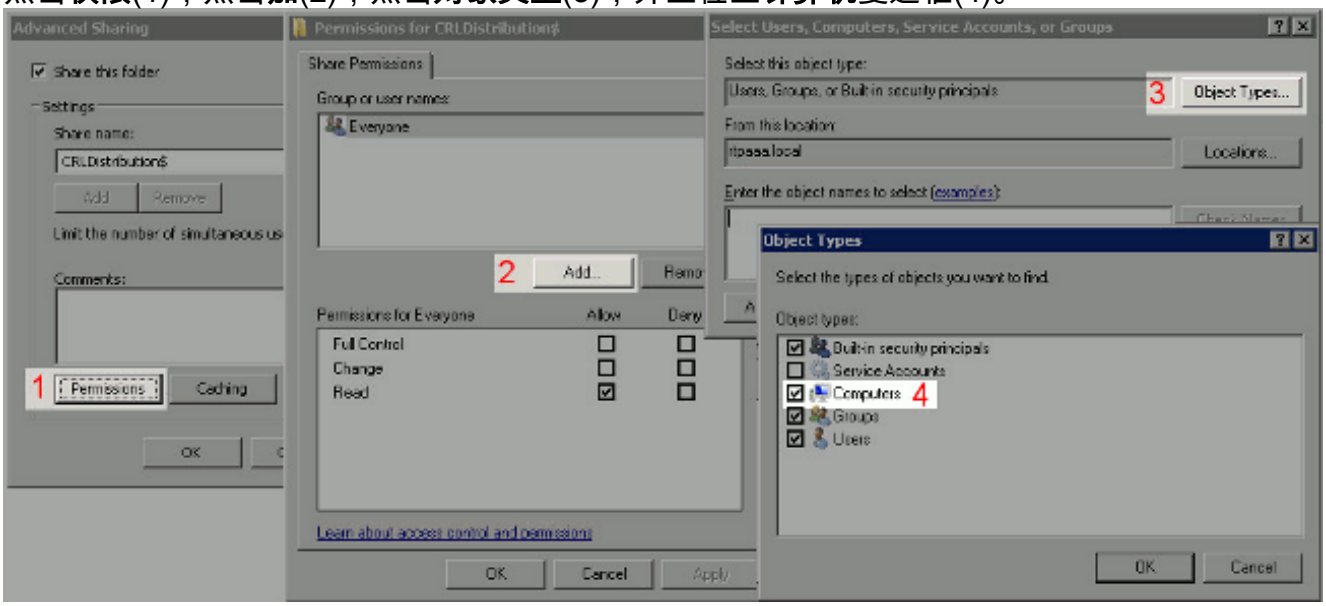


3. 为了共享文件夹，请检查**共用此文件夹**复选框然后添加美元的符号($)到共用名字的结尾在共用

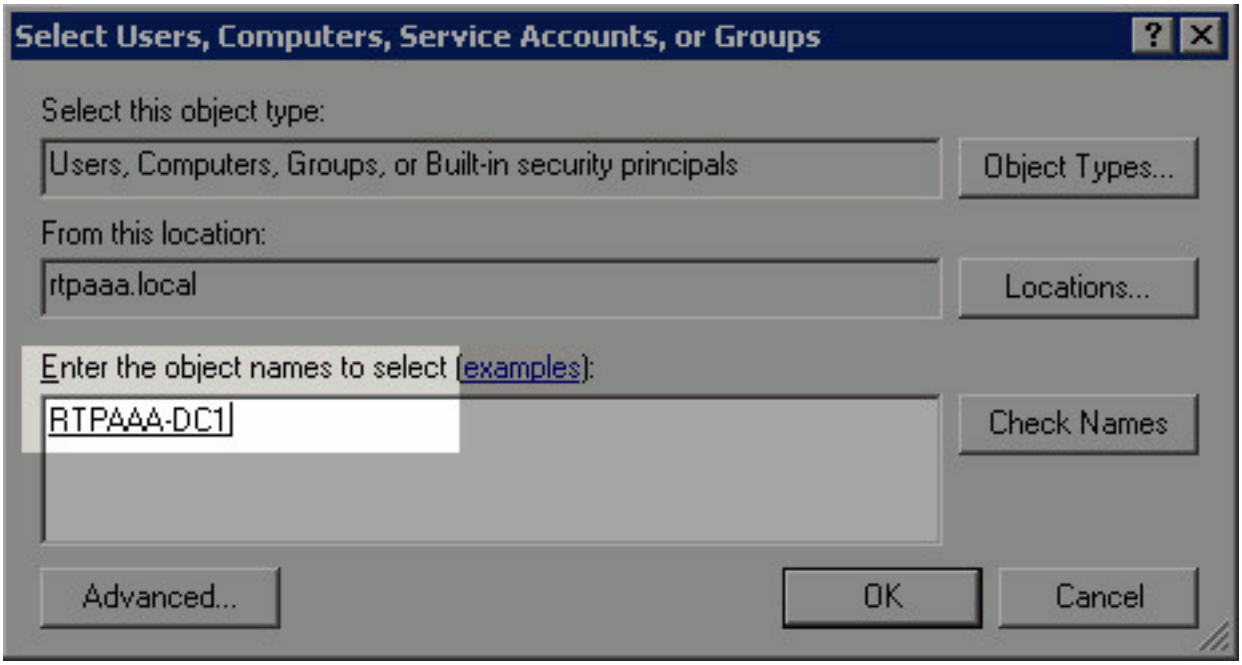


名称字段的隐藏共用。

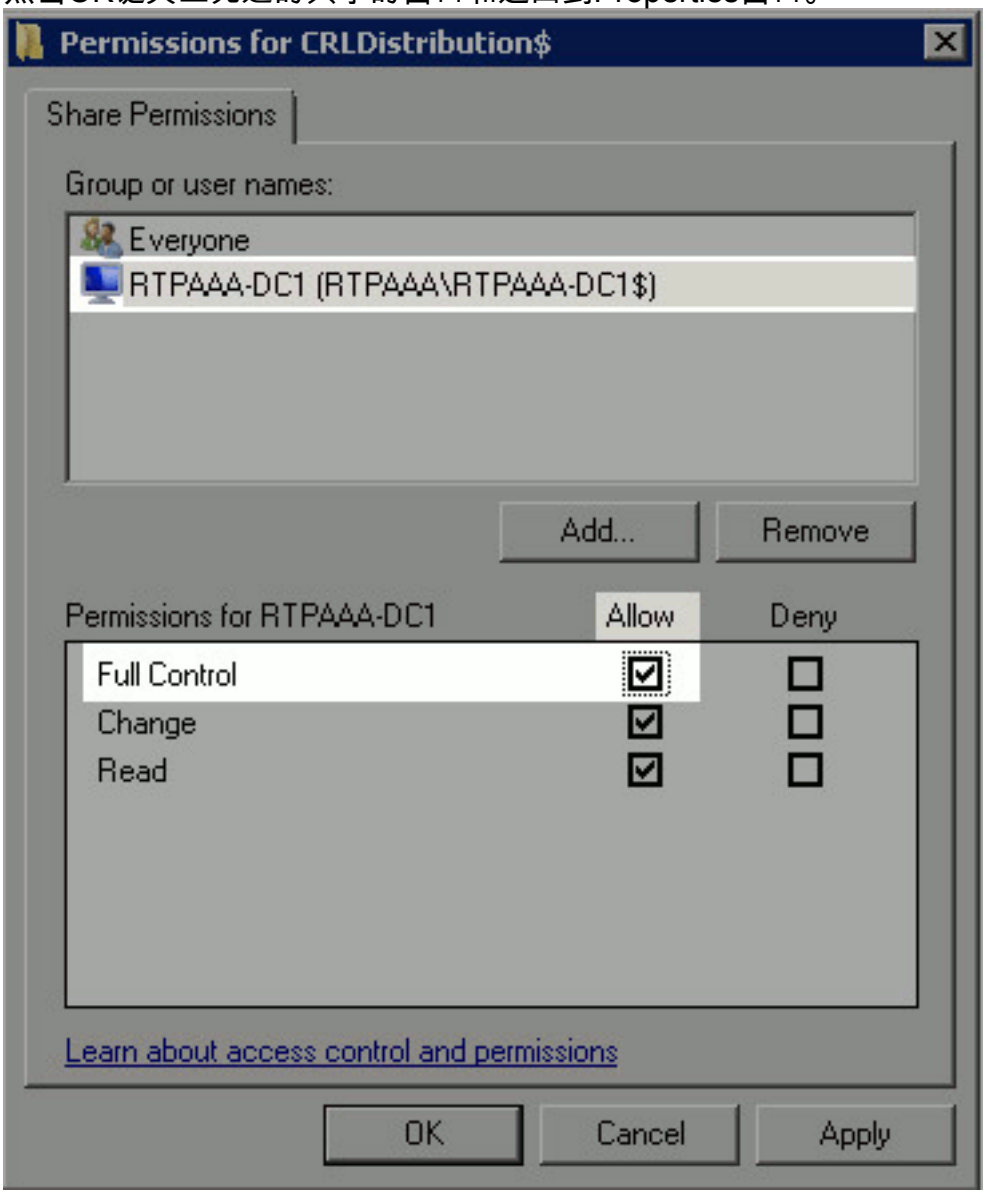
4. 点击**权限**(1)，点击**加**(2)，点击**对象类型**(3)，并且检查**计算机**复选框(4)。



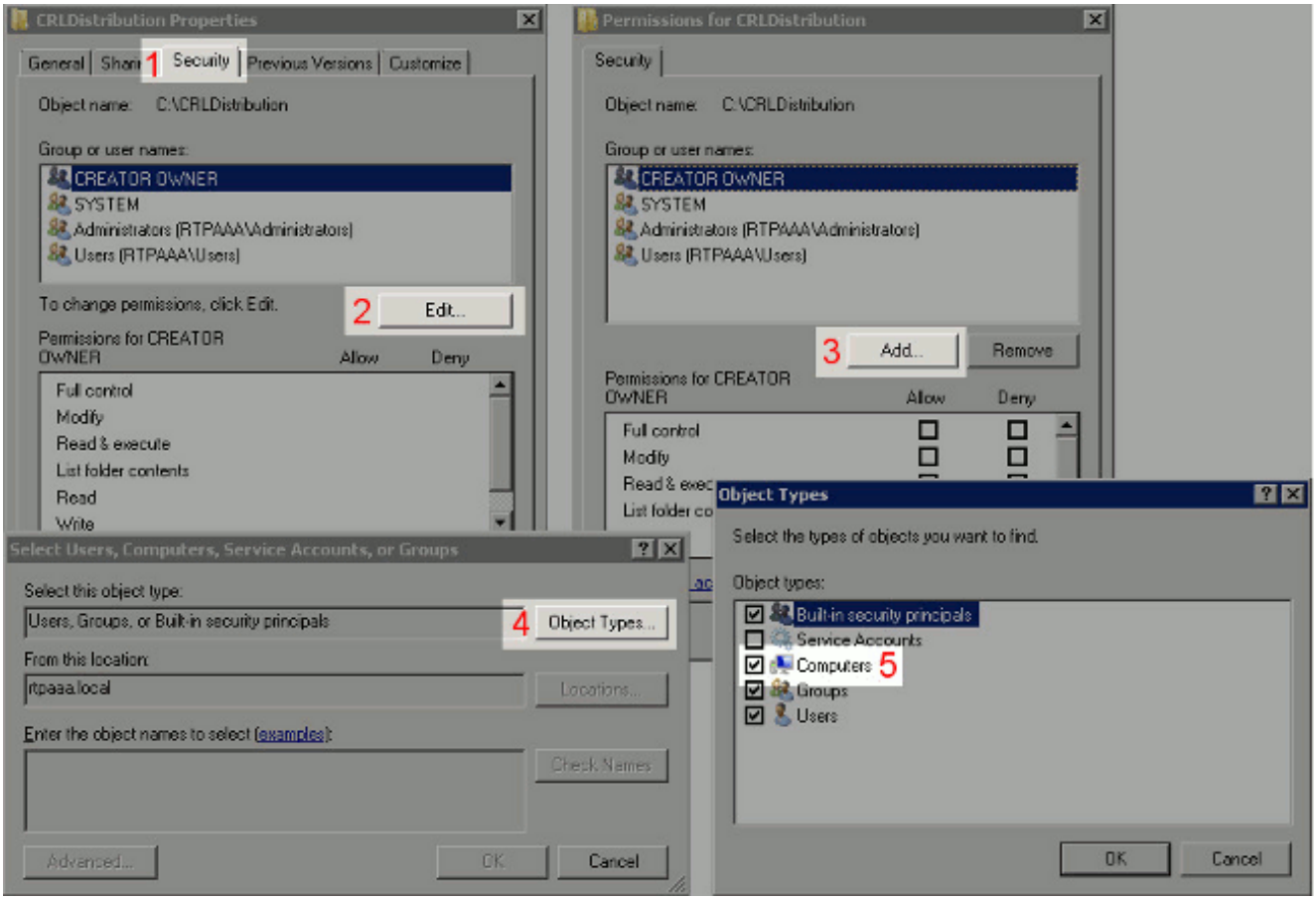
5. 为了返回到挑选用户，计算机，服务帐户或者Groups窗口，点击OK键。在进入对Select字段的对象名，输入CA服务器的计算机名称并且点击**检查名字**。如果输入的名字是有效的，名字刷新并且看上去加下划线。单击 **Ok**。



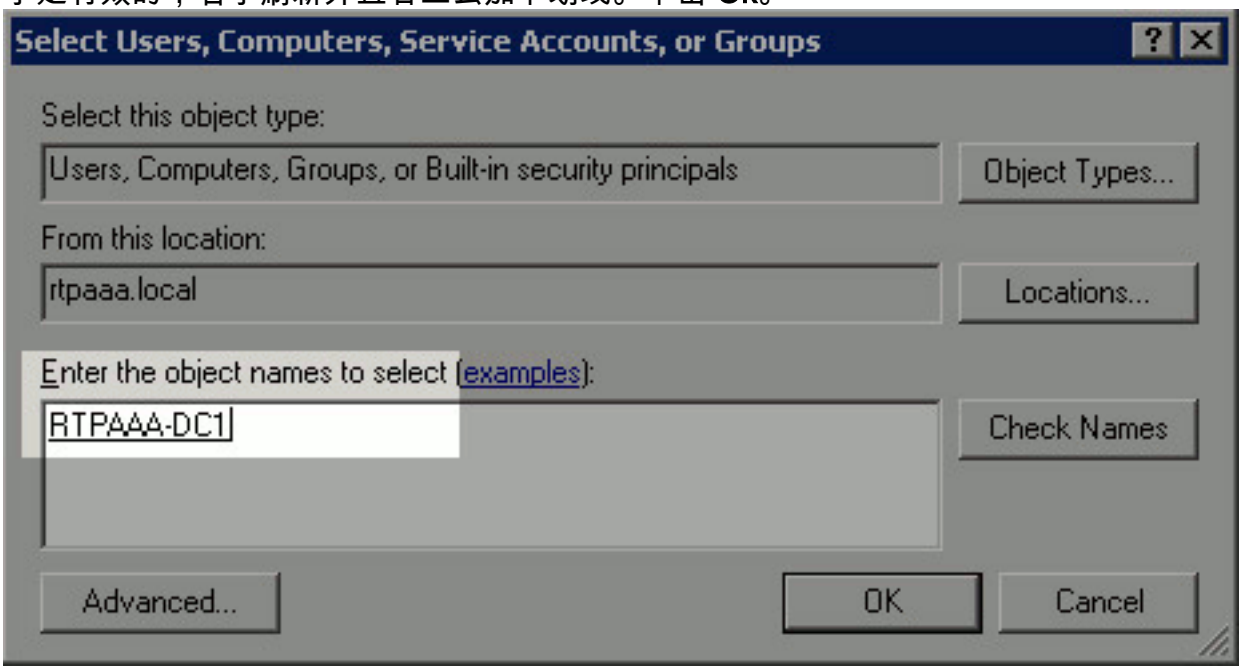
6. 在组或用户名名称字段，请选择CA计算机。检查**允许**完全控制授予全部存取CA.点击**OK**。再点击OK键关上先进的共享的窗口和返回到Properties窗口。



7. 为了允许CA把CRL文件写到新文件夹，请配置适当的安全权限。点击**安全**选项(1)，点击**编辑**(2)，点击**加**(3)，点击**对象类型**(4)，并且检查**计算机**复选框(5)。

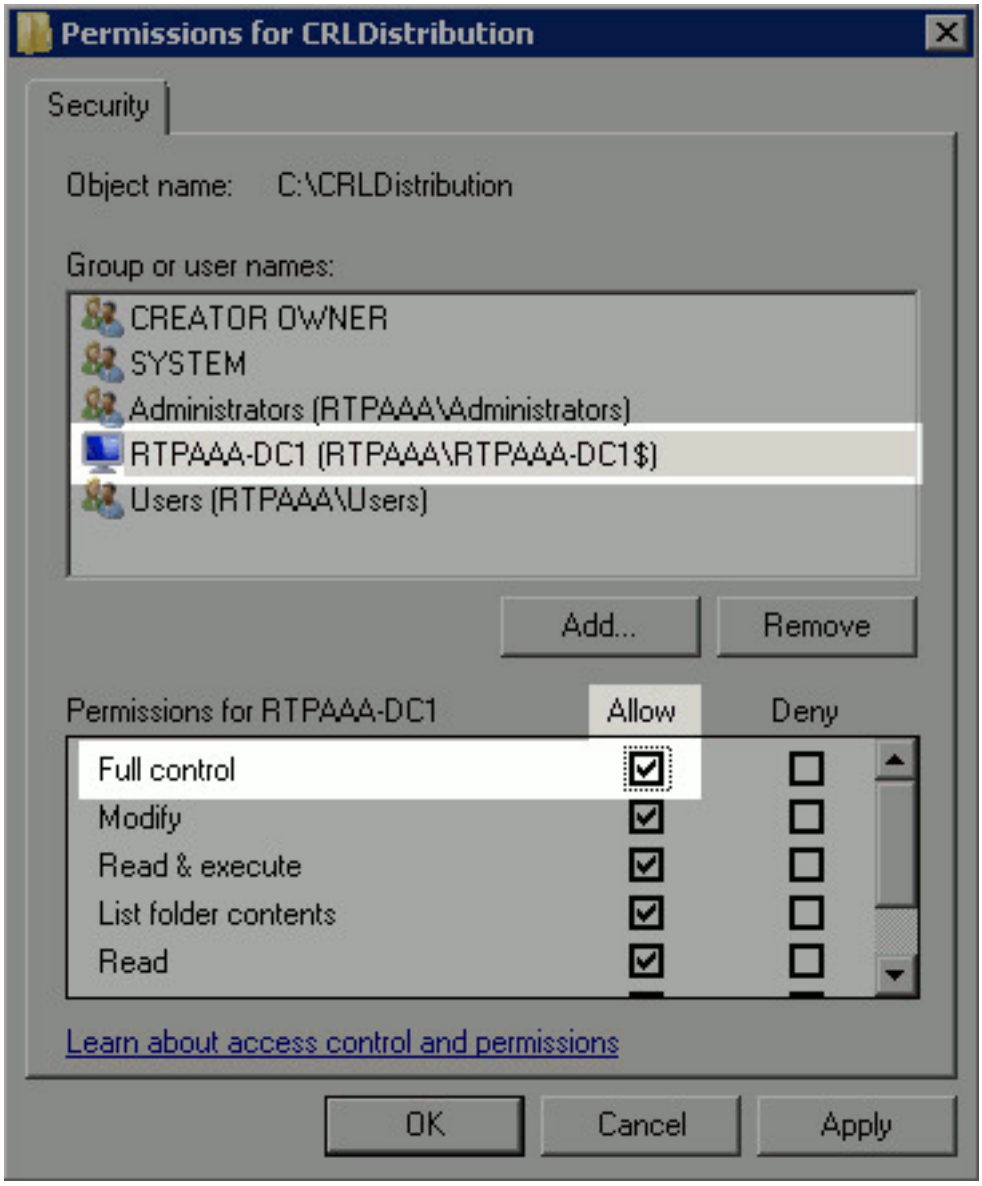


8. 在进入对Select字段的对象名，输入CA服务器的计算机名称并且点击**检查名字**。如果输入的名字是有效的，名字刷新并且看上去加下划线。单击 **Ok**。



9. 选择在组或用户名名称字段的CA计算机然后检查**允许**完全控制授予全部存取CA.点击**OK**然后

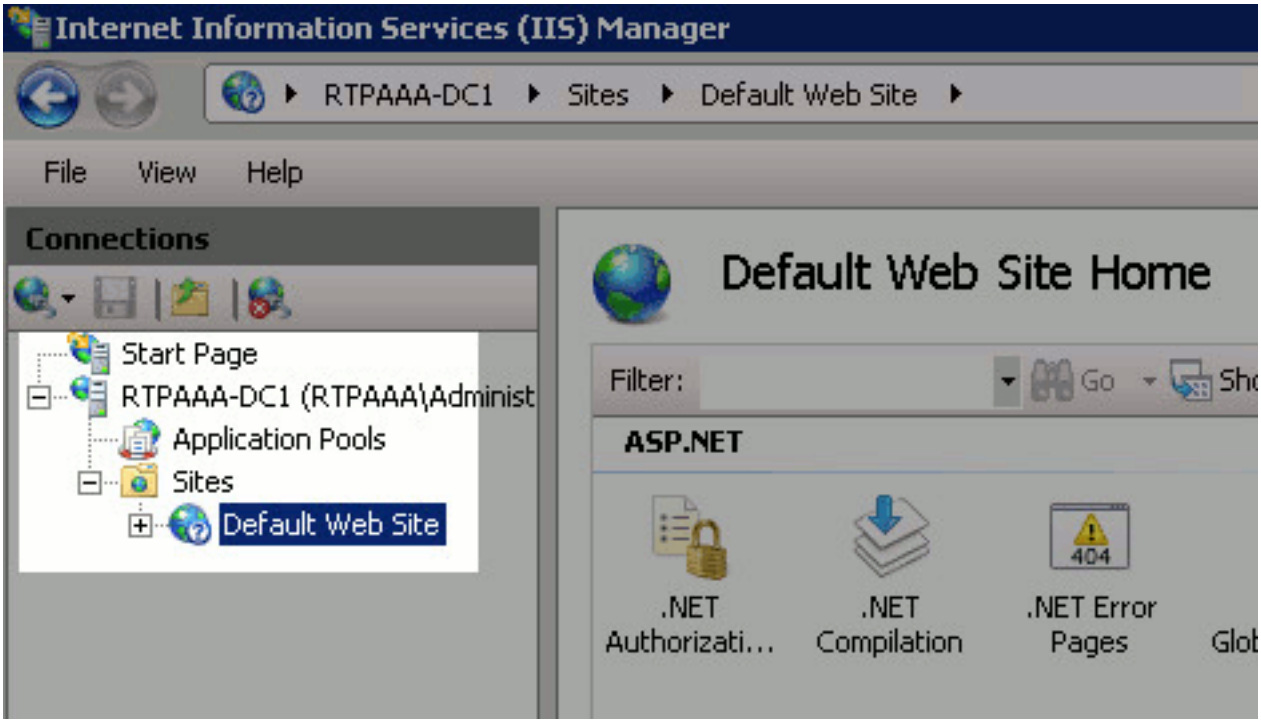
点击**接近**完全任务。



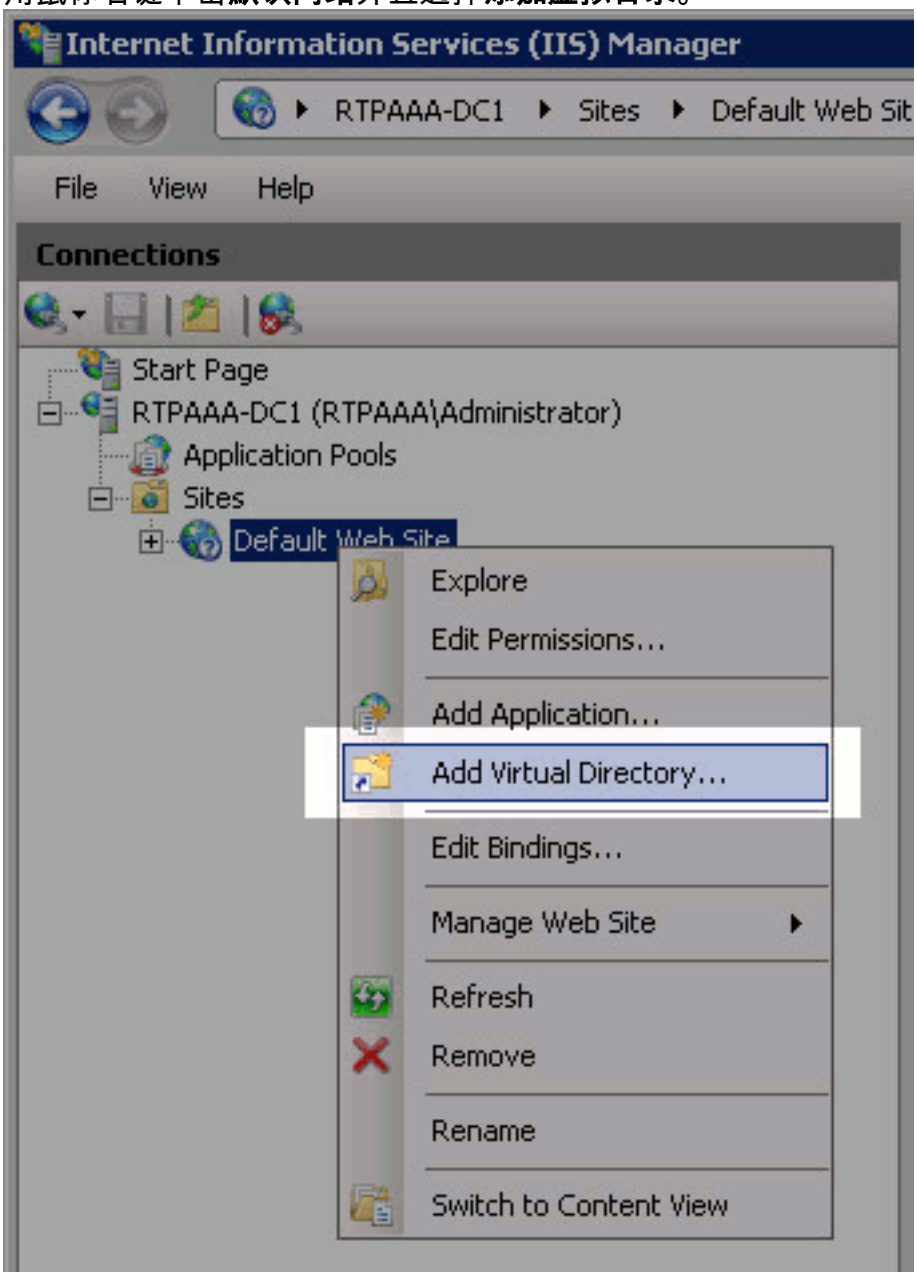
第2.部分创建IIS的站点显示新的控制分配点

为了ISE能访问CRL文件，请做安置CRL文件可访问通过IIS的目录。

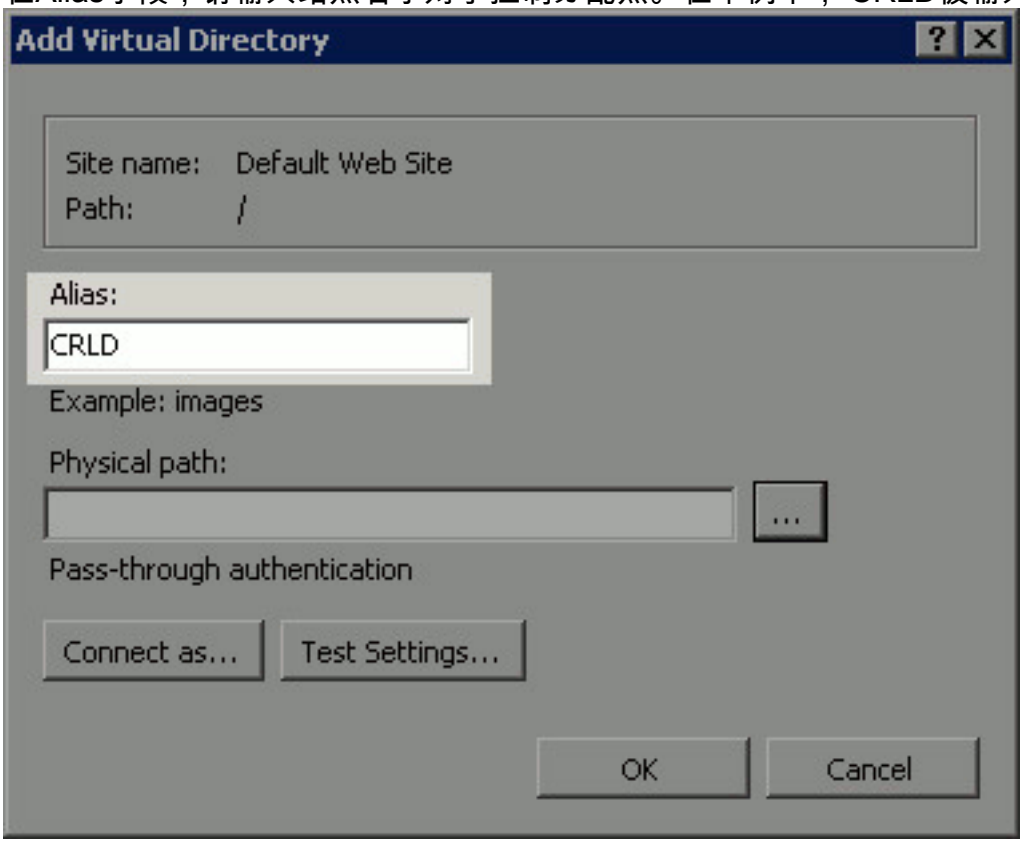
1. 在IIS服务器工具栏，请点击**开始**。选择**管理工具> Internet信息服务(IIS)管理器**。
2. 在左窗格中(叫作控制台结构树)，请扩展IIS服务器名然后扩展**站点**。



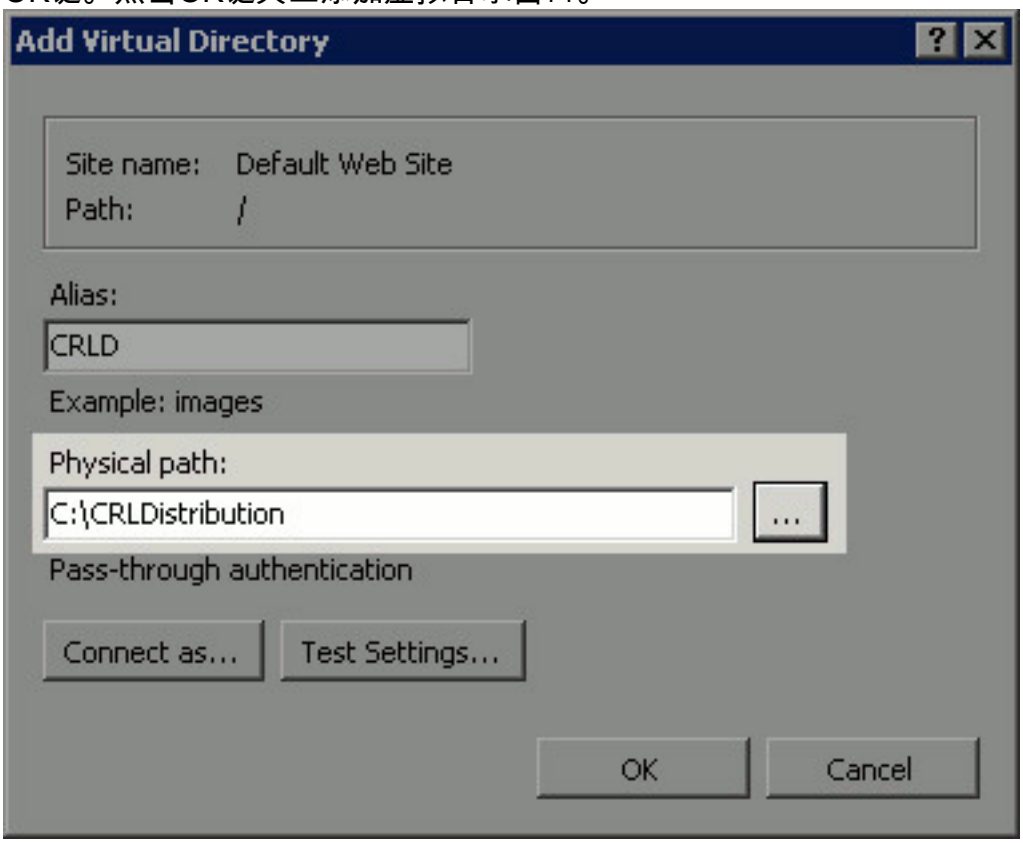
3. 用鼠标右键单击**默认网站**并且选择**添加虚拟目录**。



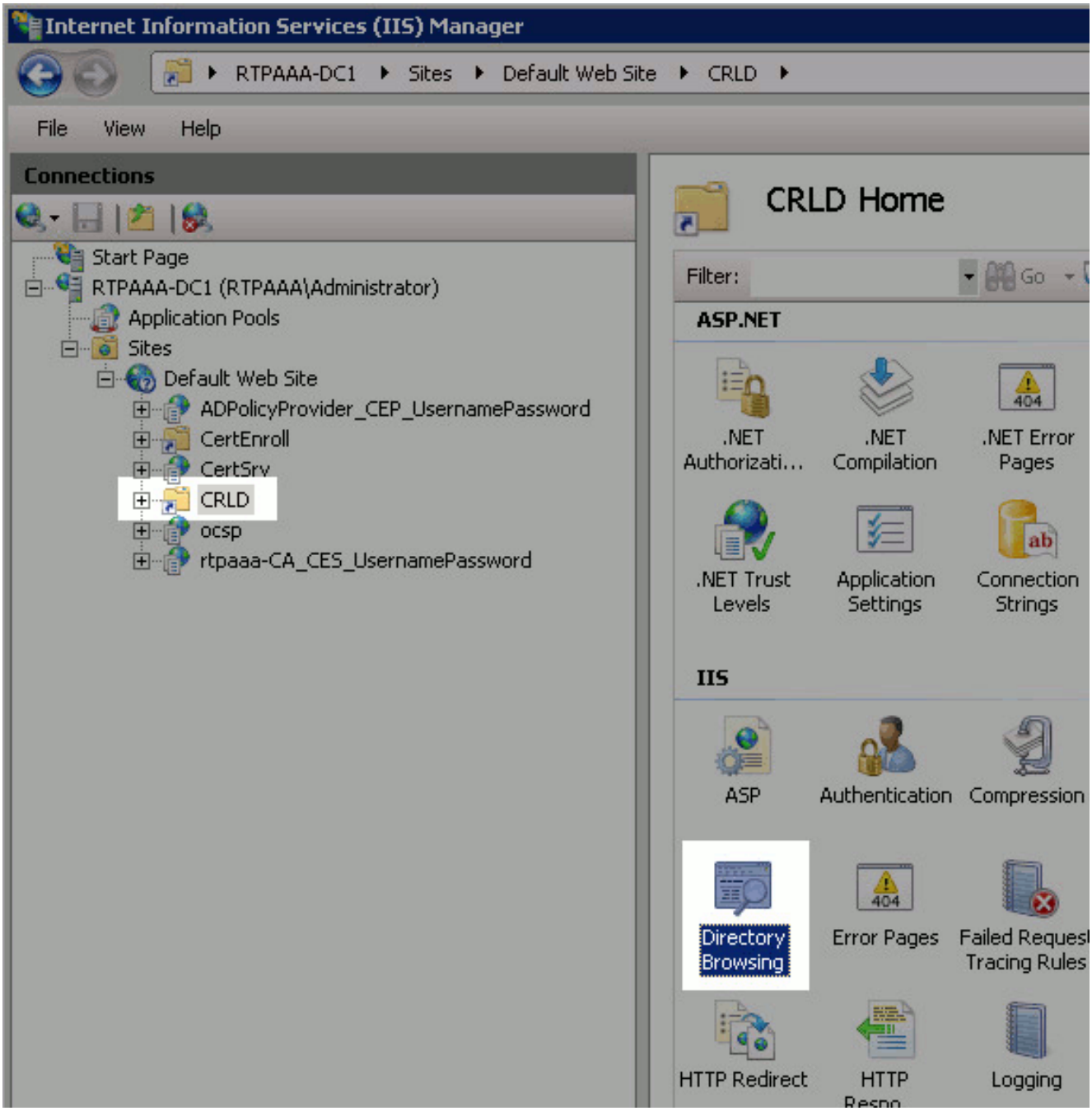
4. 在Alias字段，请输入站点名字对于控制分配点。在本例中， CRLD被输入。



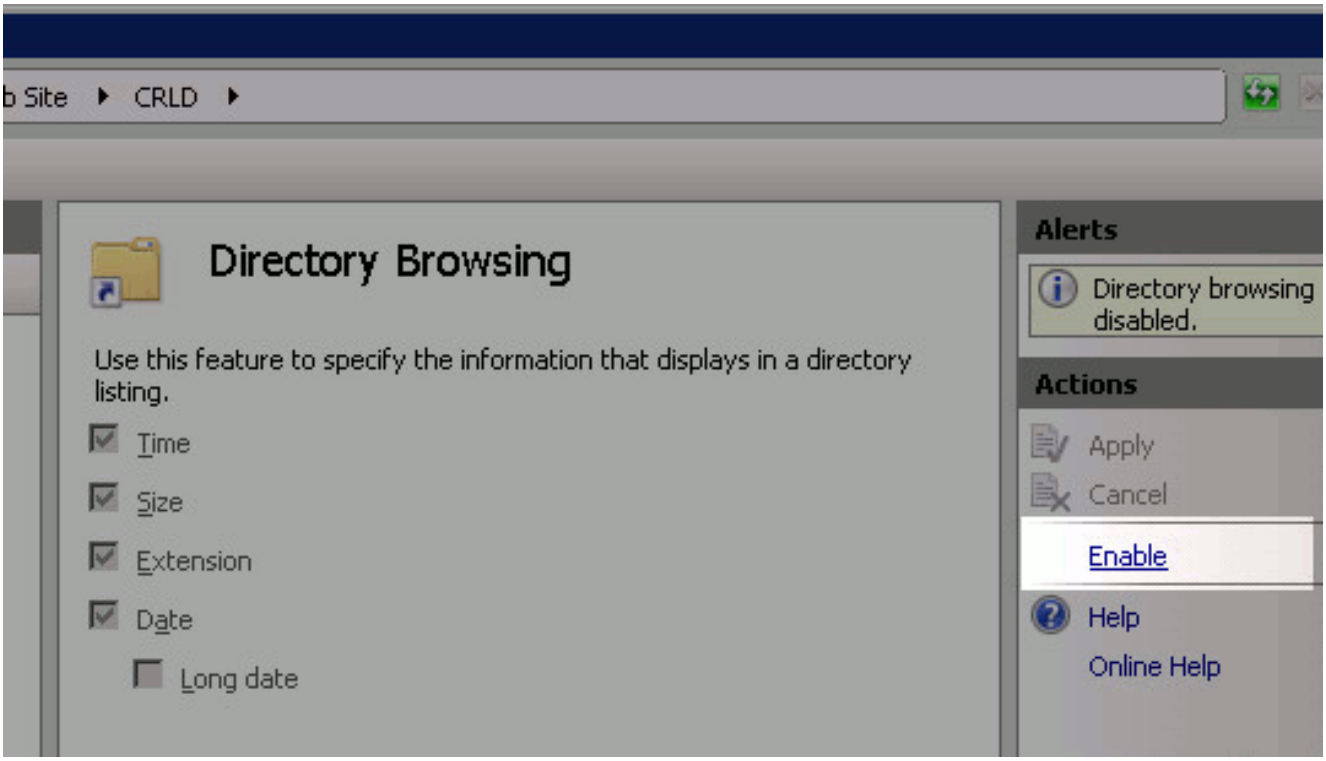
5. 在物理路径领域右边点击省略号(…)并且访问到在创建的文件夹第1.部分精选文件夹并且点击OK键。点击OK键关上添加虚拟目录窗口。



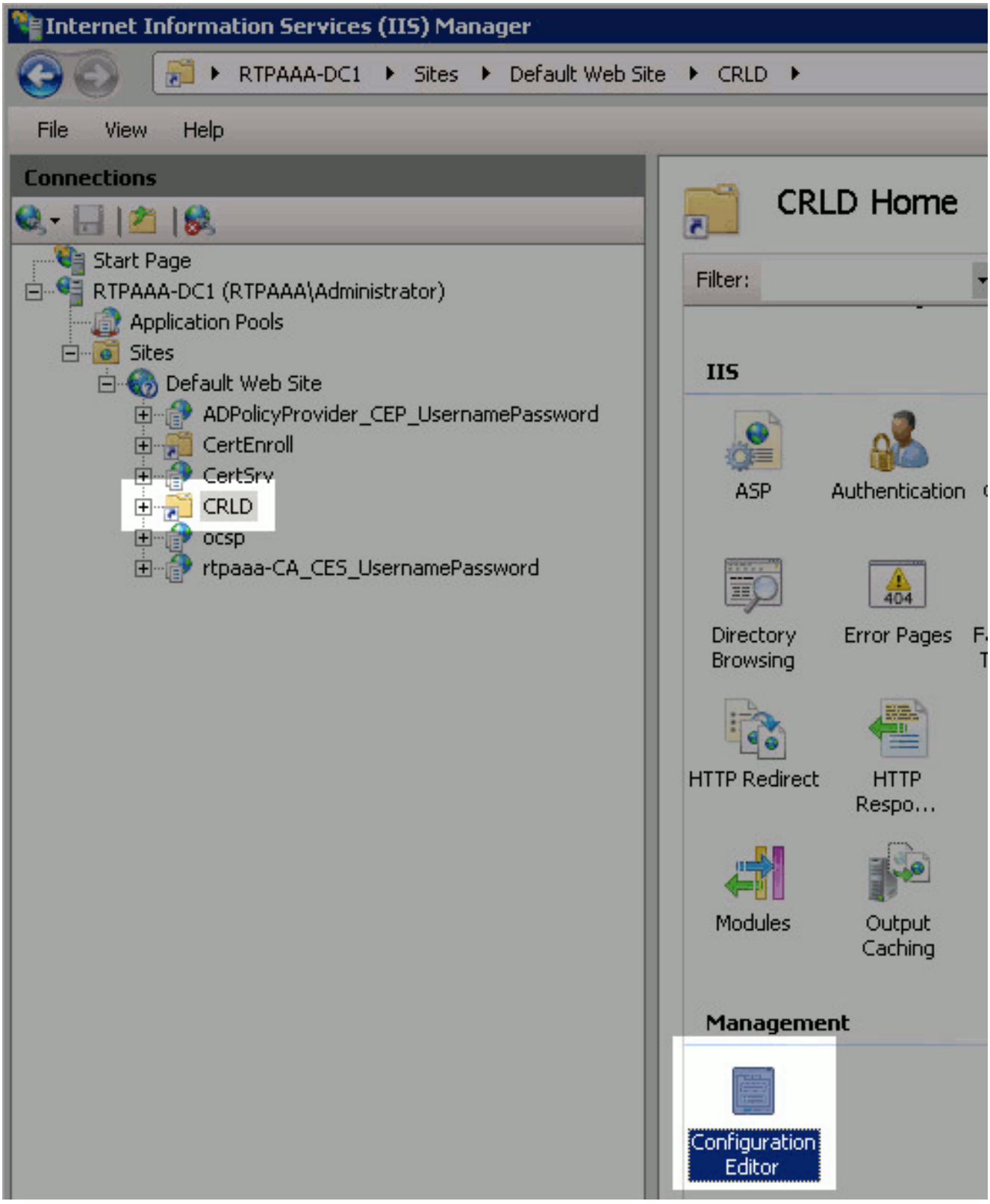
6. 应该用左窗格突出显示在输入的站点名字第4步。否则，当前请选择它。在中心的面中，请双击**目录访问**。



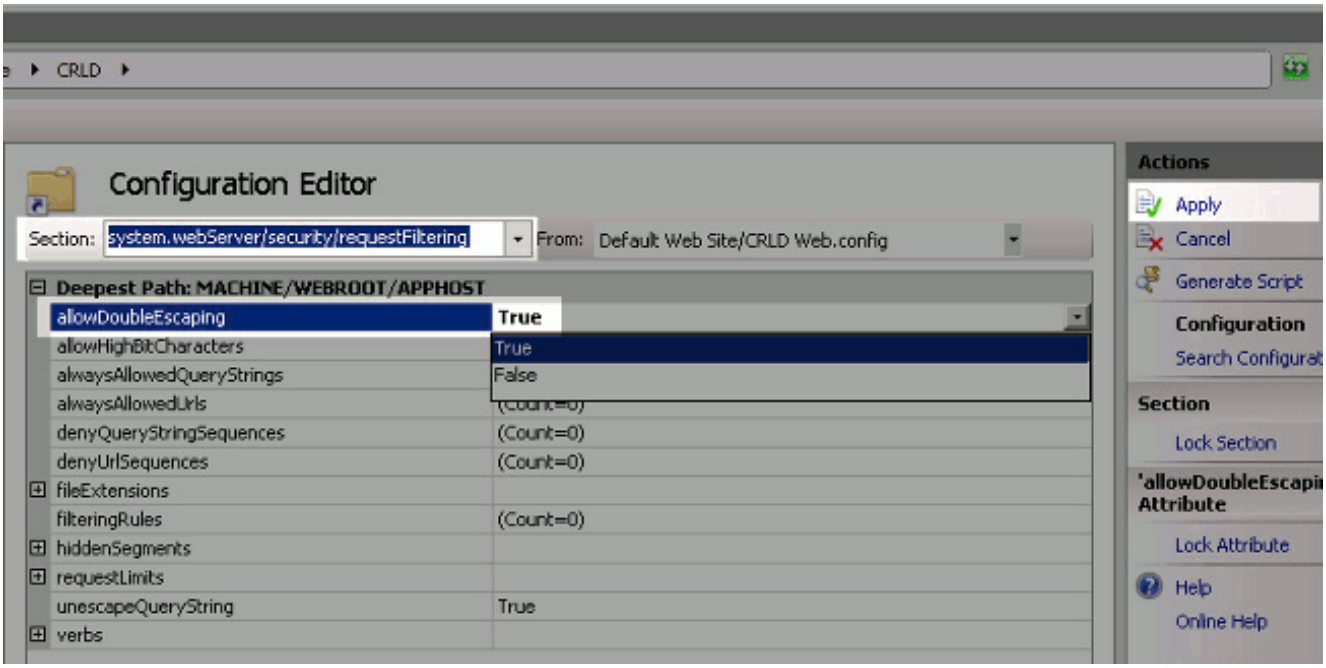
7. 在右窗格中，请点击**Enable (event)**对enable (event)目录访问。



8. 在左窗格中，再请选择站点名字。在中心的面中，请双击**配置编辑器**。



9. 在部分下拉列表中，请选择**system.webServer/安全/requestFiltering。在**allowDoubleEscaping的下拉列表中，请选择**真。在**右窗格中，请点击**适用。**

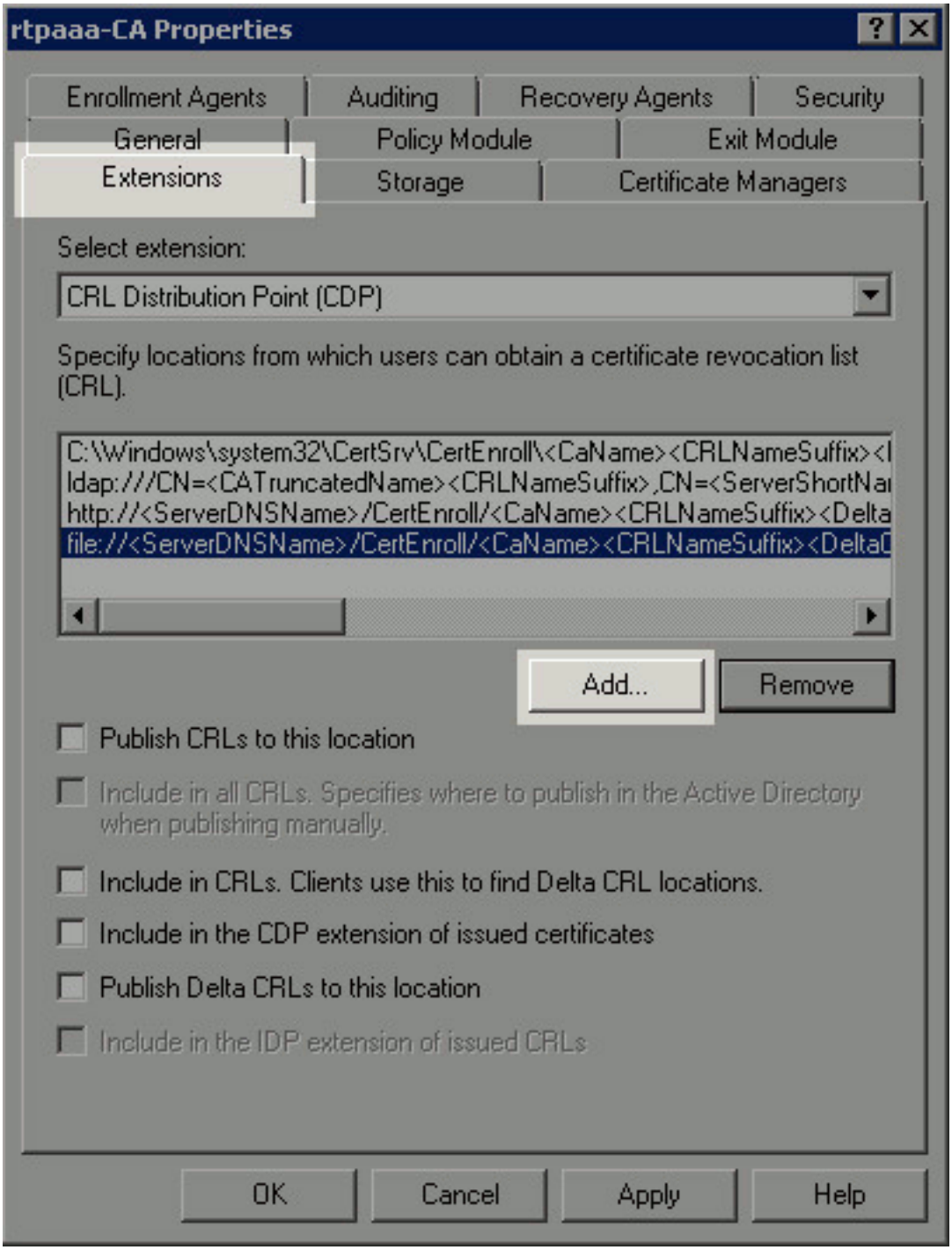


文件夹应该当前是可访问的通过IIS。

第3.部分配置Microsoft CA服务器发布CRL文件到分配点

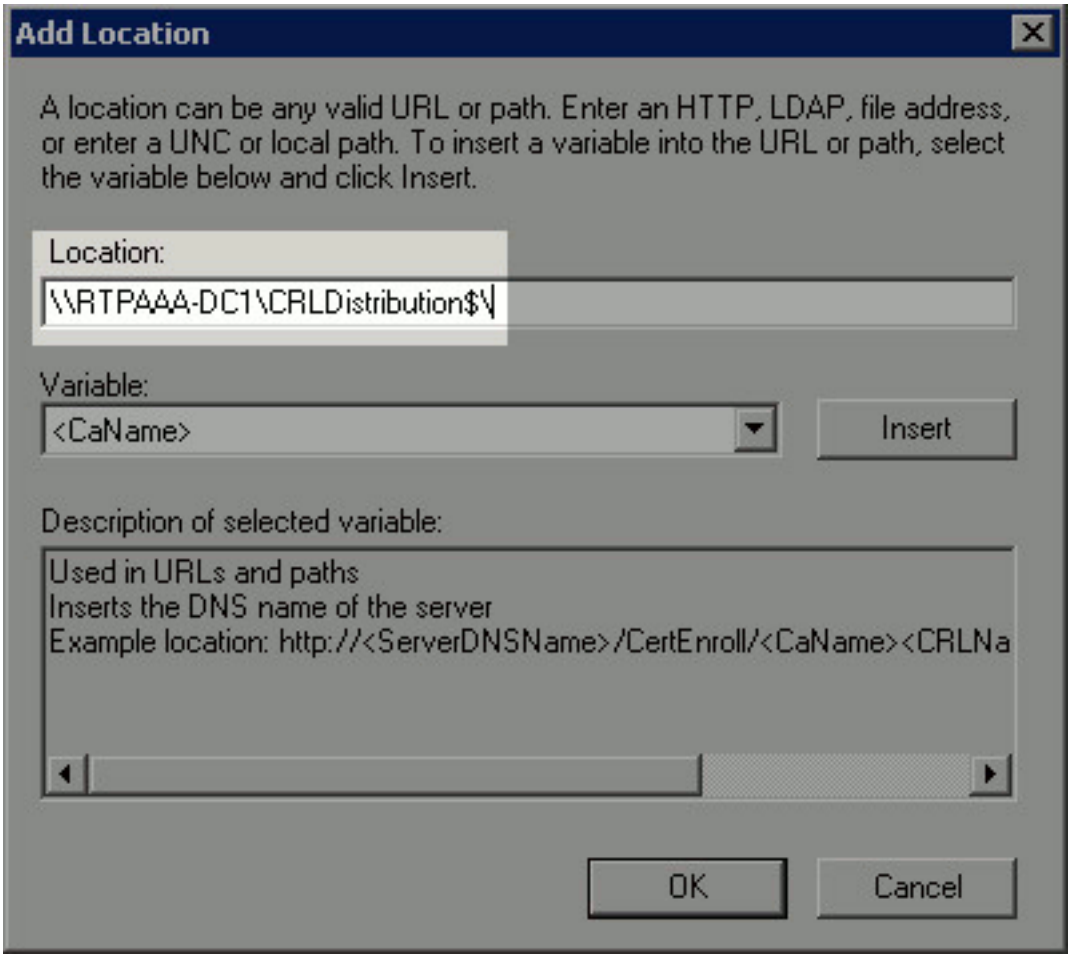
即然配置新文件夹安置CRL文件，并且文件夹在IIS显示了，请配置Microsoft CA服务器发布CRL文件到新的位置。

1. 在CA服务器工具栏，请点击**开始**。选择**管理Tools>认证机关**。
2. 在左窗格中，请用鼠标右键单击CA名字。选择**属性**然后点击**扩展**选项。为了添加新的控制分配点，请点击**添加**。

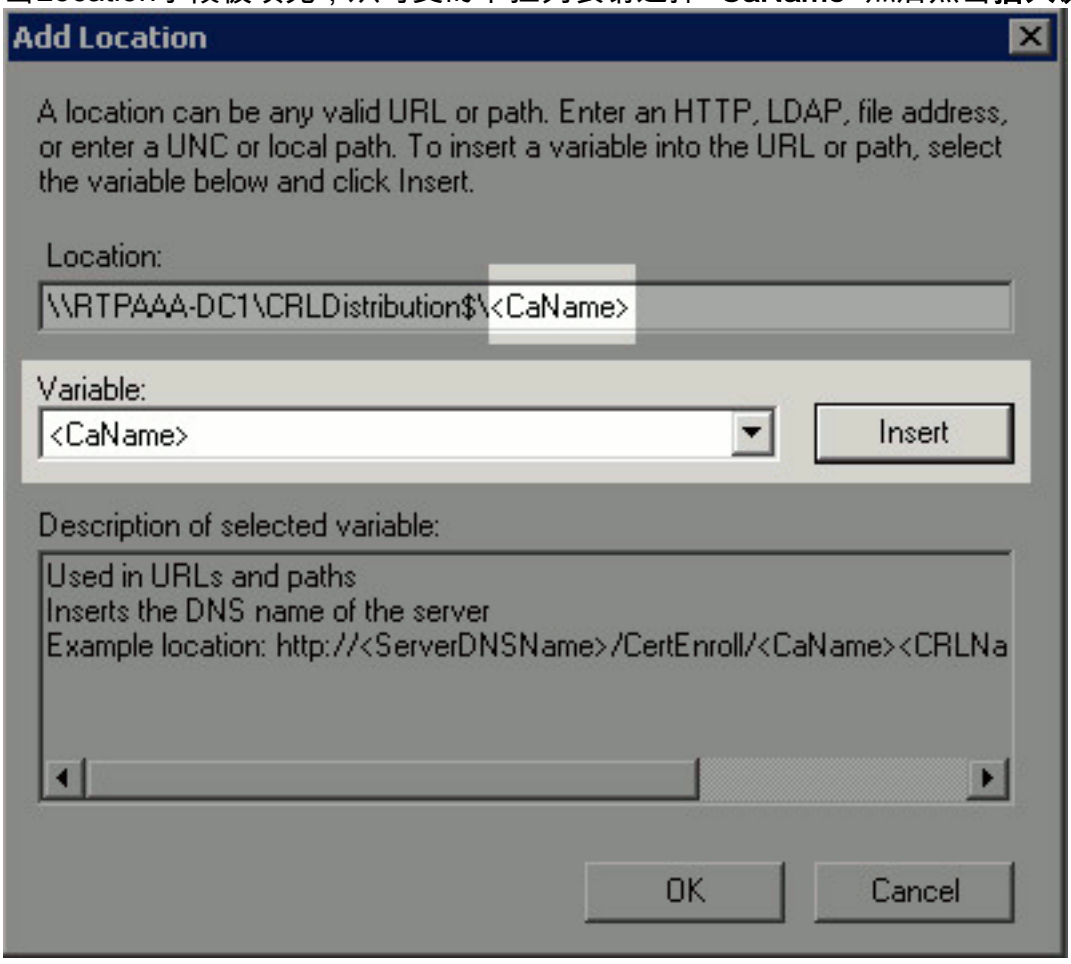


3. 在Location字段，请输入路径到被创建和共有的文件夹在第1.部分。在第1部分的示例中，路径是：

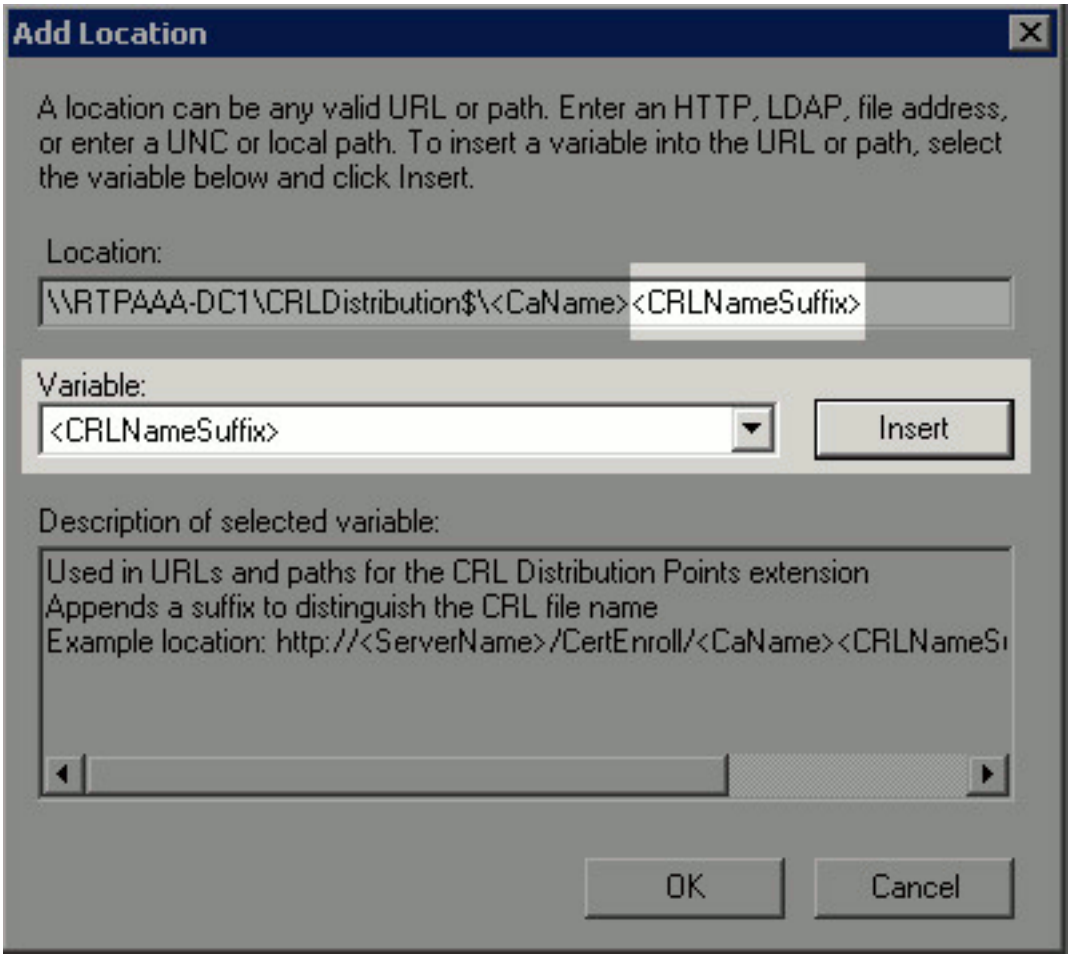
```
\\RTPAAA-DC1\CRLDistribution$\
```



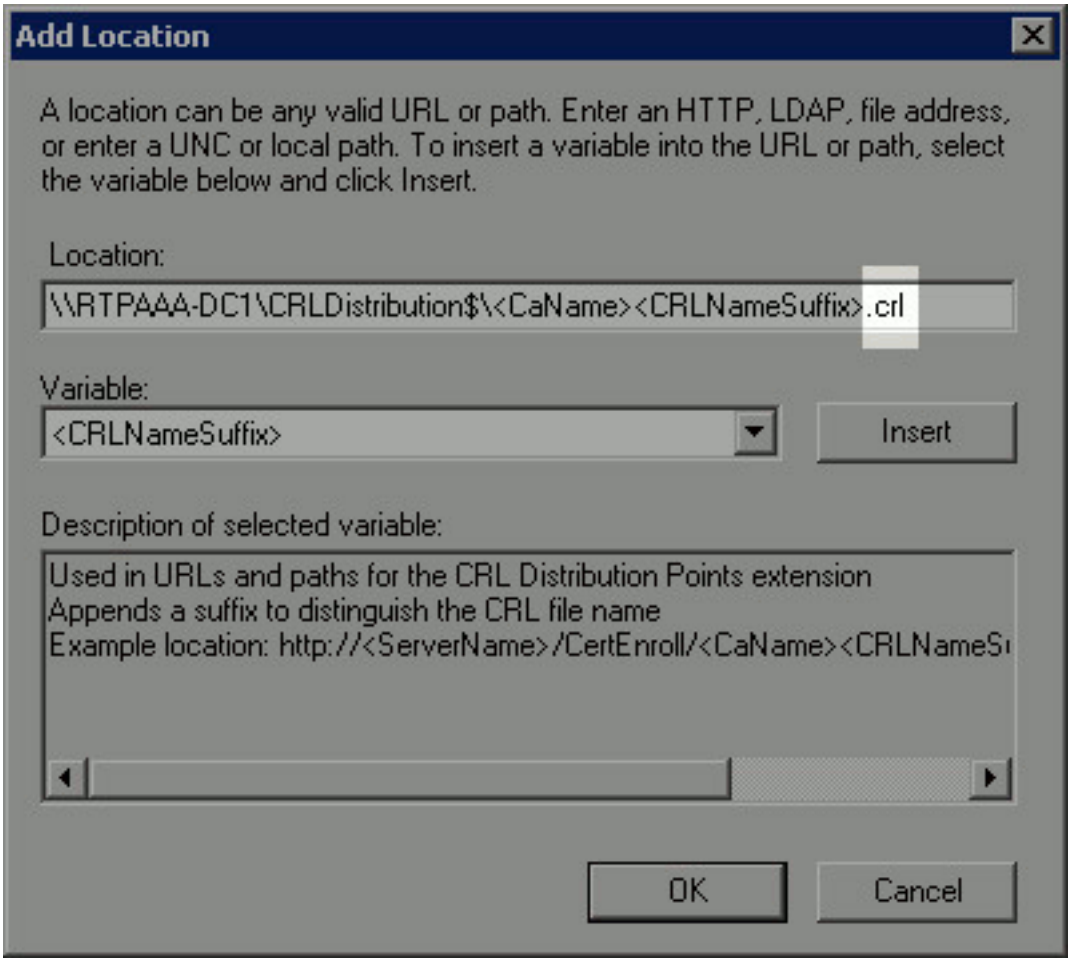
4. 当Location字段被填充，从可变的下拉列表请选择**<CaName>**然后点击**插入键。**



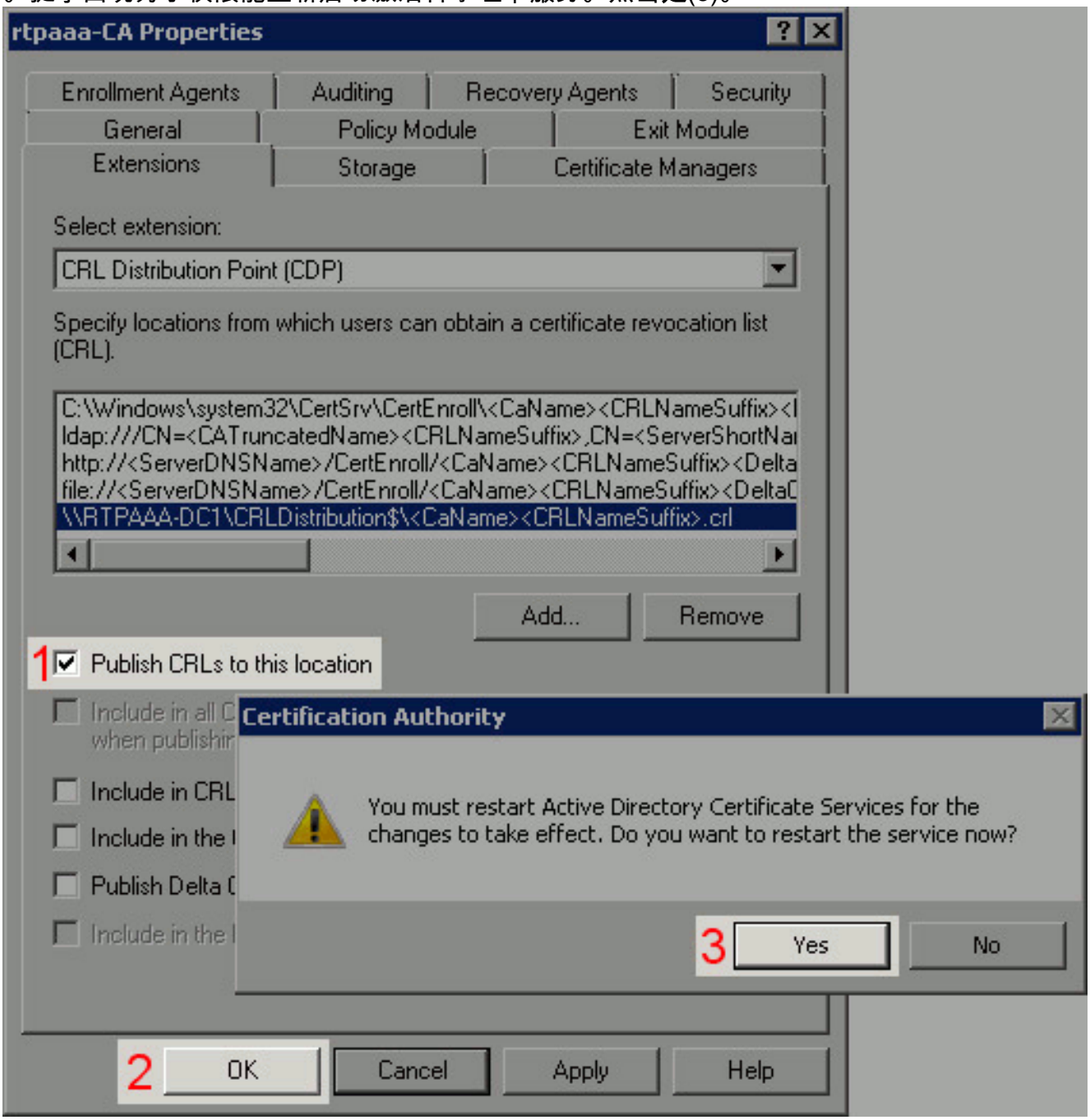
5. 从可变的下拉列表，请选择**<CRLNameSuffix>**然后点击**插入键。**



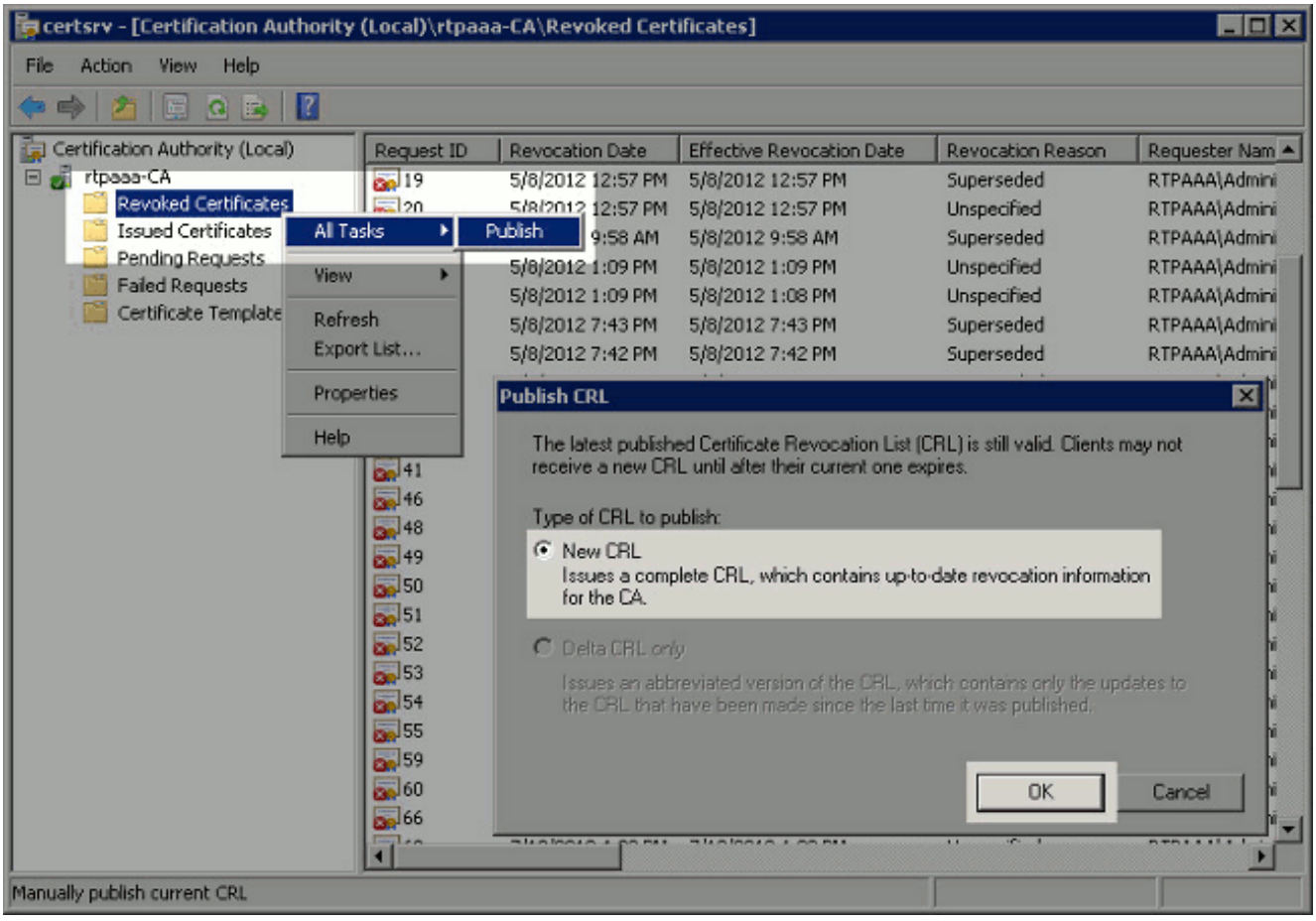
6. 在Location字段，请添附.crl对路径的末端。在本例中，位置是：
`\\RTPAAA-DC1\CRLDistribution$\<CaName><CRLNameSuffix>.crl`



7. 点击OK键返回到扩展选项。检查**发布Crl到此位置**复选框(1)然后点击**OK(2)**关上Properties窗口。提示出现为了权限能重新启动激活目录证书服务。点击**是**(3)。



8. 在左窗格中，请用鼠标右键单击**被废除的证书**。选择**所有任务>发布**。保证新的CRL选择然后点击OK键。

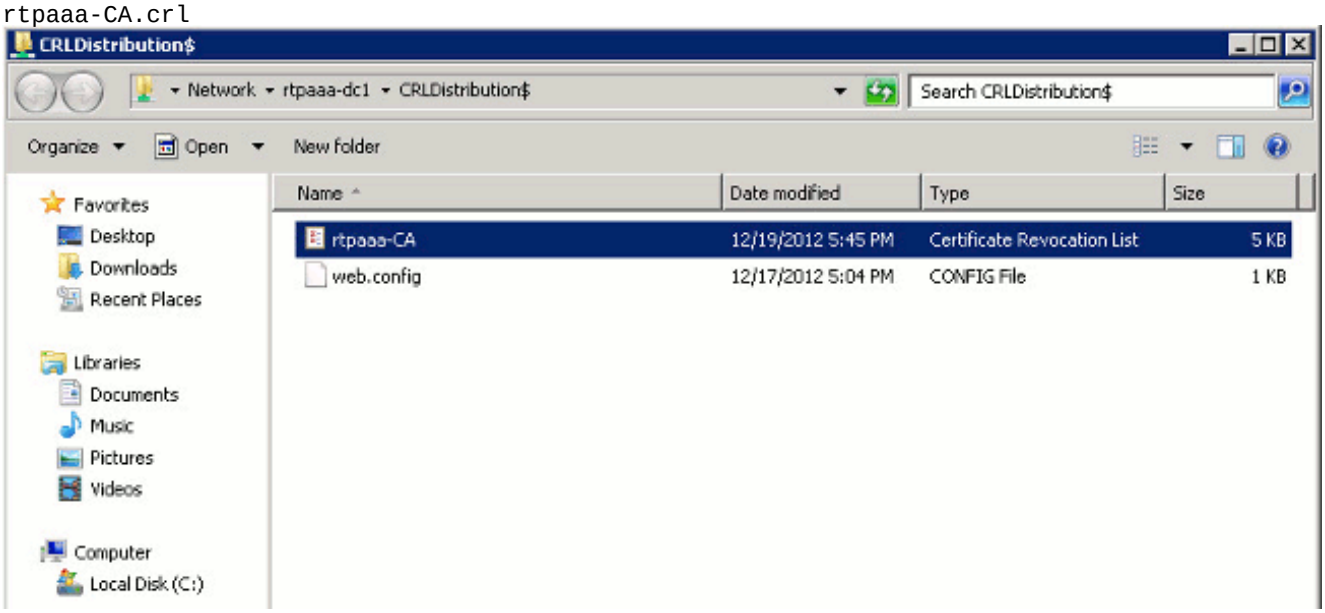


Microsoft CA服务器应该创建在创建的文件夹的一个新的.crl文件第1.部分。如果新的CRL文件顺利地被创建将没有对话，在好后点击。如果错误关于新的分配点文件夹返回，请仔细重复在此部分的每个步骤。

第4.部分验证CRL文件存在并且通过IIS是可访问的

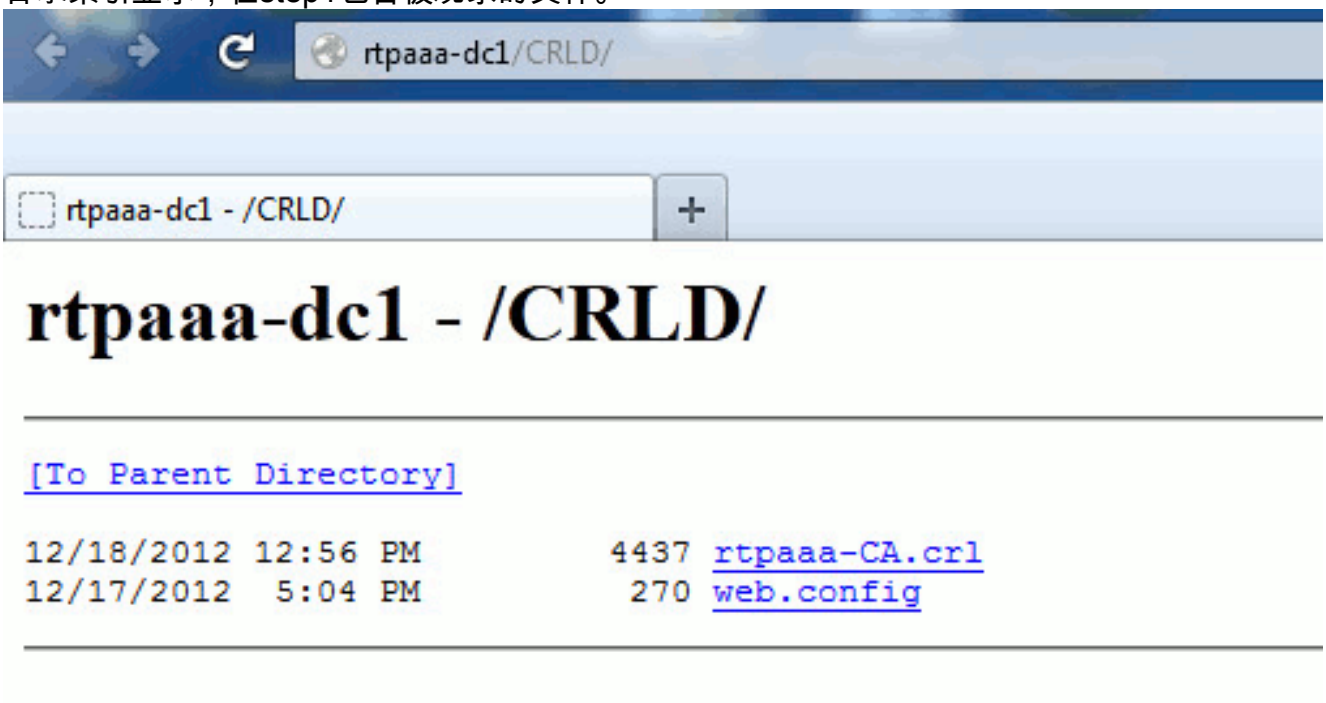
验证新的CRL文件存在，并且那他们通过从另一个工作站的IIS是可访问的，在您开始此部分前。

1. 在IIS服务器上，请打开在创建的文件夹第1.部分。应该有单个.crl文件当前与<CANAME>是CA服务器的名字的表<CANAME>.crl。在本例中，文件名是：
   `rtpaaa-CA.crl`



2. 从网络的一个工作站(理想地说在网络和ISE主要的Admin节点一样)，请打开Web浏览器并且访问对<SERVER>是在配置的IIS服务器服务器名第2部分的http:// <SERVER>/<CRLSITE>，并

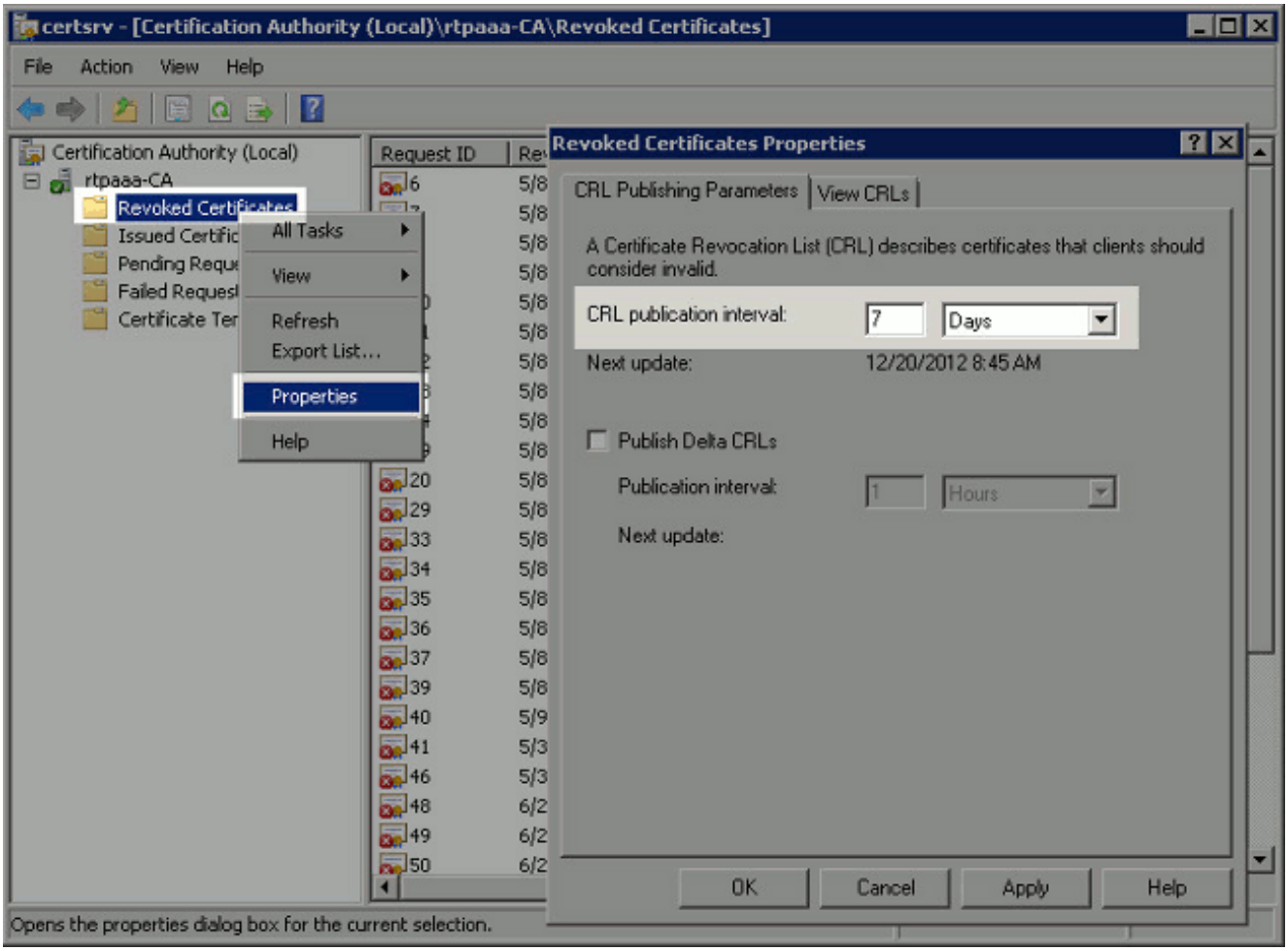
且<CRLSITE>是为在第2.部分的分配点选择的站点名字。在本例中， URL是：
`http://RTPAAA-DC1/CRLD`
目录索引显示，在step1包含被观察的文件。



第5.部分配置ISE使用新的控制分配点

在配置ISE检索CRL前，请定义间隔发布CRL。确定此间隔的策略是超出本文的范围之外。潜在的值(在Microsoft CA)是1小时到411年，包含的。DEFAULT值是1个星期。一旦确定了您的环境的一个适当的间隔，请设置与这些指令的间隔：

1. 在CA服务器工具栏，请点击**开始**。选择**管理Tools>认证机关**。
2. 在左窗格中，请扩展CA.用鼠标右键单击**被取消的证书**文件夹并且选择**属性。**
3. 在CRL出版物间隔字段，请输入所需数量的并且选择时间。点击OK键关上窗口和应用更改。在本例中，配置出版物间隔7天。



您应该当前确认几个注册值，将帮助确定在ISE的CRL检索设置。

4. 输入**certutil - getreg CA \ Clock***命令确认ClockSkew值。DEFAULT值是10分钟。输出示例：

```
Values:
    ClockSkewMinutes        REG_DWORS = a (10)
CertUtil: -getreg command completed successfully.
```

5. 输入**certutil - getreg CA \ CRLov***命令验证是否手工设置CRLOverlapPeriod。默认情况下CRLOverlapUnit值是0，表明未设置手工的值。除0之外，如果值是值，请记录值和单元。输出示例：

```
Values:
    CRLOverlapPeriod      REG_SZ = Hours
    CRLOverlapUnits        REG_DWORD = 0
CertUtil: -getreg command completed successfully.
```

6. 输入**certutil - getreg CA \ CRLpe***命令验证CRLPeriod，在第3.步设置。输出示例：

```
Values:
    CRLPeriod      REG_SZ = Days
    CRLUnits        REG_DWORD = 7
CertUtil: -getreg command completed successfully.
```

7. 计算CRL宽限期如下：如果CRLOverlapPeriod在第5步设置：重叠= CRLOverlapPeriod，以分钟;：重叠= (CRLPeriod/10)，以分钟如果重叠> 720然后重叠= 720如果重叠< (1.5 * ClockSkewMinutes)然后重叠= (1.5 * ClockSkewMinutes)如果重叠> CRLPeriod，在分钟然后重叠= CRLPeriod以分钟宽限期= 720分钟+ 10分钟= 730分钟**示例：**

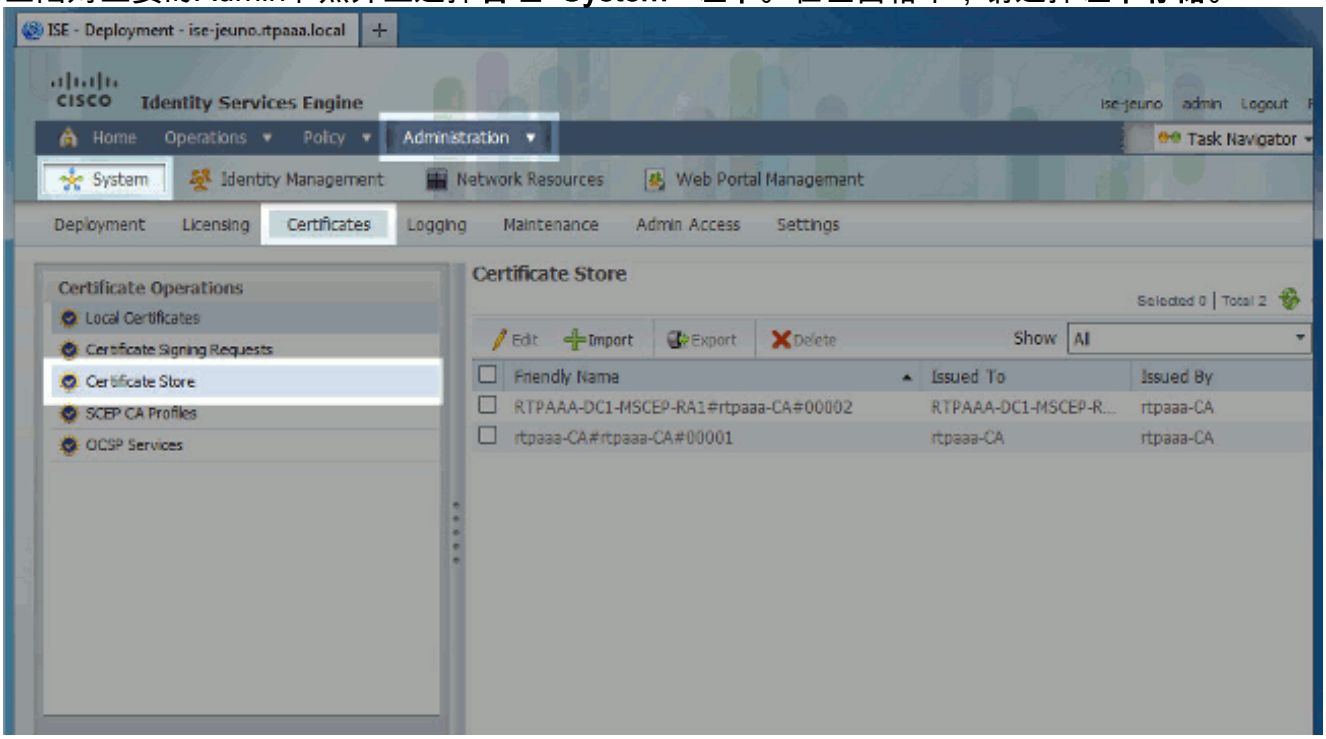
As stated above, CRLPeriod was set to 7 days, or 10248 minutes and CRLOverlapPeriod was not set.

a. OVERLAP = (10248 / 10) = 1024.8 minutes
b. 1024.8 minutes is > 720 minutes : OVERLAP = 720 minutes

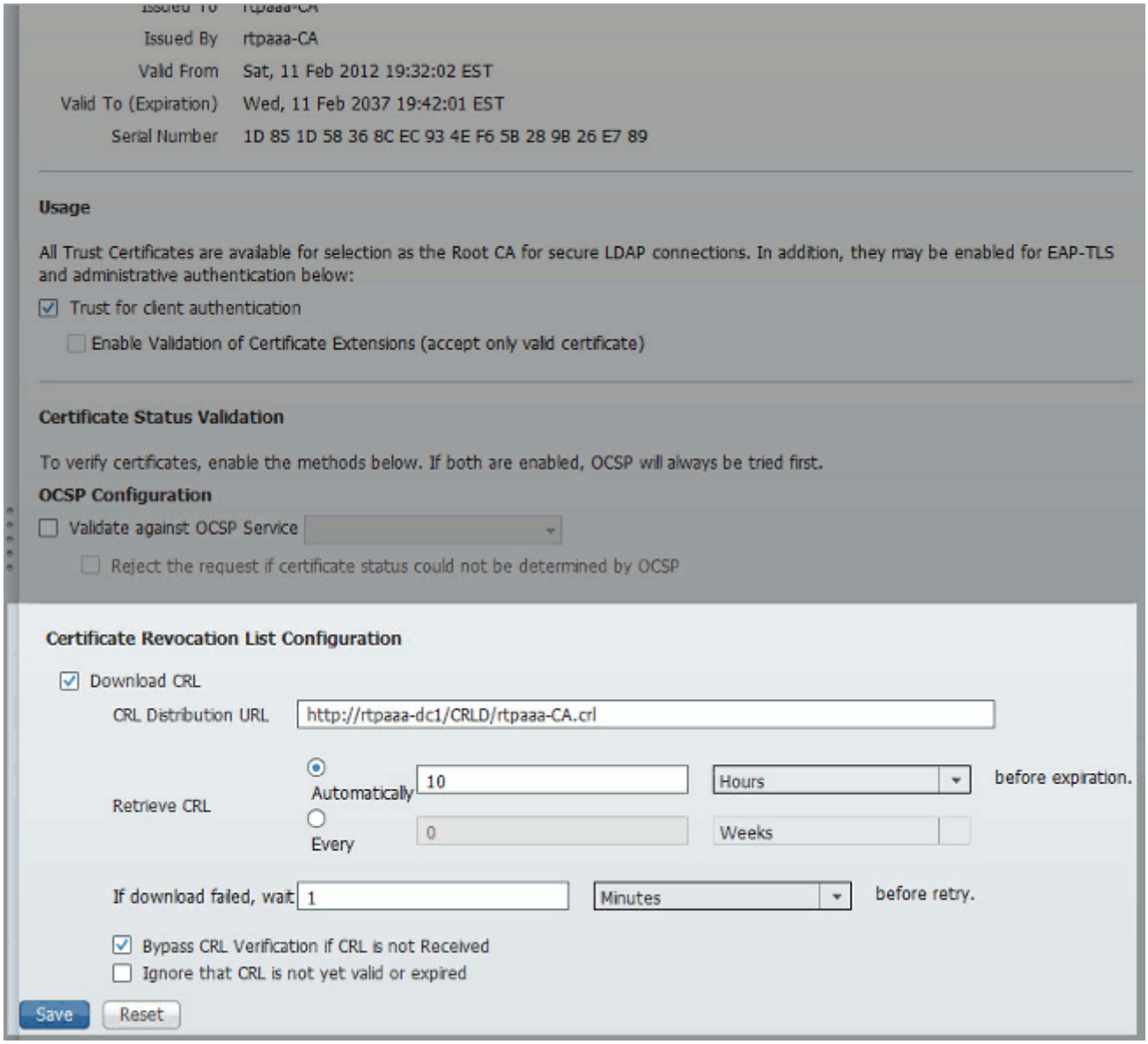
c. 720 minutes is NOT < 15 minutes : OVERLAP = 720 minutes
d. 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes
e. Grace Period = 720 minutes + 10 minutes = 730 minutes

被计算的宽限期是时间在之间，当CA发布下个CRL时，并且，当当前CRL到期时。需要配置ISE相应地检索Crl。

8. 登陆对主要的Admin节点并且选择**管理>System >证书**。在左窗格中，请选择**证书存储**。



9. 在您打算配置Crl的CA证书旁边检查证书存储复选框。点击**编辑**。
10. 在窗口的底部附近，请检查**下载CRL**复选框。
11. 在CRL分配URL字段，请输入路径对控制分配点，包含.crl文件，被创建在第2.部分。在本例中， URL是：
    `http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl`
12. 可以配置ISE定期检索CRL或根据，一般来说，也是一个固定的间隔)的到期(。当CRL发布时间隔是静态，更加及时的CRL更新获得，当使用时后选项。点击**自动地**单选按钮。
13. 比在计算的宽限期设置检索的值为值第7.步。如果值集比宽限期长， ISE检查控制分配点，在CA发布了下个CRL前。在本例中，宽限期被计算是730分钟或者12小时和10分钟。10小时的值将使用检索。
14. 设置重试间隔如适当为您的环境。如果ISE不能检索CRL在上一步的配置的间隔，将再试在此更短的间隔。
15. 请检查**旁路CRL验证，如果CRL不是**允许基于认证的认证的**接收的**复选框通常进行(和没有CRL检查)，如果ISE无法检索此CA的CRL在其前个下载尝试。如果此复选框没有被检查，与此CA发行的证书的所有基于认证的认证将发生故障，如果CRL不可能被检索。
16. 检查**忽略CRL不是有效或过期的**复选框允许ISE使用过期(或没有效) CRL文件，好象他们有效的。如果此复选框没有被检查， ISE认为CRL无效在他们的有效日期之前和在他们的下一次更新时间之后。点击**“Save”**完成配置。



Verify

当前没有可用于此配置的验证过程。

Troubleshoot

目前没有针对此配置的故障排除信息。

Related Information

- Technical Support & Documentation - Cisco Systems