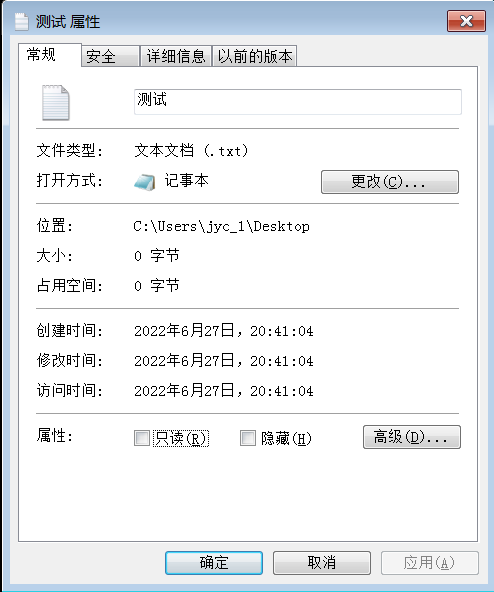
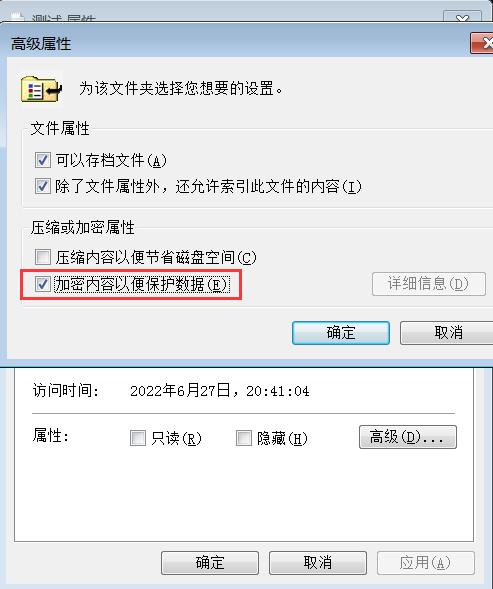
# 1 透明加解密EFS的使用

## 1.1 EFS的使用

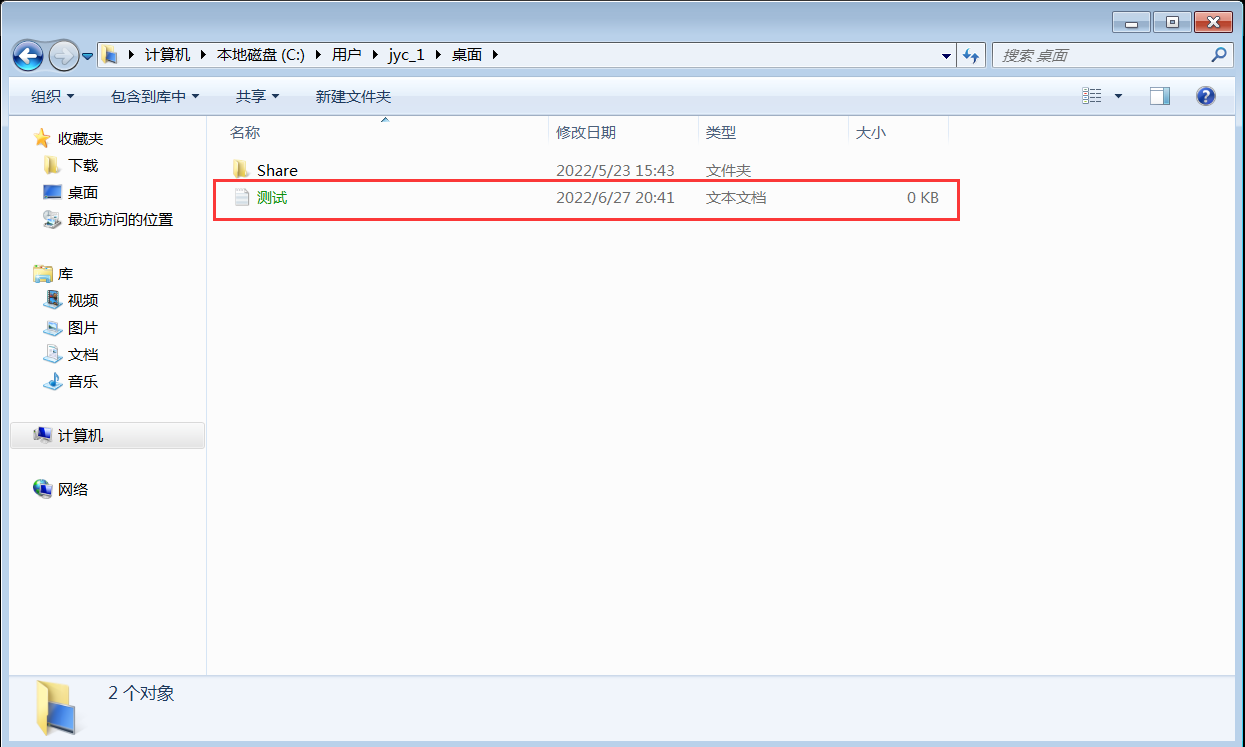
（1）右键点击要加密的文件或目录，点击“属性”。



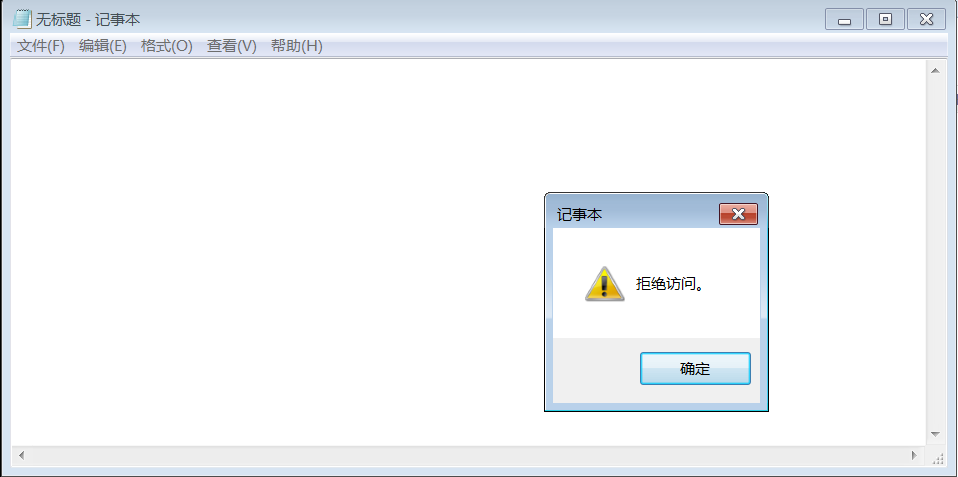
1. 点击“高级”，勾选“加密内容以保护数据”。



1. 可以看到此时文件名显示为绿色，说明EFS加密成功。

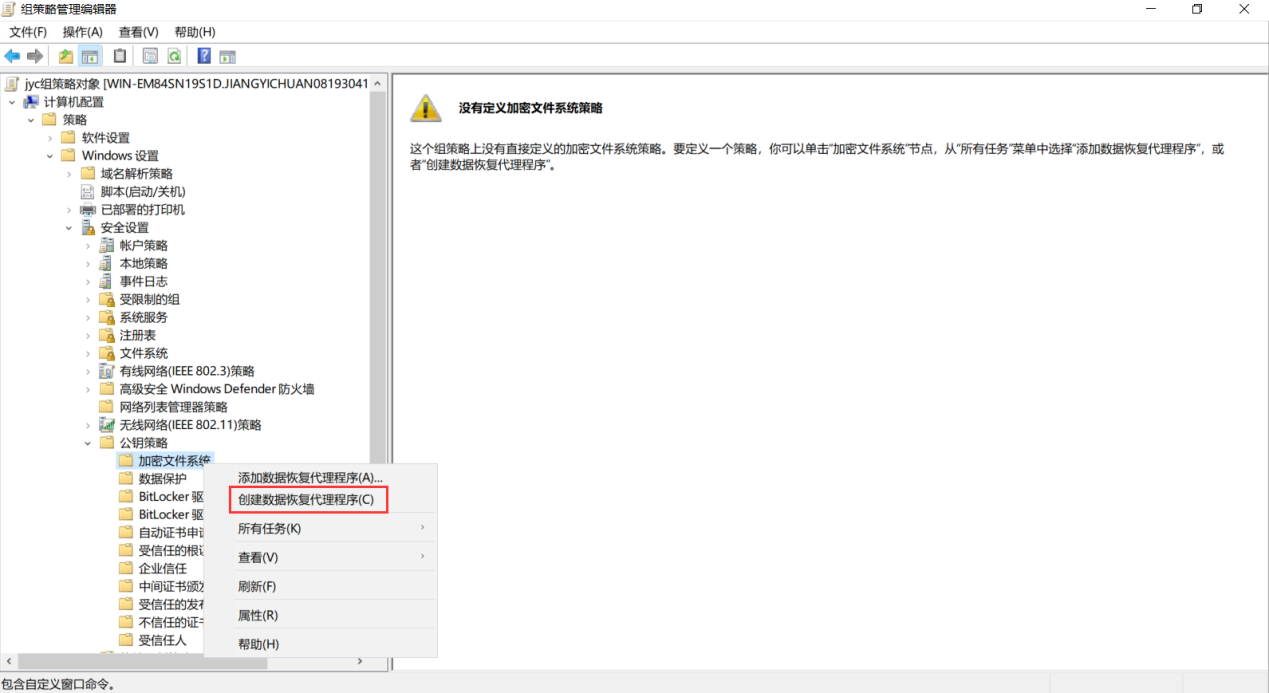


（4）切换其它账号登录，尝试访问该文件，拒绝访问。

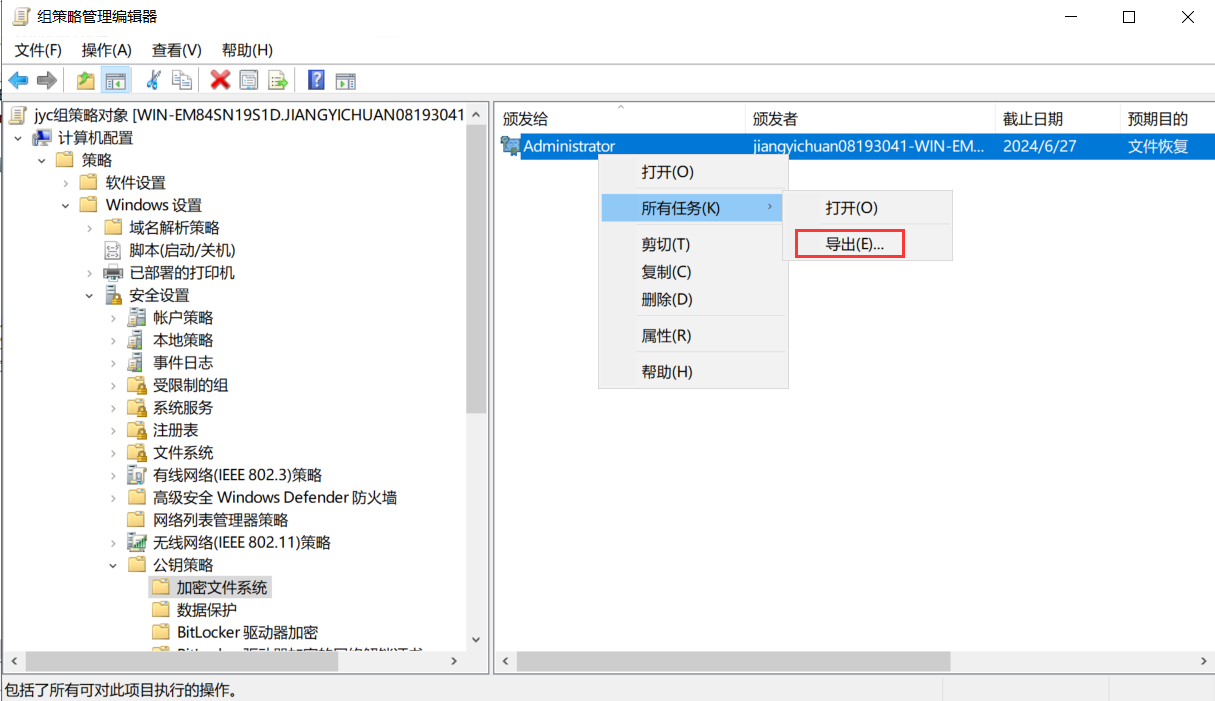


## 1.2 故障恢复代理设置

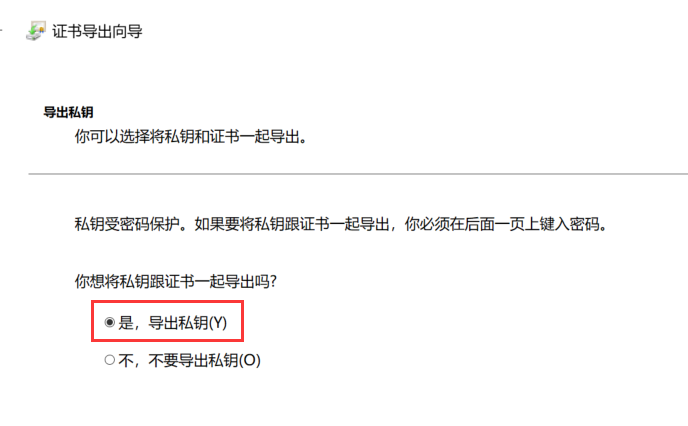
（1）在域控服务器上打开组策略管理器，找到公钥策略、加密文件系统，创建文件恢复代理。



（2）接着我们导出刚创建的证书。



（3）选择导出私钥。



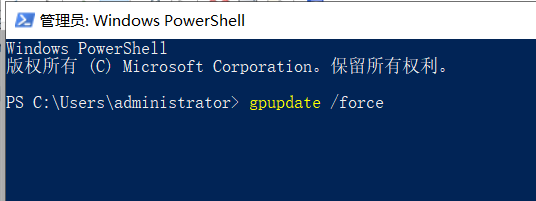
（4）设置密码。



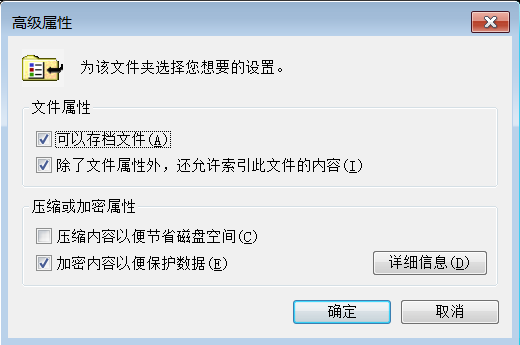
（5）完成导出。



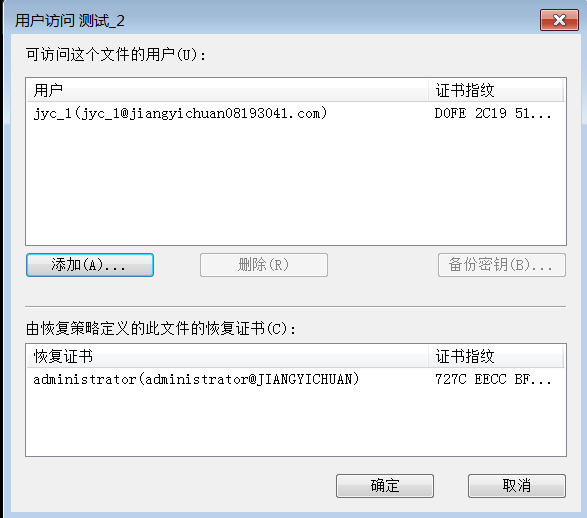
1. 使用 gpupdate /force 下发组策略。



（7）再次登录客户机创建一个加密文件（文件恢复代理只能恢复其创建后加密的文件）。



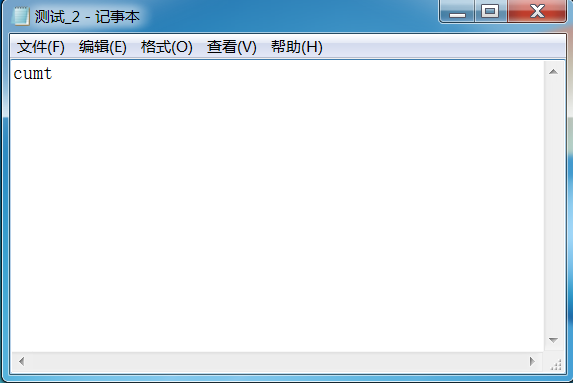
（8）可以看到恢复代理已经存在。



（9）接着我们用域管理员账号登录客户机，将之前导出的私钥导入到客户机中，输入导出时设置的密码。

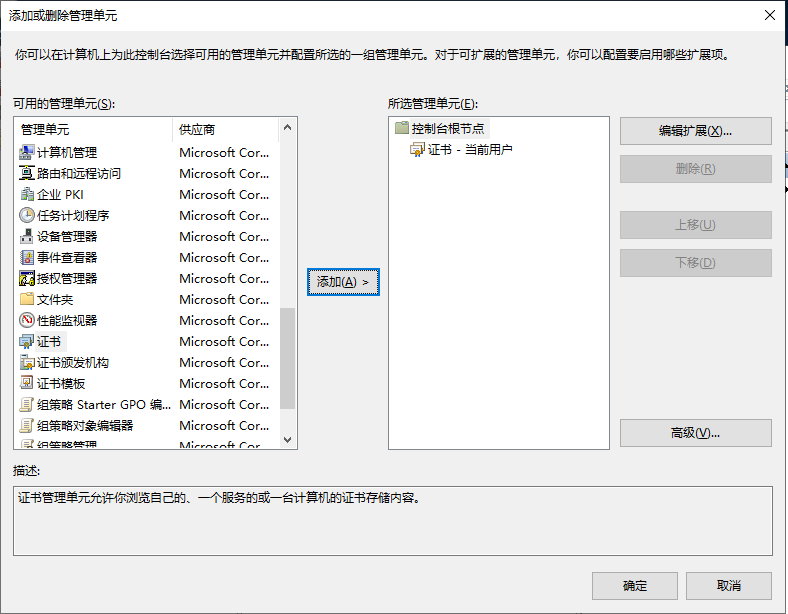


（10）导入成功后，再次尝试访问加密文件，发现成功打开。

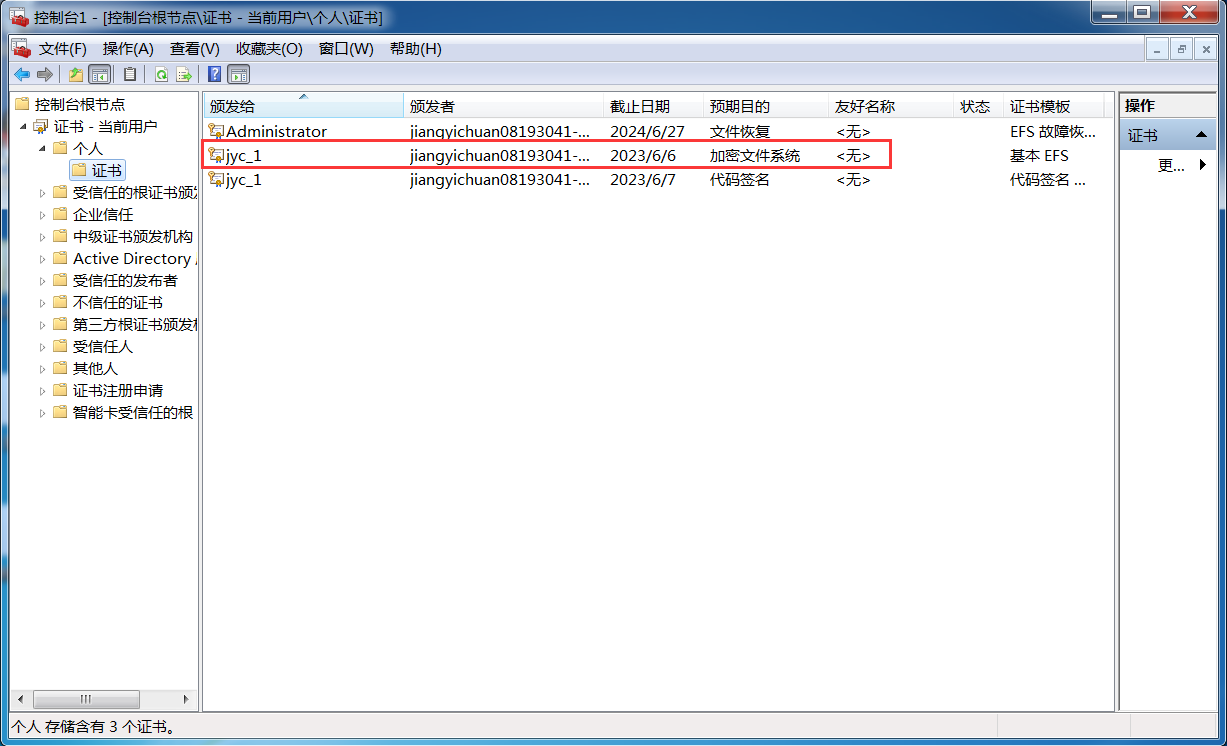


## 1.3 利用备份密钥进行数据恢复

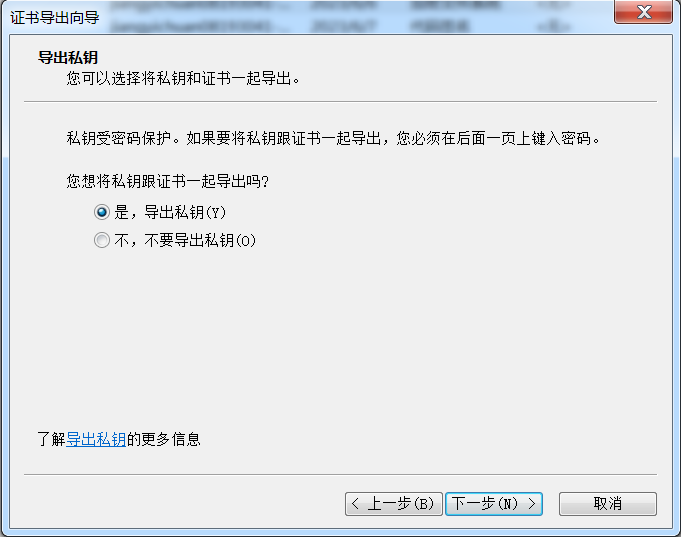
（1）打开控制台并在其中添加“证书”。



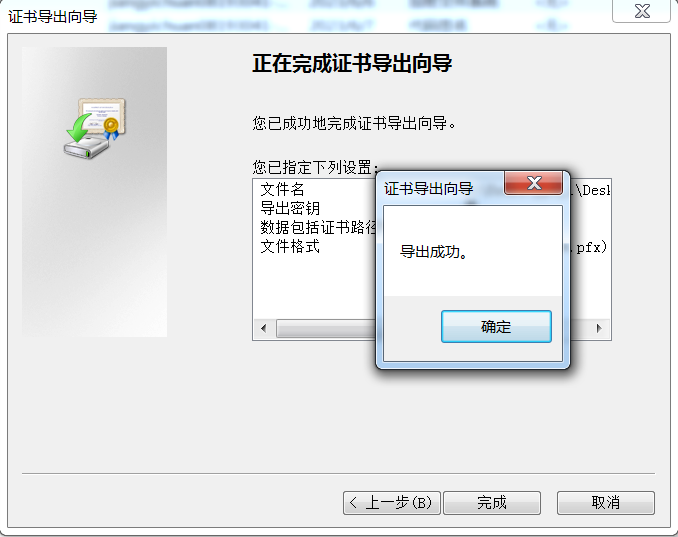
（2）选择个人证书，可以看到加密系统的证书。



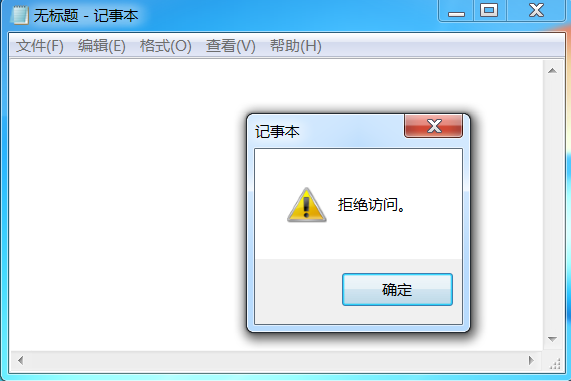
（3）右键点击该证书，选择导出证书，并选择导出私钥。



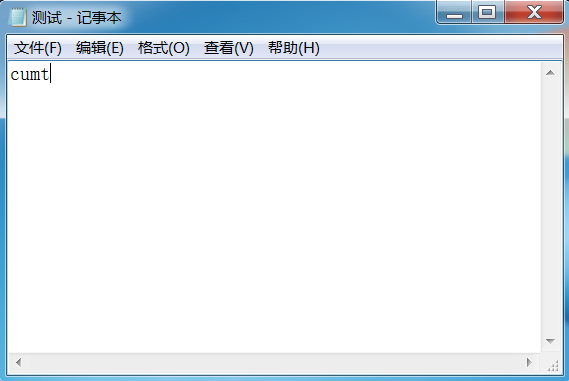
（4）设置密码后成功导出。



（5）假设删除加密文件系统证书，并重新登录，发现无法访问加密文件。

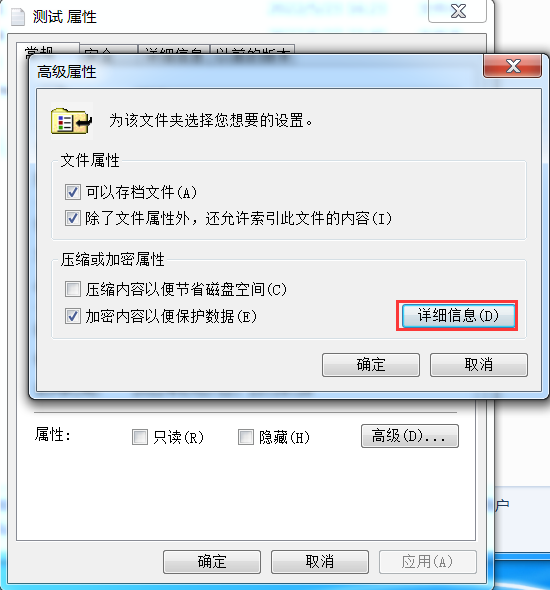


（6）重新导入证书后，发现可以成功访问。

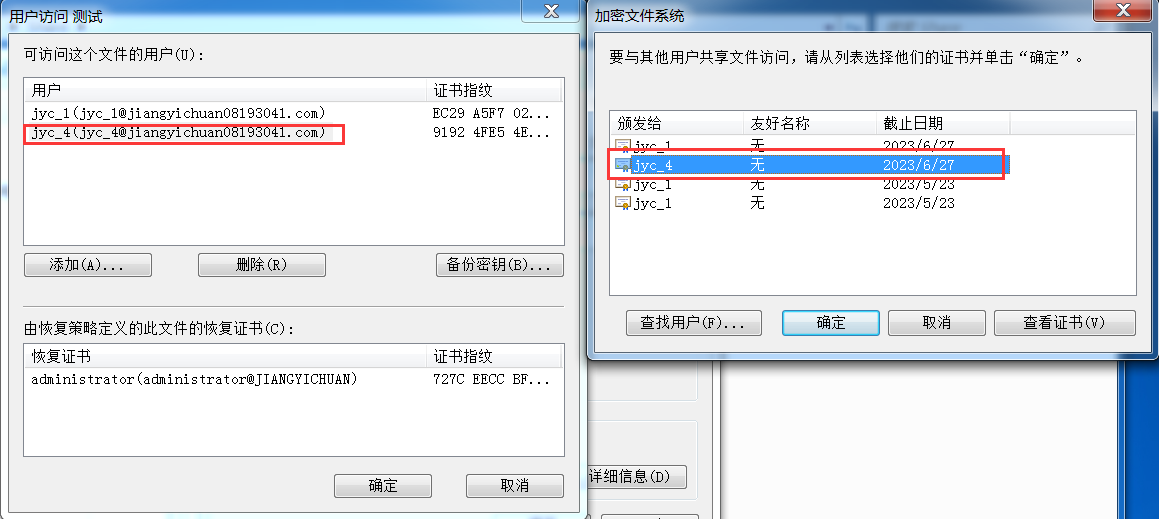


## 1.4 多用户共享加密文件

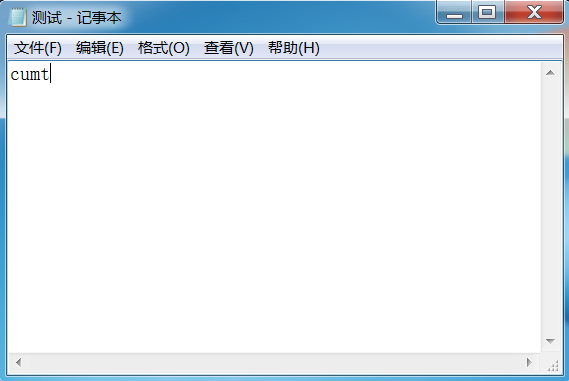
（1）使用加密文件所有者的账号登录客户机，在加密文件上右键属性，点击“高级->详细信息”。



（2）然后在“可访问这个文件的用户”中添加相应的域用户的证书。



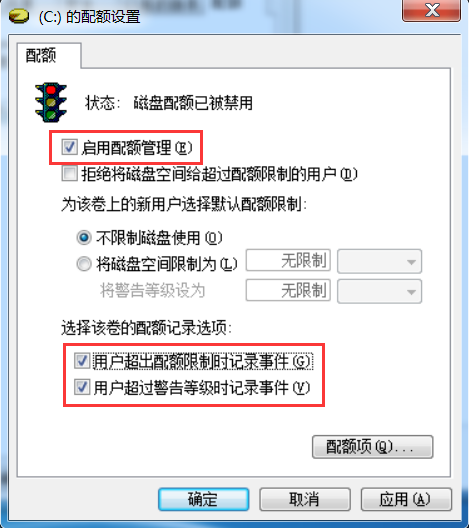
（3）登录jyc\_4用户，成功访问加密文件。



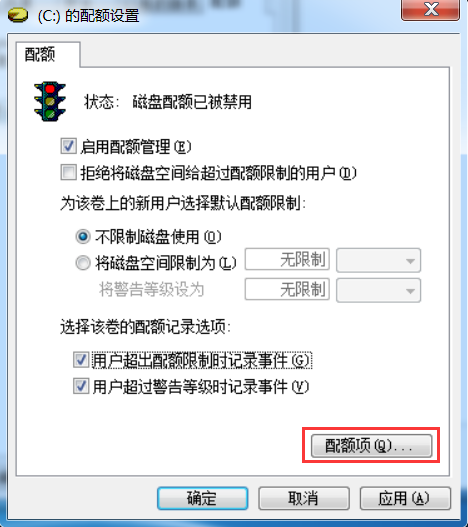
# 2 磁盘阵列RAID

## 2.1 磁盘配额的使用

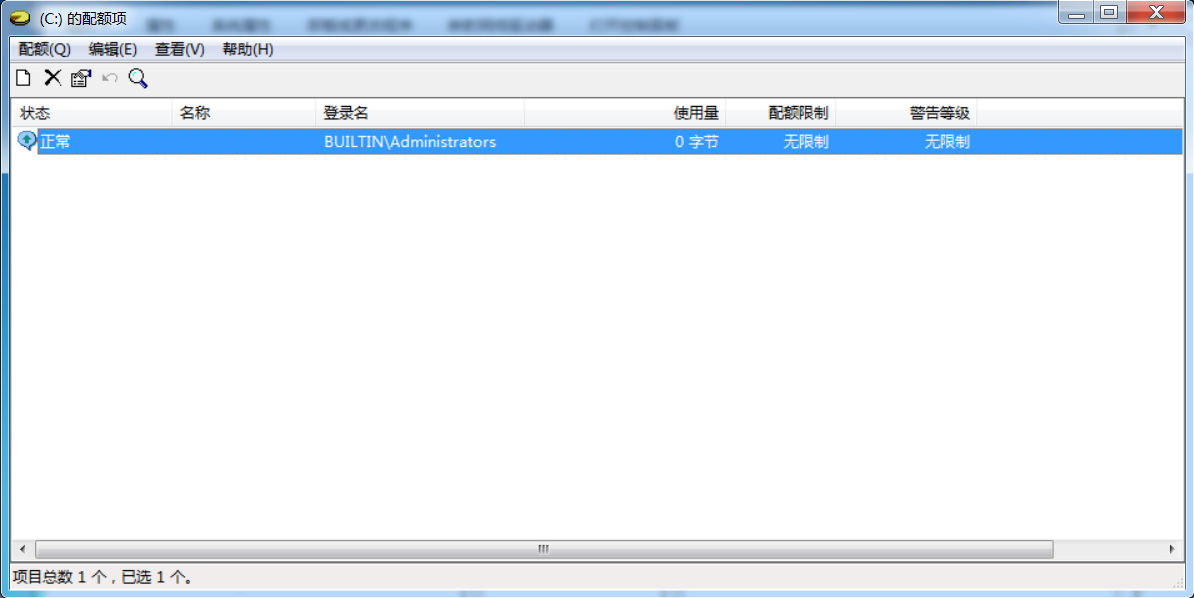
（1）右键点击“磁盘”，选择“属性->配额->显示配额设置”，点击“启用配额管理”。



（2）选择磁盘“配额项”。



（3）查看配额项。



## 2.2 软 RAID 的使用

### **2.2.1 RAID0的使用**

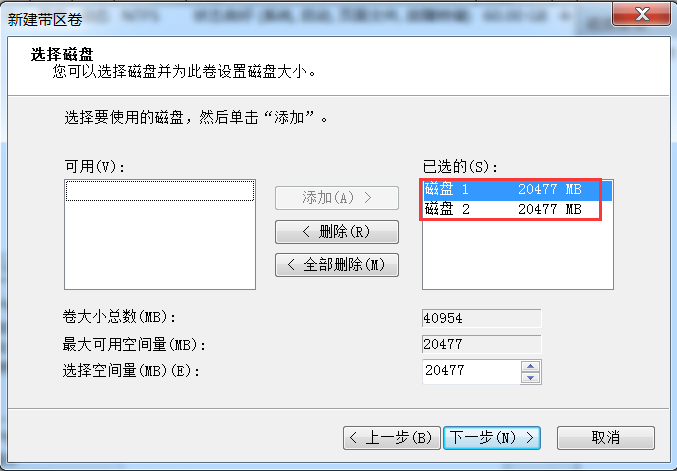
（1）打开“计算机管理->磁盘管理”，将磁盘转换为“动态磁盘”。



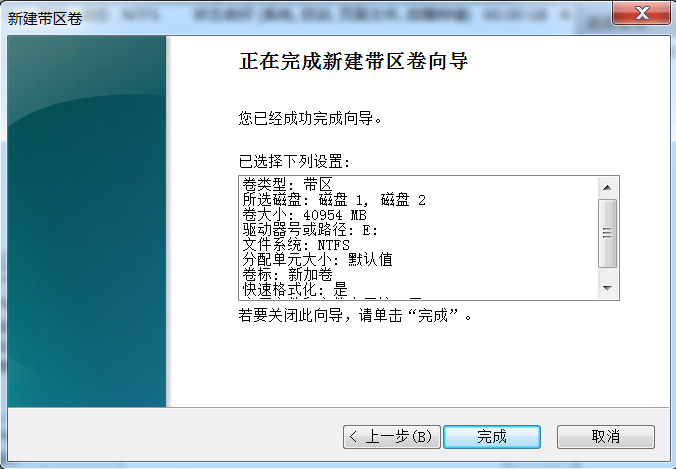
（2）RAID0至少需要两块磁盘，右键选择“新建带区卷”。



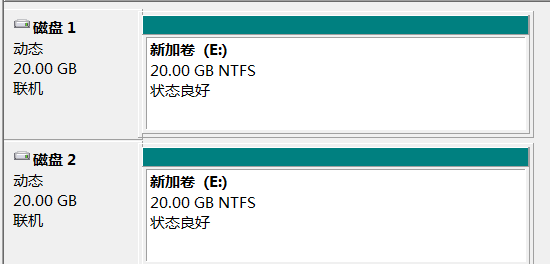
（3）选择磁盘1和磁盘2两个磁盘。

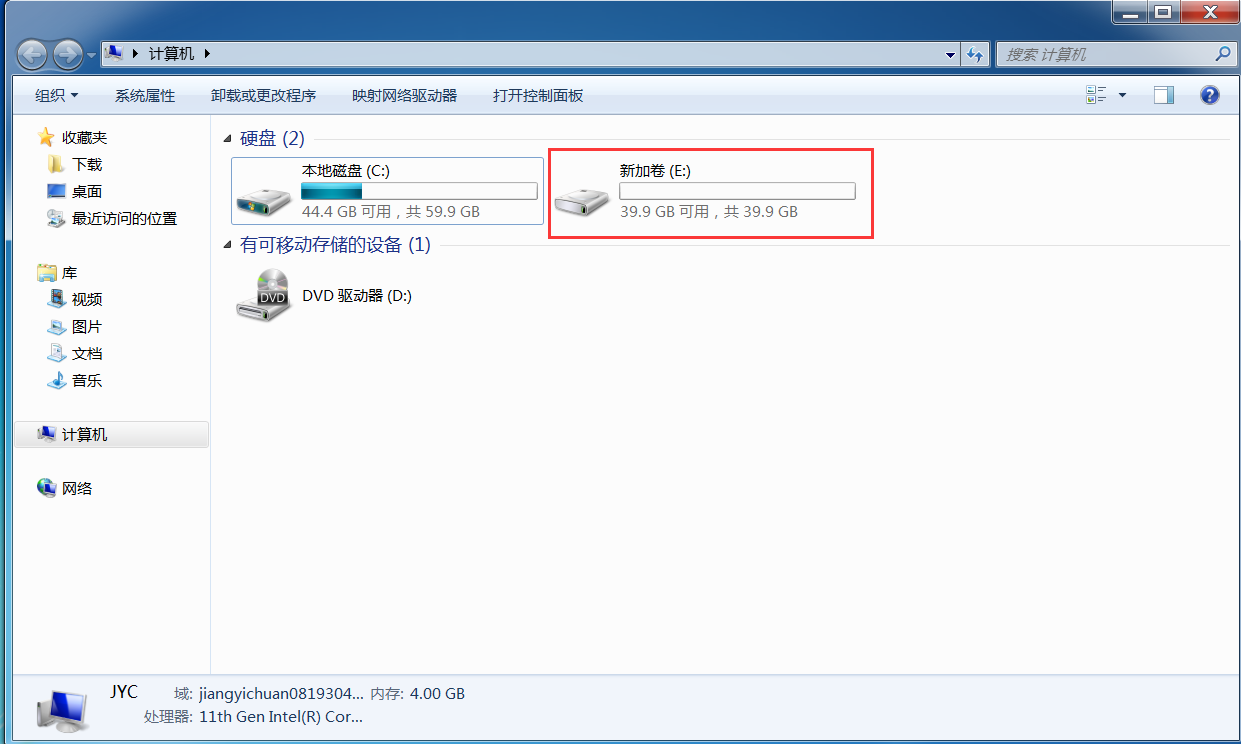


（4）一直选择默认选项，直到创建完成。



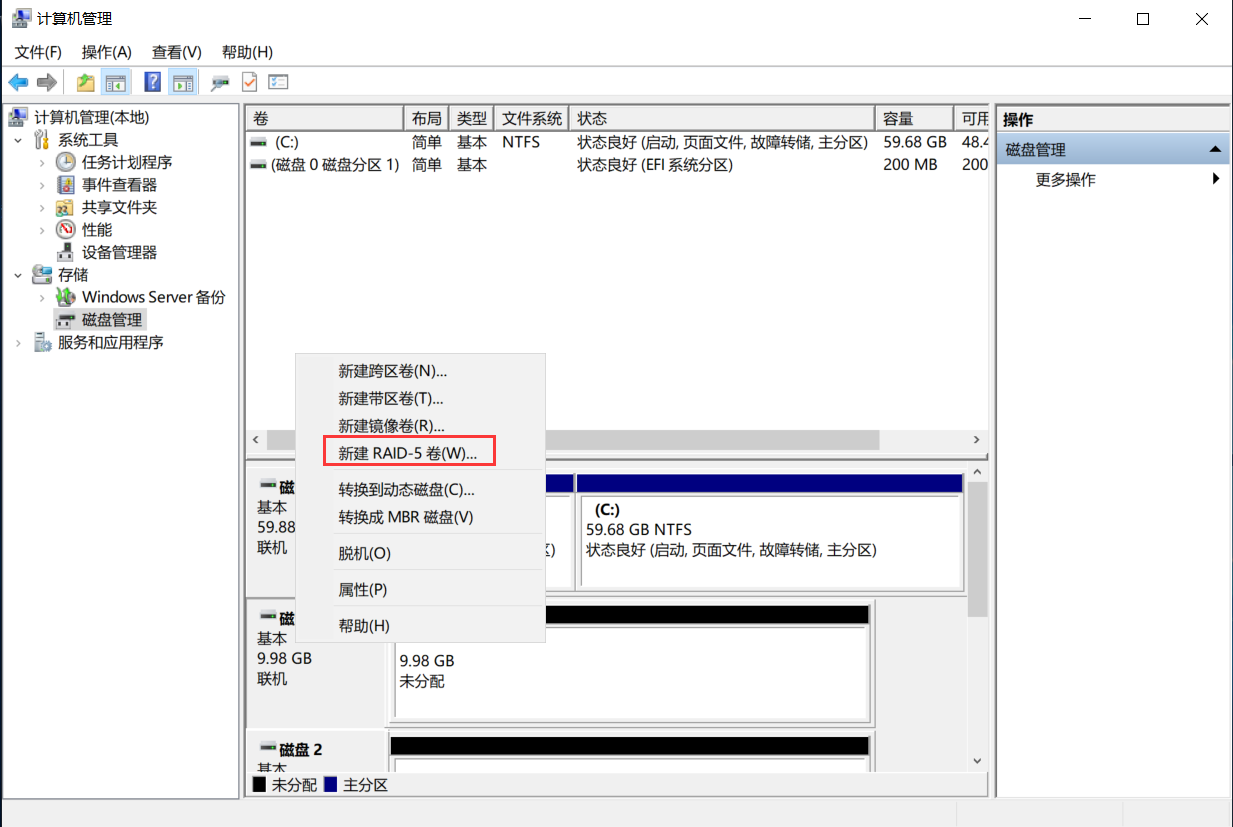
（5）可以看到已经成功创建RAID0。



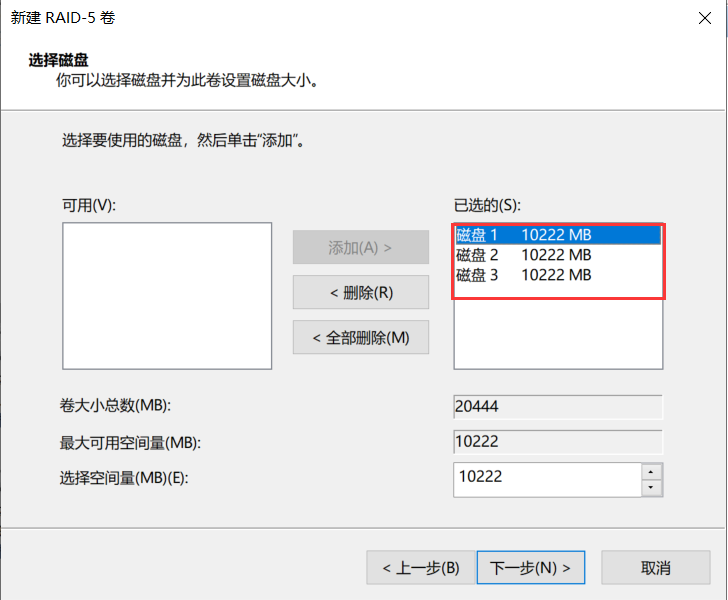


### **2.2.2 RAID5 的使用**

（1）由于win7并不支持创建RAID5，因此选择在windows server 2019中操作。RAID5需要三块磁盘。右键选择“新建RAID-5卷”。



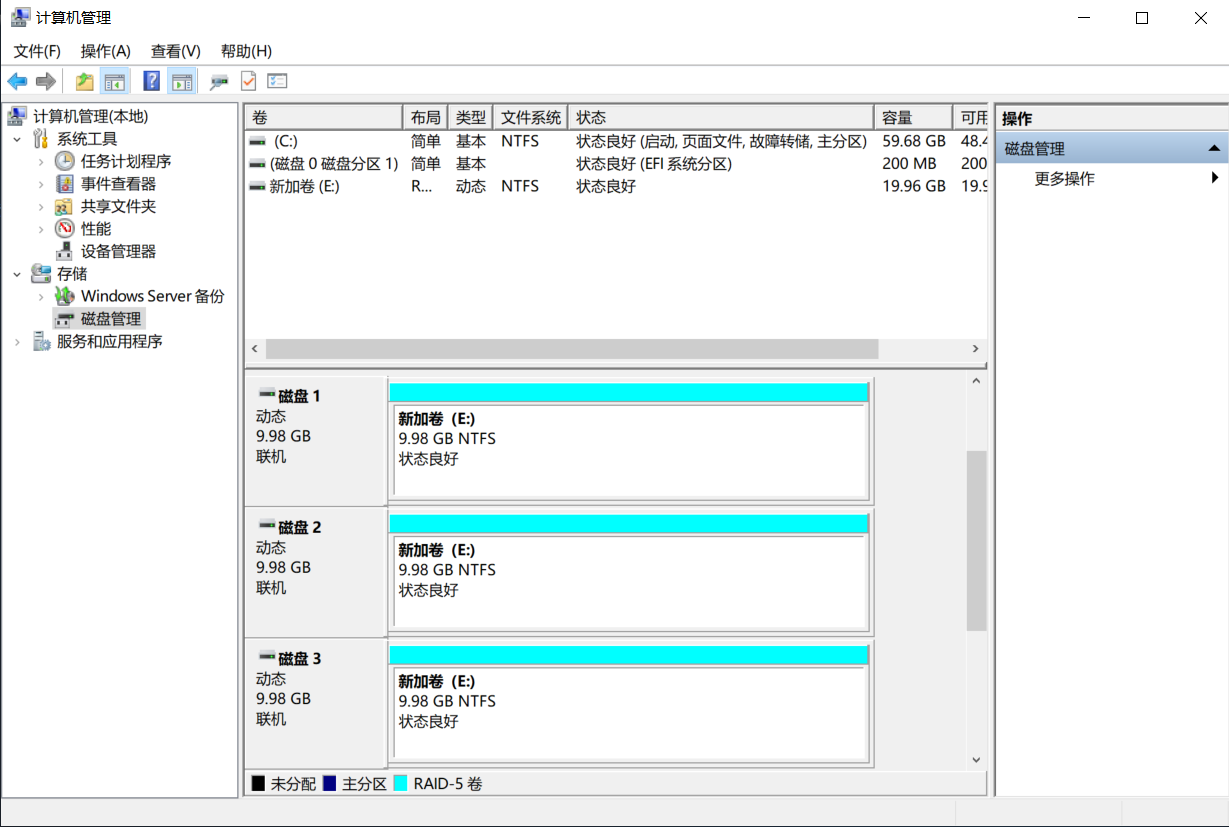
（2）选择磁盘1，磁盘2，磁盘3三块磁盘。



（3）一直选择默认选项，直至创建成功。



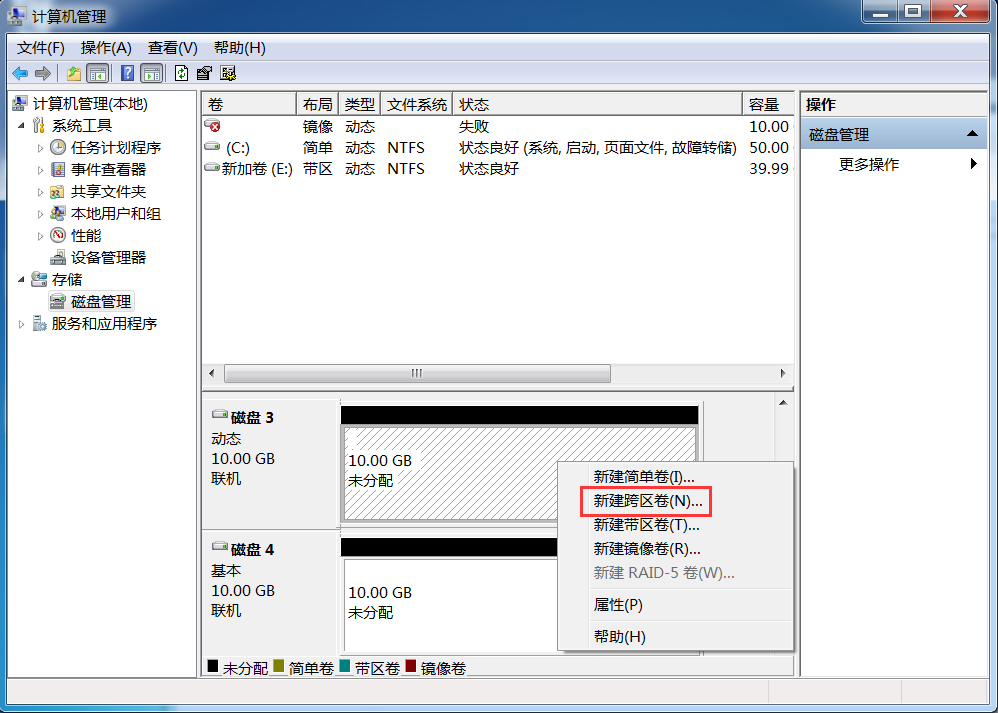
（4）可以看到RAID5已经创建成功。



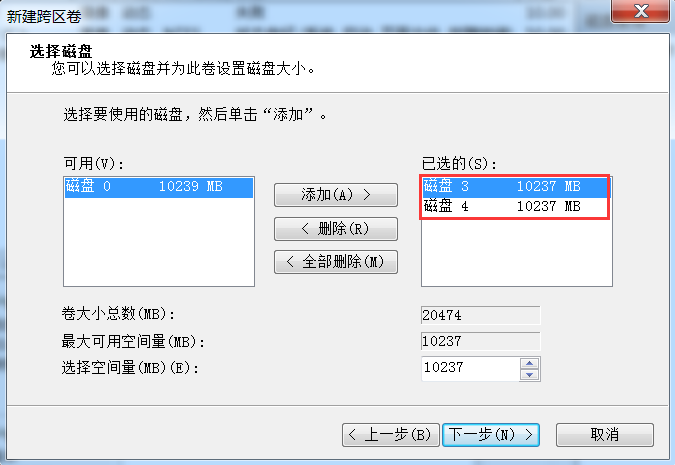


### **2.2.3 跨区卷的使用**

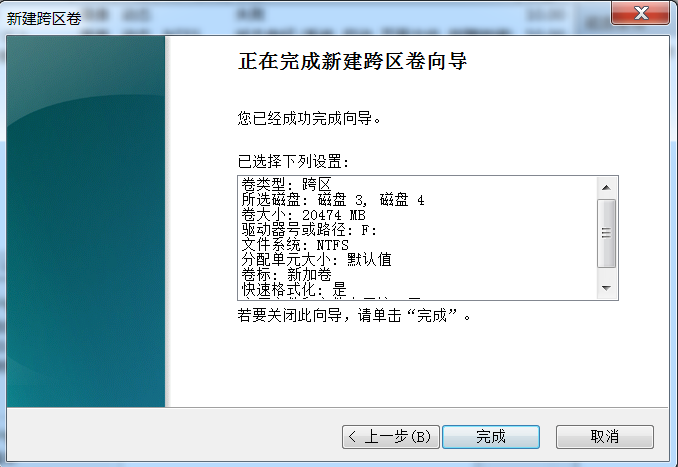
（1）跨区卷同样需要两块磁盘，右键选择新建“跨区卷”。



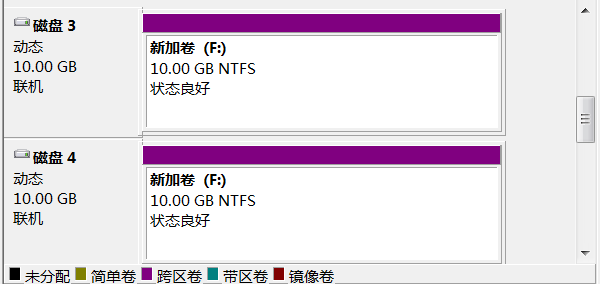
（2）选择磁盘3，磁盘4两个磁盘。

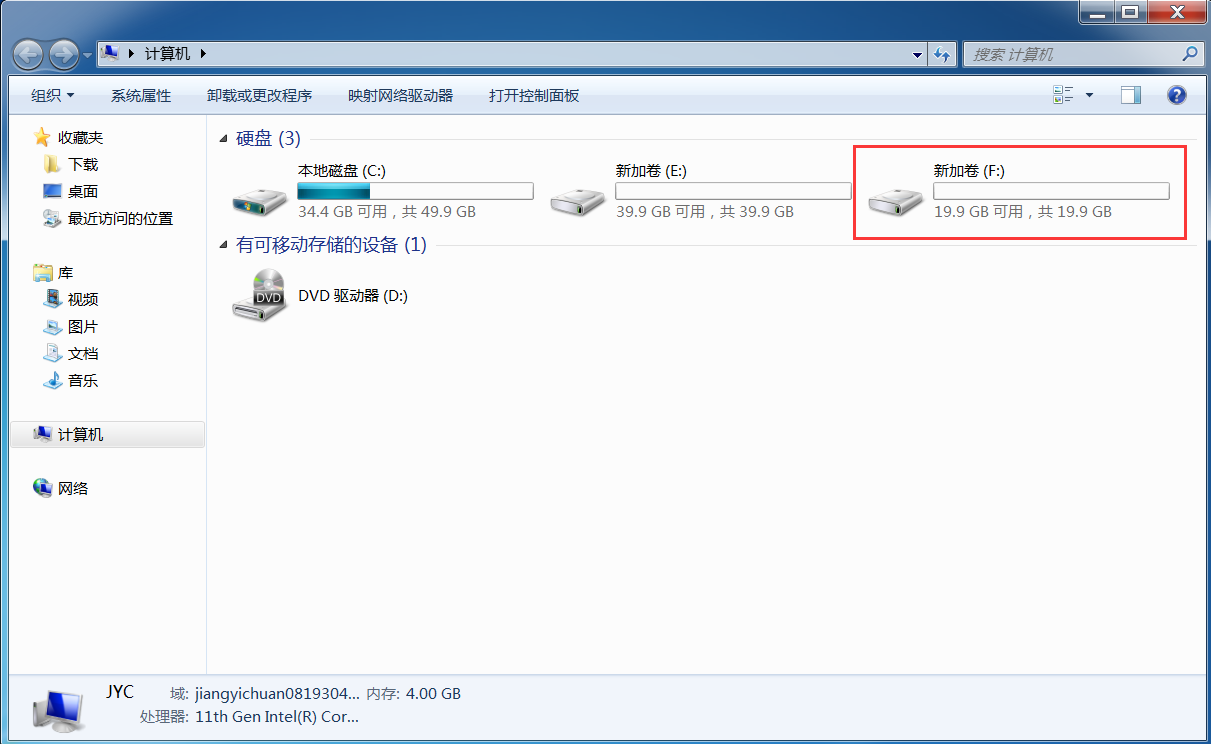


（3）一直选择默认选项，直至创建完成。



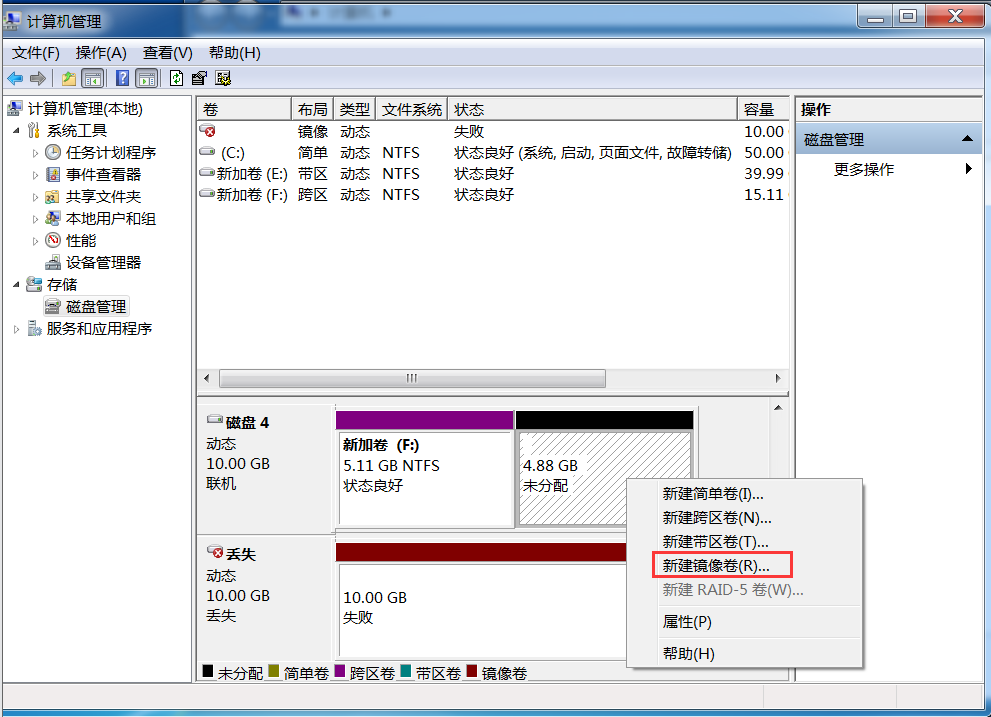
（4）可以看到跨区卷已经创建成功。



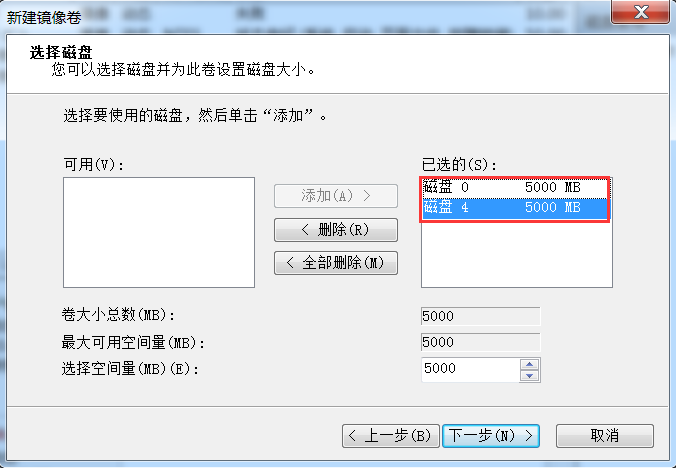


### **2.2.4 RAID1 的使用**

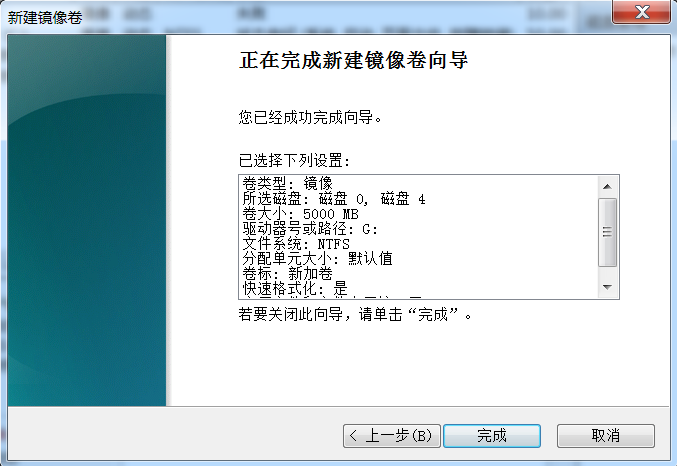
（1）RAID1同样需要两块磁盘，右键选择新建“镜像卷”。



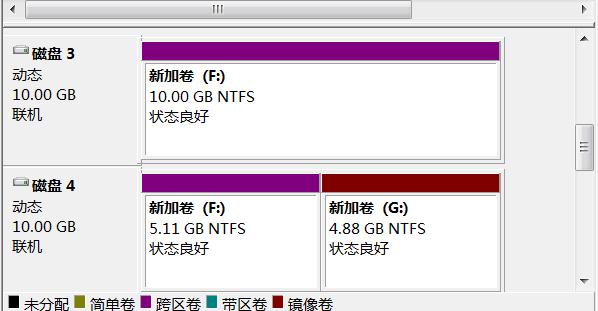
（2）选择磁盘磁盘0和磁盘4两个磁盘。

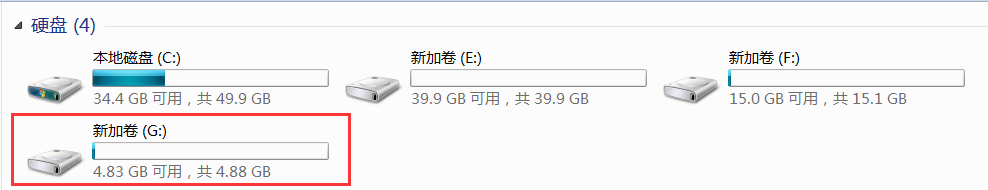


（3）一直选择默认选项直到创建完成。



（4）可以看到RAID1已经创建成功。





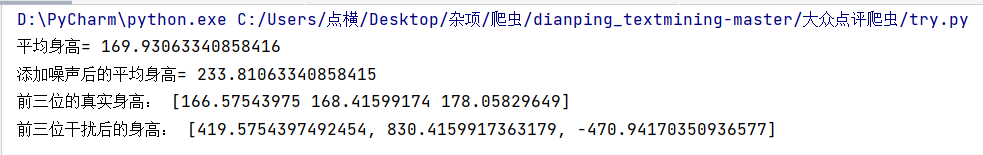
# 3 差分隐私参数的验证

## 3.1 源代码

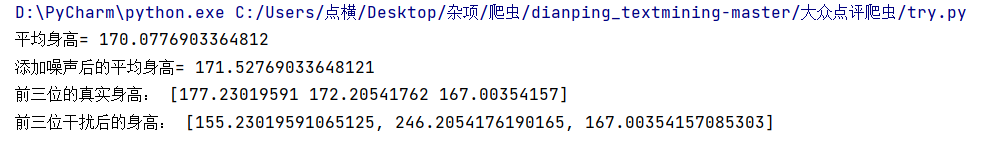
import numpy as np  
def get\_noisy(GSf, epsilon):  
 beta = GSf/epsilon  
 u=np.random.random()-0.5  
 noisy\_digit =0.0-beta\*np.sign(u)\*np.log(1.0-2\*np.abs(u))  
 return np.rint(noisy\_digit)  
  
if \_\_name\_\_=='\_\_main\_\_':  
 GSf=50 *#假设公司最高和最矮的两个人的身高差为50CM* epsilon=4  
 real\_height=np.random.normal(170,4,100)*# 随机生成100个符合正态分布的身高。* pseudo\_height=[] *#添加噪声后的身高* for i in range(100):  
 pseudo\_height.append(real\_height[i]+get\_noisy(GSf, epsilon))  
 print("平均身高=",np.average(real\_height))  
 print("添加噪声后的平均身高=",np.average(pseudo\_height))  
 print("前三位的真实身高：",real\_height[:3])  
 print("前三位干扰后的身高：",pseudo\_height[:3])

## 3.2 验证

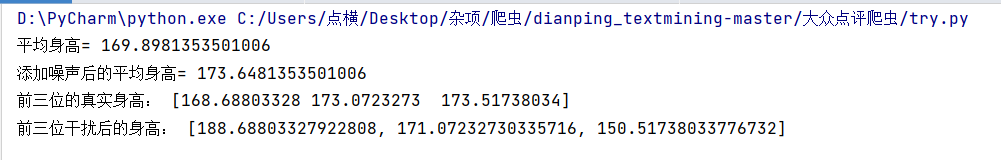
（1）epsilon=0.1



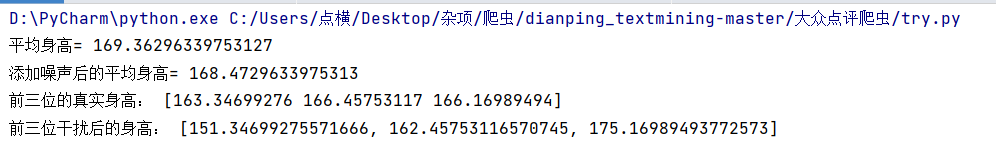
（2）epsilon=1



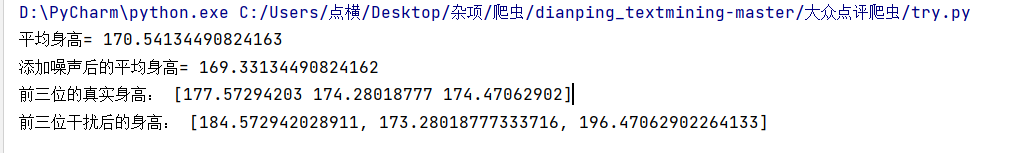
（3）epsilon=3



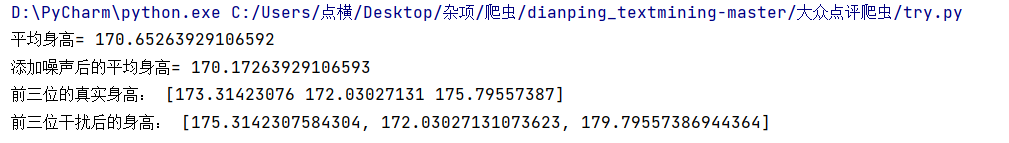
（4）epsilon=5



（5）epsilon=7



（6）epsilon=10



## 3.3 结论

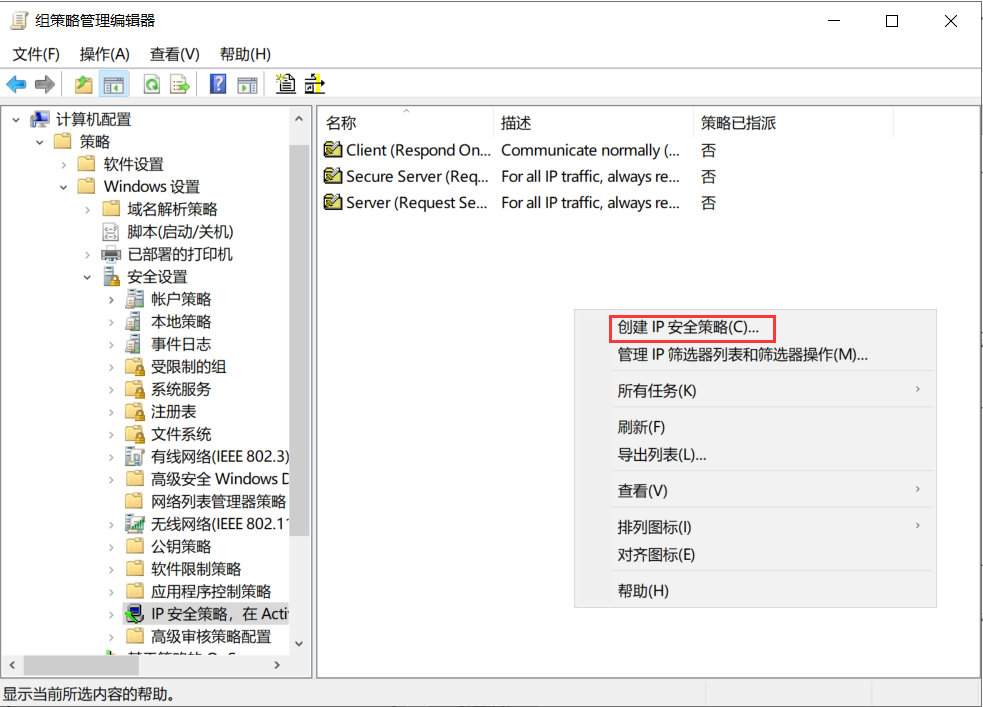
可以看到epsilon的取值越接近0，噪声越大，泄露风险越小，研究价值也越小。

epsilon越大，噪声越小，泄露的风险越大，但是研究价值也越大。

# 4 VPN的设置和使用

## 4.1 主机对主机的IPSEC使用

（1）在根域服务器（192.168.121.101）上打开“组策略管理编辑器”，在“IP安全策略”中选择“创建IP安全策略”。



（2）自定义IP安全策略名称。



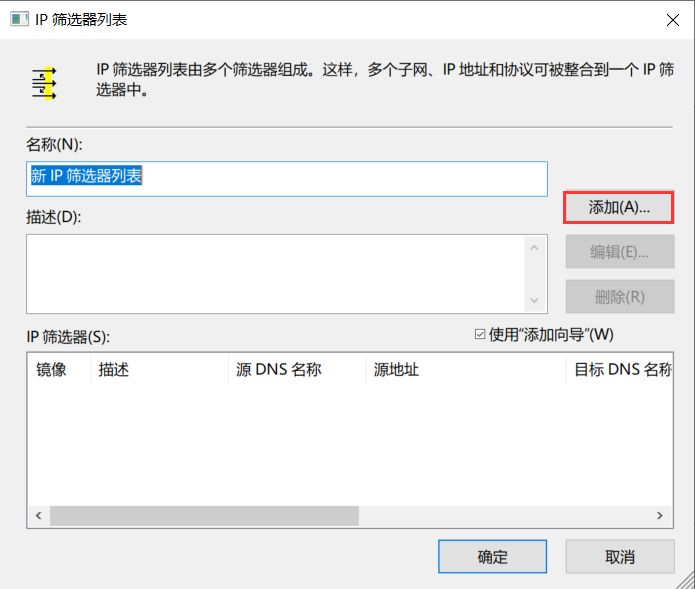
（3）编辑IP安全策略的属性，点击添加新的IP安全规则。



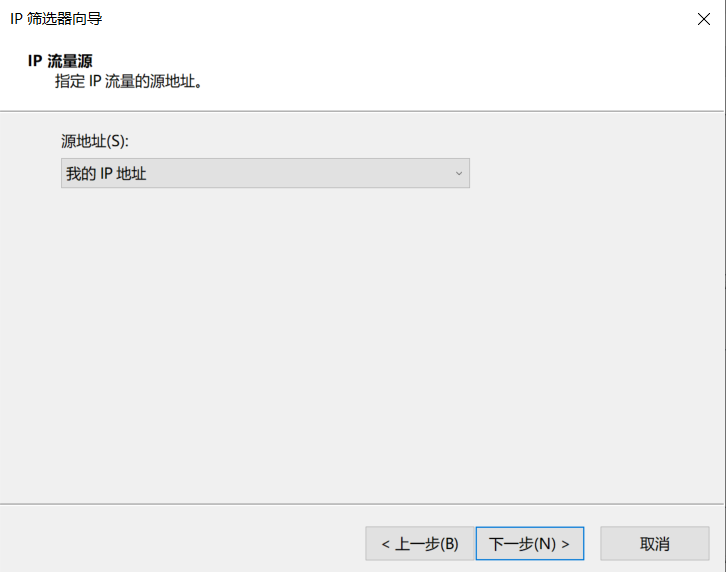
1. 添加新的IP筛选器列表。



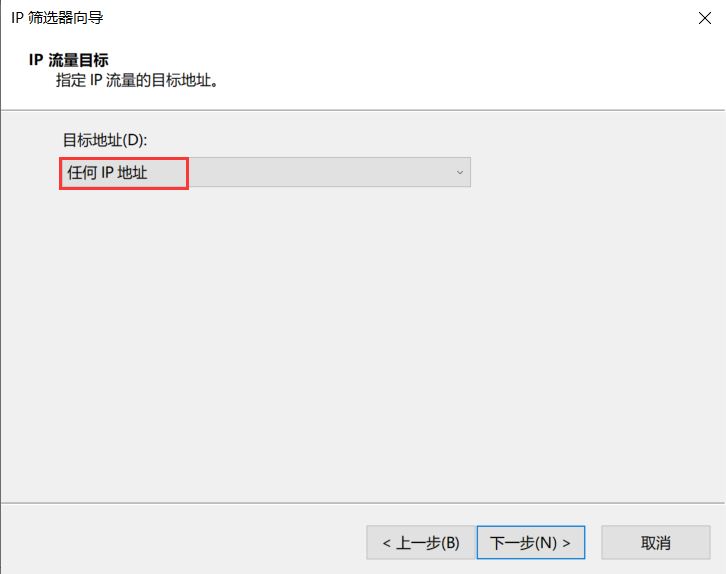
（6）对筛选器列表进行编辑。



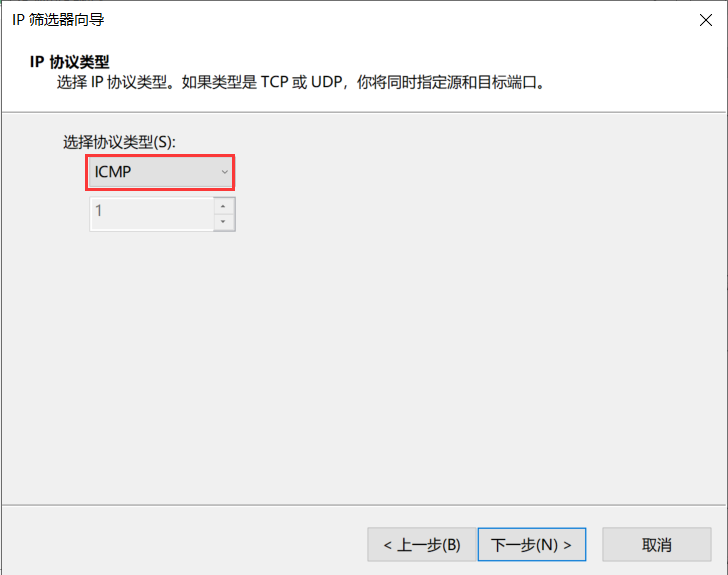
（7）选择“我的IP地址”为IP流量源选择。



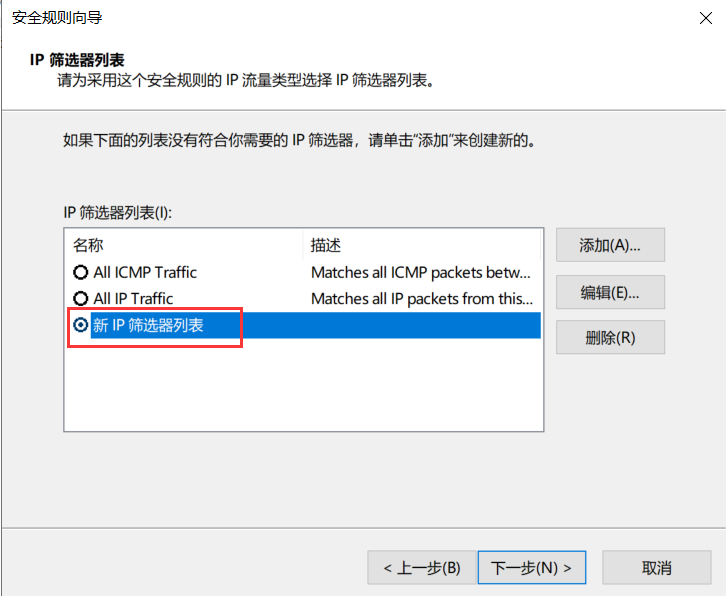
（8）选择“任何IP地址”为IP流量目标。



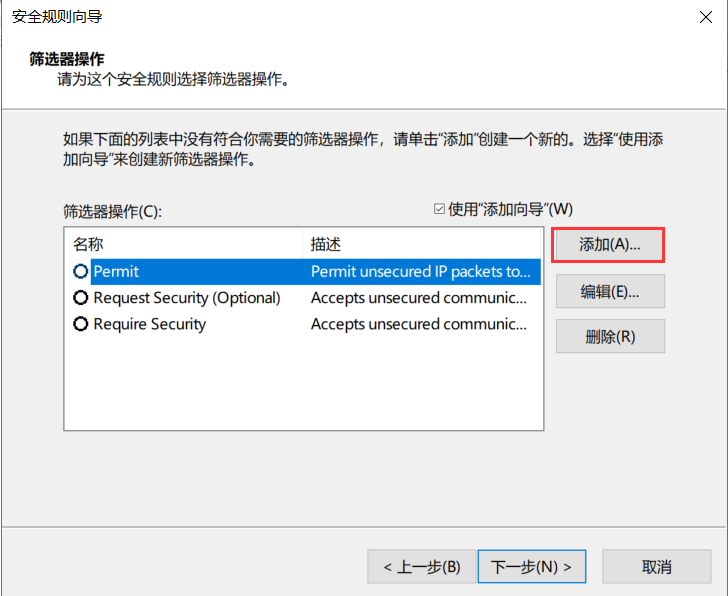
（9）选择ICMP为IP协议类型。



（10）选择新创建的IP筛选器。



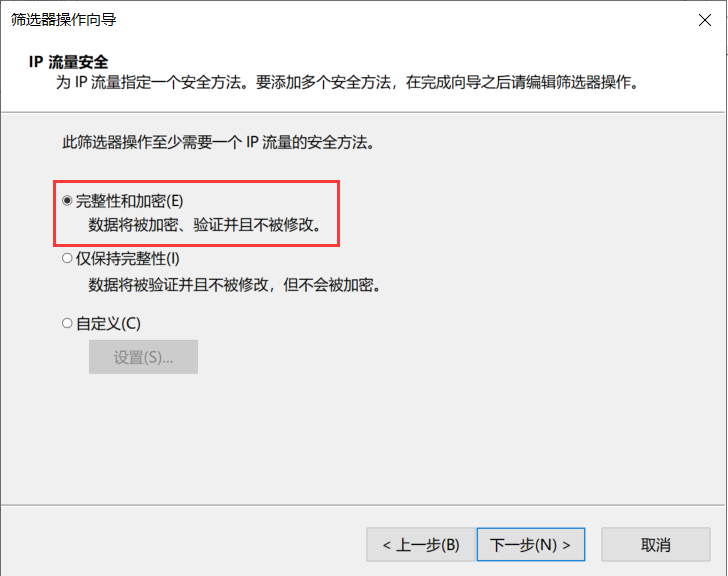
（11）选择“筛选器操作”，点击“添加”。



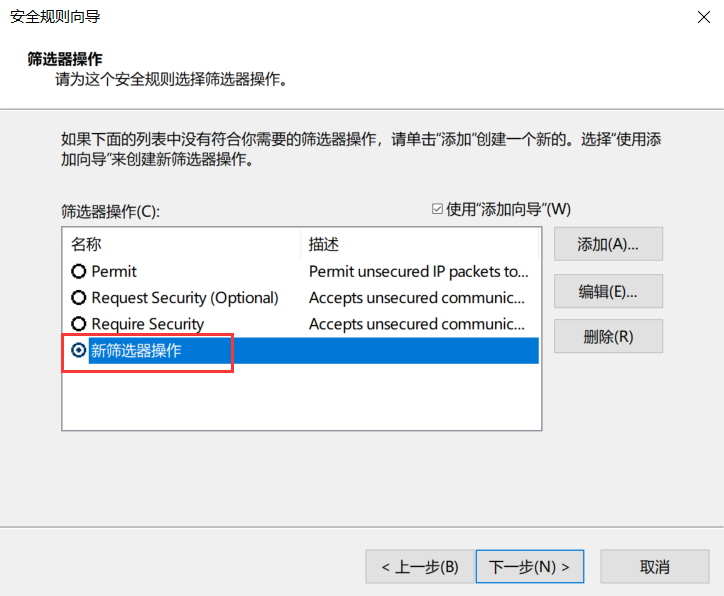
（12）选择“协商安全”。



（13）设置“IP流量安全”为“完整性和加密”。



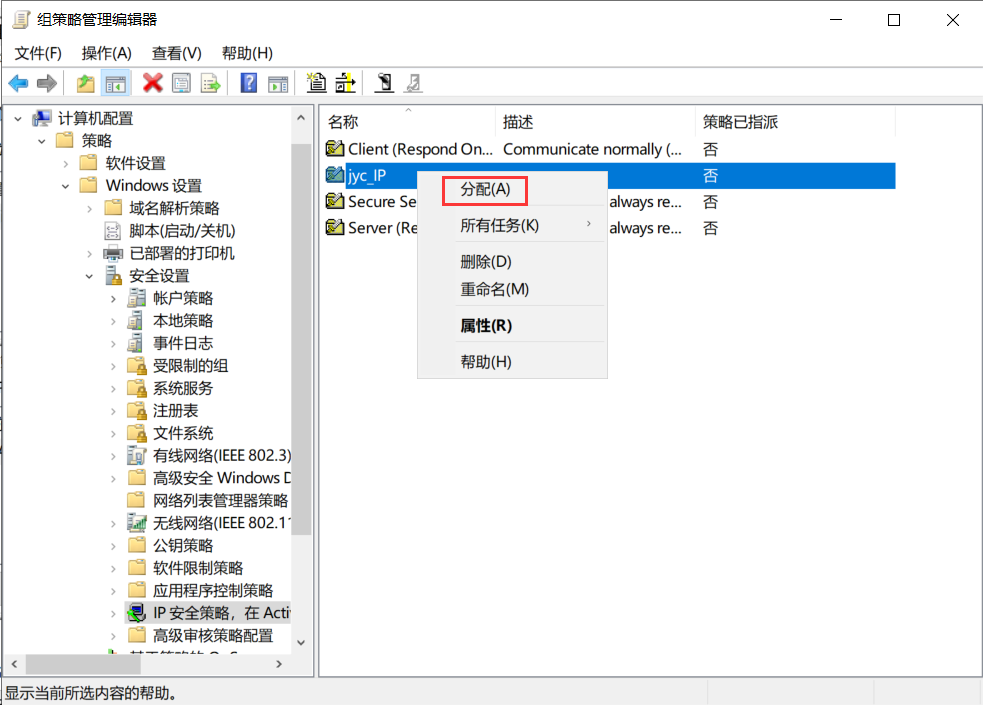
（14）选择刚创建的筛选器操作，并点击下一步。



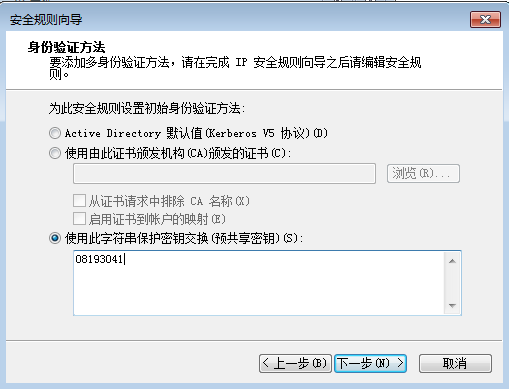
（15）选择预共享密钥，并自定义密钥为08193041，编辑完成后将“IP 安全规则”设置为“新 IP 筛选器列表”。

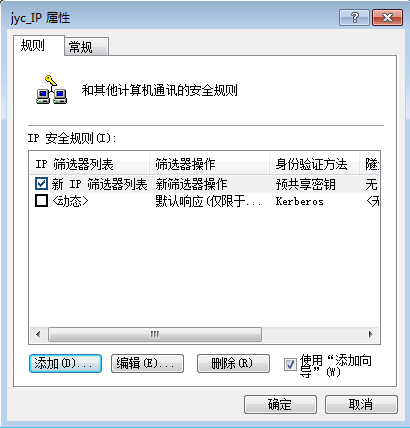


（16）进行组策略指派。

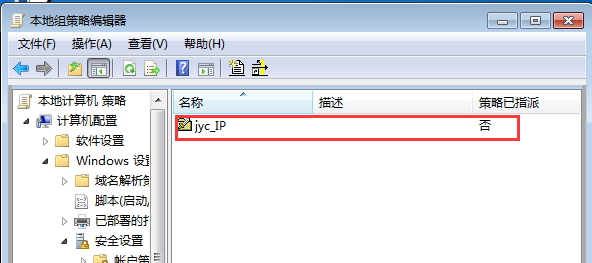


（17）接着在和域控服务器进行通信的客户机（192.168.121.105）上以同样的方式建立“IP安全规则”，与共享密钥同样设置为08193041。



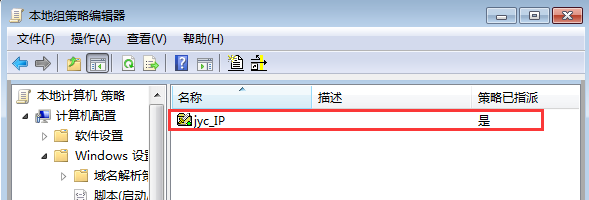


（18）可以看到在客户机未指派该“IP安全策略”前，两台计算机无法ping通。





（19）将客户机的“IP安全规则”也进行指派后，两台计算机相互可以ping通，成功实现了端到端的加密安全传输。





## 4.2 站点对站点的VPN使用

**实验拓扑：**

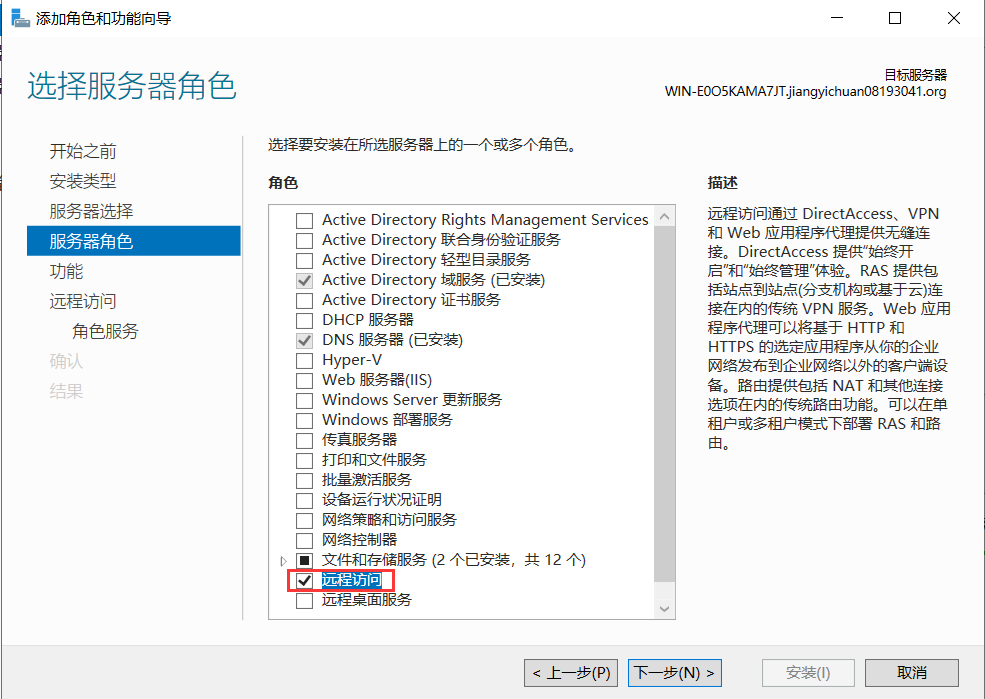
① 一台Windows Server 2019作为AD域控制器和RADIUS服务器，位于192.168.121.0/24子网，IP地址为：192.168.121.101。

② 一台Windows 7作为远程用户客户机，位于192.168.110.0/24子网，IP 地址为：192.168.110.112。

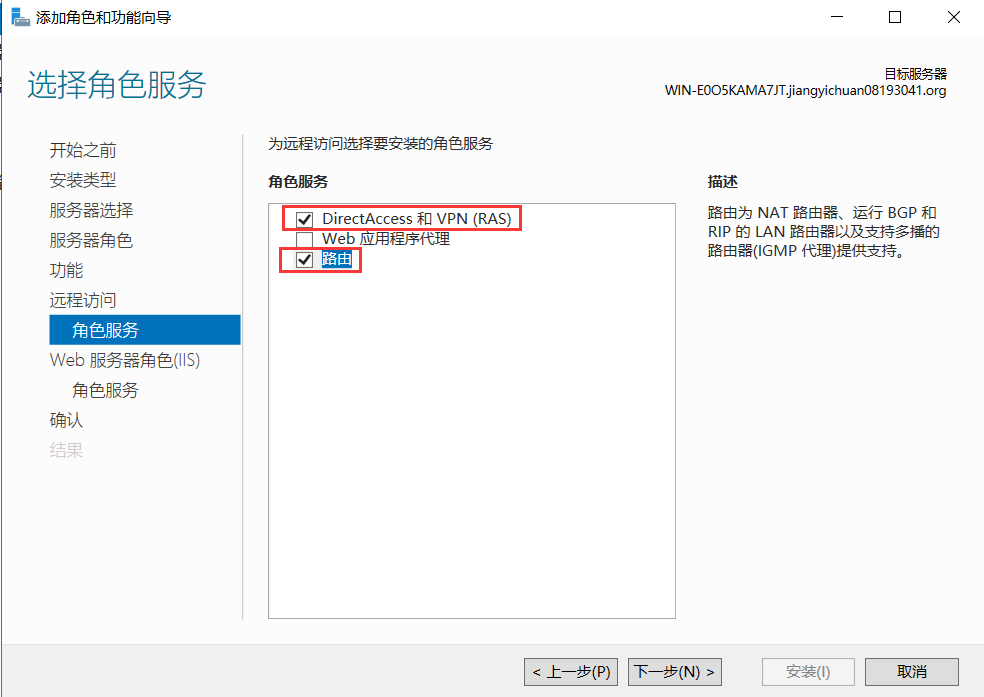
③ 一台Window Server 2019作为VPN网关，内网网卡IP 地址为：192.168.121.103，外网网卡 IP 地址为：192.168.110.111

（1）设置windows 7客户机的ip地址为192.168.110.112，DNS服务器地址为域控服务器的ip地址192.168.121.101，将VPN网关服务器的两个网卡分别设置为内网网卡192.168.121.103和外网网卡192.168.110.111。

（2）在VPN网关服务器上安装“远程访问”功能。



（3）选择“VPN”和“路由”服务。



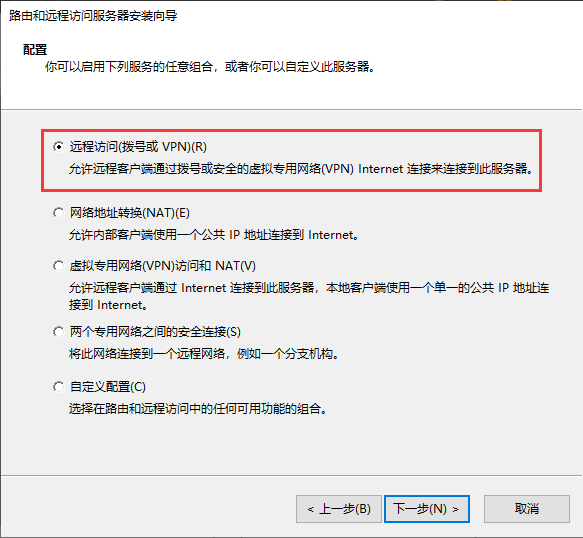
（4）其它选项均选择默认配置，直至安装完成。



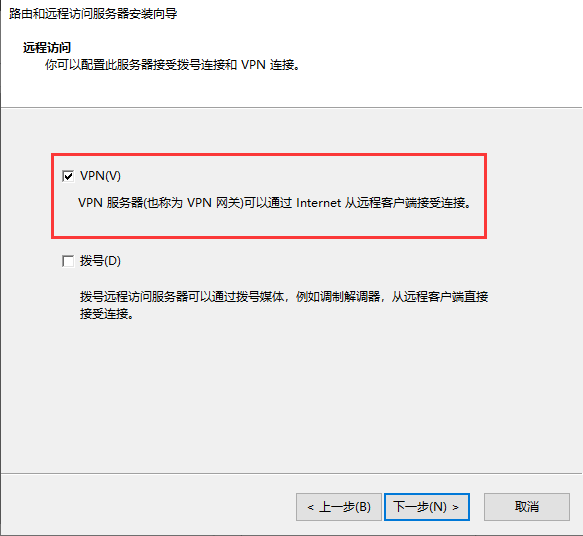
（5）进入“路由和远程访问”进行配置。



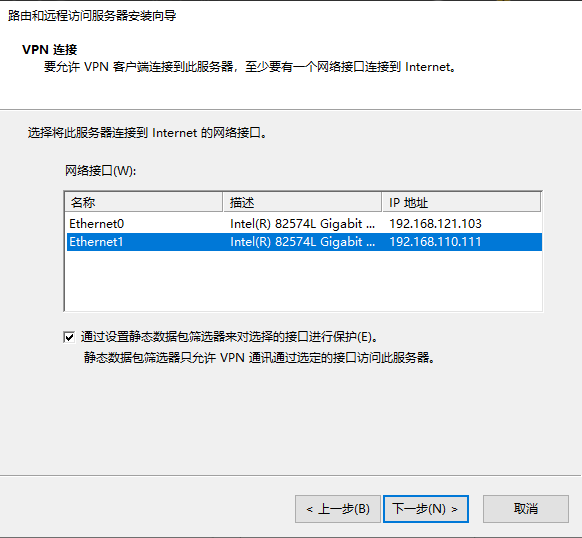
（6）选择“远程访问（拨号或VPN）”。



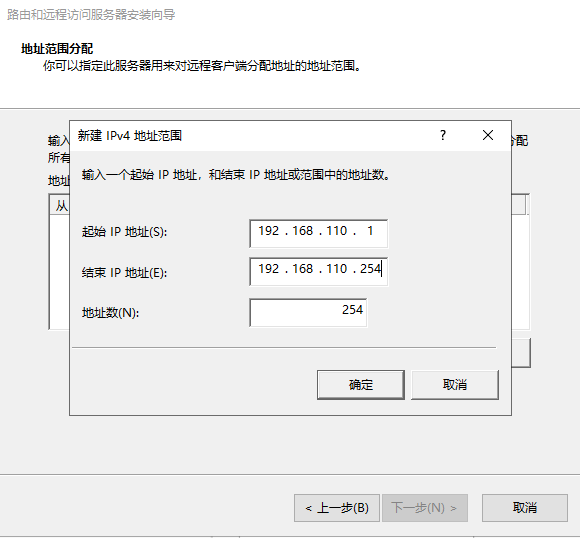
（7）选择“VPN”。



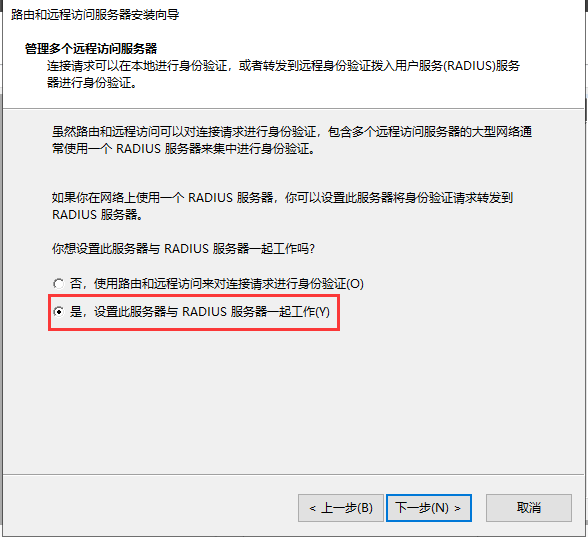
（8）选择外网网卡。



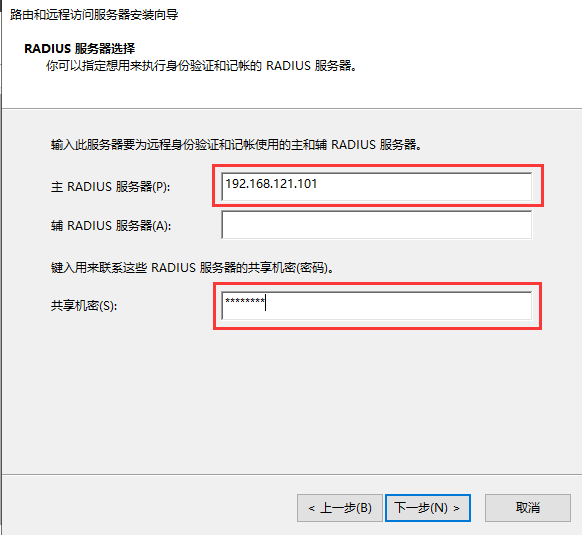
（9）设置VPN客户端网段。



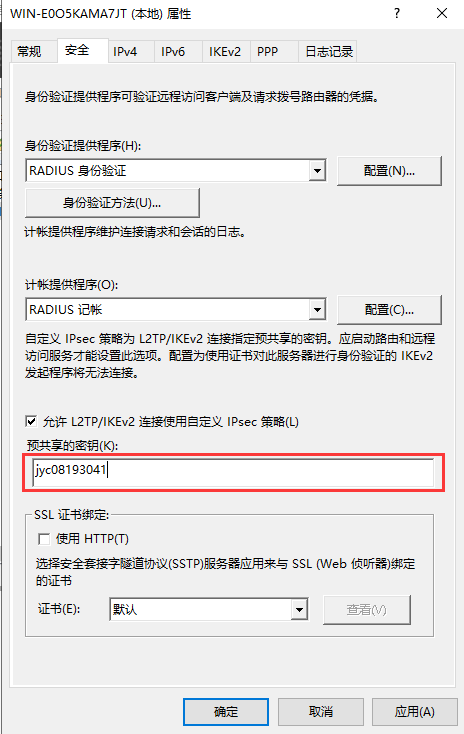
（10）选择使用RADIUS服务器进行验证。



（11）设置RADIUS服务器地址以及共享密钥。



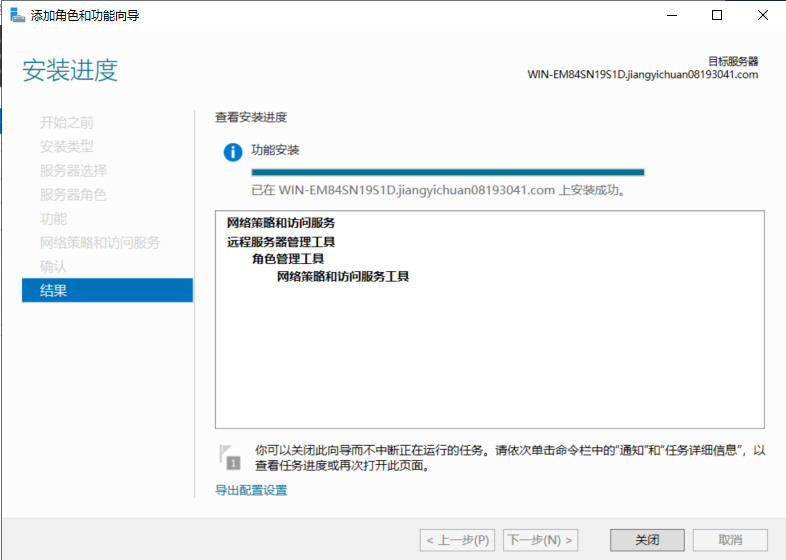
（12）配置完成后，进入“属性->安全”，设置L2TP/IKEv2的预共享密钥为 jyc08193041。



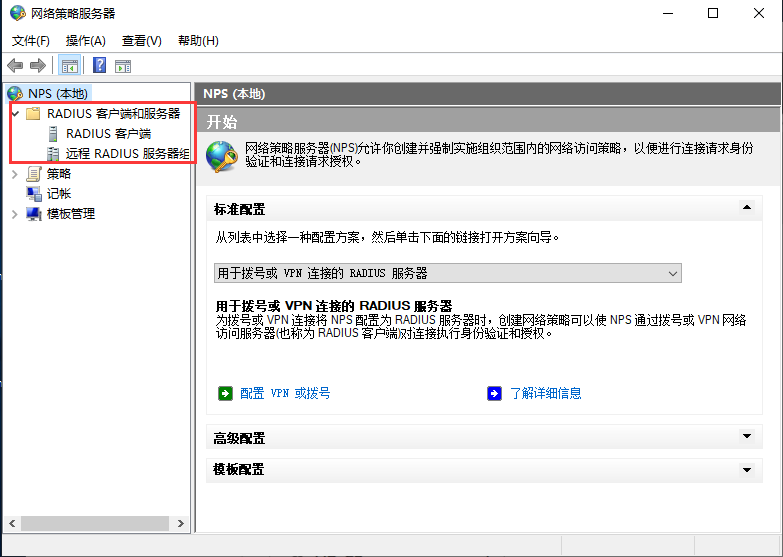
（13）打开“添加角色和功能向导”，并安装“网络策略和访问服务”。



（14）其余选项均选择默认配置，直到安装完成。



（15）可以看到RADIUS服务成功安装。



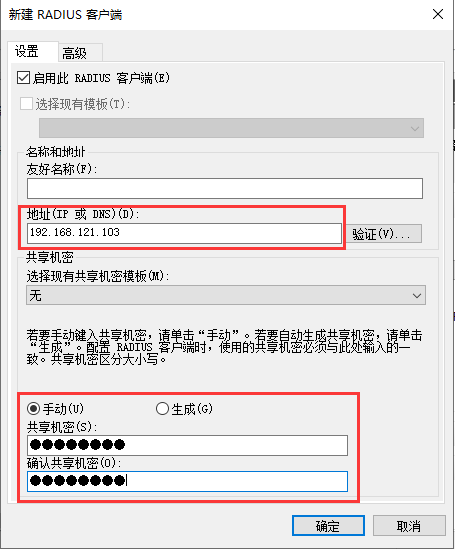
（16）安装完成后，在AD注册服务器。



（17）将VPN服务器新建为RADIUS客户端。



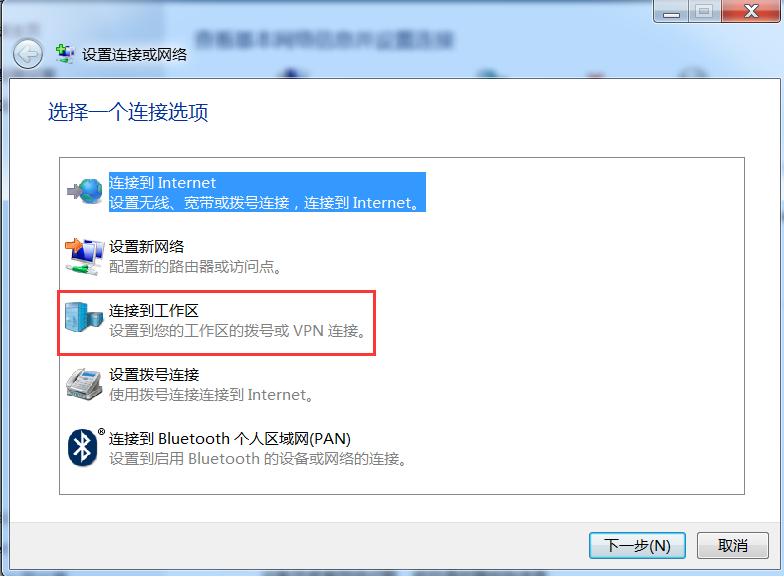
（18）输入VPN服务器内网网卡地址以及设置的共享密码。



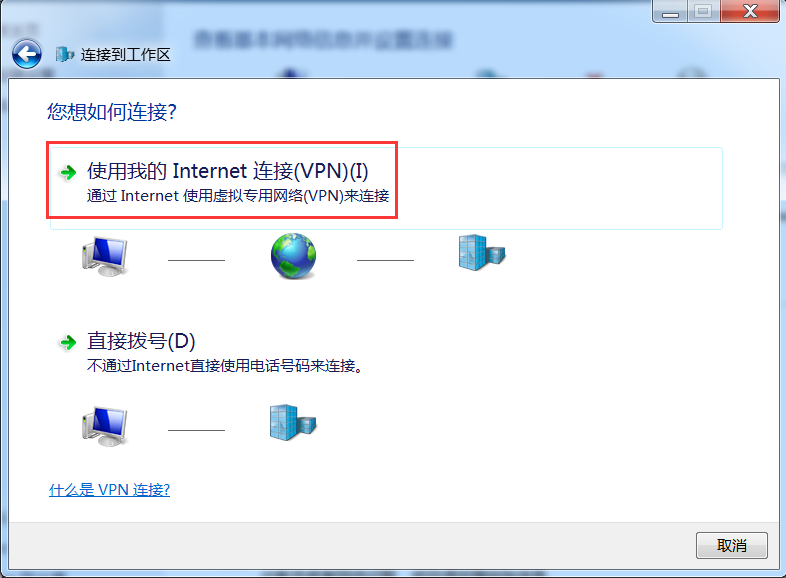
（19）最后设置用于登录VPN的域账户的访问权限。



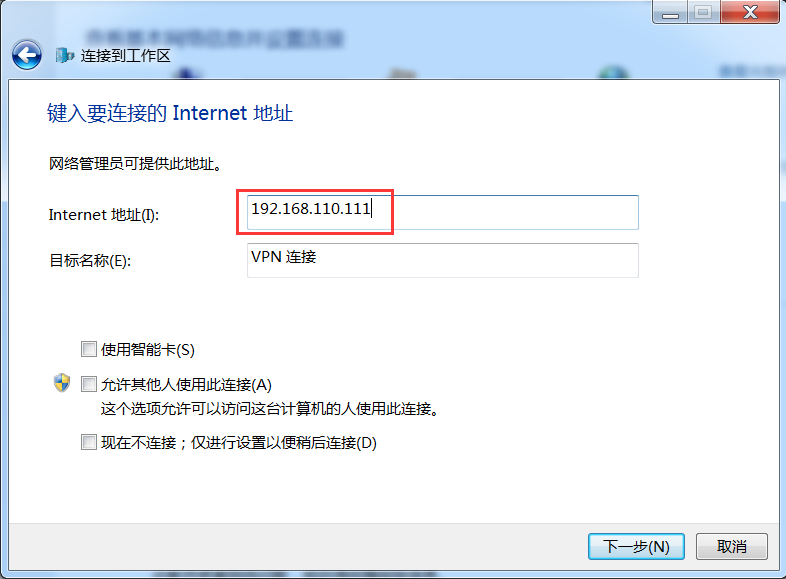
（20）登录客户机，进入“设置连接或网络”，选择“连接到工作区”。



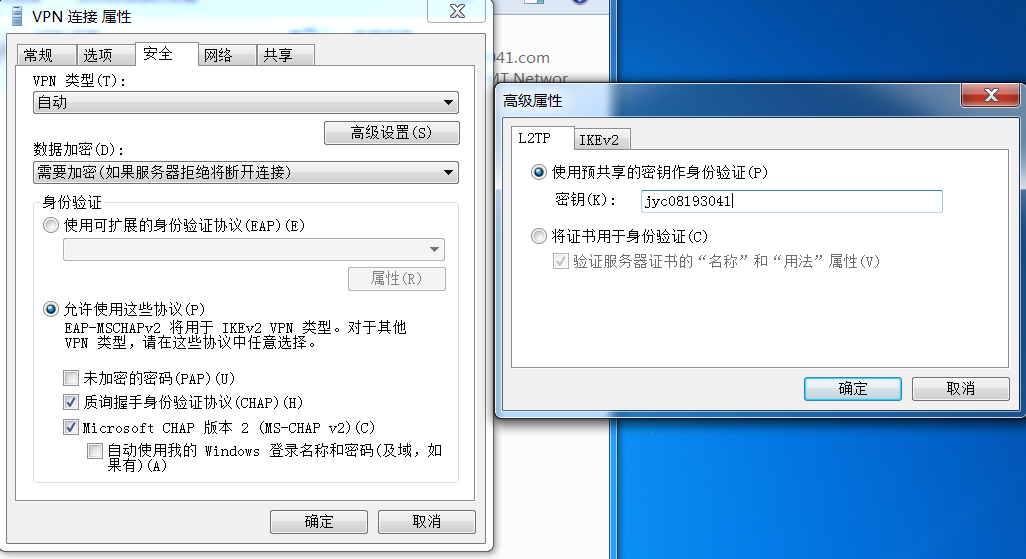
（21）选择VPN。



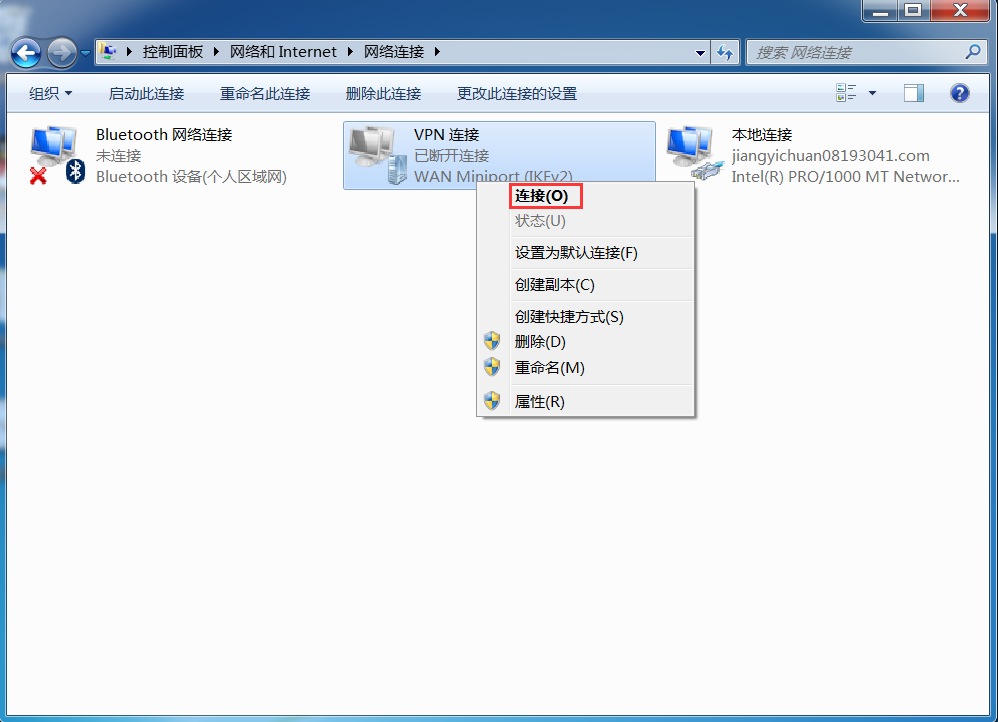
（22）选择“稍后设置 Internet 连接"，接着设置 VPN 服务器的外网网卡地址。



（23）设置完成后可以看到新建的 VPN 连接，点击“属性->安全”，选择“L2TP”并在“高级设置中”设置 L2TP 的预共享密钥。



（24）配置完成后，右键选择“连接”。



（25）输入设置过权限的域用户及密码。



（26）可以看到VPN连接成功。

