Active Directory 权限管理服务 (AD RMS) 是一种信息保护技术，它与支持 AD RMS 的应用程序协同工作，以防止在未经授权的情况下使用数字信息（无论是联机和脱机，还是在防火墙内外）。AD RMS 适用于需要保护敏感信息和专有信息（例如财务报表、产品说明、客户数据和机密电子邮件消息）的组织。AD RMS 通过永久使用策略（也称为使用权限和条件）提供对信息的保护，从而增强组织的安全策略，无论信息移到何处，永久使用策略都保持与信息在一起。AD RMS 永久保护任何二进制格式的数据，因此使用权限保持与信息在一起，而不是权限仅驻留在组织网络中。这样也使得使用权限在信息被授权的接收方访问（无论是联机和脱机，还是在防火墙内外）后得以强制执行。AD RMS 可以建立以下必要元素，通过永久使用策略来帮助保护信息：

- **受信任的实体。**组织可以指定实体，包括作为 AD RMS 系统中受信任参与者的 个人、用户组、计算机和应用程序。通过建立受信任的实体，AD RMS 可以通过将访问权限仅授予适当的受信任参与者来帮助保护信息。

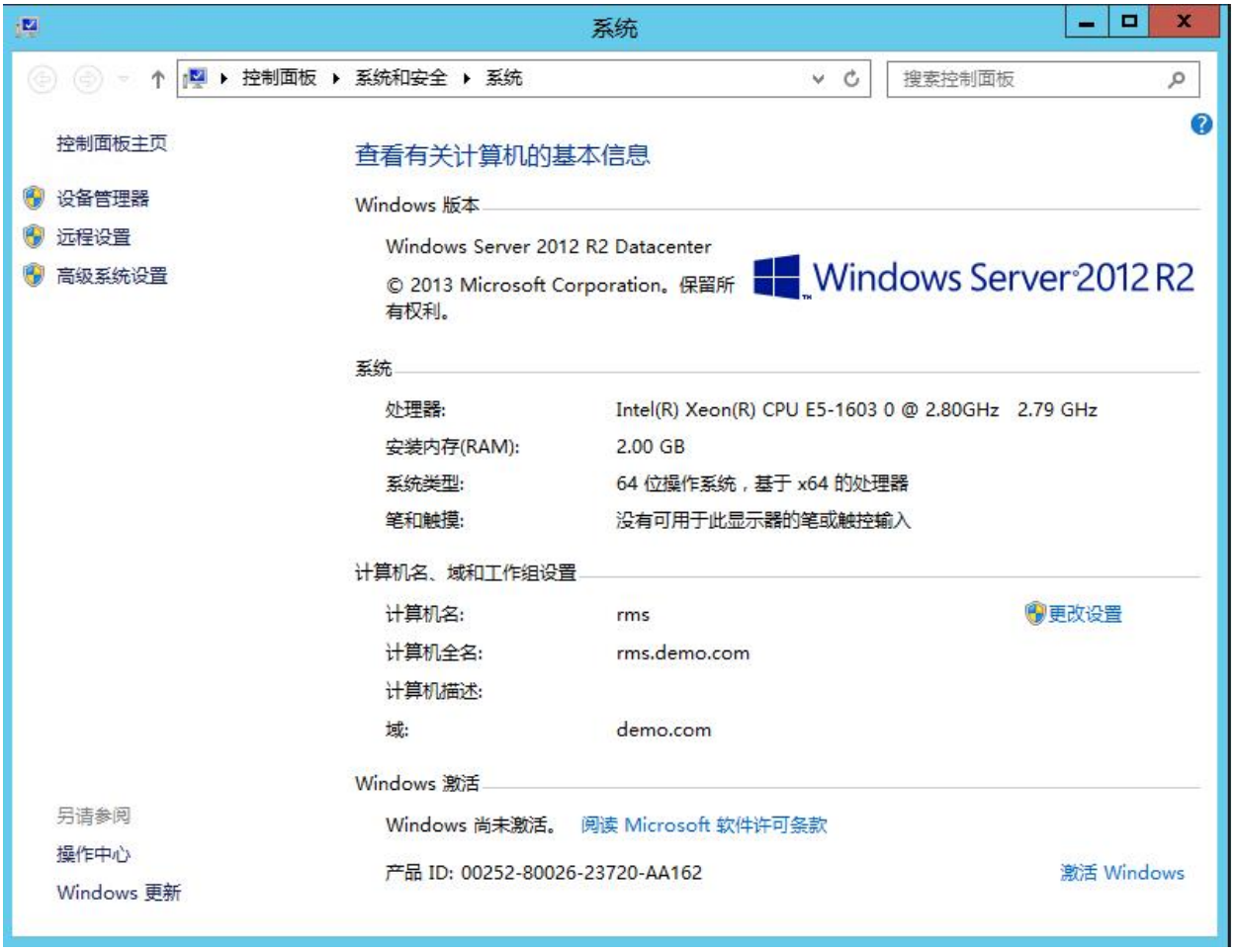
- **使用权限和条件。**组织和个人可以指定定义了特定受信任实体如何可以使用受权限保护的内容的使用权限和条件。读取、复制、打印、保存、转发和编辑的权限都是使用权限。使用权限可以附加条件，例如这些权限何时过期。组织可以阻止应用程序和实体访问受权限保护的内容。

- **加密。**加密是通过使用电子密钥锁定数据的过程。AD RMS 可加密信息，使访问建立在成功验证受信任实体的条件之上。一旦信息被锁定，只有在指定条件（如果有）下授予了使用权限的受信任实体可以在支持 AD RMS 的应用程序或浏览器中对信息解除锁定或解密。随后应用程序将强制执行已定义的使用权限和条件。

具体可以参考：
https://technet.microsoft.com/zh-cn/library/cc772403.aspx
本次系列文章来讨论如何结合ADRMS保护exchange 2016邮件通讯。

（一）准备操作系统

本次我们部署RMS使用的系统是Windows server 2012 R2操作系统。加入到了demo.com测试域中。



（二）证书服务器准备

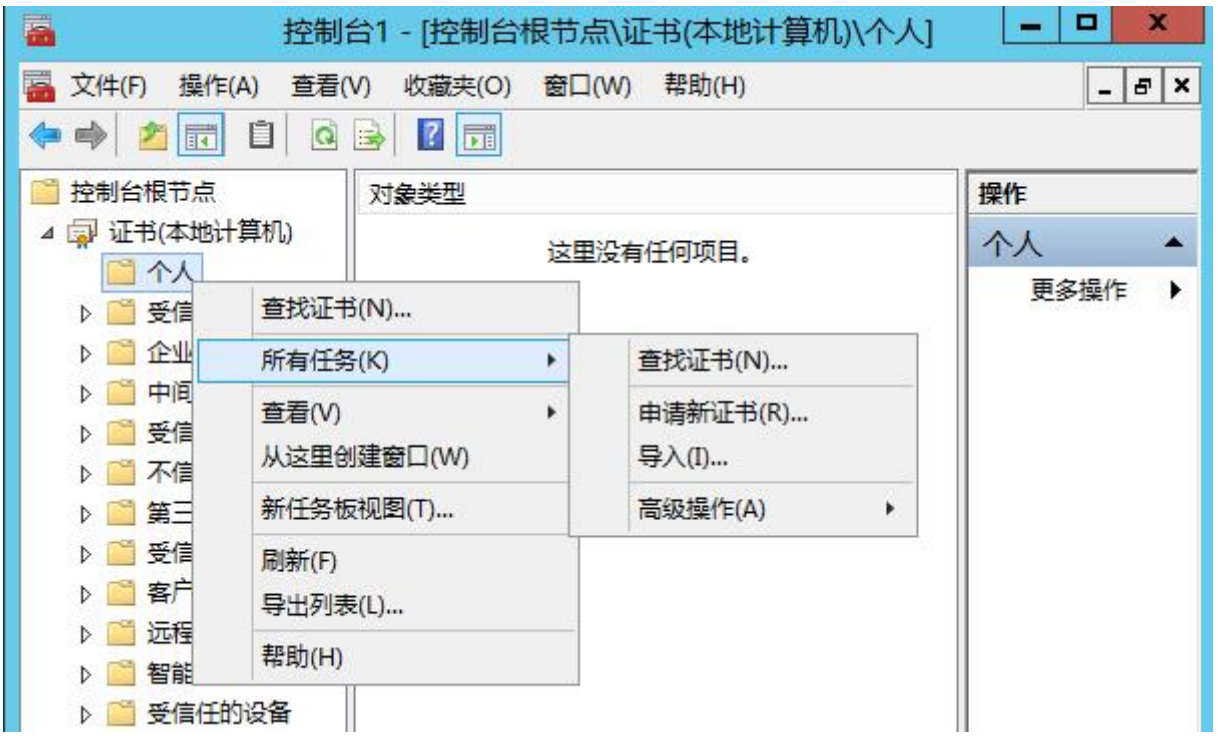
这里我使用内网的私有CA，该CA在测试环境中并置在DC服务器上，生产环境建议CA和DC分开部署。

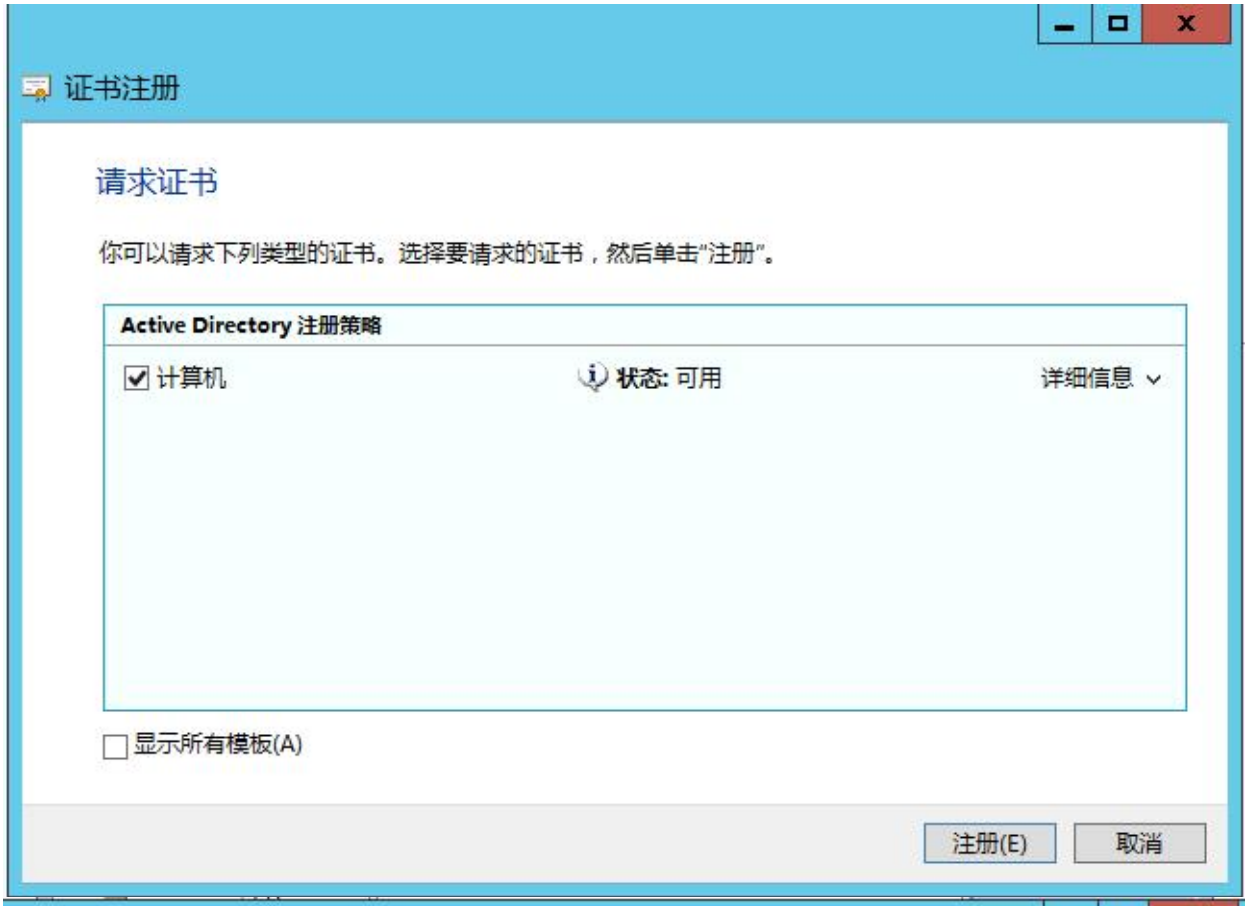
为RMS服务器申请一张专用的计算机证书。

登录到RMS服务器，使用MMC加载证书控制台进行申请。


控制台1 - [控制台根节点]
文件(F) 操作(A) 查看(V) 收藏夹(O) 窗口(W) 帮助(H)
控制台根节点
证书(本地计算机)
名称
证书(本地计算机)
操作
控制台根...
更多操作

选择申请证书。


控制台1 - [控制台根节点\证书(本地计算机)\个人]
文件(F) 操作(A) 查看(V) 收藏夹(O) 窗口(W) 帮助(H)
控制台根节点
证书(本地计算机)
个人
对象类型
这里没有任何项目。
操作
个人
更多操作
查找证书(N)...
所有任务(K)
查看(V)
从这里创建窗口(W)
新任务板视图(T)...
刷新(F)
导出列表(L)...
帮助(H)
查找证书(N)...
申请新证书(R)...
导入(I)...
高级操作(A)
受信任的设备


证书注册
请求证书
你可以请求下列类型的证书。选择要请求的证书，然后单击"注册"。
Active Directory 注册策略
计算机
状态: 可用
详细信息
显示所有模板(A)
注册(E)
取消


证书注册
证书安装结果
下列证书已注册并已安装在这台计算机上。
Active Directory 注册策略
计算机
状态: 成功
详细信息
完成(F)

完成后，如图。

（三）RMS服务账户准备

生产环境建议为RMS创建单独的服务账户。如果RMS和DC是分开部署的，只需要将服务账户加入到RMS服务器的本地管理员组中，权限是domain user即可。

同时设置密码永不过期，账户永不过期。

加入到RMS服务器的本地管理员组。


Administrators 属性
常规
Administrators
描述(E):
管理员对计算机/域有不受限制的完全访问权
成员(M):
Administrator
DEMO\Domain Admins
DEMO\rmssrv (rmssrv@demo.com)