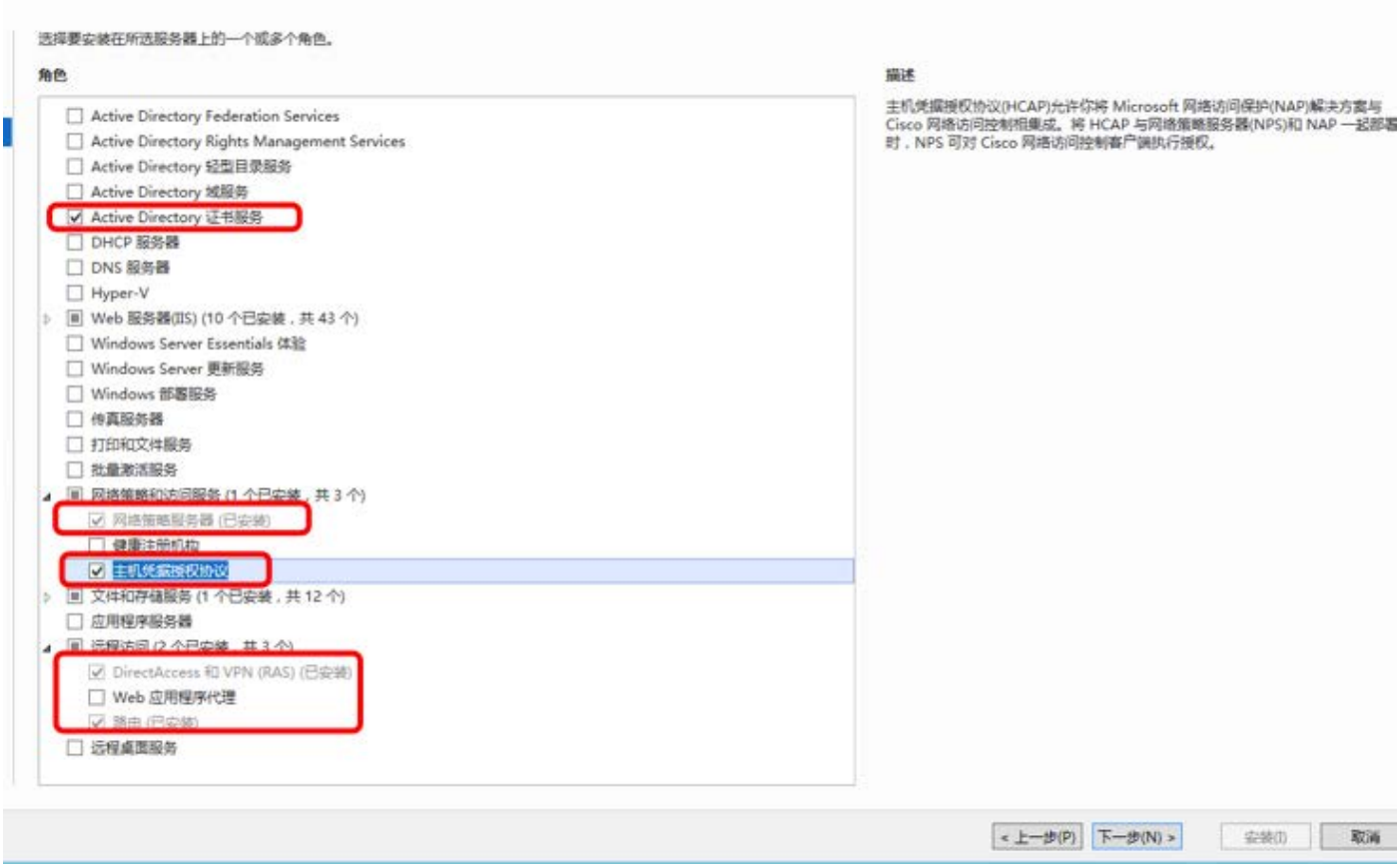
https://blog.csdn.net/b1250372262/article/details/79084932

原
分享一下 window2012r2 搭建 sstpvpn 的过程
2018 年 01 月 17 日 15:33:45
阅读数：2149

首先点击服务器管理　然后添加角色和功能

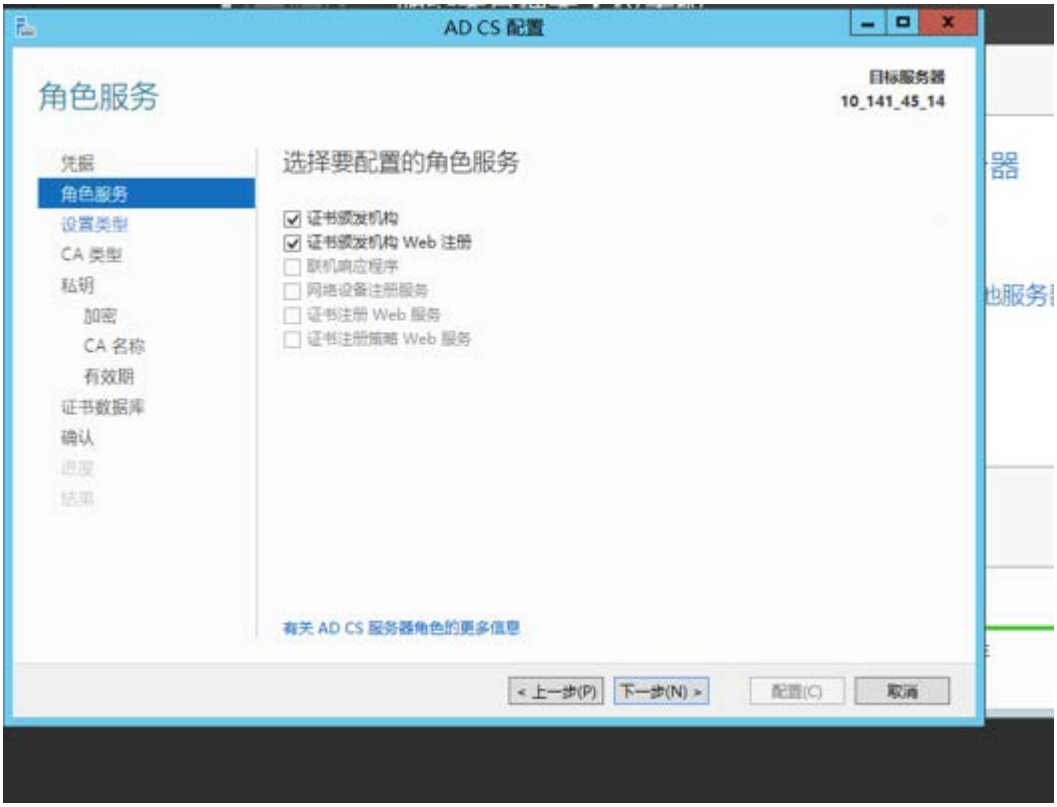


选择红框内的功能添加　注意 健康注册机构先不添加，后面再添加，然后点击下一步

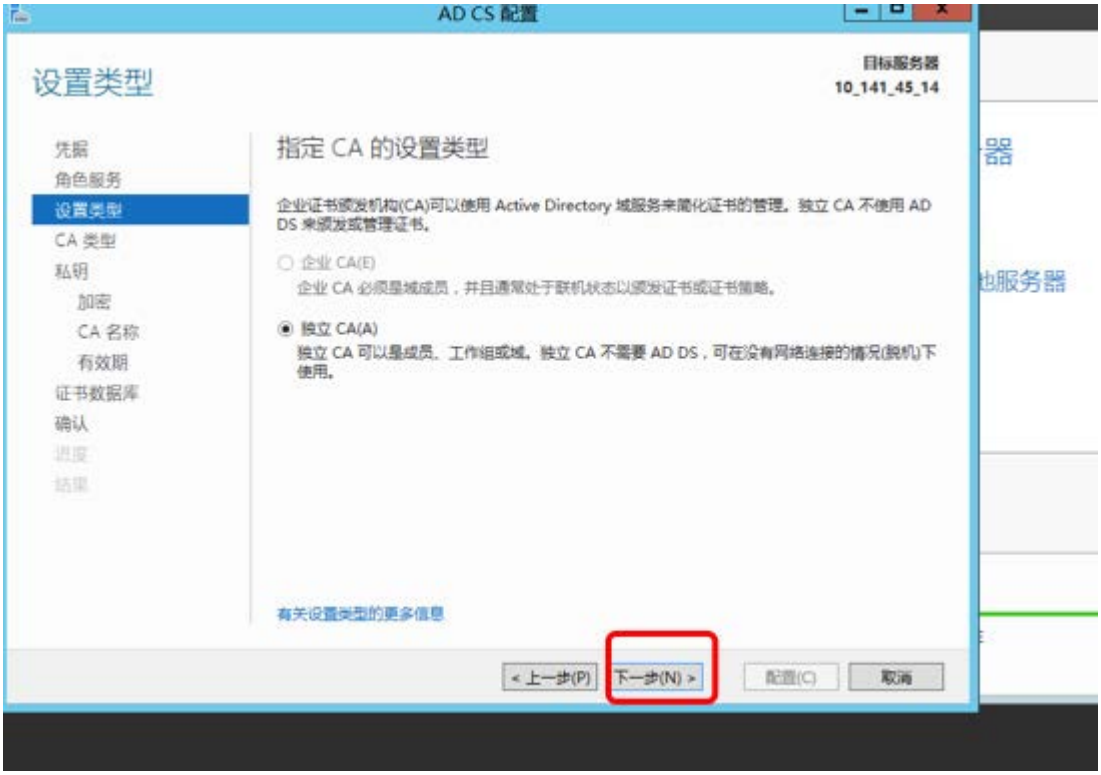
这个页面选择这两个选项即可，然后一直按照操作下一步执行就可以

安装完成之后 点击黄色叹号 然后配置证书服务

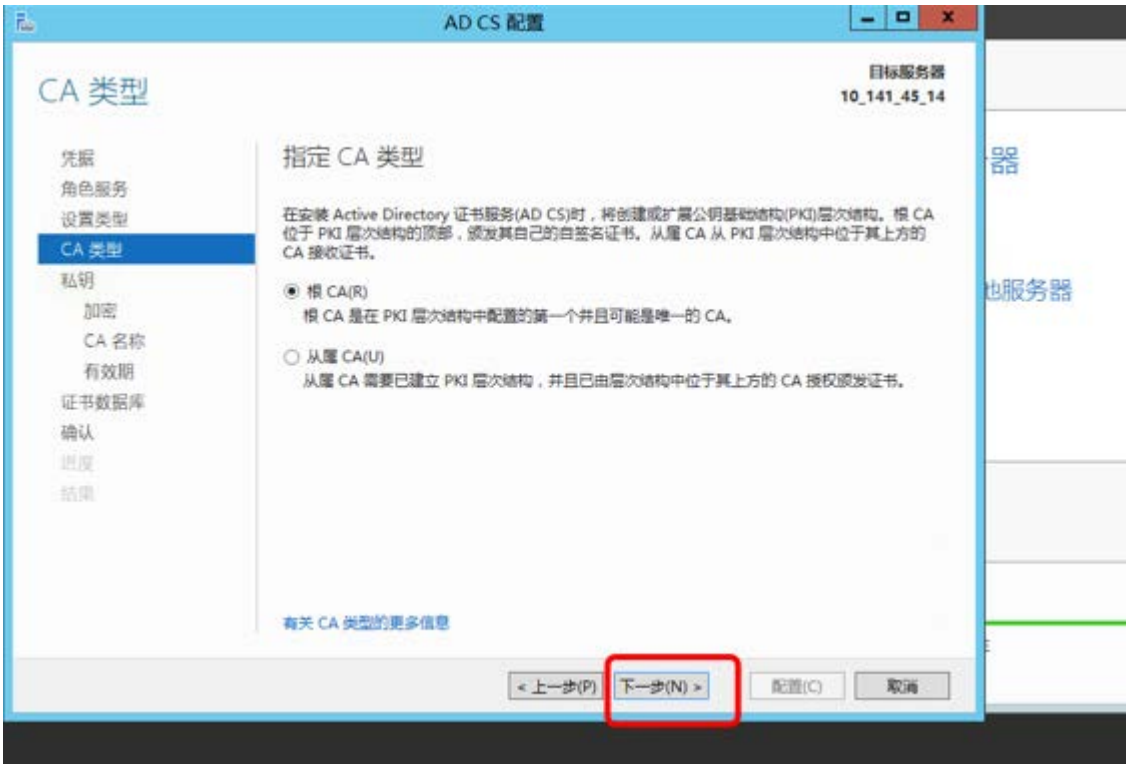
直接下一步就行



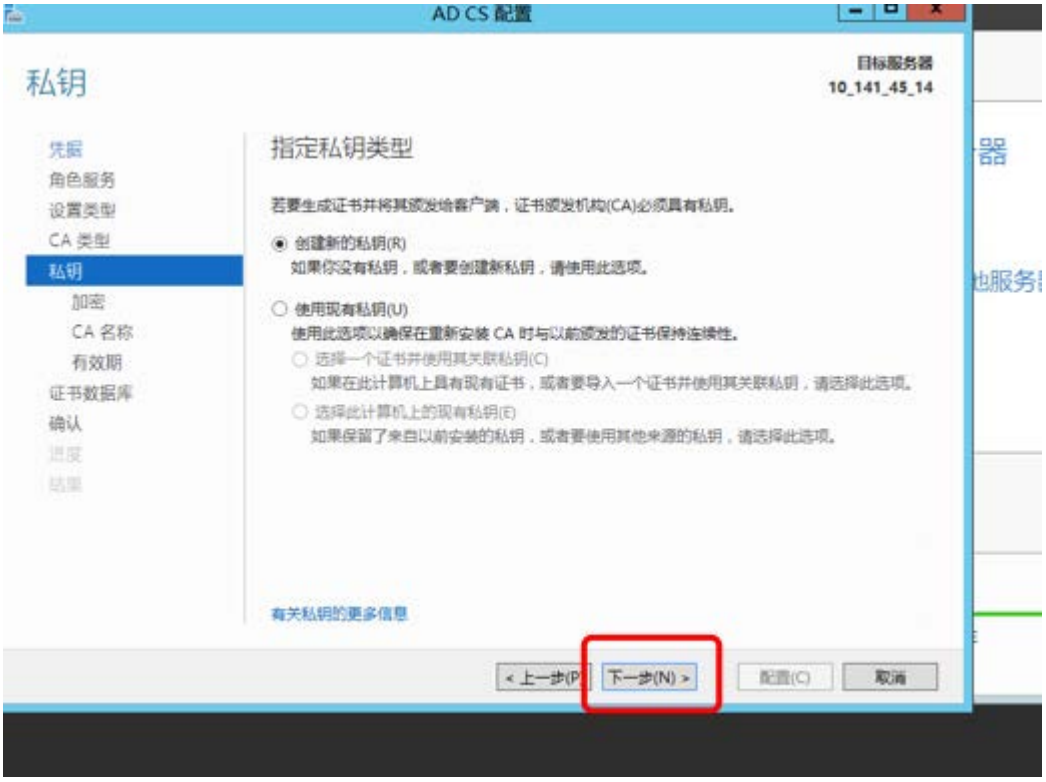
勾选这两个属性 然后继续下一步



ca 类型选择独立 不知道怎滴　企业的选择不上　点击下一步

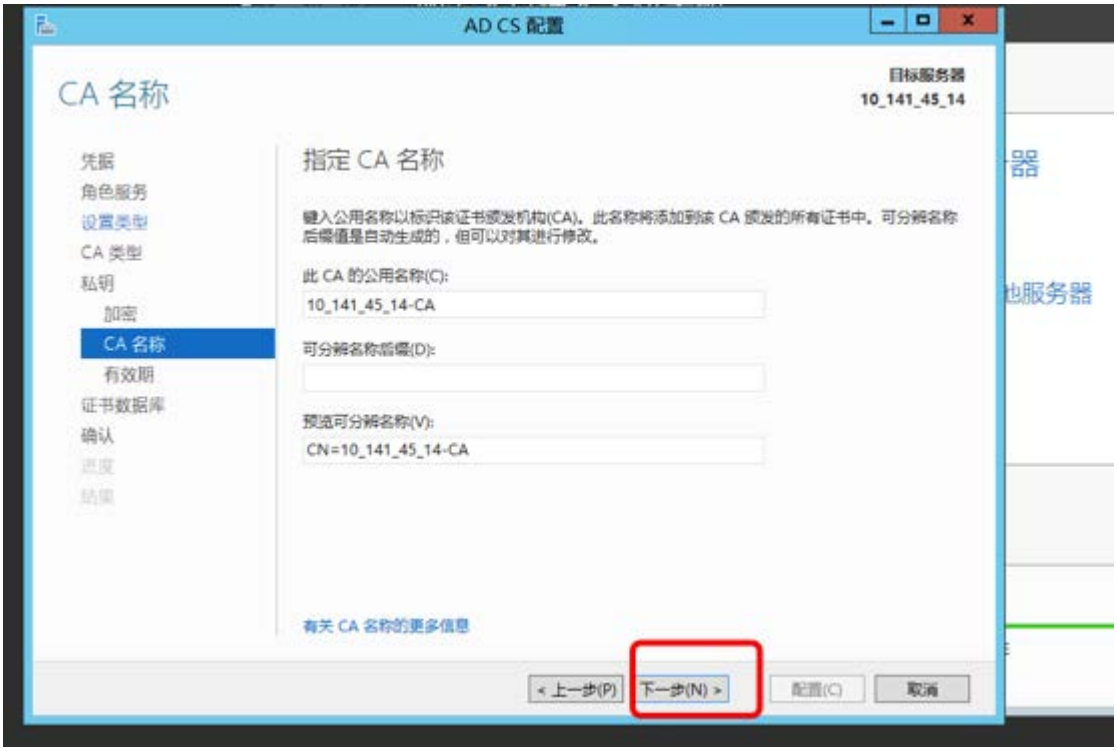


选择根　直接下一步

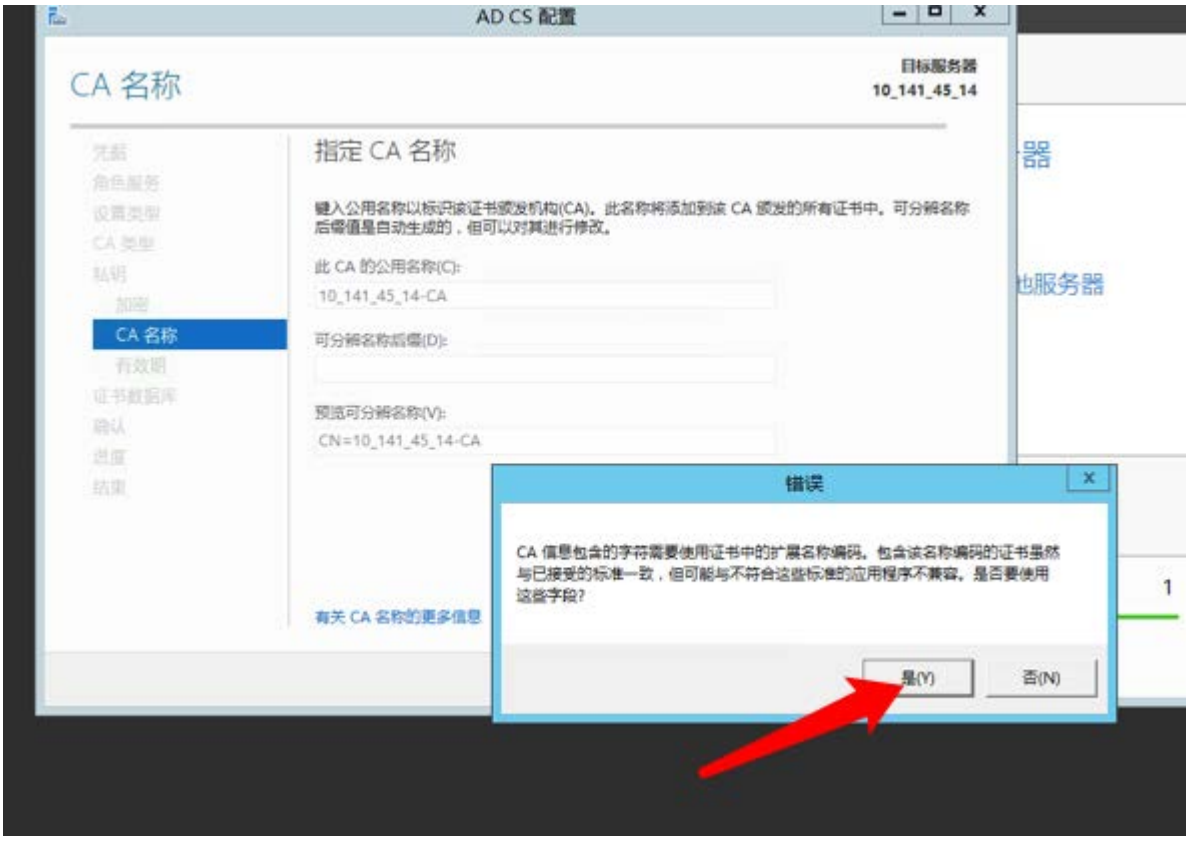


要创建新的私钥

按照图上的选项去选择 然后下一步

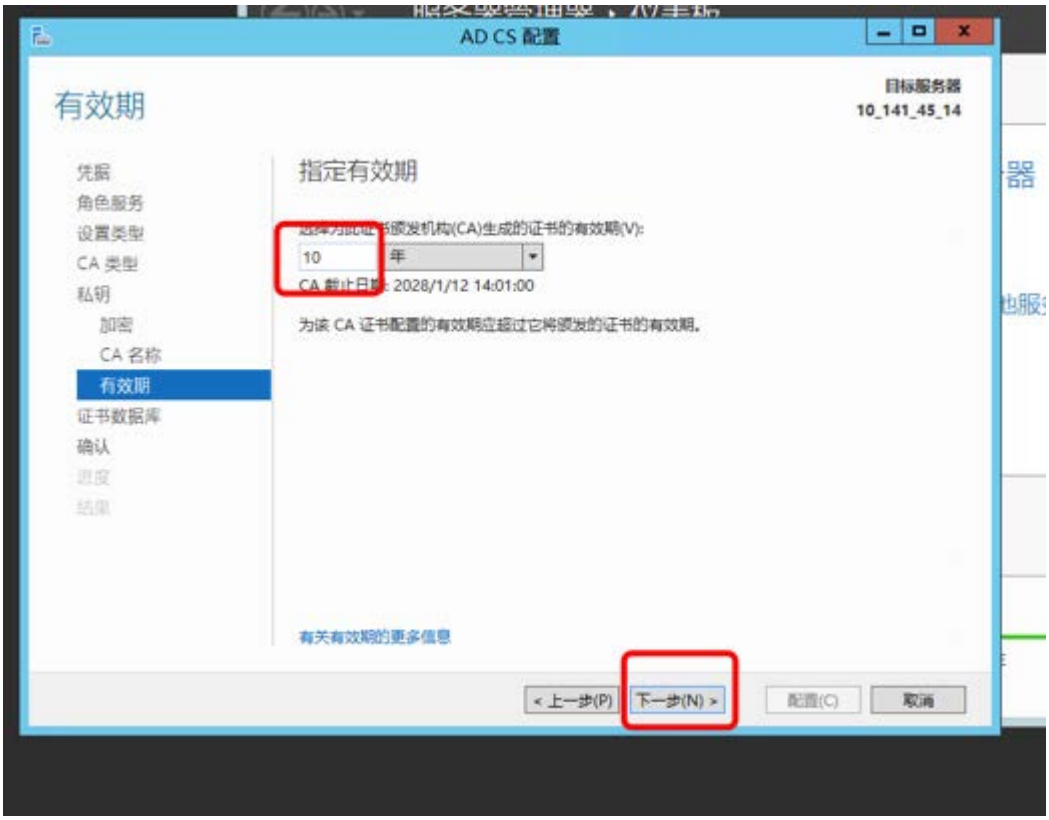


直接下一步就可以

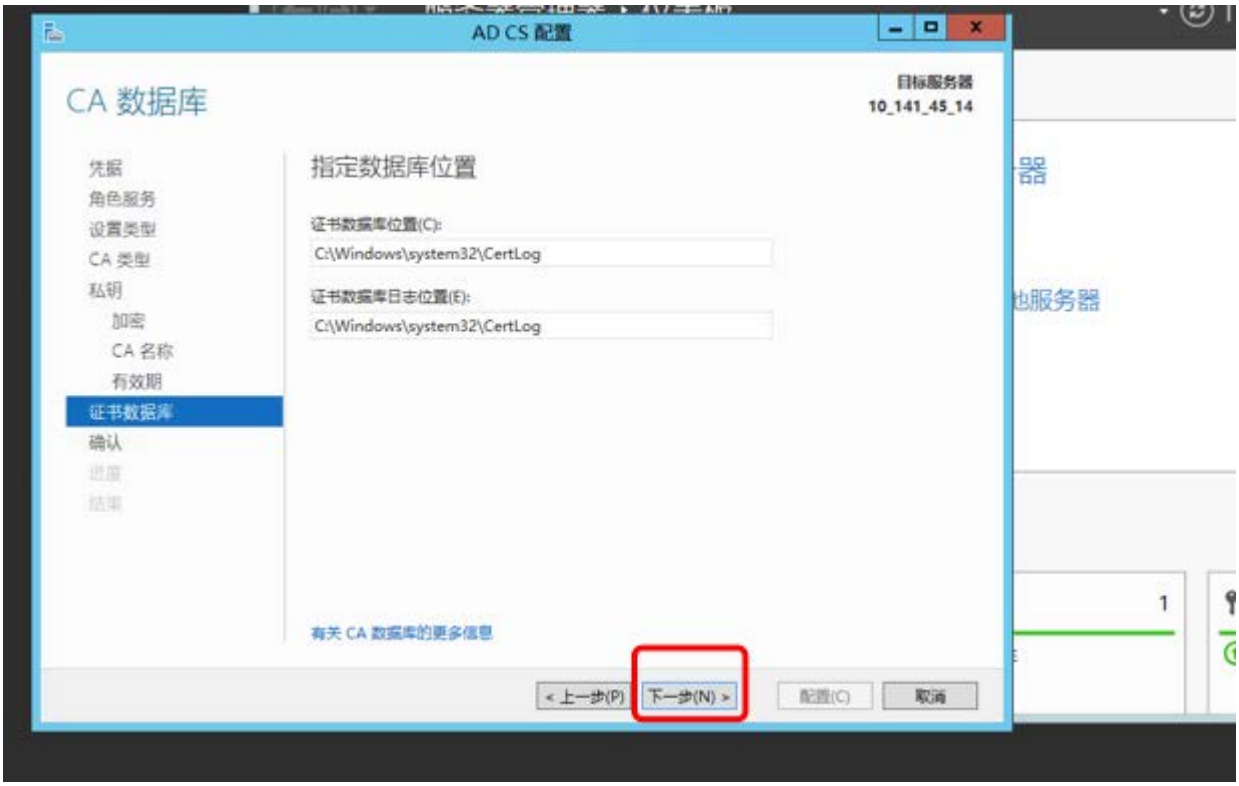


选择是 不用管它的提示

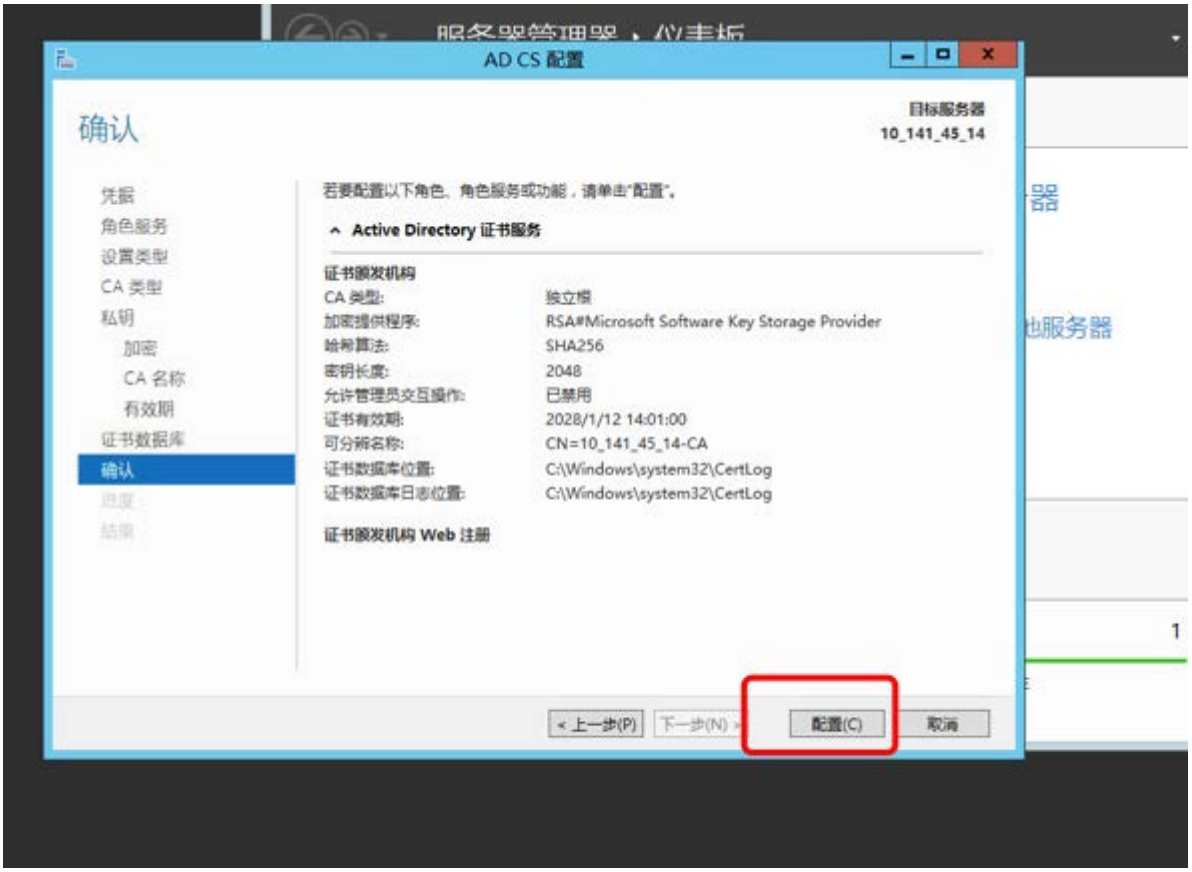
（此处不对，CA 名称就应该是服务器的 IP 地址，并且将后面的-CA 去除。否则之后连接 VPN 时会出现 证书的 CN 名与传递的值不匹配的错误）



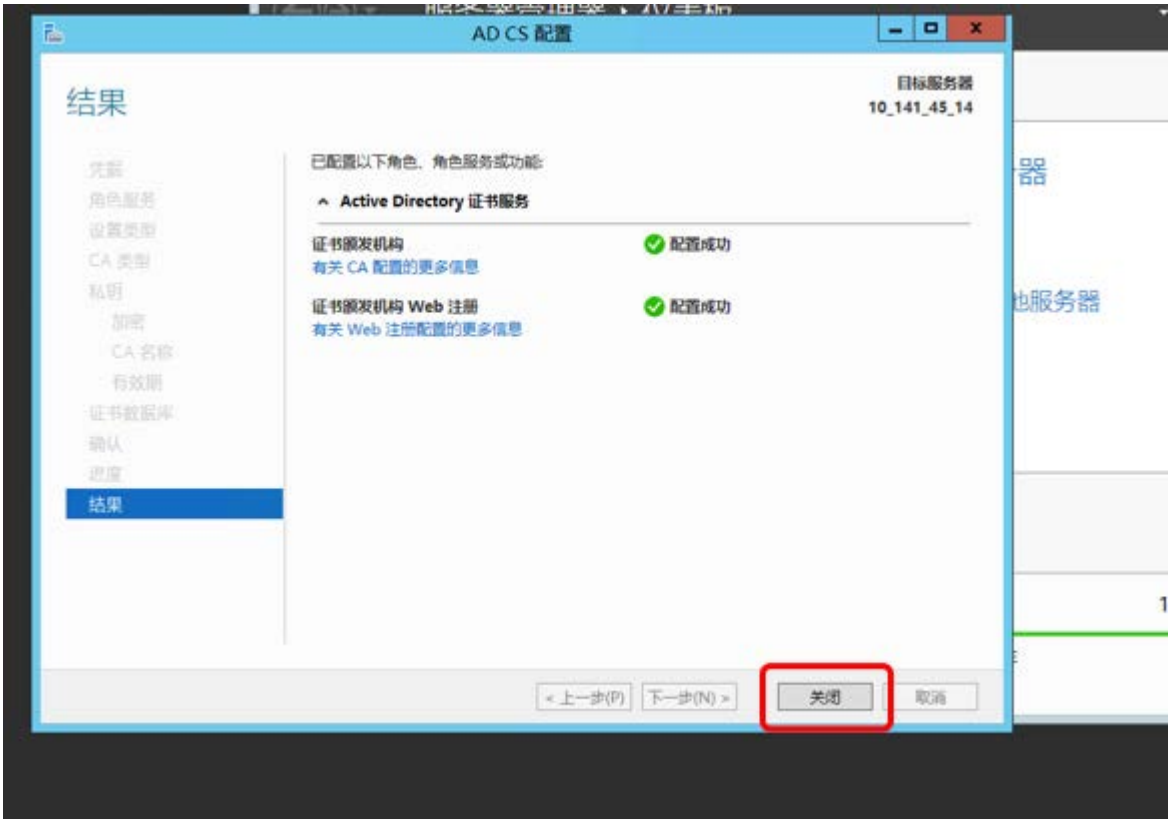
选择 10 年　下一步（有效期未必需要十年）



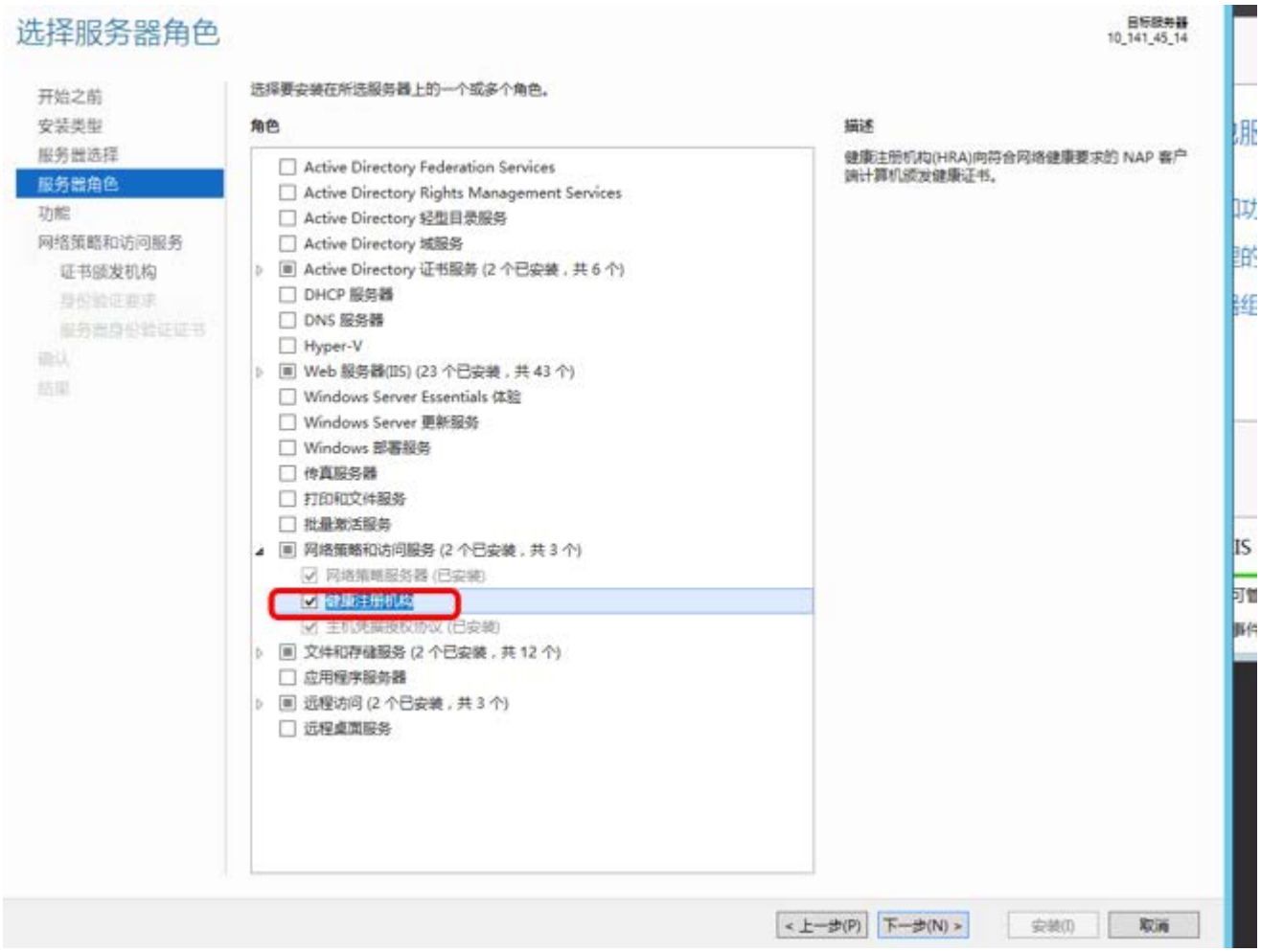
直接下一步就可以



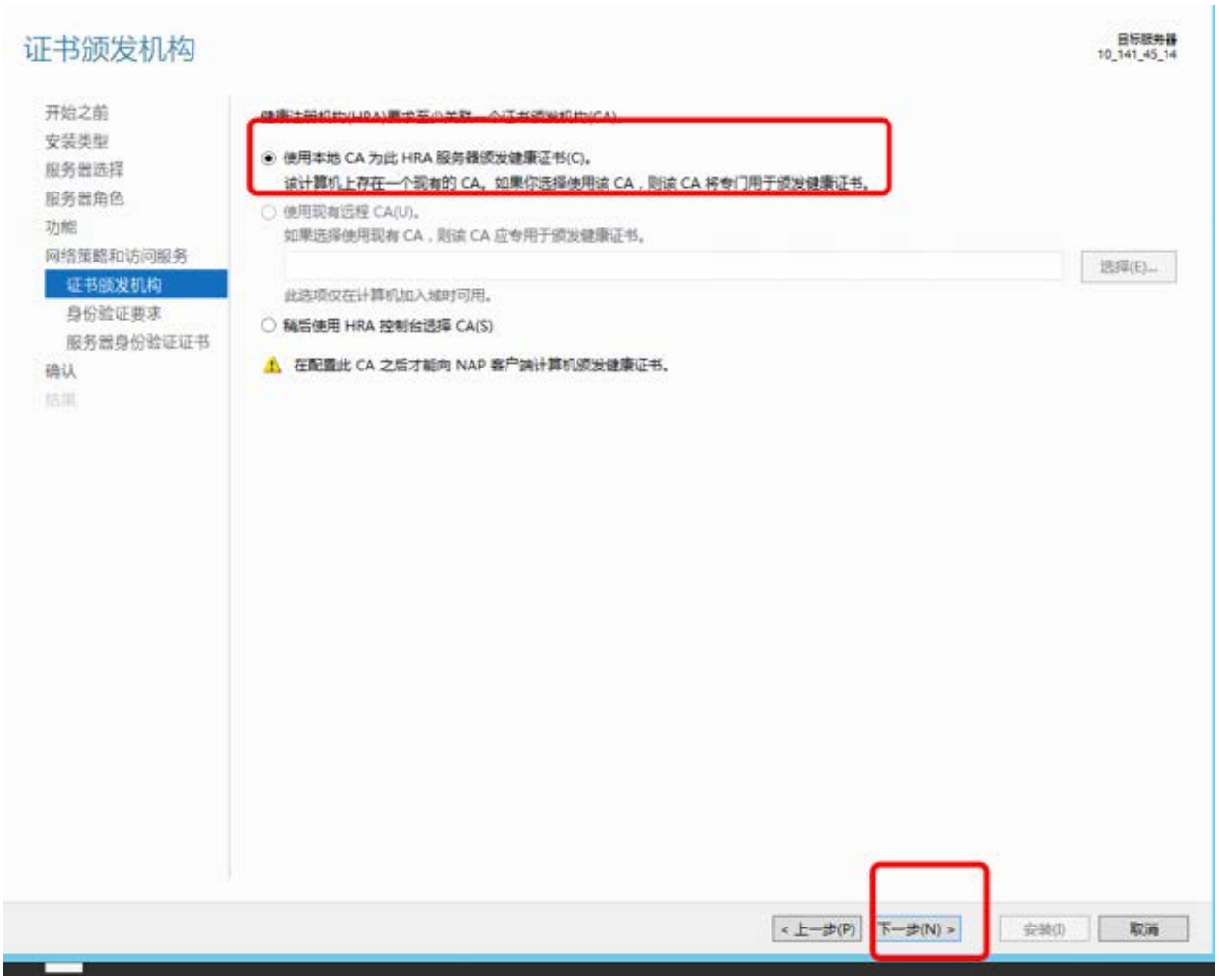
点击配置



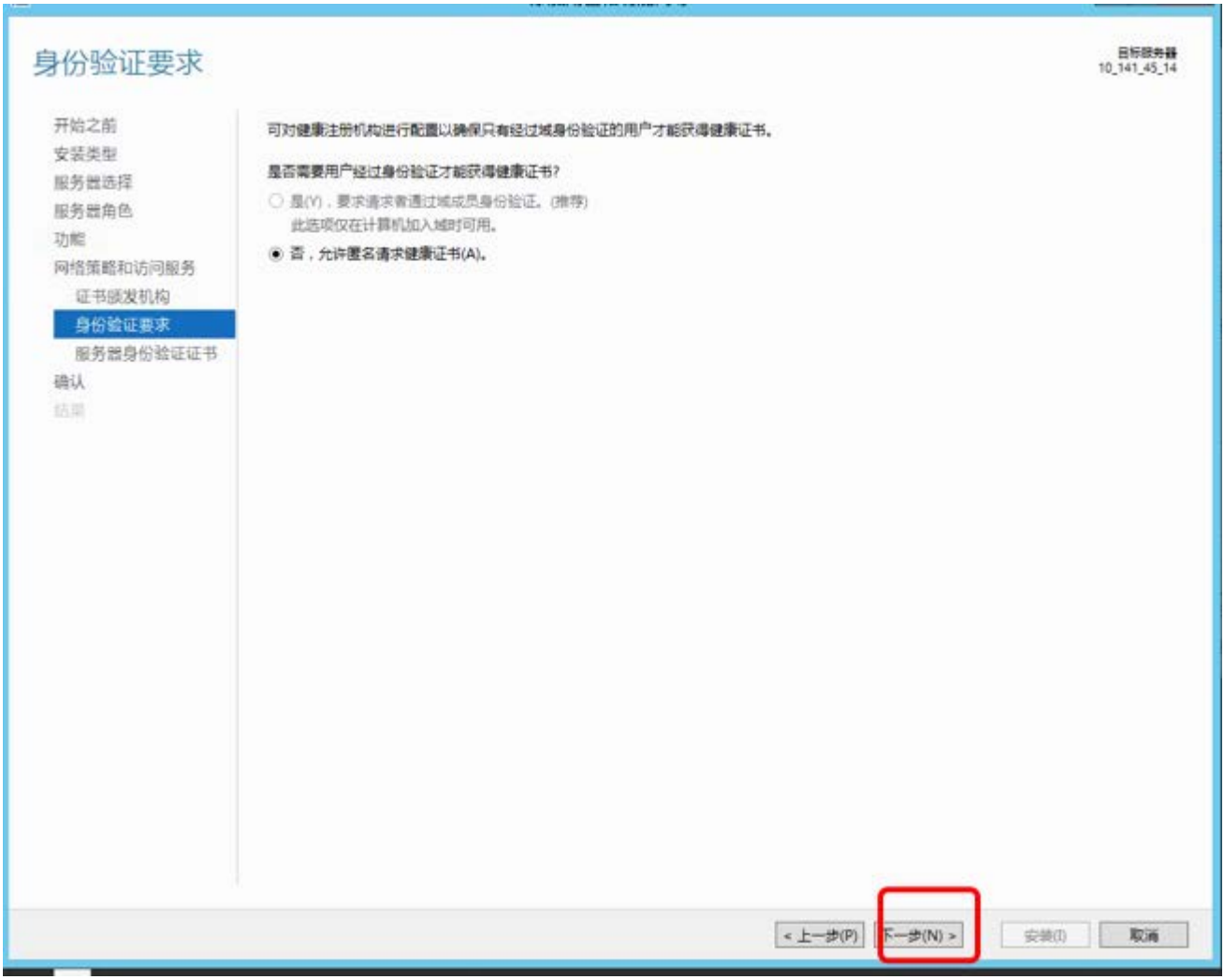
证书就安装成功了



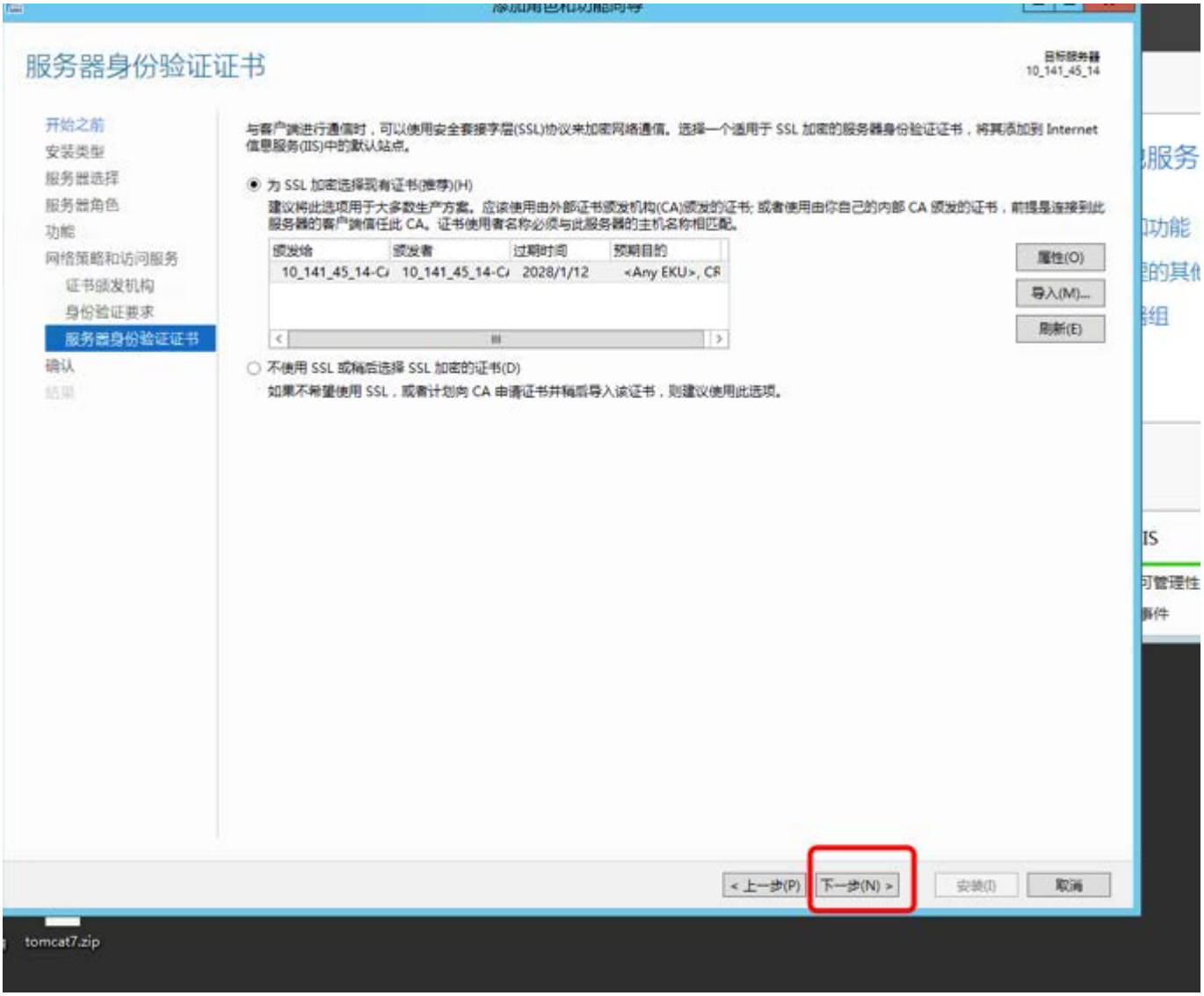
然后继续在服务器管理 添加角色　把没有安装的健康计划 添加一下



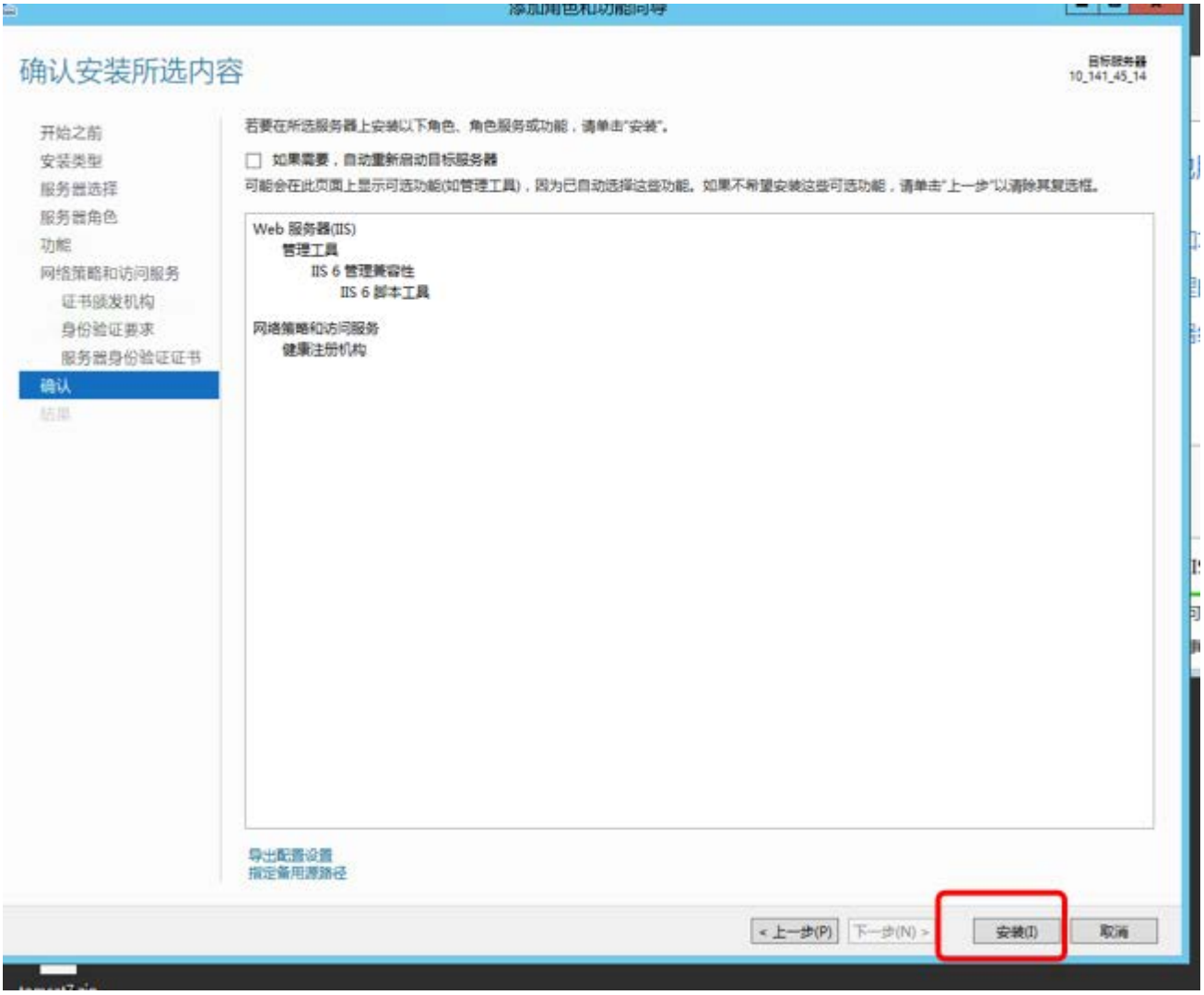
使用本地的证书



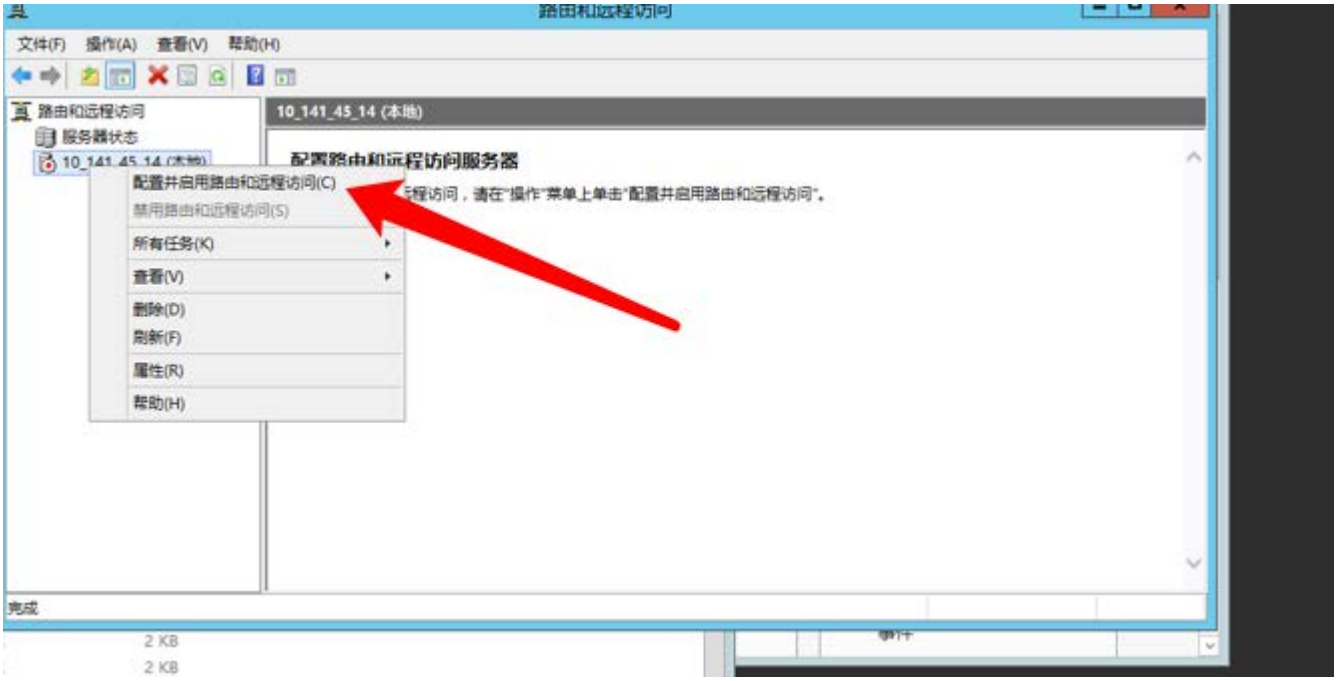
按图上的选择 点击下一步


服务器身份验证证书
目标服务器
10_141_45_14
开始之前
安装类型
服务器选择
服务器角色
功能
网络策略和访问服务
证书颁发机构
身份验证要求
服务器身份验证证书
确认
结果
与客户端进行通信时，可以使用安全套接字层(SSL)协议来加密网络通信。选择一个适用于 SSL 加密的服务器身份验证证书，将其添加到 Internet 信息服务(IIS)中的默认站点。
为 SSL 加密选择现有证书(推荐)(H)
建议将此选项用于大多数生产方案。应该使用由外部证书颁发机构(CA)颁发的证书；或者使用由你自己的内部 CA 颁发的证书，前提是连接到此服务器的客户端信任此 CA。证书使用者名称必须与此服务器的主机名称相匹配。
颁发给
颁发者
过期时间
预期目的
10_141_45_14-C
10_141_45_14-C
2028/1/12
<Any EKU>, CR
属性(O)
导入(M)...
刷新(E)
不使用 SSL 或稍后选择 SSL 加密的证书(D)
如果不希望使用 SSL，或者计划向 CA 申请证书并稍后导入该证书，则建议使用此选项。
< 上一步(P)
下一步(N) >
安装(I)
取消
tomcat7.zip

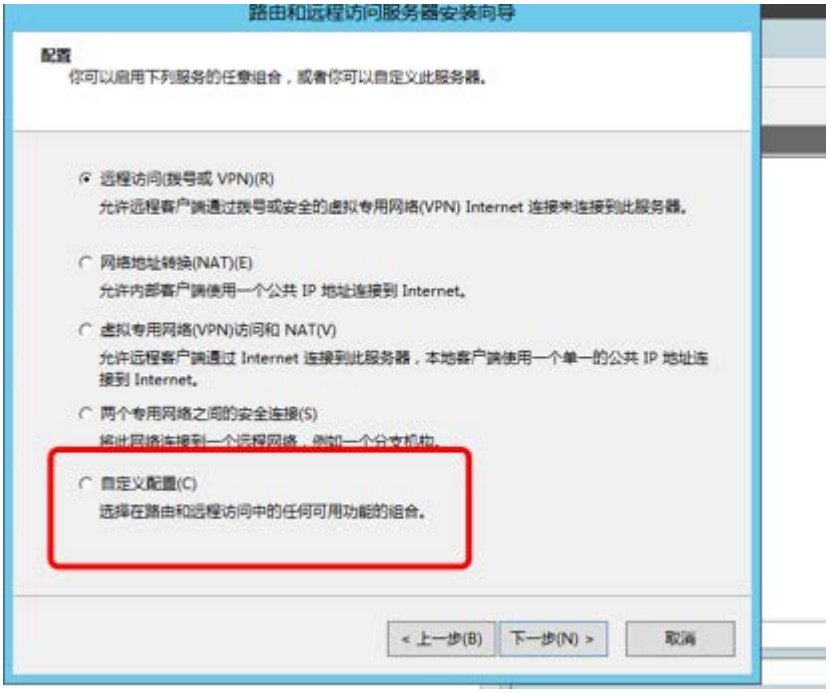
直接下一步



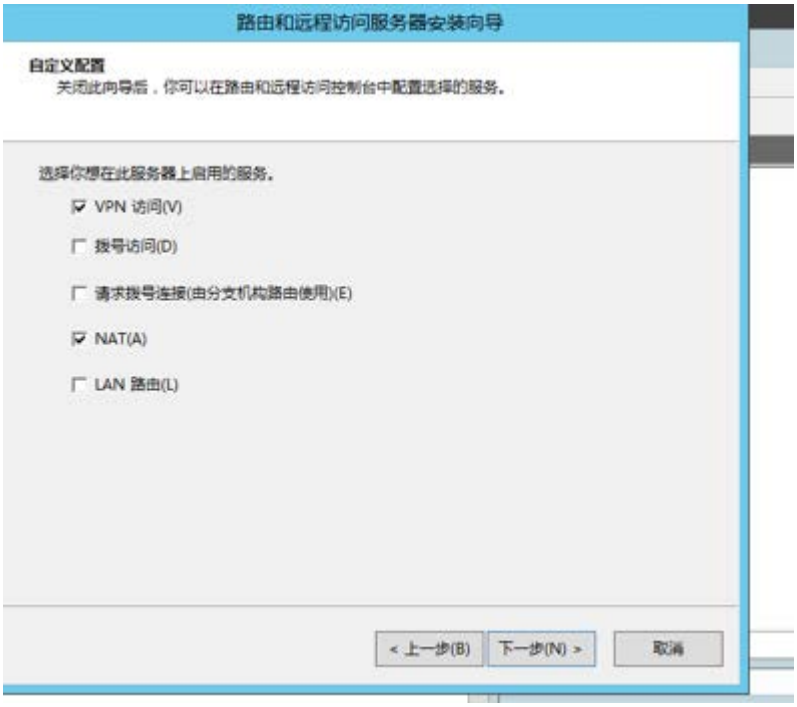
直接安装就可以



然后在管理工具里面　打开路由和远程访问　　右键服务器　　配置路由和远程访问

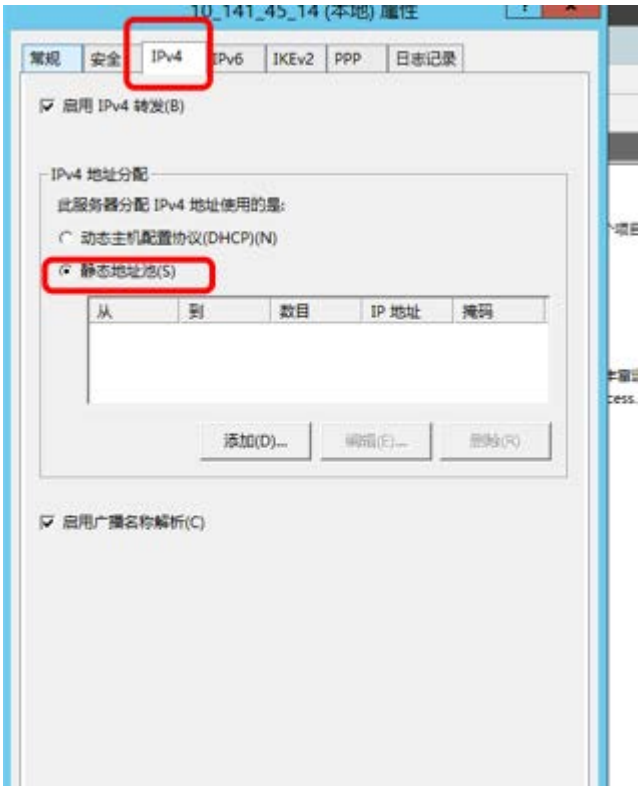


然后选择自定义配置



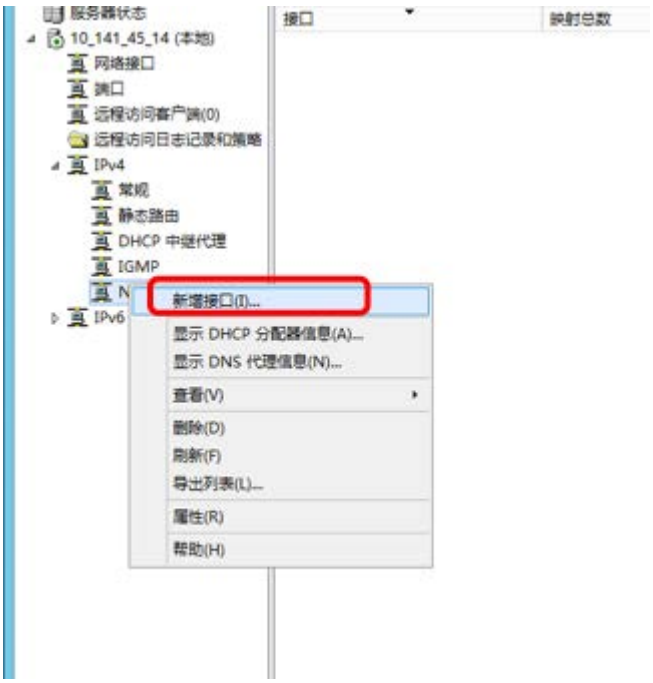
勾选这个　都要勾选然后下一步 一直按照提示操作

配置完成之后 右键服务　点击属性

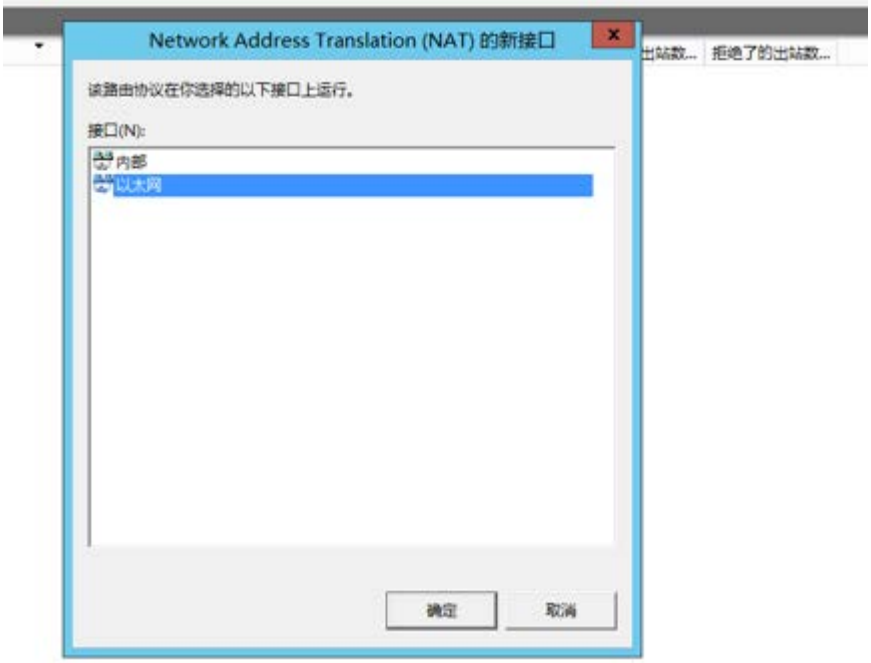


选择 ip4 点击静态地址池 然后点击添加 注意 这个地方可以选择动态分配 如果动态不好用（VPN 会连不上）就只能选择静态了

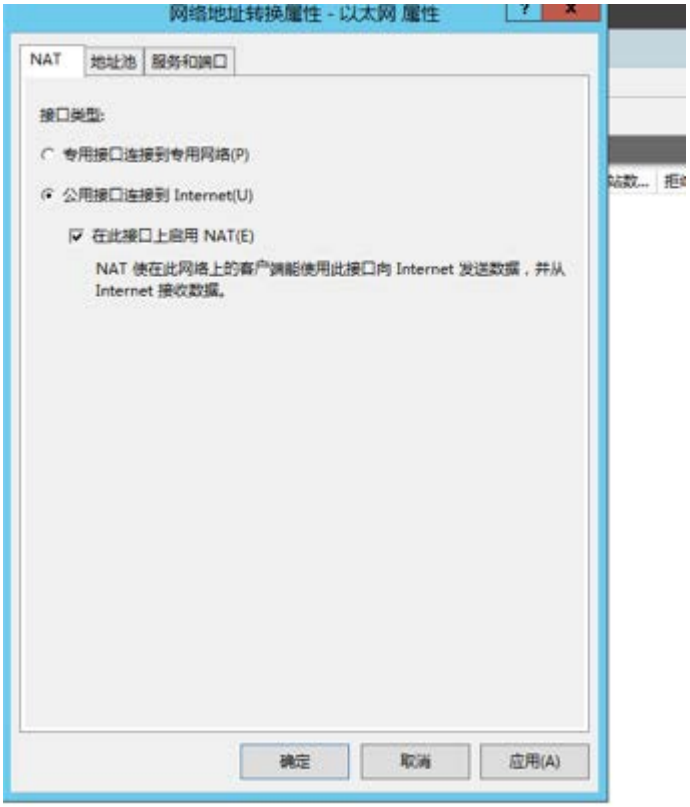
然后输入一个 ip 段 点击确定 （IP 段根据云服务器提供商显示的本地 IP 地址填写）



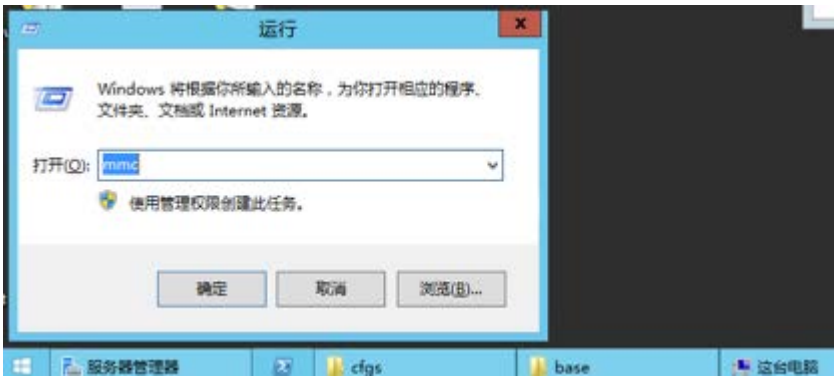
然后右键 nat　选择新增接口　注意 这个地方如果不设置 后期连接上 vpn 之后 可能不能上网



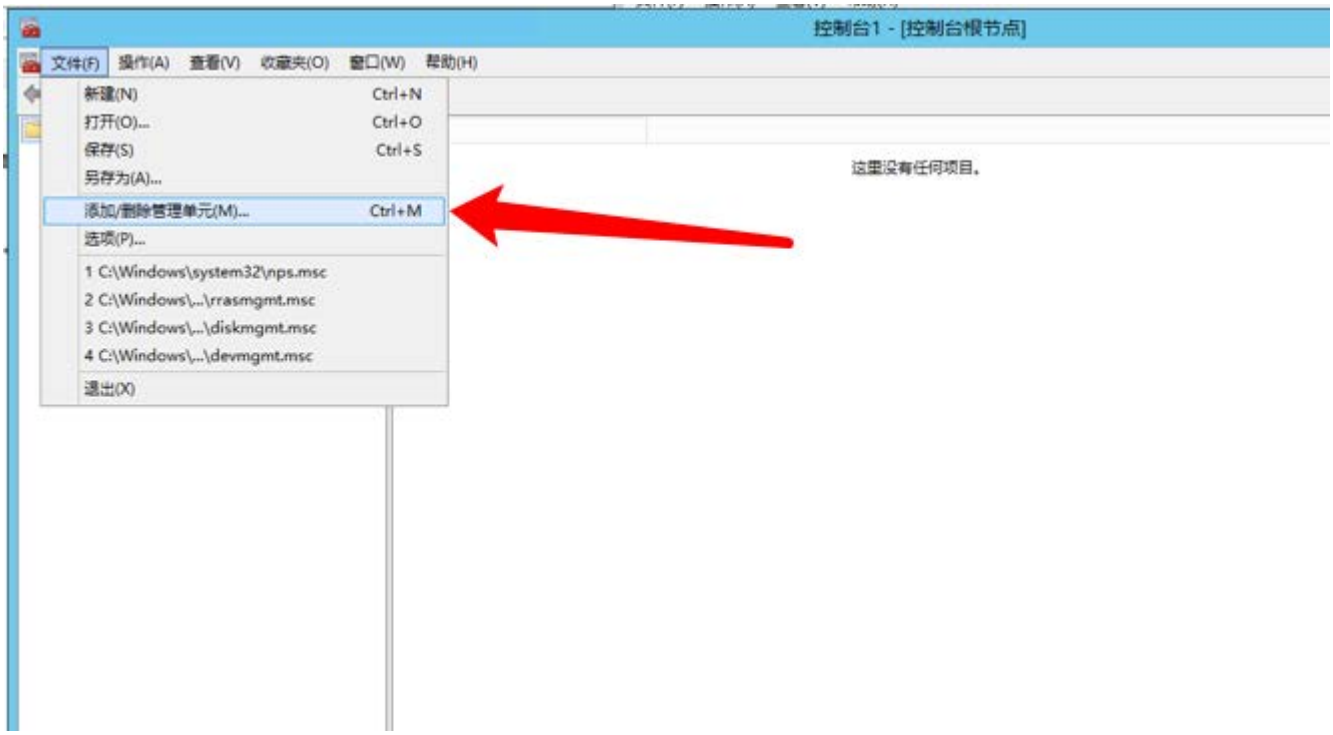
选择以太网，如果是 window2008 的版本 是选择本地连接



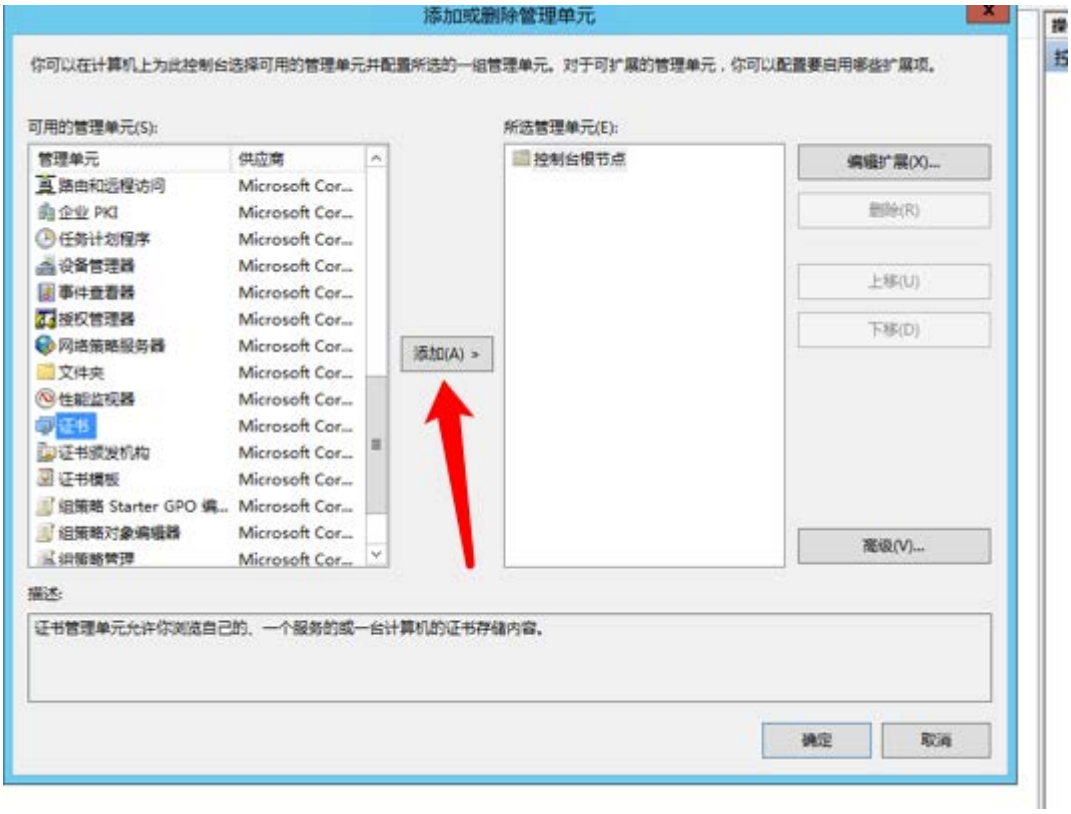
按照图上的选择即可　注意 建议在照着这个步骤把内部也操作一次　如果后期能连接上网 就不需要操作内部



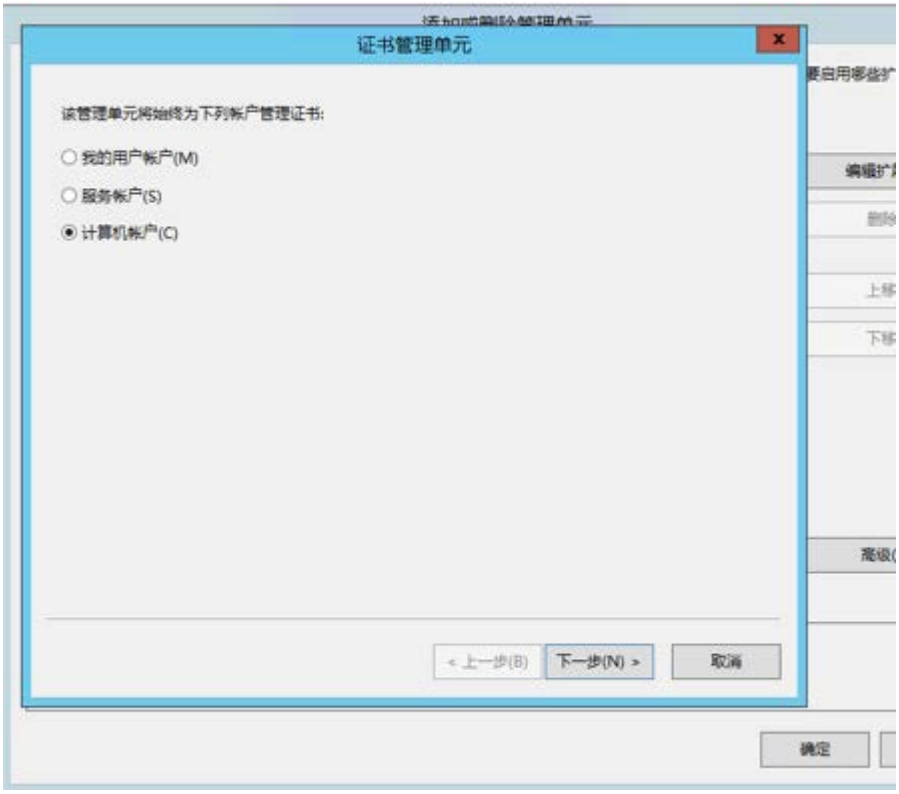
然后 window+r 输入 mmc 咱们开始导出服务端的证书



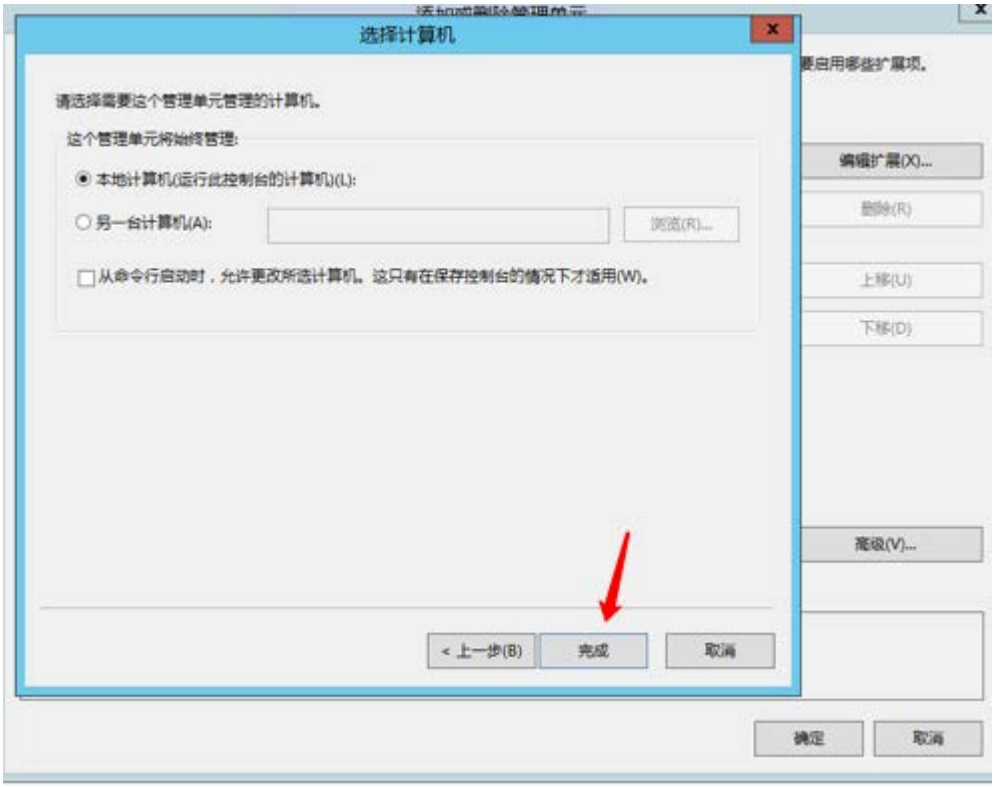
点击文件 添加管理单元



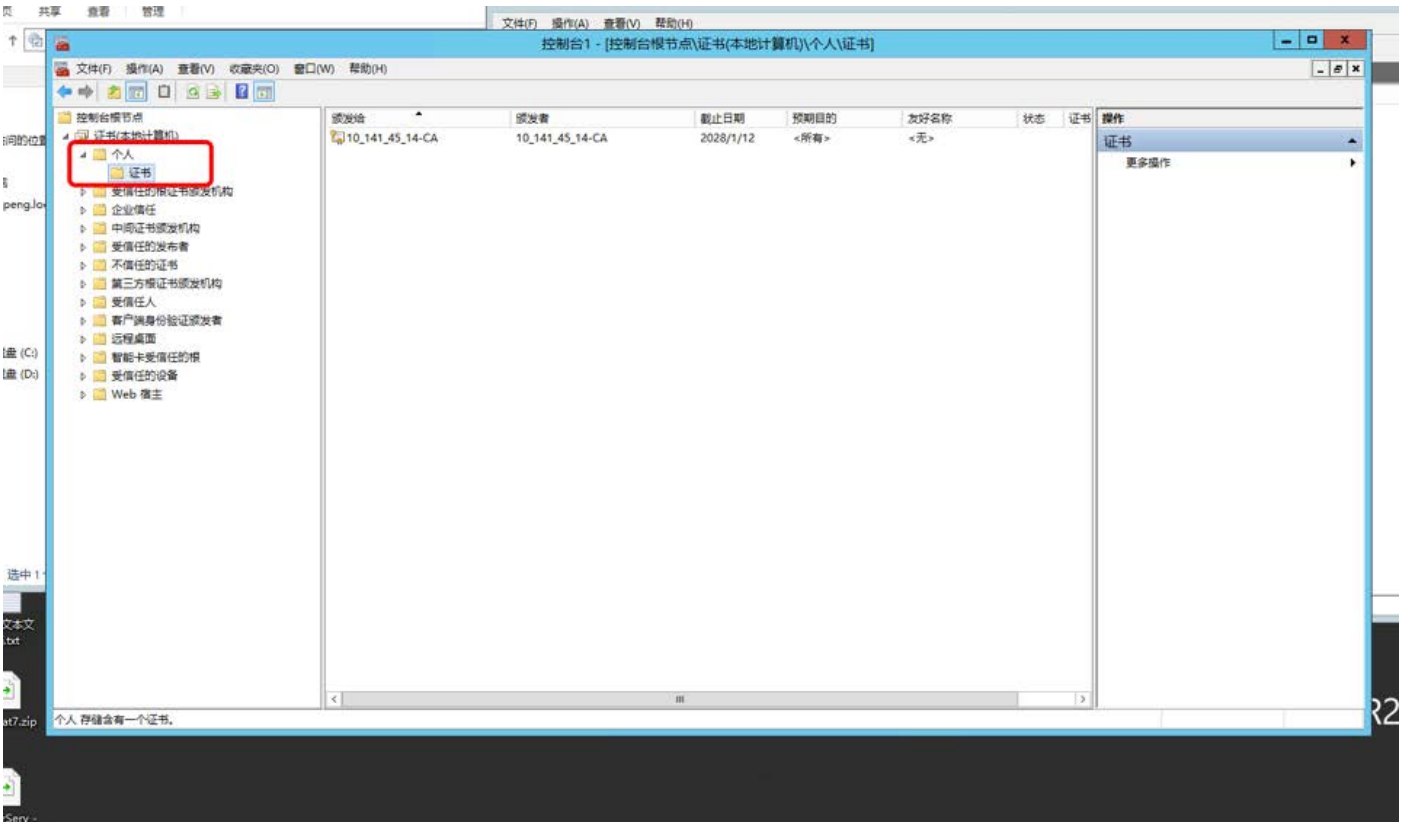
选择证书 点击添加



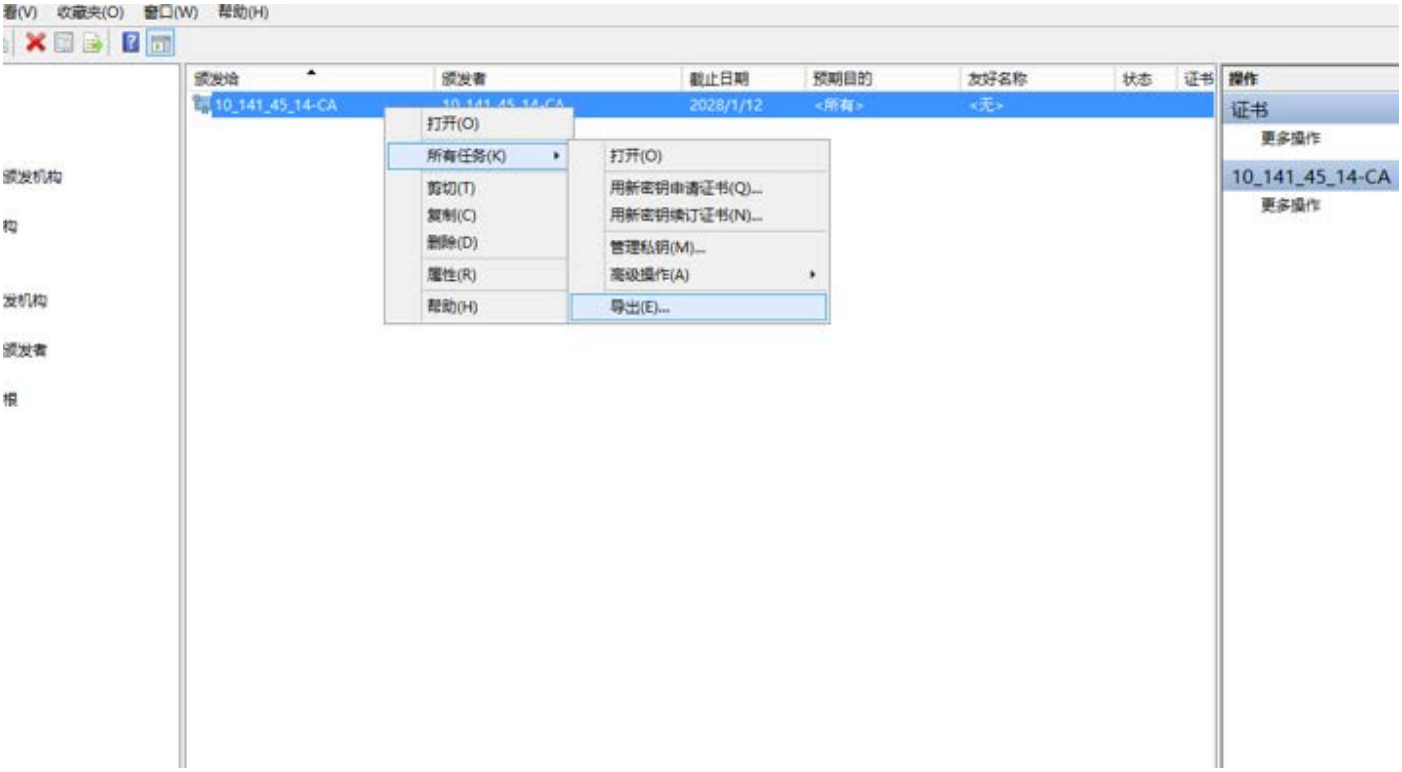
选择计算机账户 然后点击下一步



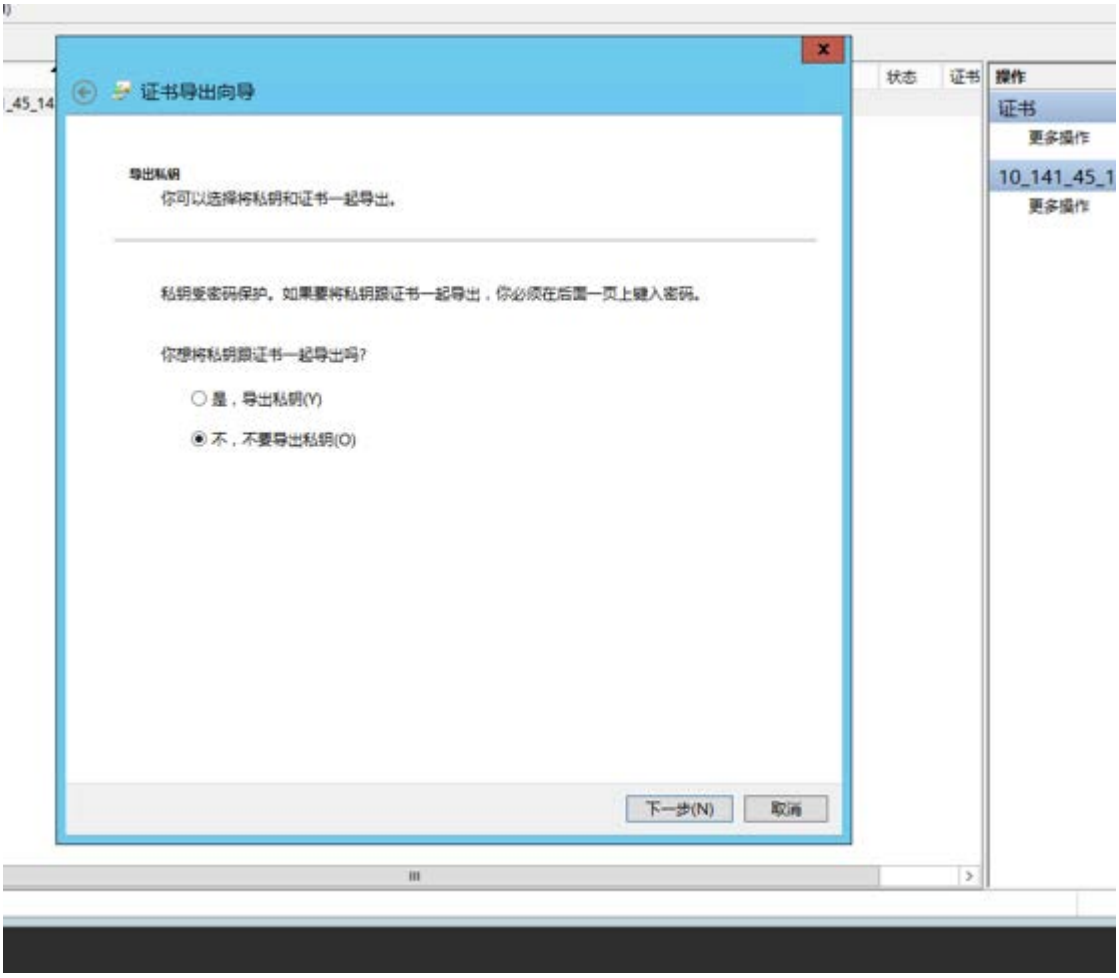
然后直接点击完成 然后直接按操作完成



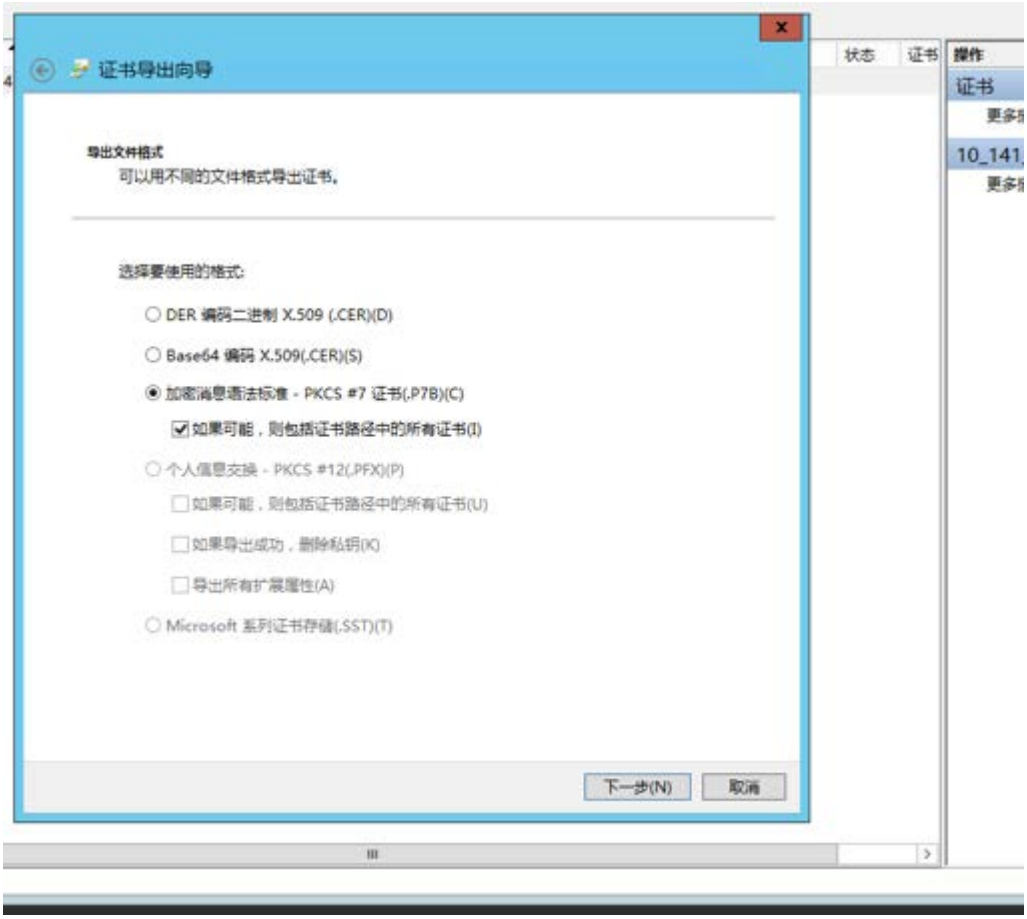
点击个人 证书　右侧就会有刚才生成的证书



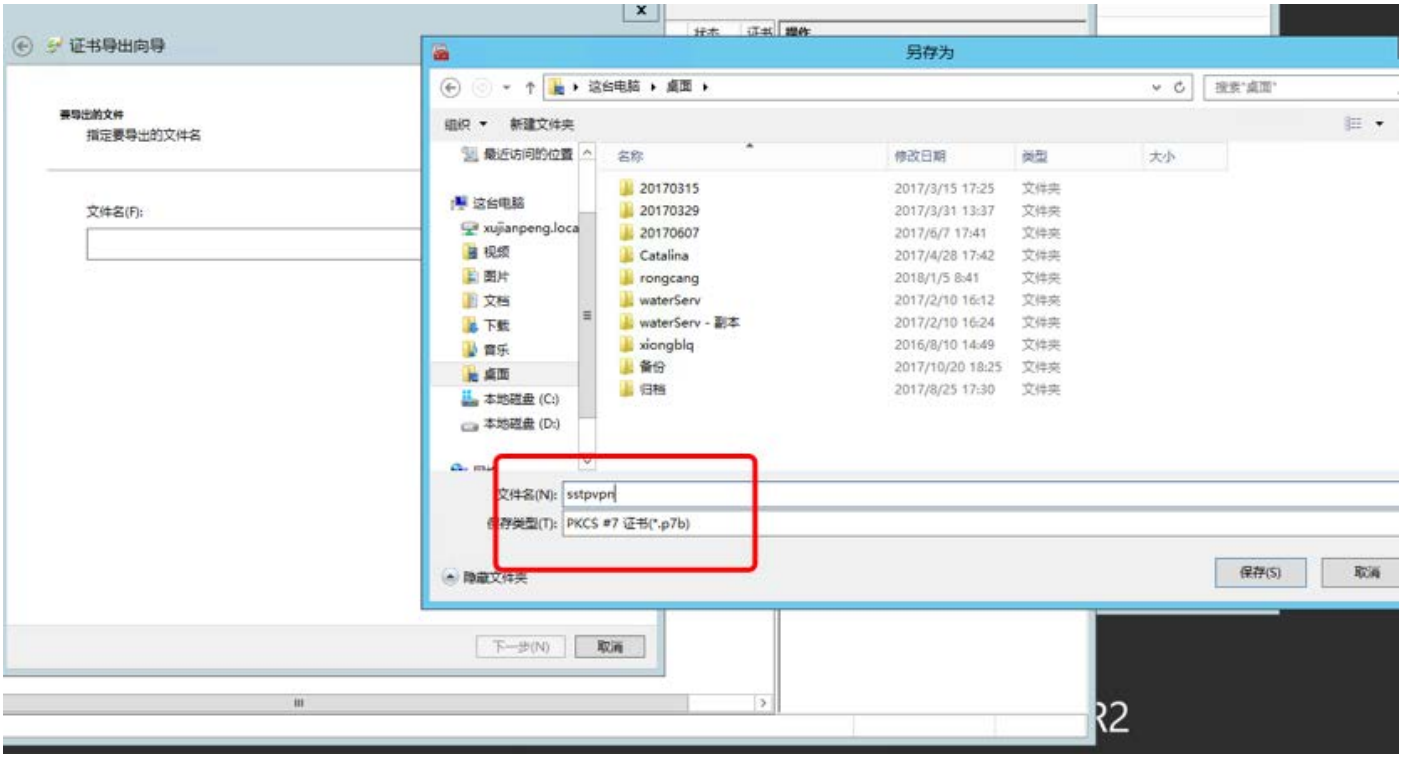
右键证书　所有任务 然后导出



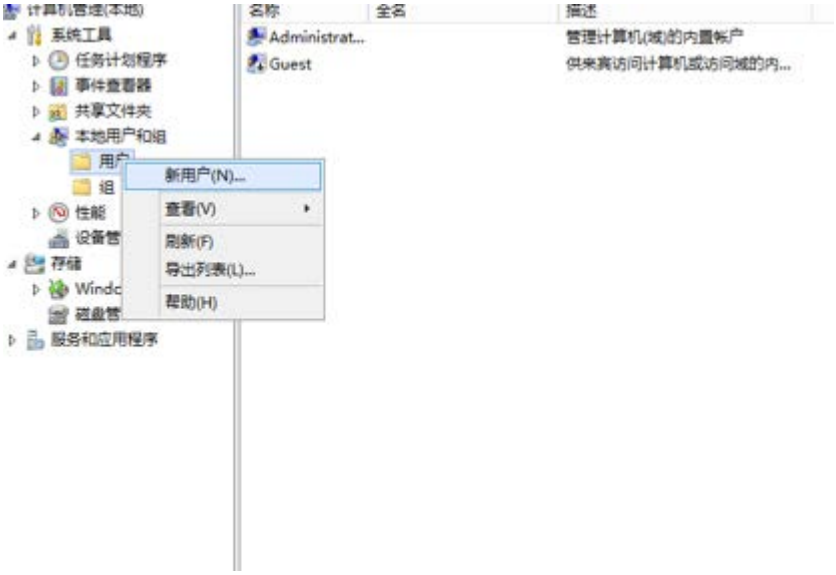
按图上选择 点击下一步



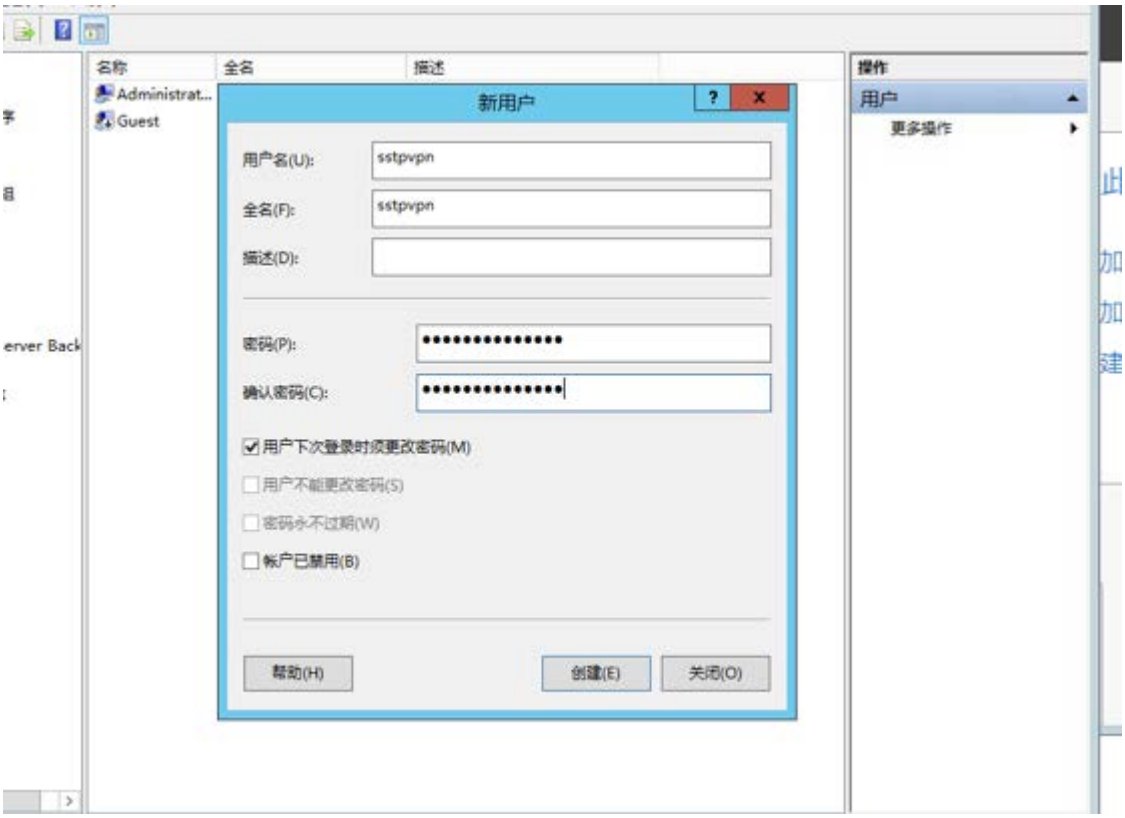
按图上选择 点击下一步



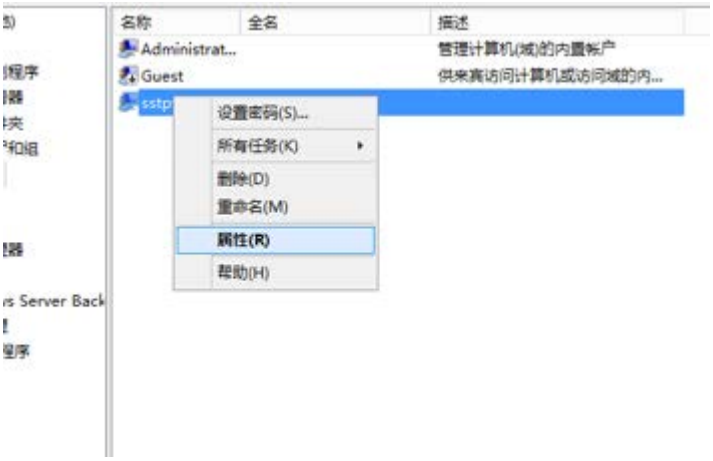
然后选择证书的位置 和类型　按照图上选择　　证书就导出成功了



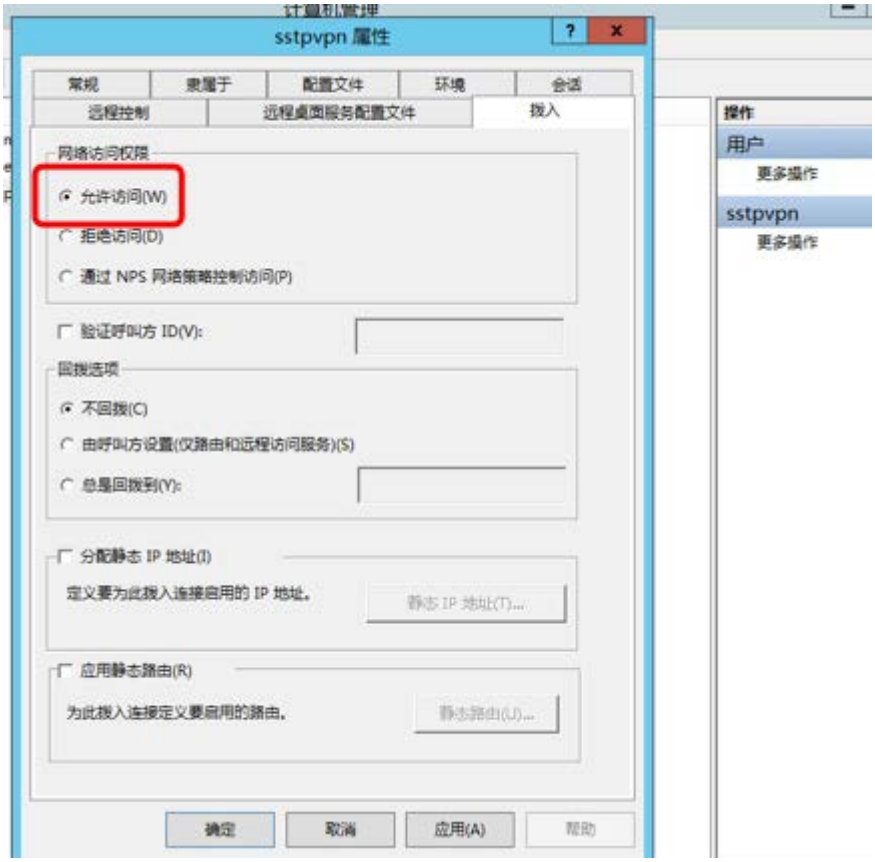
计算机管理 本地用户和组 添加一个新的用户



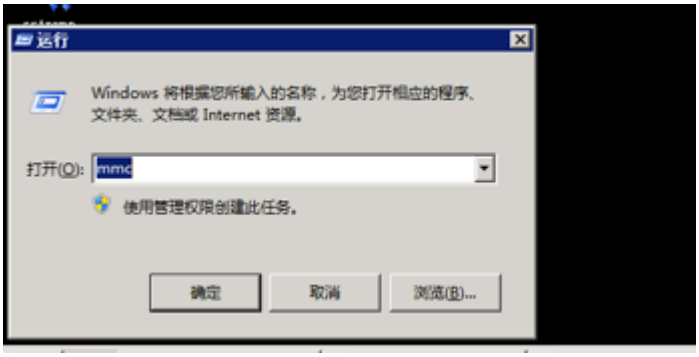
点击创建



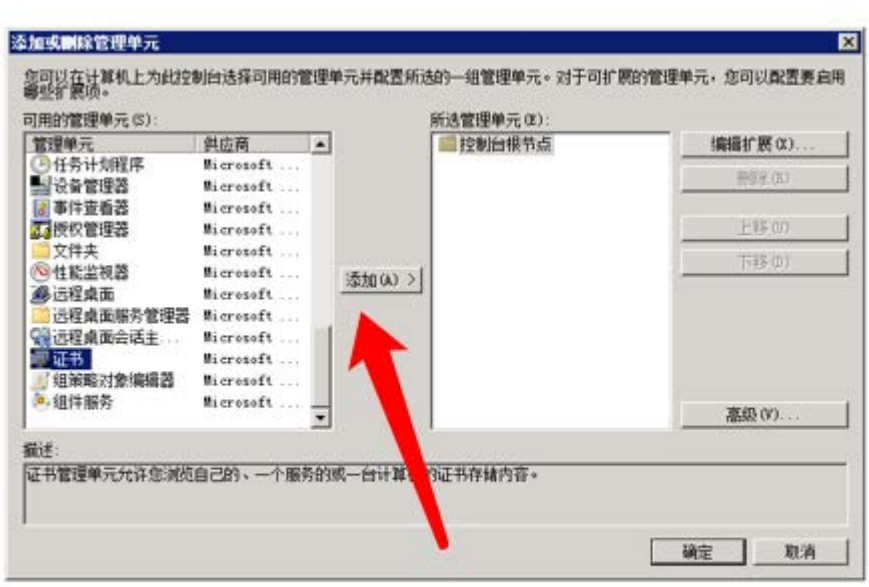
然后右键用户 给用户设置属性

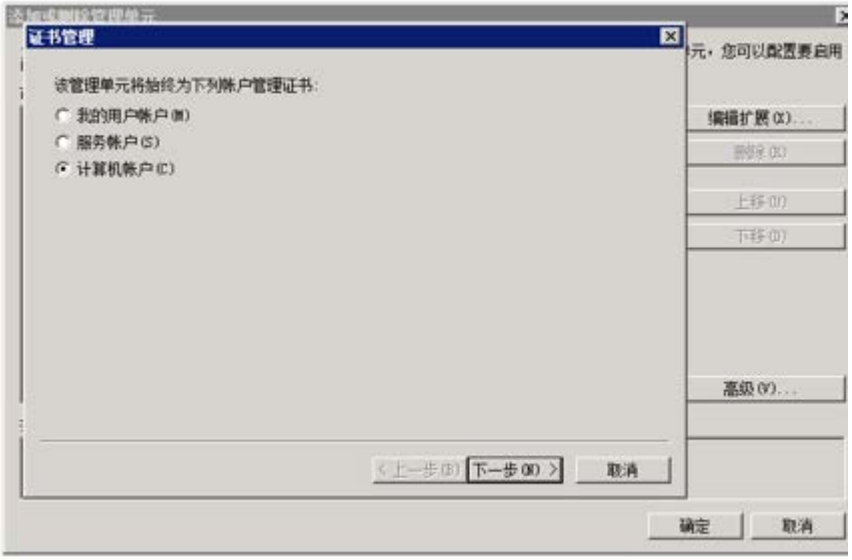


按照图上选择的就可以　然后点击确定　用户就添加完了 注意 这个用户就是你客户端连接 vpn 时候的用户名和密码　也可以直接用远程的用户　用远程的用户 添加用户可以省略，如果新添加的用户连接 vpn 的时候不好用，使用远程登录的用户即可



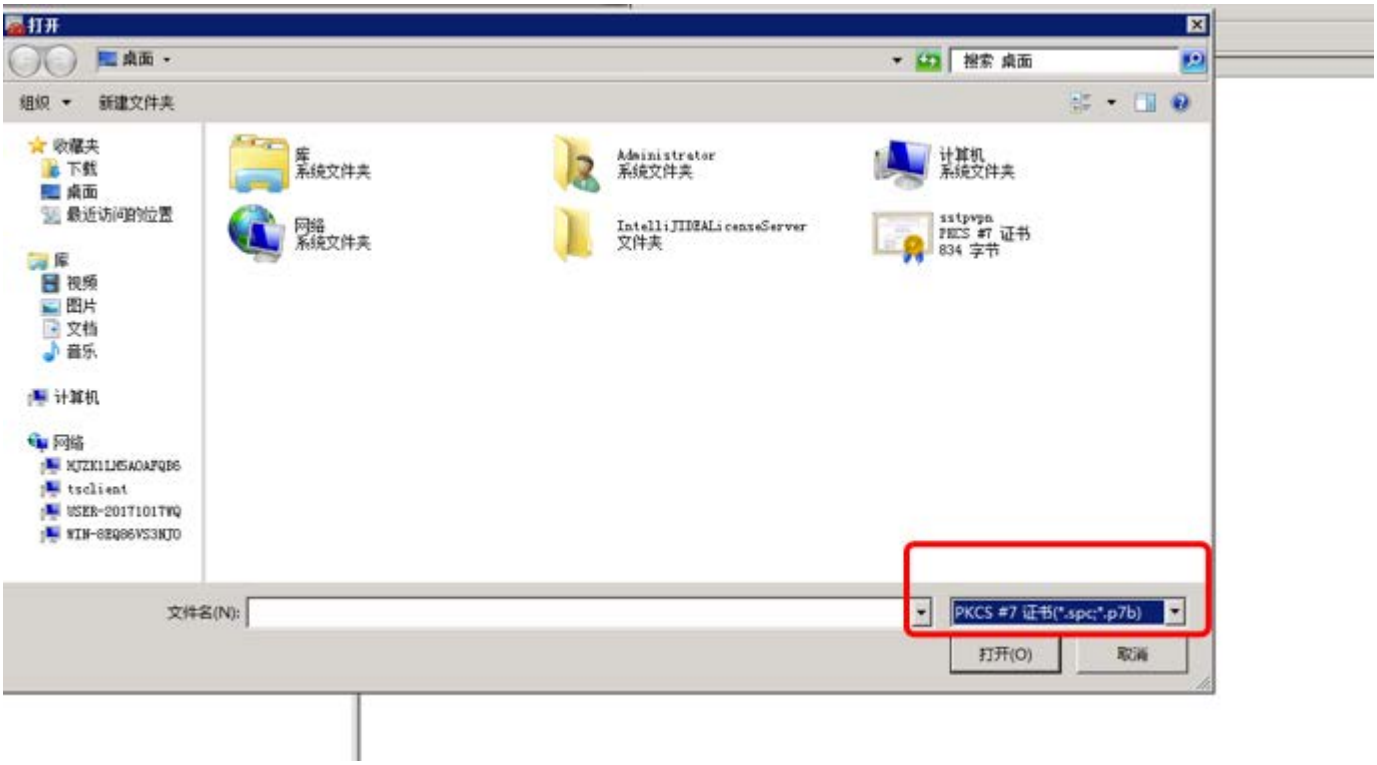
然后把证书复制到客户端（即要连 VPN 的电脑或服务器），在客户端也是同样的方式　，咱们要开始添加证书



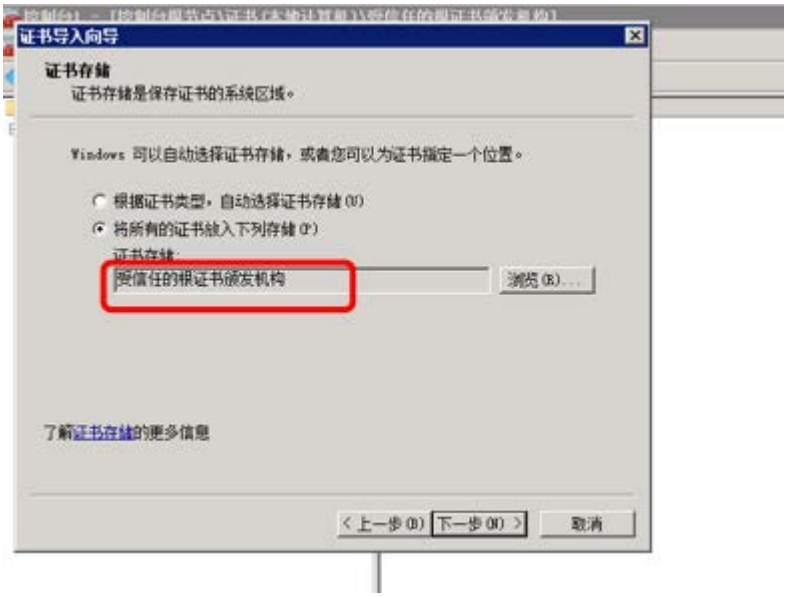


这两步跟导出证书是一样的

然后在受信任。。。右键 所有任务 导入

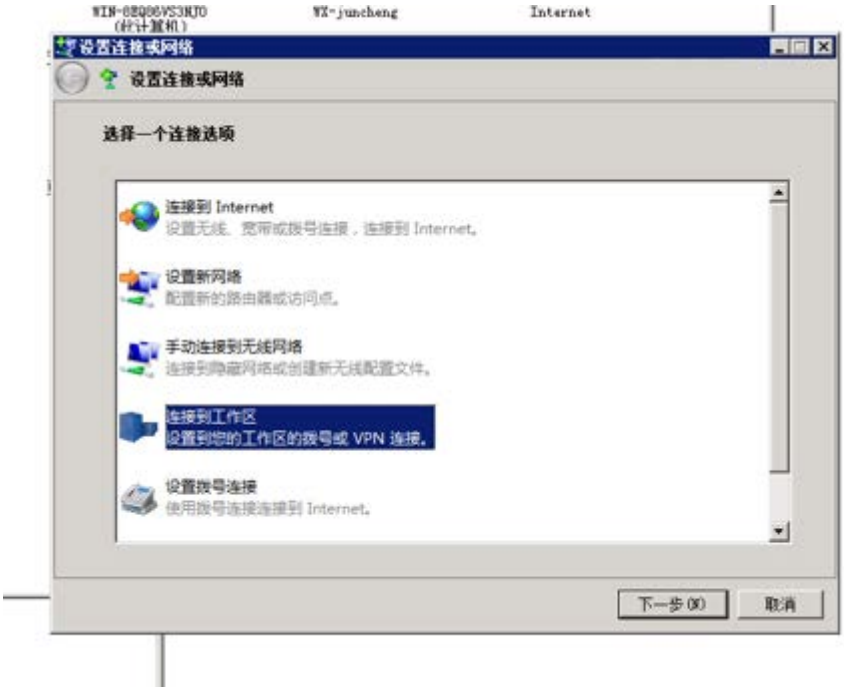


然后选择你刚才复制进去的证书，一点要注意类型 类型 类型

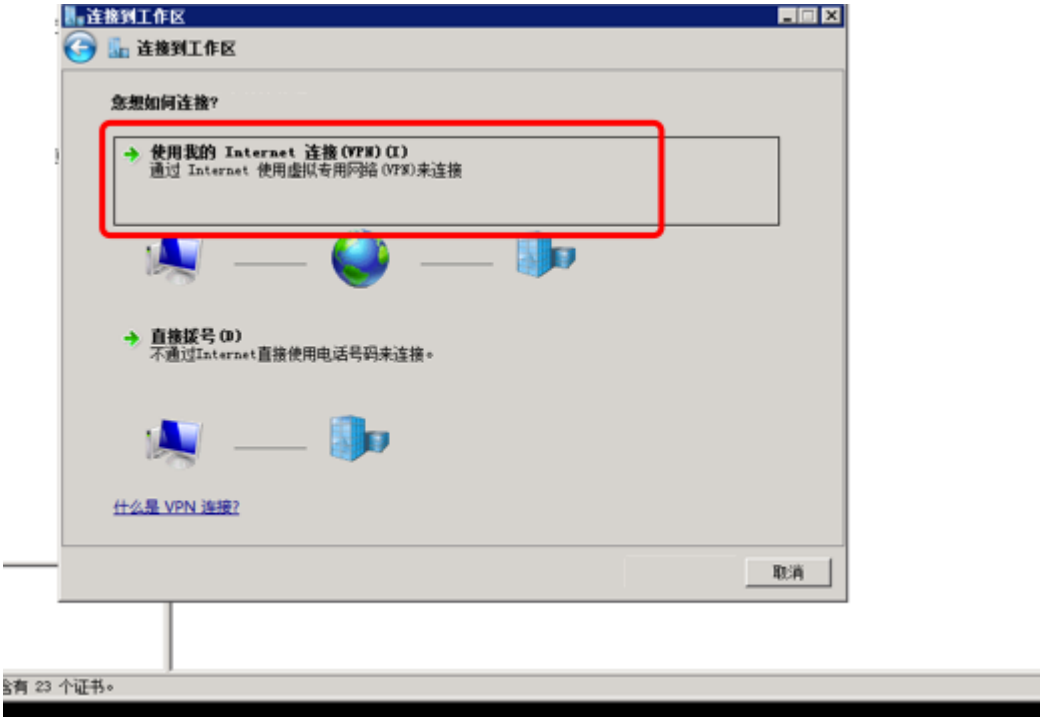


红框内一定是这个选项，其他的不可以 注意注意注意　然后下一步 证书就导入成功了

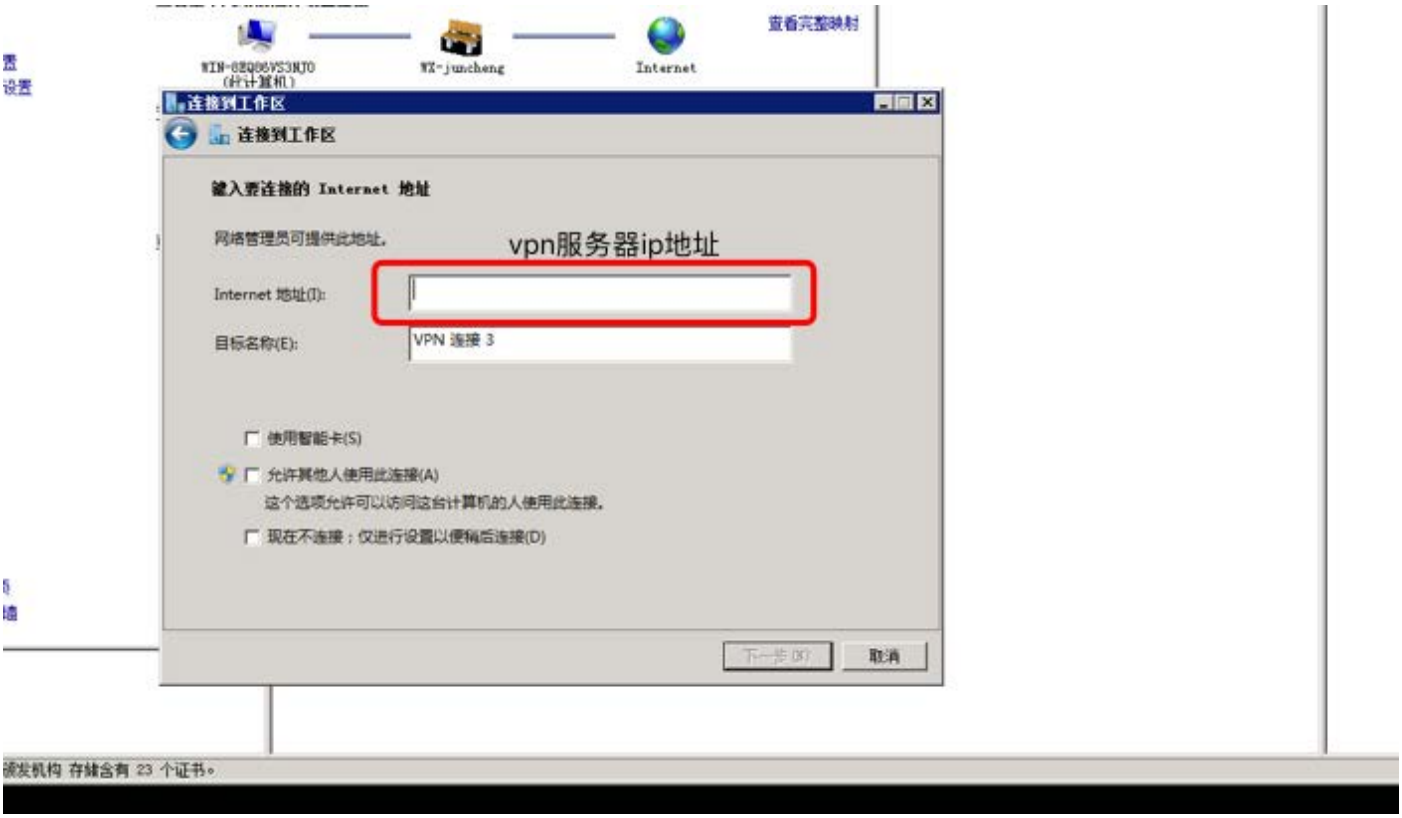
下面开始连接 vpn 了　进到网络共享中心　点击设置新的连接



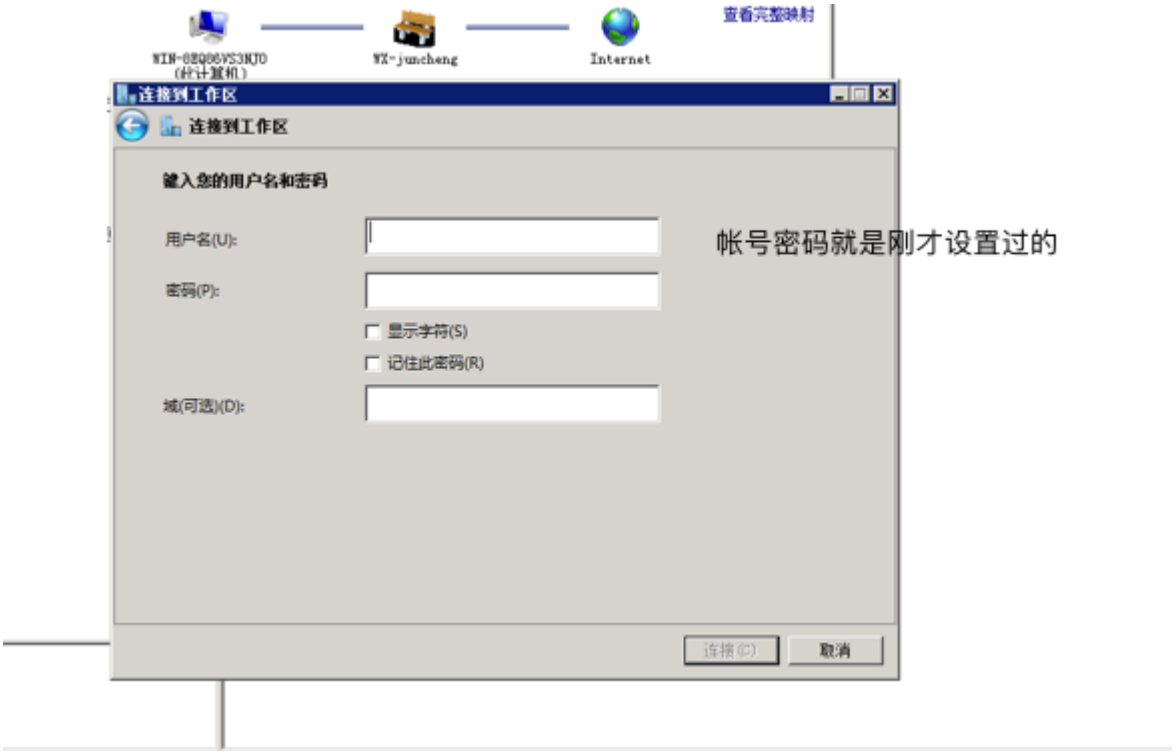
连接到工作区



按图上选择



红框内是服务器的 ip 地址



输入用户名密码 连接就可以了。这样从设置 vpn 到连接就完成了　有问题可以回复

之后，要在网络连接，也就是适配器设置中，右键该 VPN 连接，属性，安全，将 VPN 类型改为 SSTP。另外，最好再转到属性的网络选项卡，分别双击 IPv4 与 IPv6，高级，在 IP 设置中取消“在远程网络上使用默认网关”。

最好将 windows server 的防火墙关闭。

如果出现能够连接 VPN，但是却仍然上不了外网，但是境内网站可以访问，好像没有翻墙成功的情况，除了取消“在远程网络上使用默认网关”，还可以尝试将电脑的网络连接中不必要的适配器全部禁用，以保证电脑确实是从自己创建的 VPN 连接和以太网或无线网端口联网的。

可以使用已有的 VPN 软件连接到该服务器，例如可以在服务器上创建一个用户名、密码与 purevpn 相同的账户，然后用 purevpn 连接服务器即可。

当然，创建账户时也许系统会提示密码不符合强度要求，此时可以打开策略组，也就是运行 gpedit.msc，在本地计算机策略，计算机配置，windows 设置，安全设置，账户策略，密码策略中，将密码必须符合复杂性要求禁用。