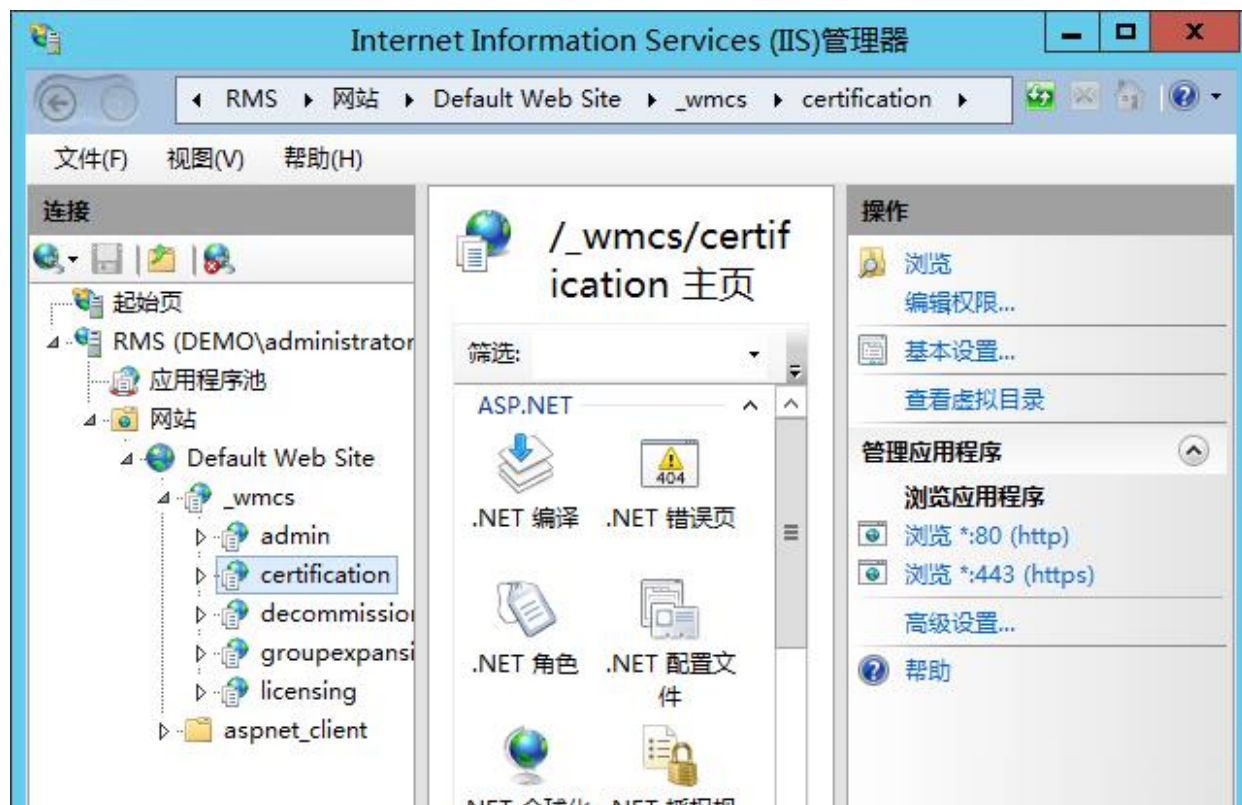


(一) IIS权限设置

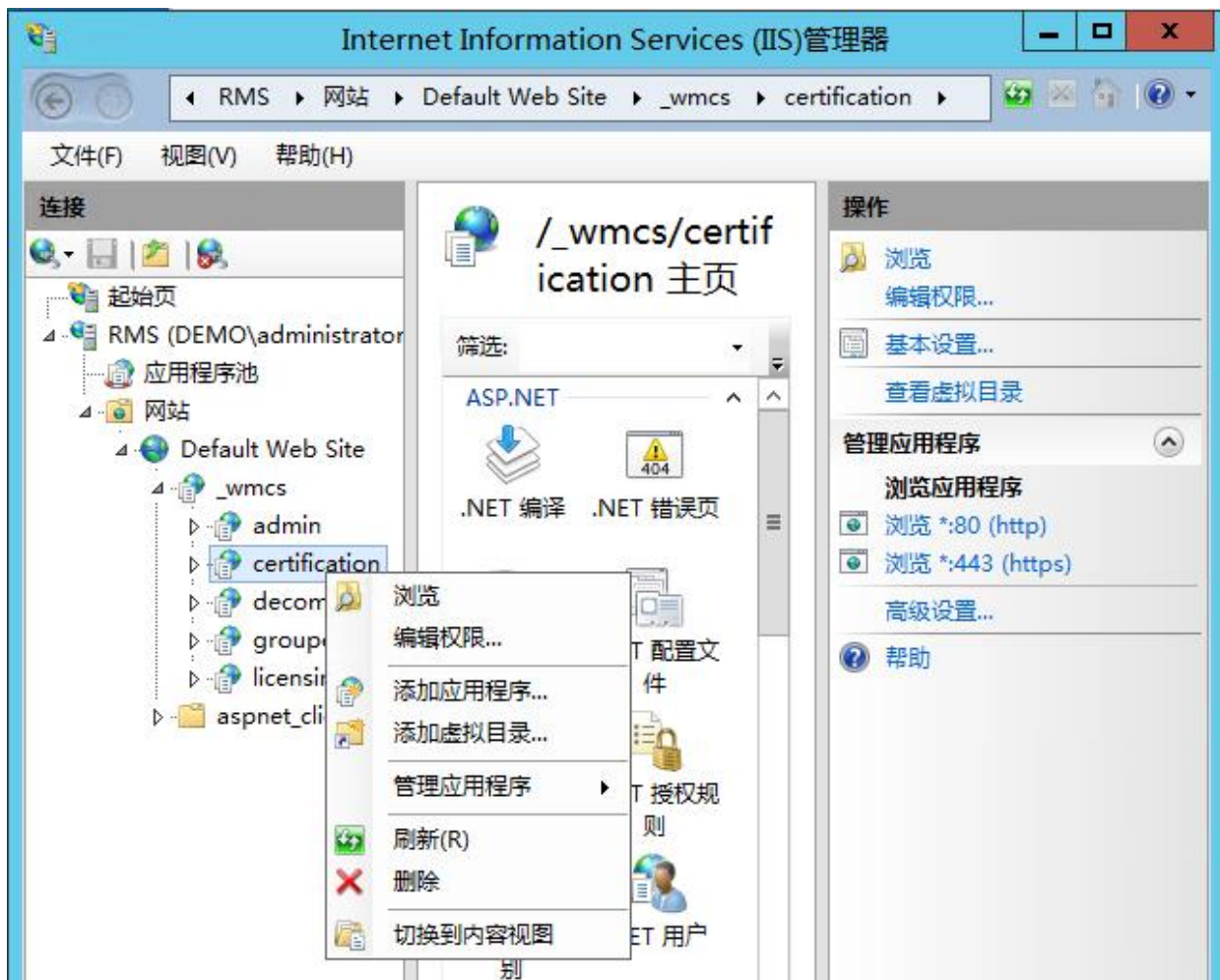
接下来我们需要手动配置RMS组件的相应的IIS权限。RMS依赖IIS服务，因此要配置IIS的相关权限，RMS的一些组件才能正常运行。

RMS服务端应用程序通过IIS的server certification组件申请RMS服务，需要在该对象上设置相应权限。

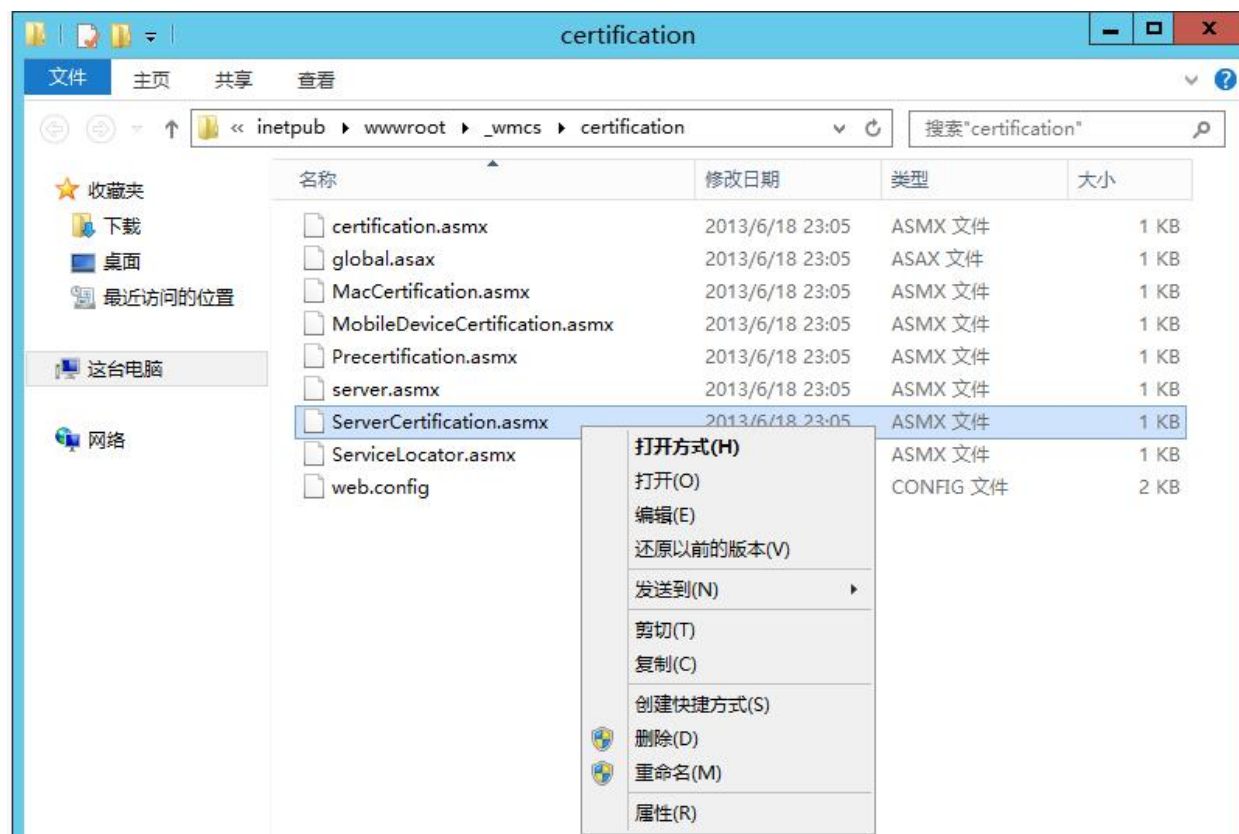
我们打开IIS控制台，定位到如下的位置。



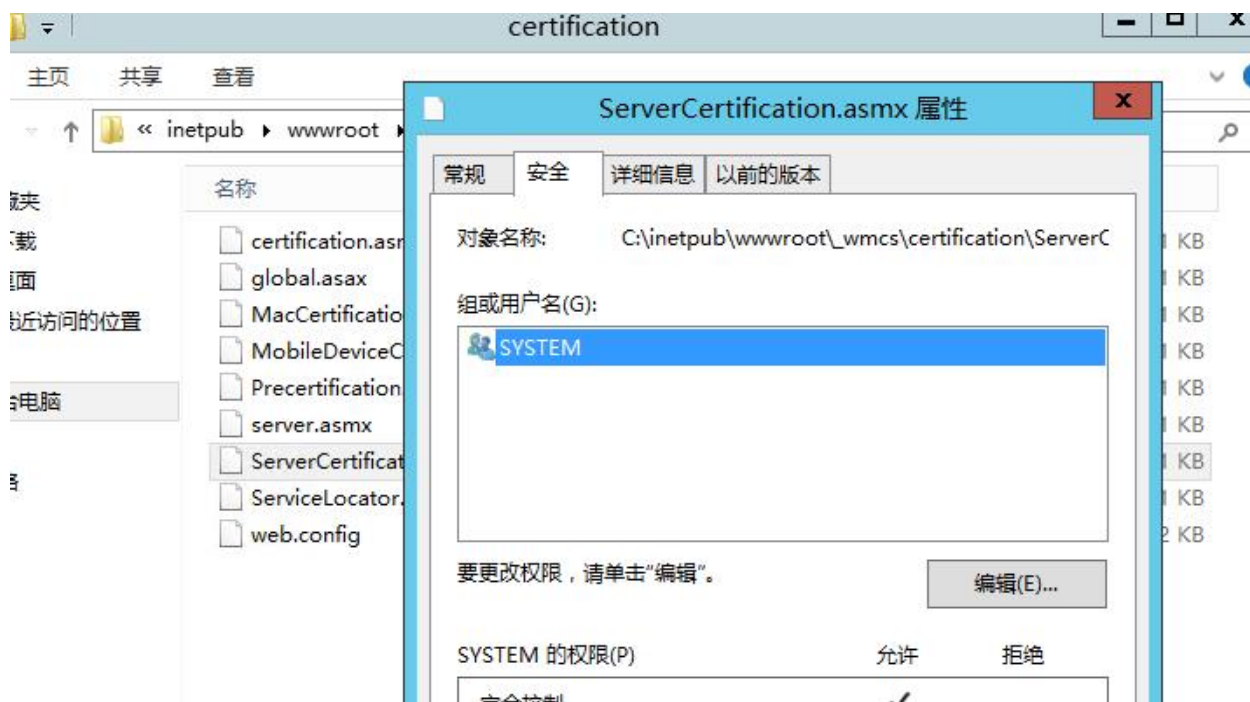
右击certification，选择“浏览”。



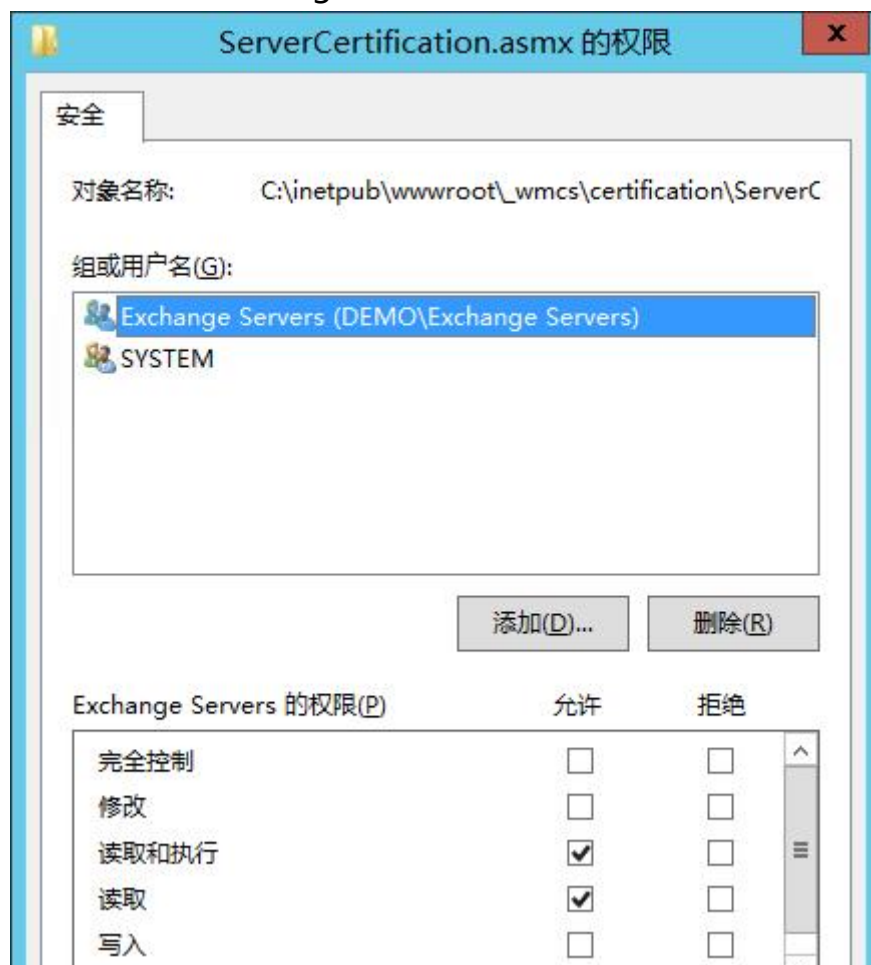
然后选servercertification.asmx文件，右击选择“属性”。



切换到安全选项卡，可以看到默认该文件只有SYSTEM权限。



我们需要新增exchange server组、ADRMS服务组针对该文件的相应权限。
首先添加域组exchange server针对该文件的读取和执行、读取的权限。



然后添加本地的ADRMS服务组针对该文件的读取和执行、读取的权限。



(二) 创建RMS超级管理组

AD RMS允许使用一个独立的exchange邮箱用户或者邮件通讯组成为超级管理员（超级用户）。出于维护的方便，建议使用通讯组作为超级用户。

超级用户组默认是禁用的需要手动启用。

首先登陆exchange 2016的管理中心，创建一个通讯组。

企业版Office 365

Administrator

Exchange 管理中心

收件人

权限

合规性管理

组织

保护

邮件流

移动

公用文件夹

统一消息

服务器

混合

工具

邮箱组资源联系人共享迁移

+ -

显示名称	组类型	电子邮件地址
IT Group	动态通讯组	ITGroup@demo.com
room list	通讯组	roomlist@demo.com
RMSadmins	通讯组	RMSadmins@demo.com

RMSadmins

通讯组

RMSadmins@demo.com

便笺

(无)

所有者

Administrator

成员身份

成员身份审批:

打开

邮件审批:

已禁用

然后打开AD用户和计算机，定位到该通讯组，我们把RMS超级用户添加到该组中，因为我当前是用administrator做的测试，该用户默认就在组里了。

RMSadmins 属性

常规

成员

隶属于

管理者

成员(M):

名称	Active Directory 域服务
Administrator	demo.com/Users
Exchange Servers	demo.com/Microsoft E:
FederatedEmail.4c1f4d8b-8179-4148-93...	demo.com/Users
rmssrv	demo.com/IT/IT2

(三) 在RMS服务器上启用超级用户 (组)
打开AD RMS控制台，定位到超级用户节点。

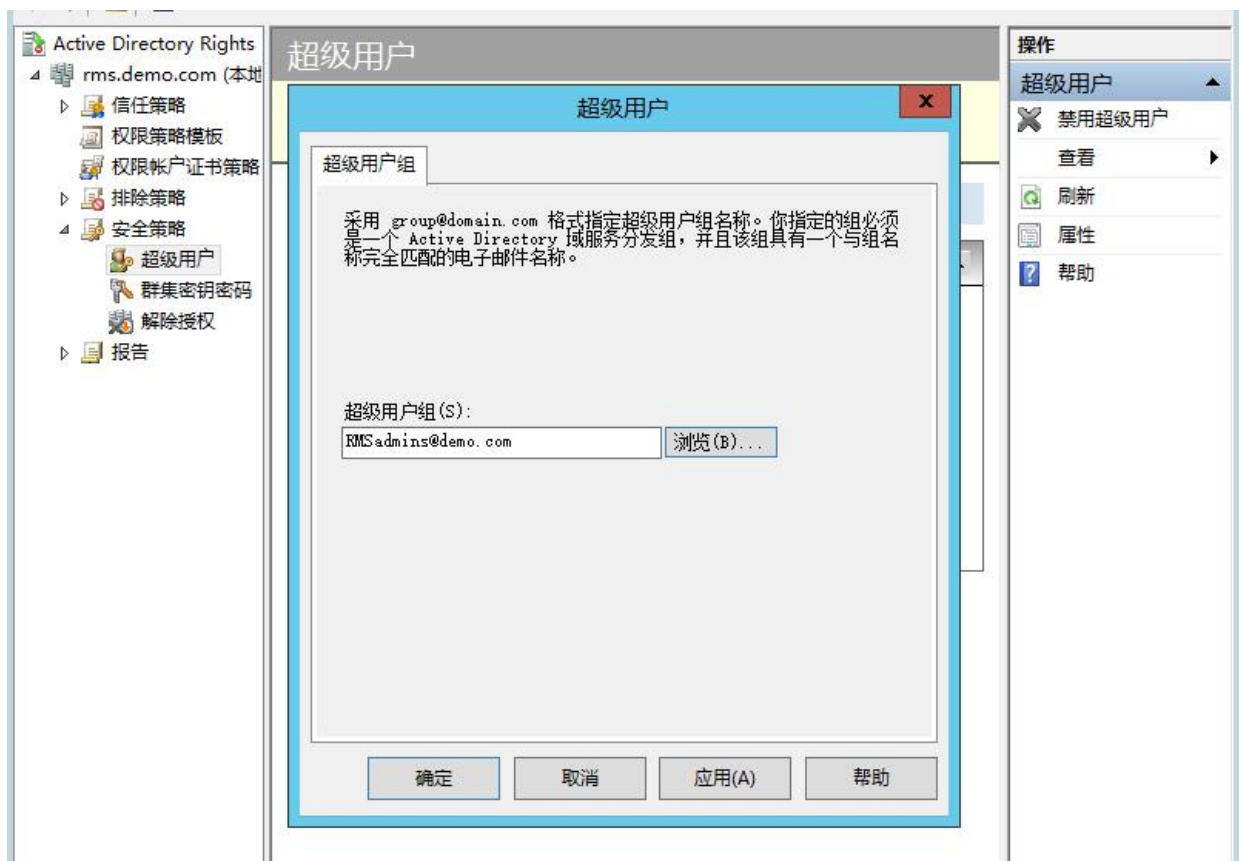


选择上图右上角位置的“启用超级用户”，启用之后如图。



然后我们点击“更改超级用户组”。

浏览选择我们前面新建的RMSadmins通讯组。



RMS超级用户或组，可以无限制地访问被保护的数据，该组的成员可以进行解密工作。启用完成后，如图。

