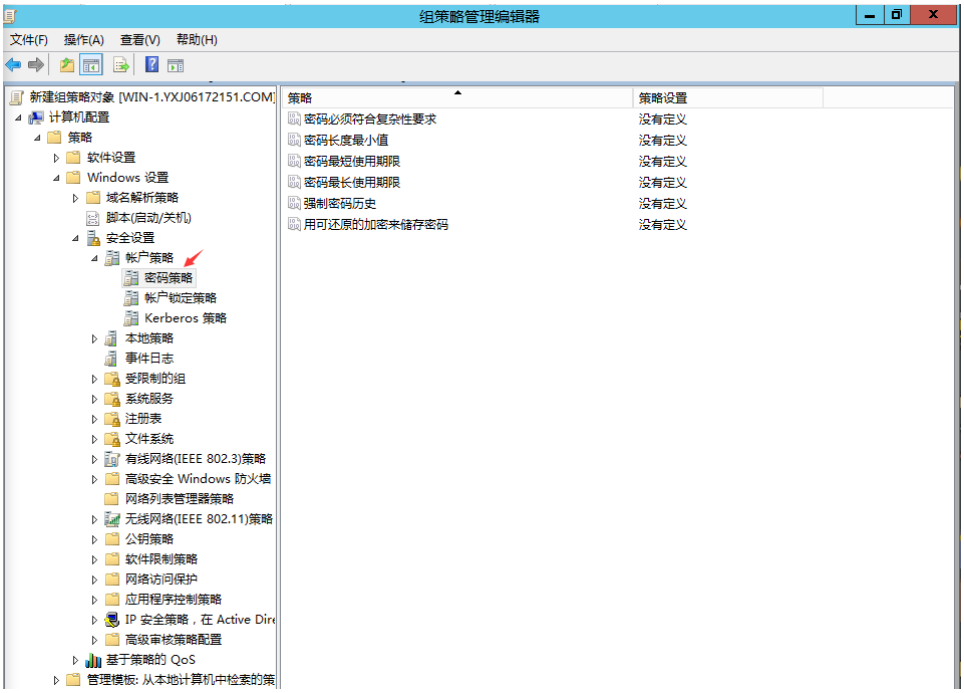
目　录

1 配置域边界认证安全策略

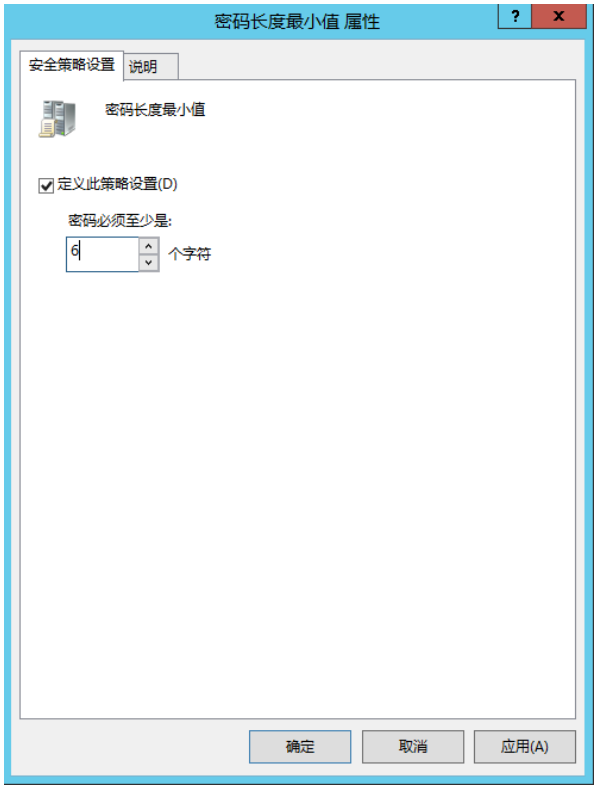
1.1 密码策略

（1）在域控中打开组“策略管理编辑器”—“Windows 设置”—“安全设置”—“账户策略”—“密码策略”：

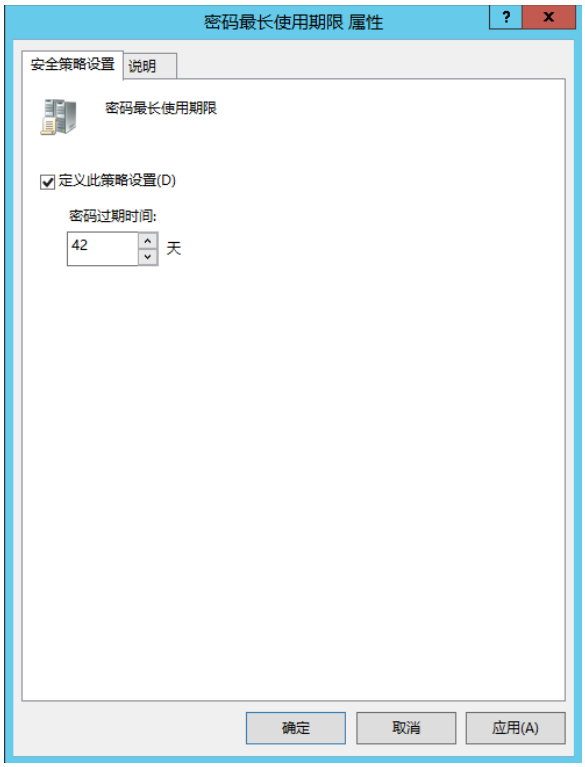


（2）然后可以对账户密码进行安全策略的配置，如下对密码长度和使用期限等的配置：

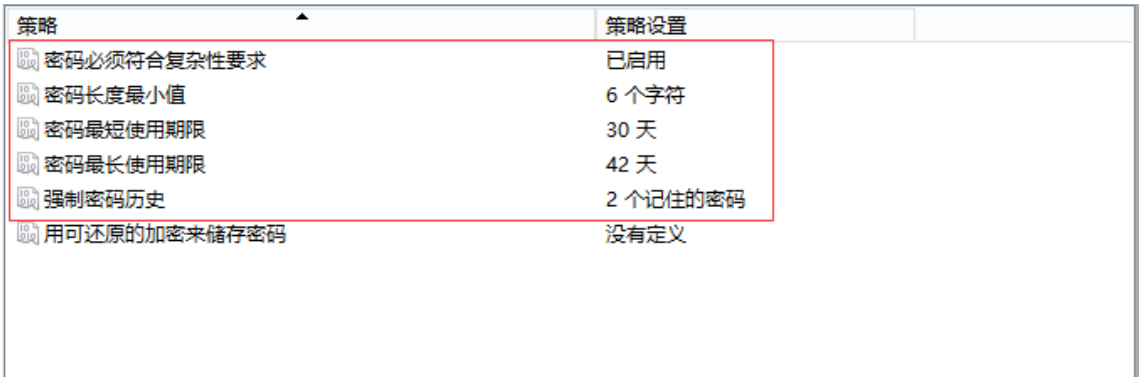
①密码长度最小值：


密码长度最小值 属性
安全策略设置
说明
密码长度最小值
定义此策略设置(D)
密码必须至少是:
6
个字符
确定
取消
应用(A)

② 密码最长使用期限：

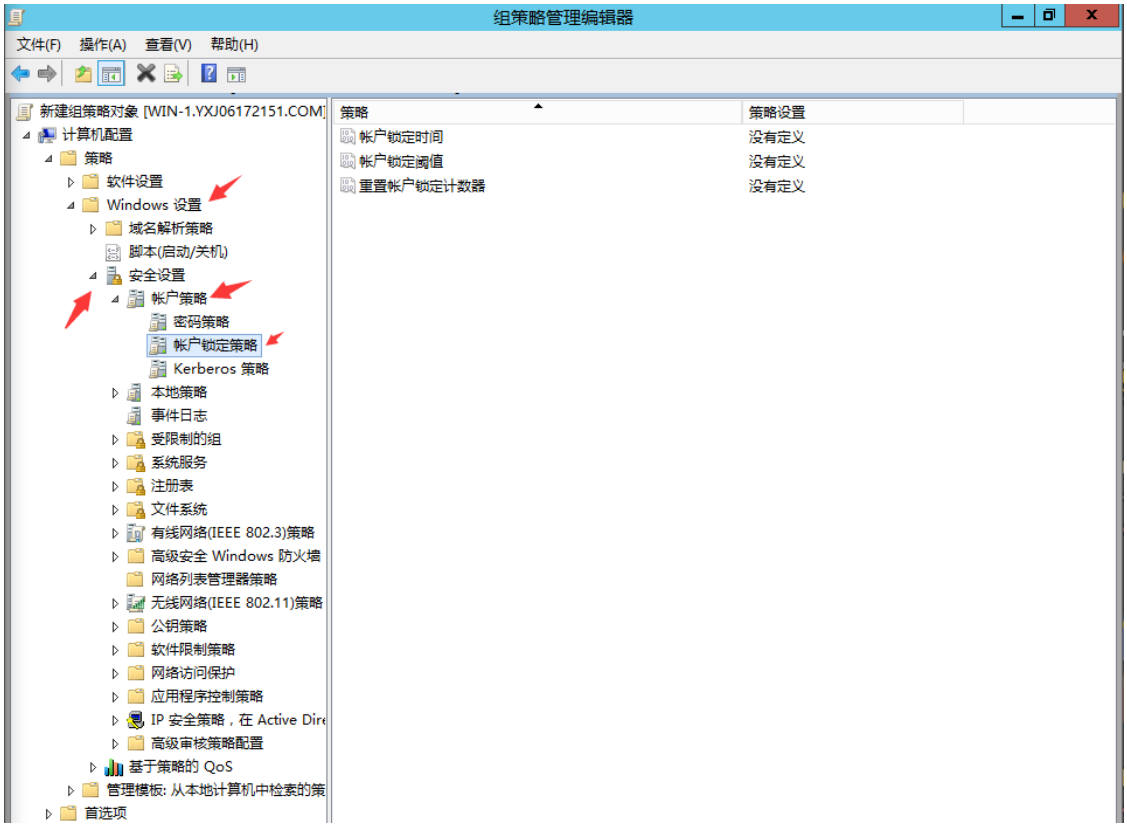

密码最长使用期限 属性
安全策略设置
说明
密码最长使用期限
定义此策略设置(D)
密码过期时间:
42
天
确定
取消
应用(A)

（3）配置后策略如下：

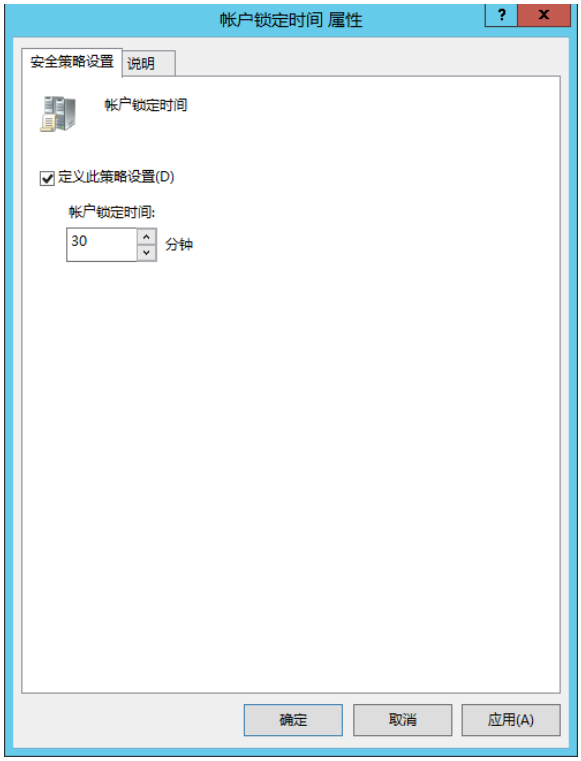


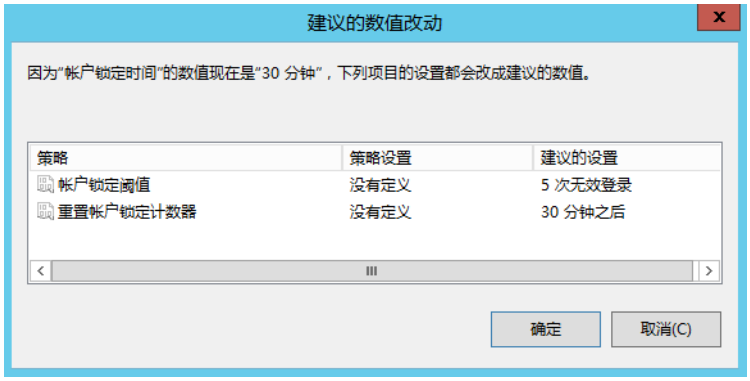
1.2 账户锁定策略

（1）在域控中打开组“策略管理编辑器”—“Windows 设置”—“安全设置”—“账户策略”—“账户锁定策略”：

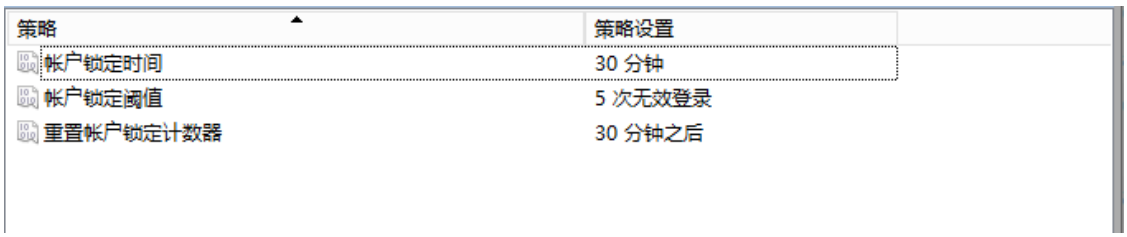


（2）然后可以对账户锁定策略进行一定的安全配置，如账户锁定时间、账户锁定阈值、重置账户锁定计数器：



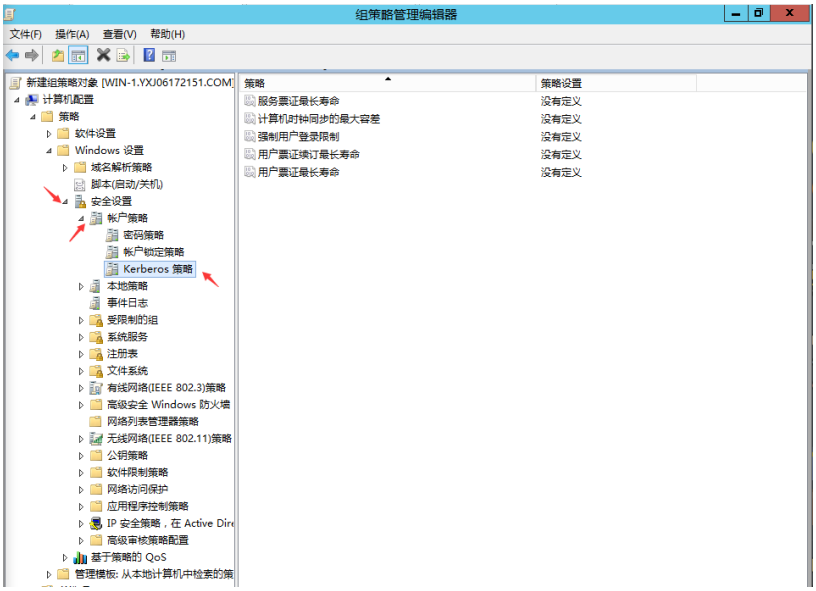


（3）配置后策略如下：

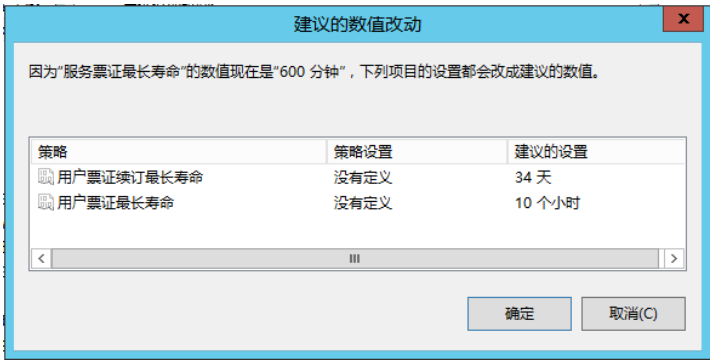


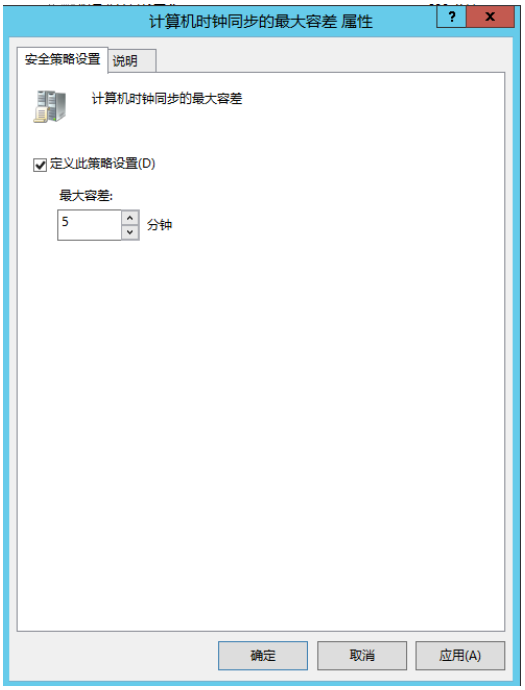
1.3 Kerberos 策略

（1）在域控中打开组“策略管理编辑器”—“Windows 设置”—“安全设置”—“账户策略”—“Kerberos 策略”：



（2）然后可以对 Kerberos 协议进行一些安全策略的配置，如服务票证最长寿命、强制用户登录限制、用户票证最长寿命等：


建议的数值改动
因为"服务票证最长寿命"的数值现在是"600 分钟"，下列项目的设置都会改成建议的数值。
策略
策略设置
建议的设置
用户票证续订最长寿命
没有定义
34 天
用户票证最长寿命
没有定义
10 个小时
确定
取消(C)

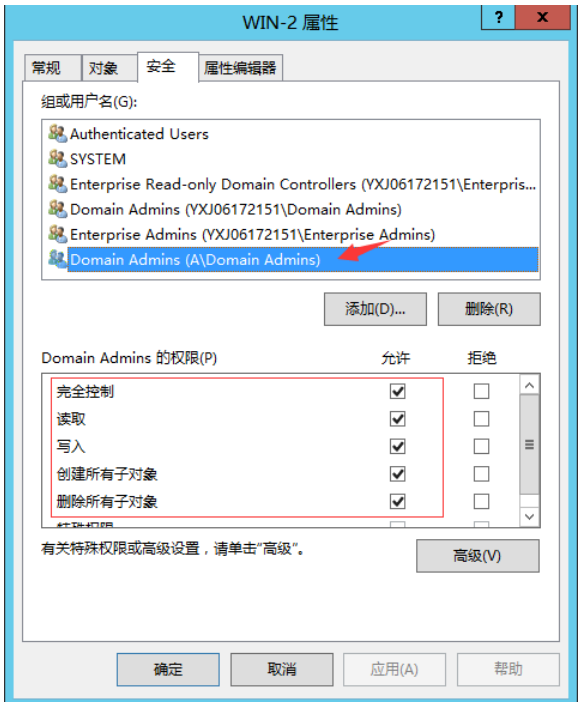

计算机时钟同步的最大容差 属性
安全策略设置
说明
计算机时钟同步的最大容差
定义此策略设置(D)
最大容差:
5
分钟
确定
取消
应用(A)

（3）配置后策略如下：

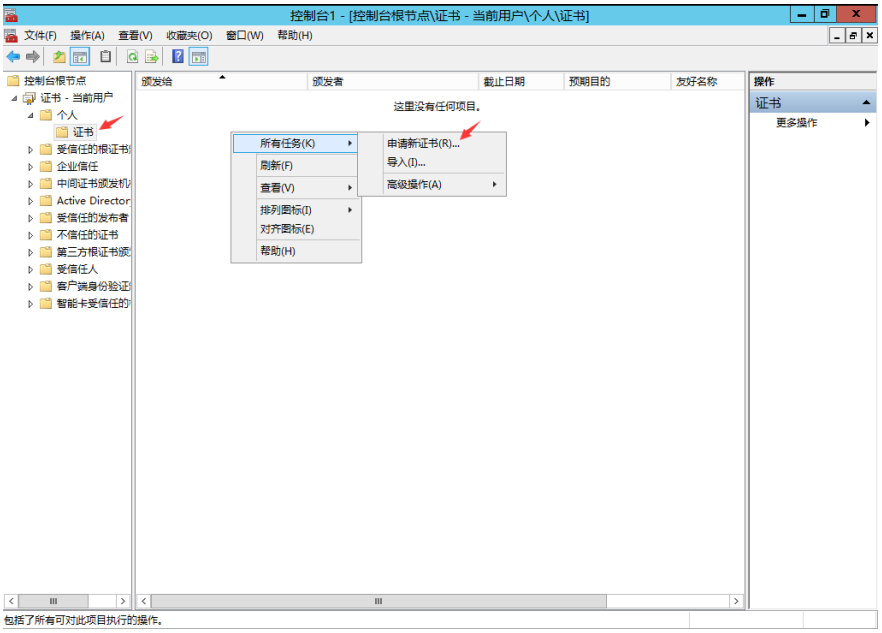

策略
策略设置
服务票证最长寿命
600 分钟
计算机时钟同步的最大容差
5 分钟
强制用户登录限制
已启用
用户票证续订最长寿命
34 天
用户票证最长寿命
10 个小时

2 PKI 服务跨域申请证书

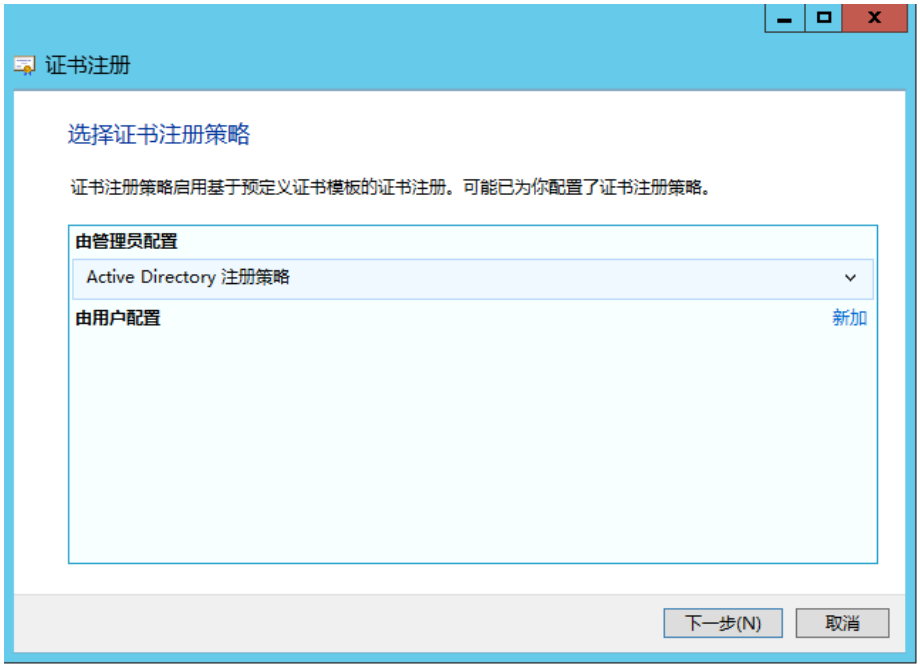
（1）首先需要保证域控及客户机的时钟同步，然后对子域用户赋予申请证书的权限，然后用子域（a.yxj06172151.com）用户登录客户机进行证书申请：



（2）打开证书控制台，选择“申请新证书”：

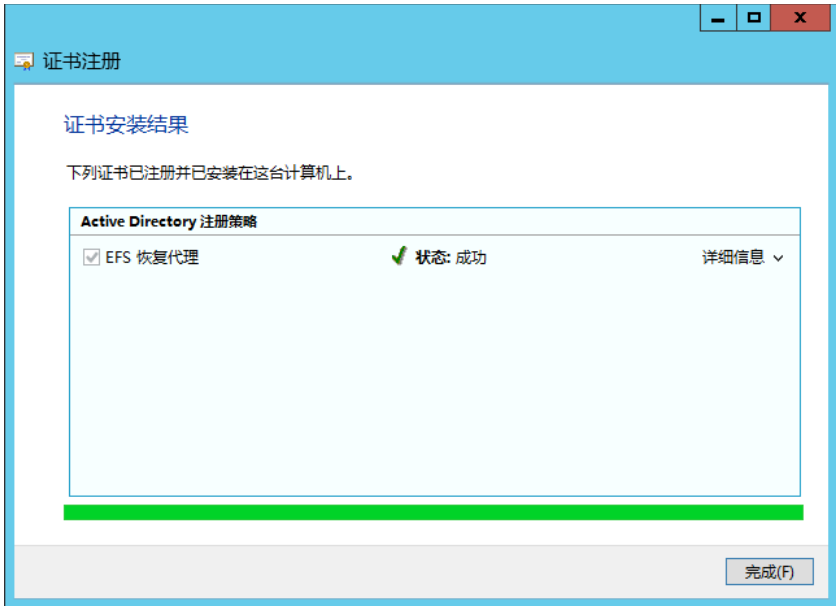


（3）依次选择“下一步”：

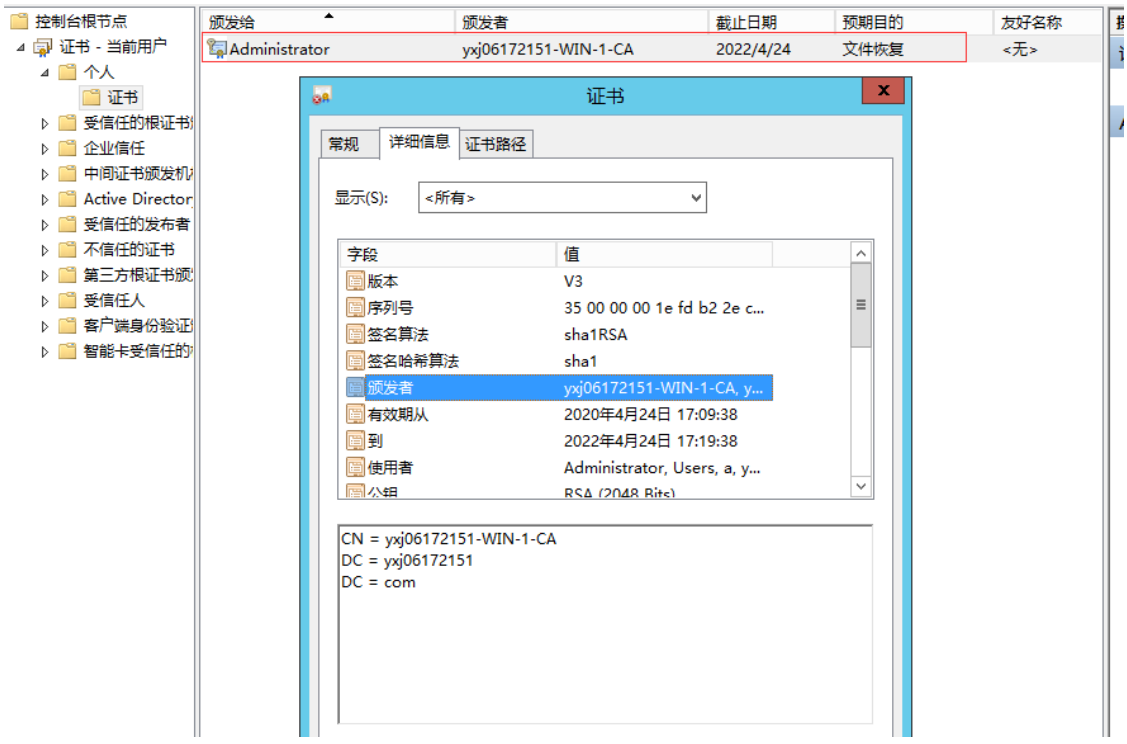


（4）选择一个证书类型：

证书申请成功：



（5）可以看到申请的证书，透明实现了 Kerberos 服务认证：

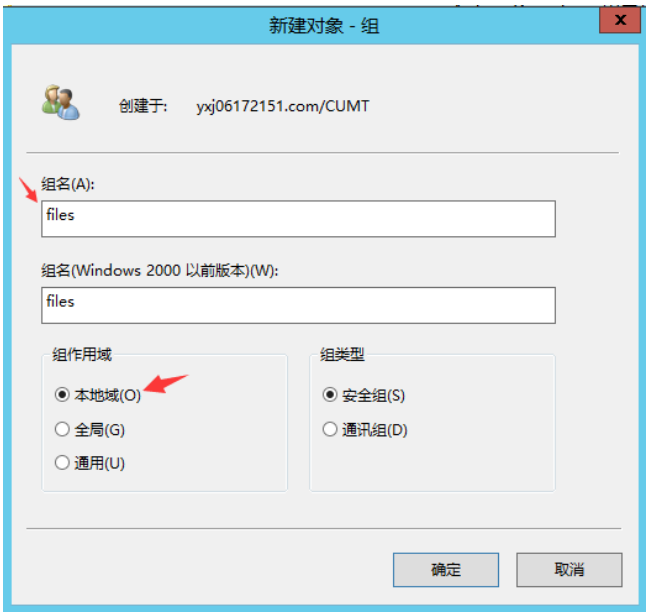


3 利用域本地组、全局组、通用组实现分布式访问控制

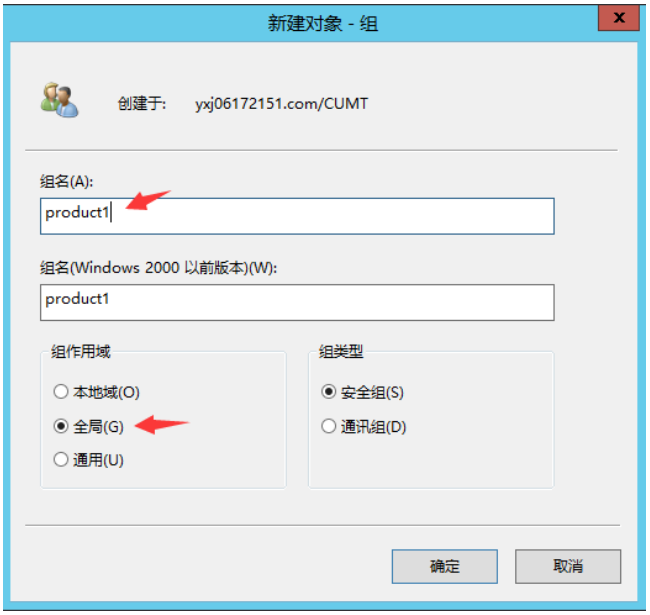
3.1 资源访问控制

（1）在顶域 yxj06172151.com 中分别创建本地组“files”和全局组“product1”。

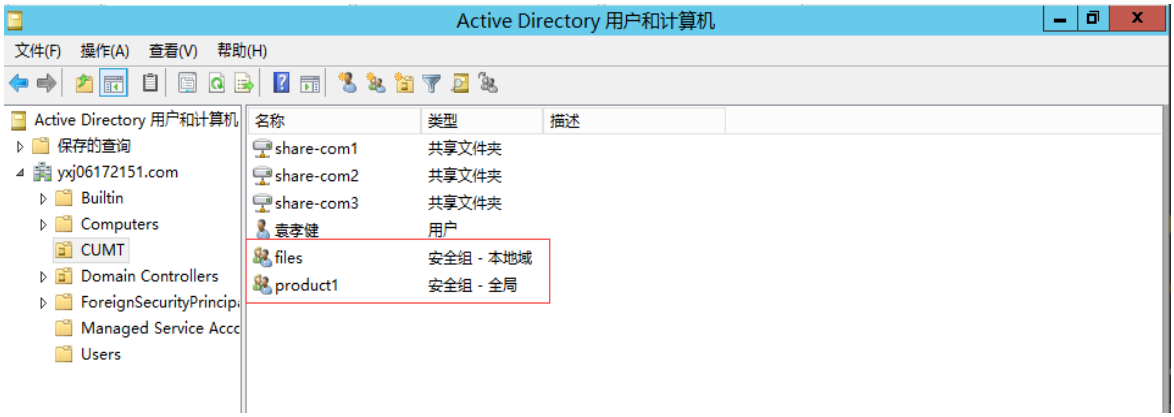
① 创建本地组



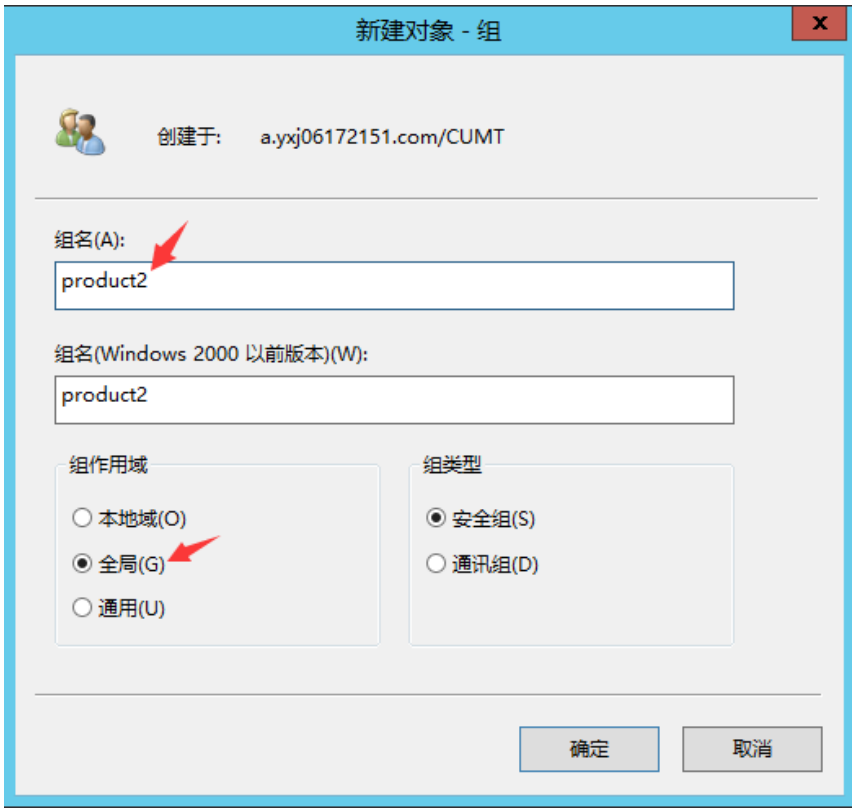
② 创建全局组



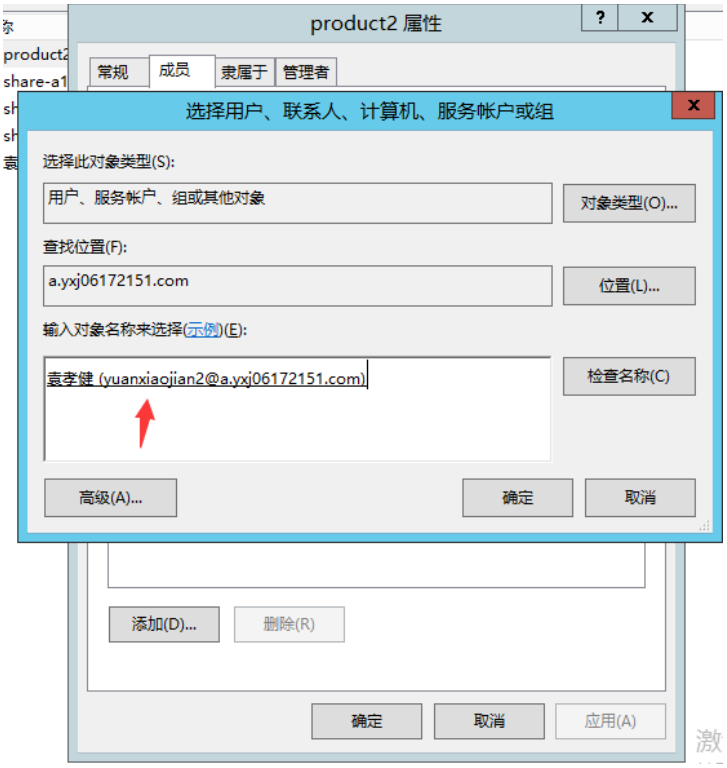
结果如下：

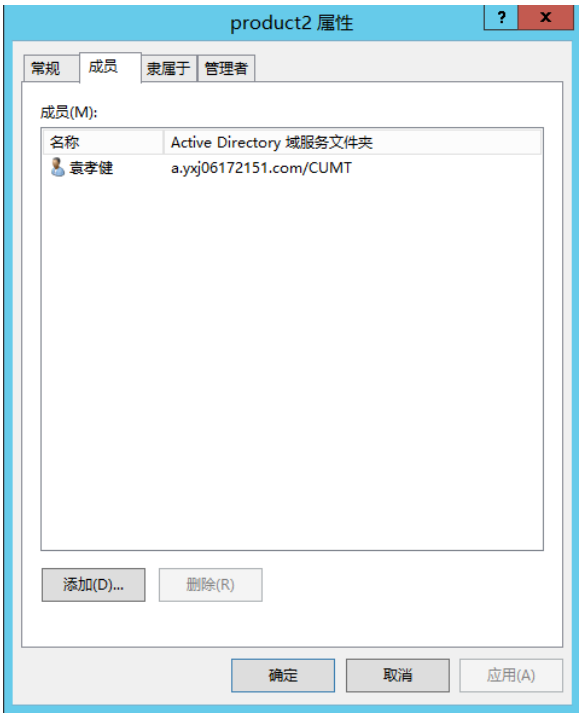


（2）在子域 a.yxj06172151.com 中创建全局组“product2”:

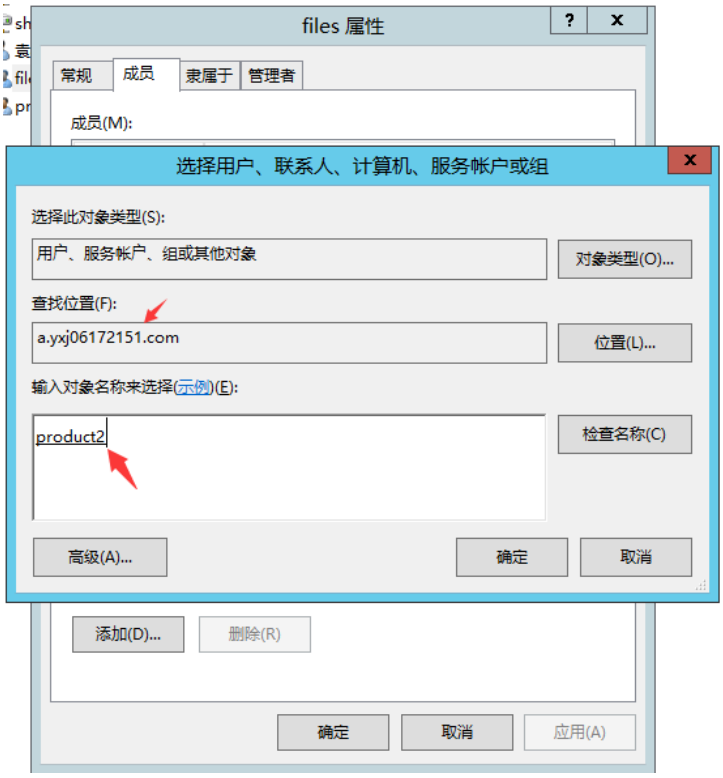


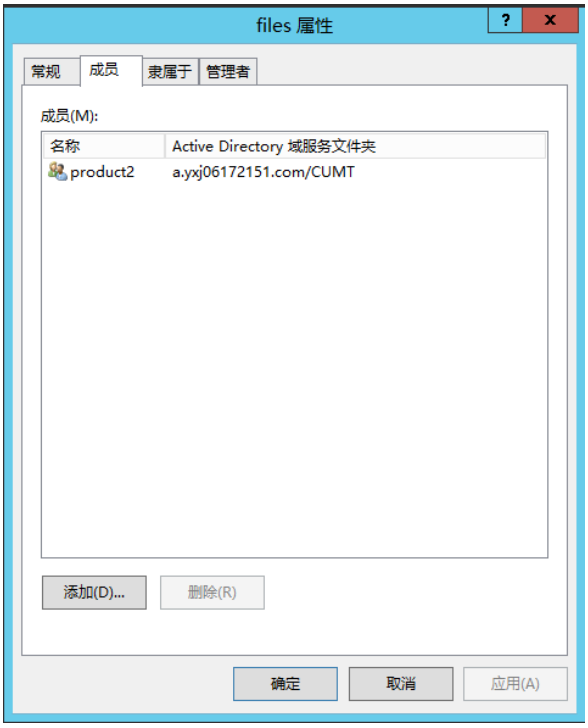
（3）将子域 a.yxj06172151.com 中的用户“yuanxiaojian2”加入全局组“product2”中：





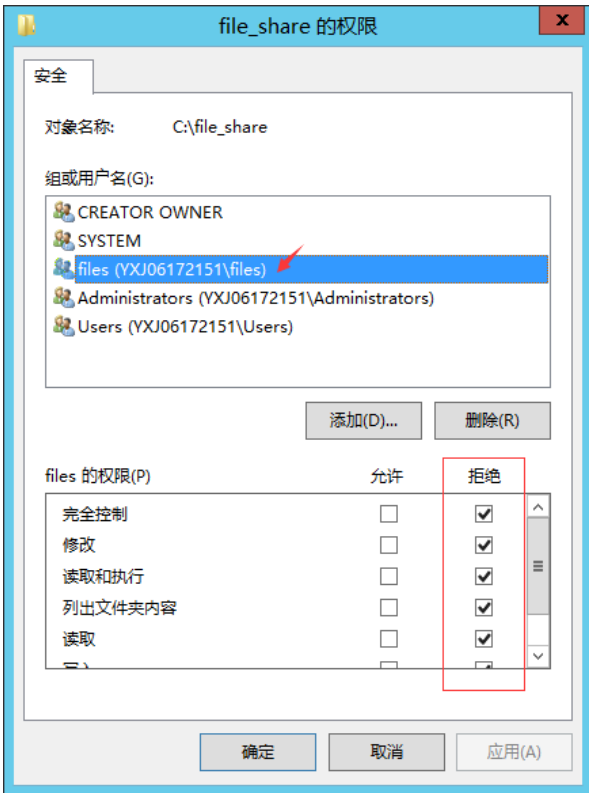
（4）在顶域 yxj06172151.com 中将顶域的全局组和子域的全局组“product2”加入本地组“files”中：



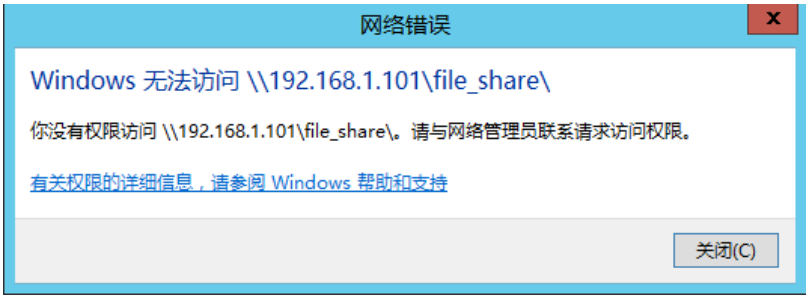


（5）在顶域 yxj06172151.com 中建立共享文件夹 file_share，并设置本地组 files 对该共享文件夹的访问权限：

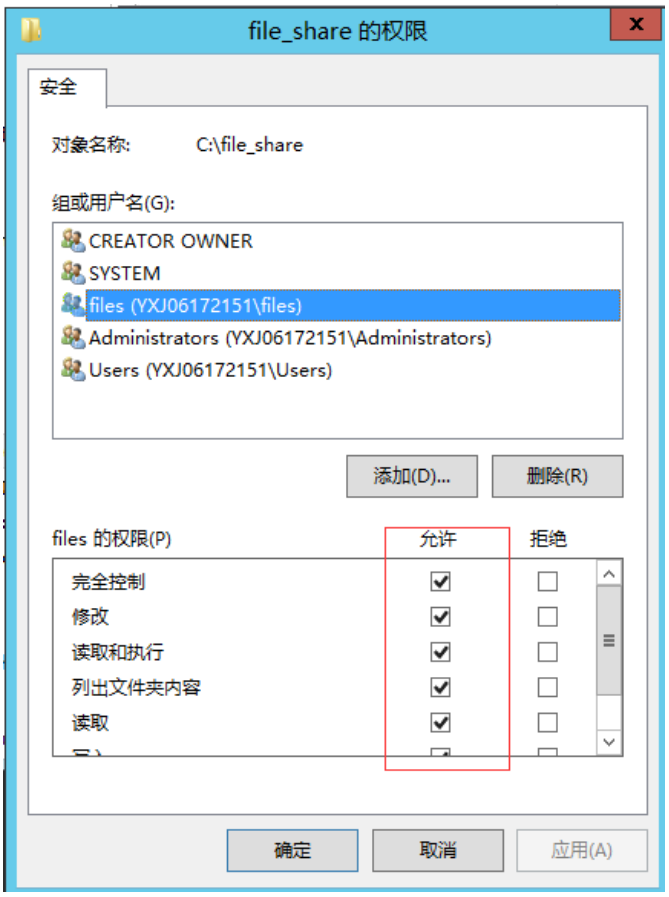
（6）先将权限设为“拒绝”：



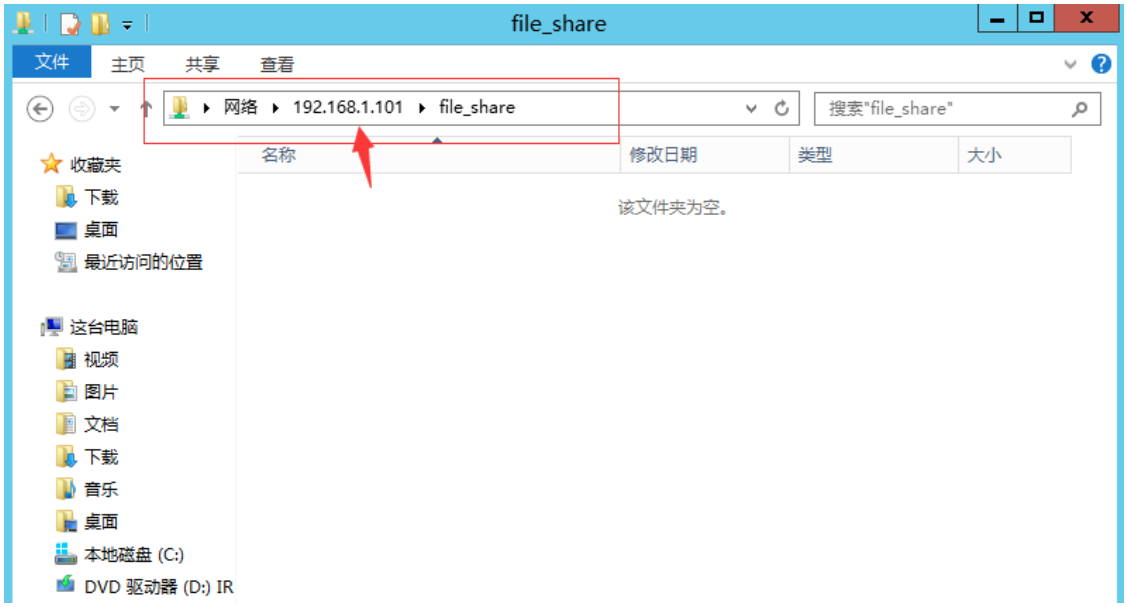
（7）用 yuanxiaojian2 用户登录子域并尝试访问 file_share 共享文件夹，提示“没有权限”：



（8）重新将 files 组的权限改为“允许“：

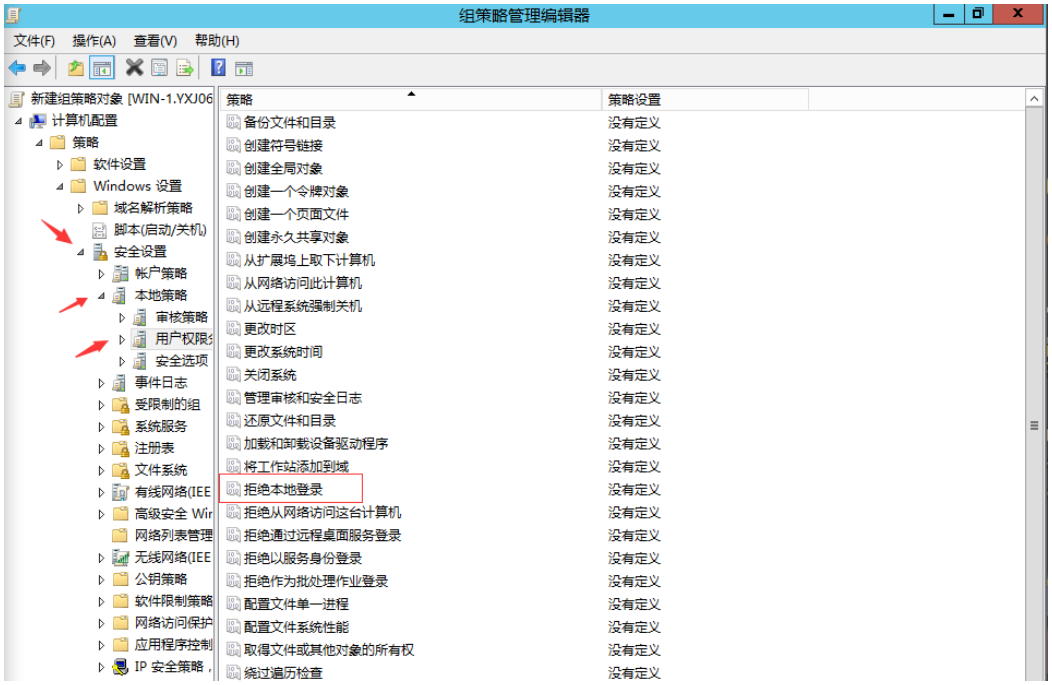


（9）再次在子域尝试访问共享文件夹，发现可以成功访问该文件夹：

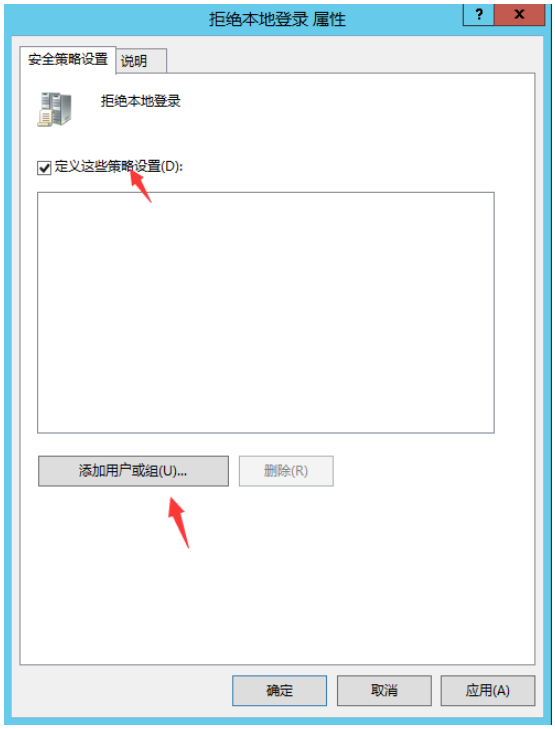


3.2 服务访问控制

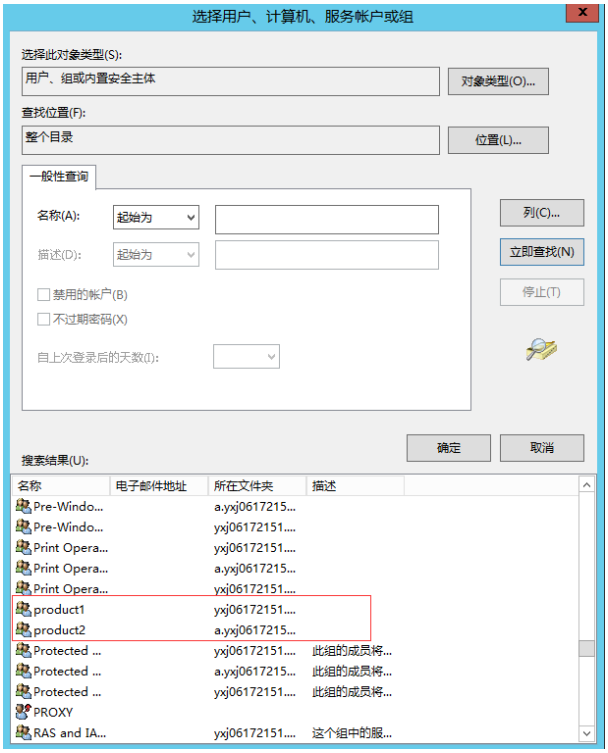
（1）除了对资源的访问控制，也可以在“组策略管理编辑器—Windows 设置—安全设置—本地策略—用户权限”中，对服务进行分布式的访问控制，如下设置“拒绝从本地登录”：



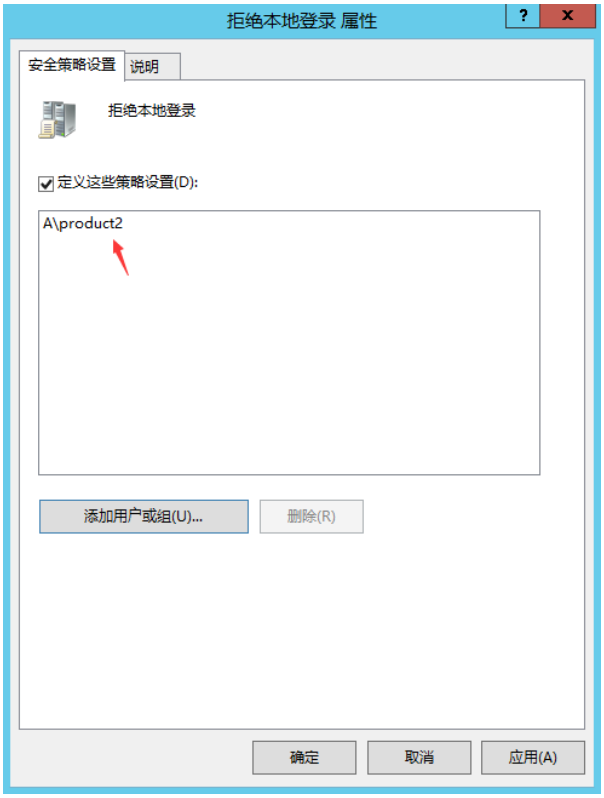
（2）右键该策略进行定义，选择“添加用户或组”：



（3）可以看到我们创建的全局组：



（4）我们将子域中的 product2 组添加进来，这样 product2 中的用户 yuanxiaojian2@a.yxj06172151.com 就无法从本地登录这台计算机：



（5）使用"gpupdate /force”更新策略后，使用 yuanxiaojian2@a.yxj06172151 账户尝试登陆顶域服务器，发现登录被拒绝：