中国矿业大学计算机学院

2017 级本科生课程报告

课程名称 操作系统安全

报告时间 2020.5.4

学生姓名 袁孝健

学　　号 06172151

专　　业 信息安全

任课教师 张爱娟

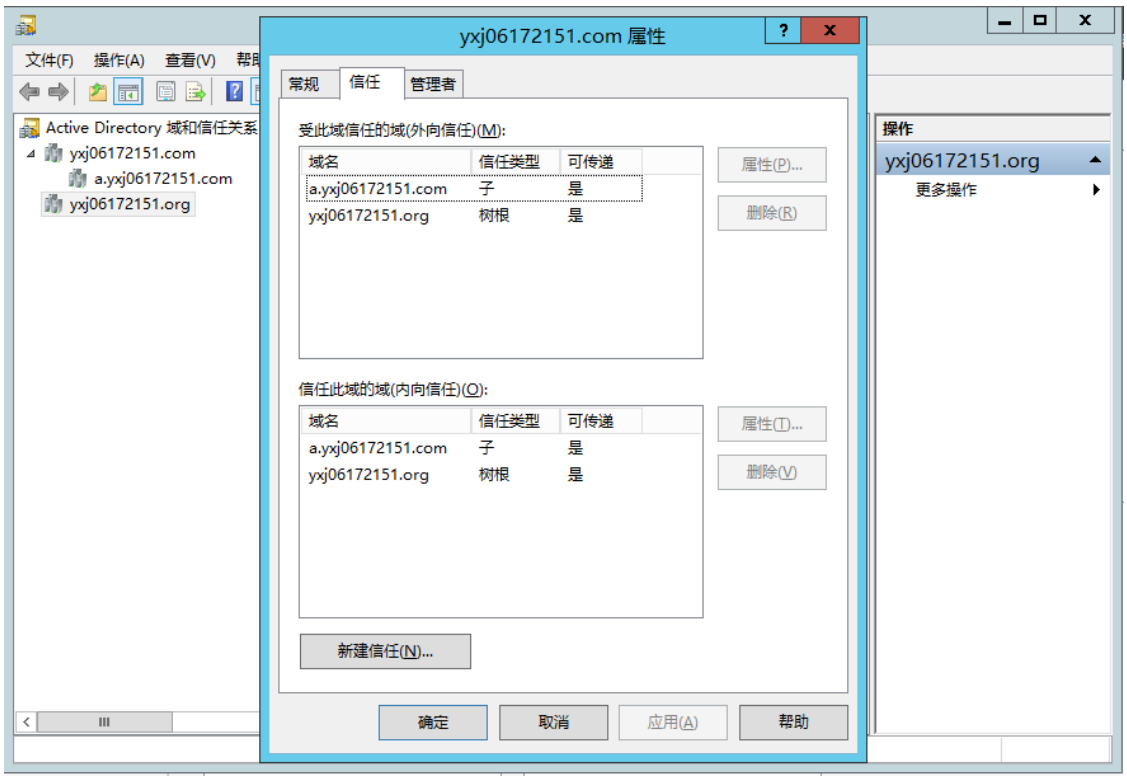
目 录

1 企业环境架构

1.1 域森林

企业共有三个域组成一个域森林，其中 a.yxj06172151.com 域是 yxj06172151.com 的子域，而 yxj06172151.com 与 yxj06172151.org 相互建立信任关系。

域信任关系如下：



1.2 企业架构

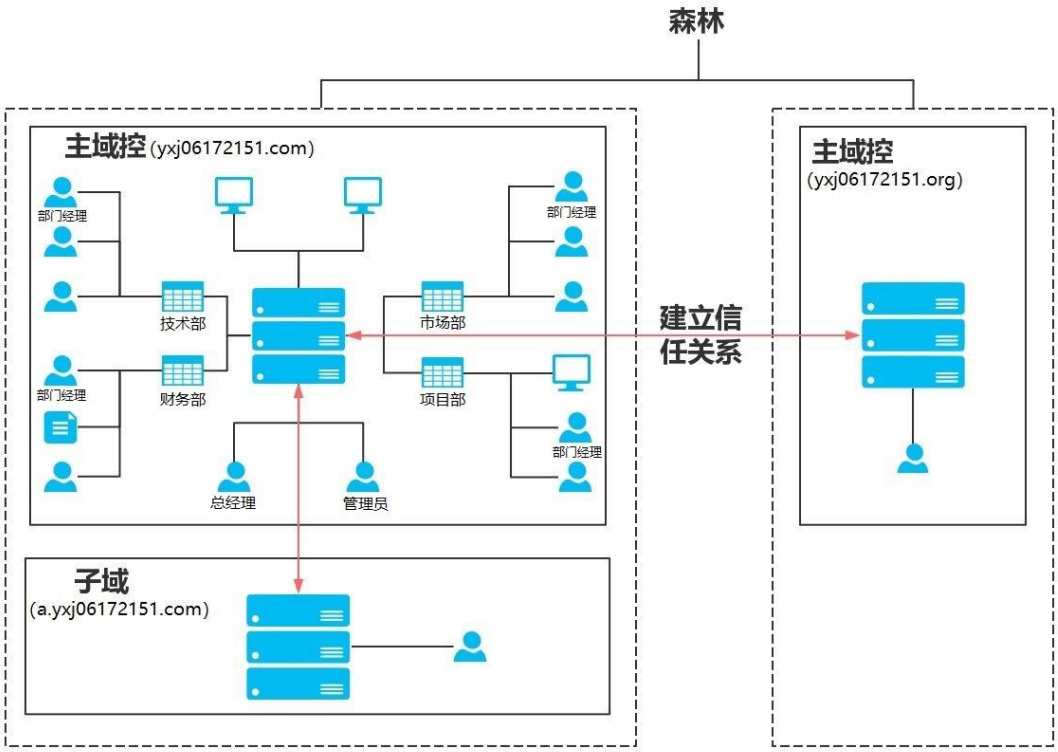
三台域控机器分别为 Windows Server 2012，客户机为 Widnows 7 Profession 根据企业内部架构，分为一个总经理以及四个部门，每个部门下设有部门经理和部门员工，如下：

- 总经理：管理四个部门以及下属部门经理和员工。
- 技术部
  - 技术部经理：管理技术部 OU 以及下属员工。
  - 技术部员工：仅具有普通员工权限。
- 市场部
  - 市场部经理：管理市场部 OU 以及下属员工。

- 市场部员工：仅具有普通员工权限。

- 财务部
  - 财务部经理：管理财务部 OU 以及下属员工。
  - 财务部员工：仅具有普通员工权限。

- 项目部
  - 项目部经理：管理项目部 OU 以及下属员工。
  - 项目部员工：仅具有普通员工权限。



2 需求一：用户管理

2.1 需求细则

（1）公司按部门进行管理，每部门设经理一名，四个部门归总经理统一管理。

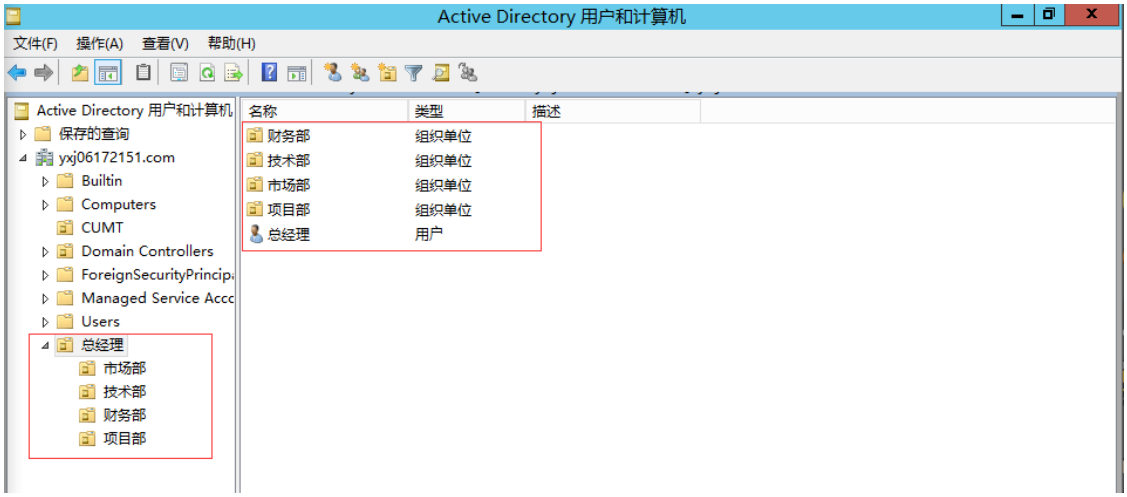
（2）每个部门的账号不能登录到其他部门。

（3）只允许在上班时间登录计算机。

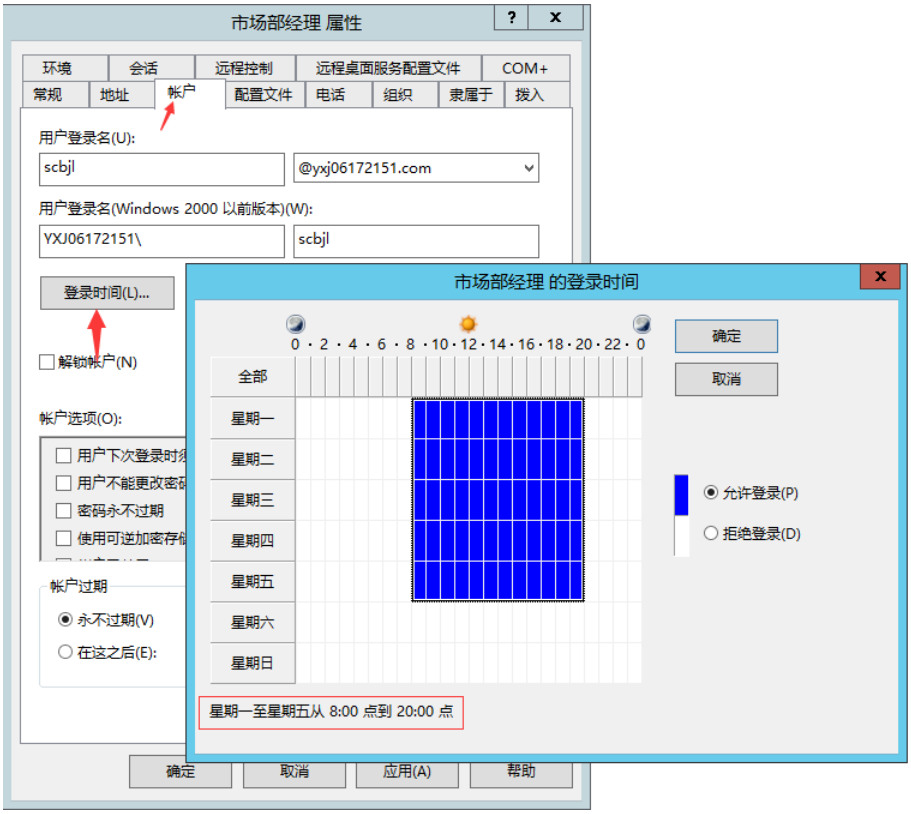
（4）部门经理要有添加本部门员工和重设本部门员工账号密码的权利，从而减少管理员工作量。

2.2 实施方案

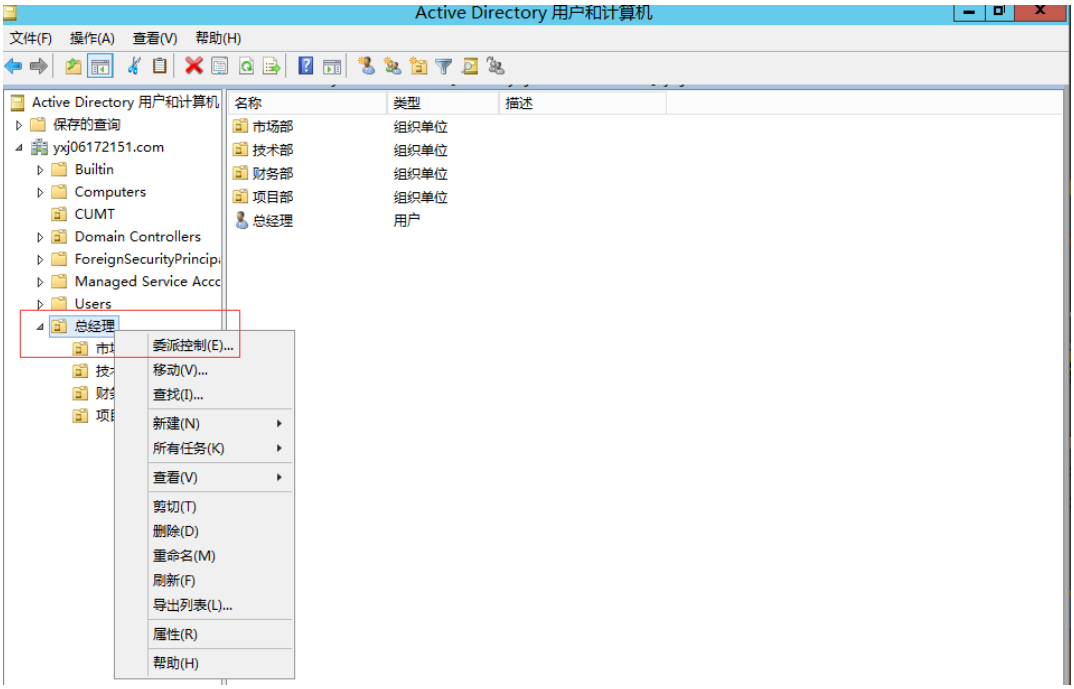
（1）建立总经理 OU，并在其 OU 下创建个部门 OU，建立总经理用户及各部门经理用户。

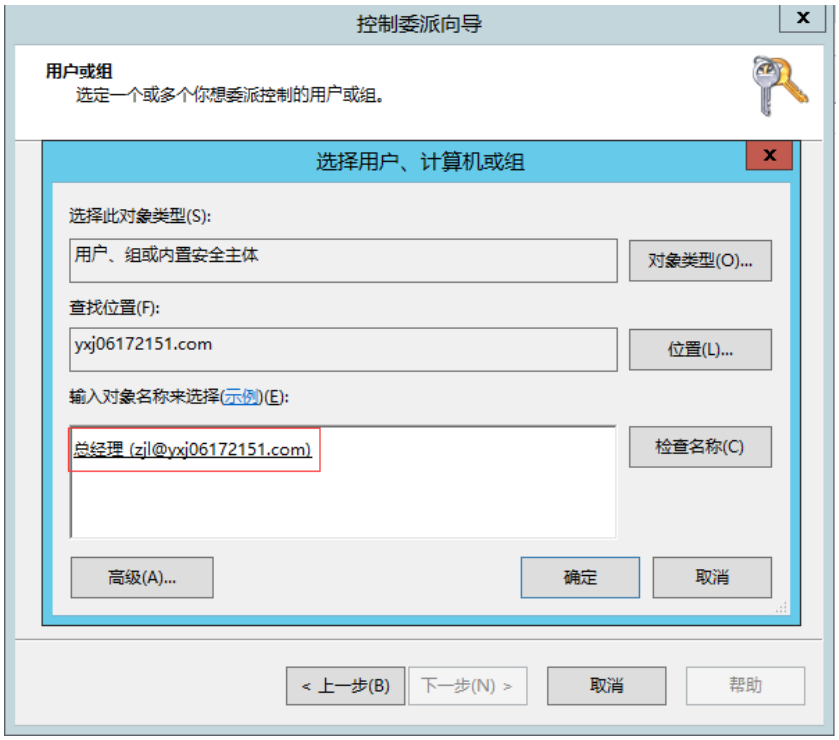


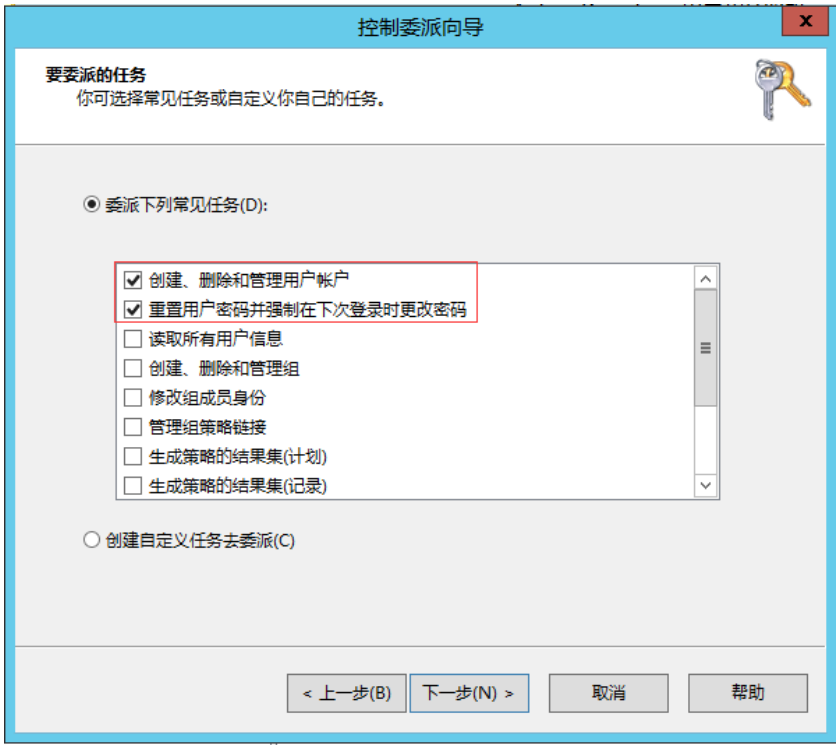
（2）将用户的登录时间限制为：星期一至星期五 8:00 到 20:00:



（3）委派总经理有修改、创建、删除账户的权限：







（4）以同样的方式委派各部门经理对自己部门 OU 有修改、创建、删除账户的权限。

3 需求二：账户安全

3.1 需求细则

（1）要保证员工账号密码的安全性，并要求员工定期更改密码。

（2）帐户密码长度不小于 8，密码不能为简单密码，如 12345678 等。

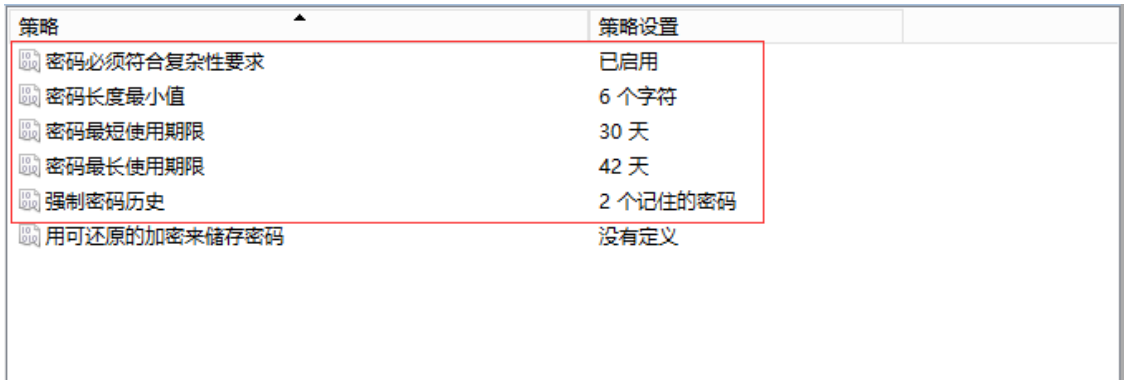
（3）对个别员工试探别人密码的行为要有所防范。

（4）设置域中账户的锁定策略，以及对 Kerberos 协议进行一定的安全策略。

3.2 实施方案

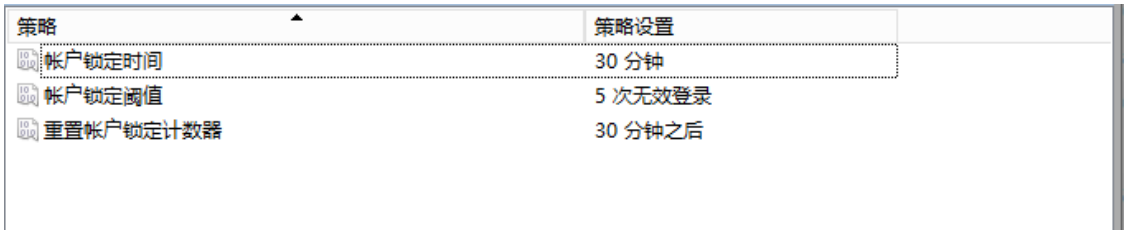
（1）打开组策略管理器，并建立 GPO：

（2）设置账户密码安全策略：



策略	策略设置
密码必须符合复杂性要求	已启用
密码长度最小值	6 个字符
密码最短使用期限	30 天
密码最长使用期限	42 天
强制密码历史	2 个记住的密码
用可还原的加密来储存密码	没有定义

（3）设置账户锁定策略：



策略	策略设置
帐户锁定时间	30 分钟
帐户锁定阈值	5 次无效登录
重置帐户锁定计数器	30 分钟之后

（4）设置域中的 Kerberos 安全策略：

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

4 需求三：统一设置

4.1 需求细则

（1）公司计算机的桌面背景一致。

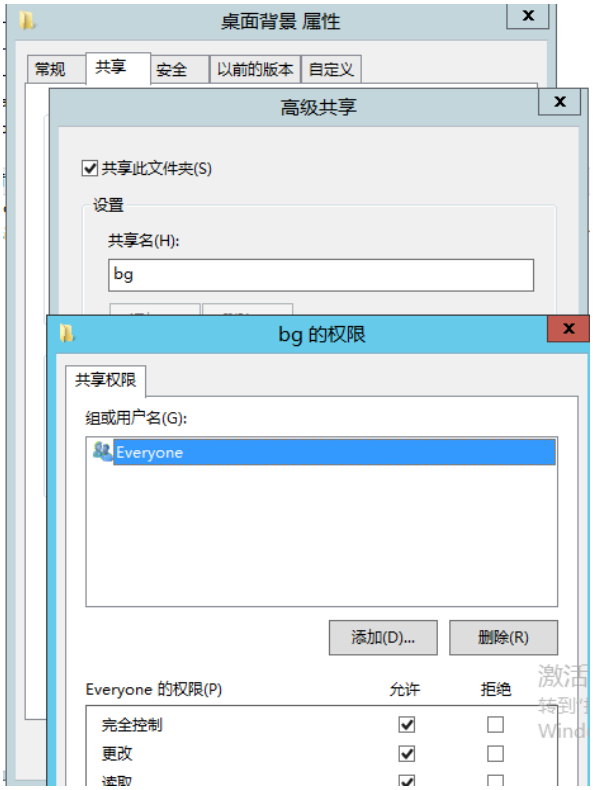
（2）员工随意更改桌面背景，但部门经理不受此限制。

（3）进行软件指派，统一按照 Office 套件。

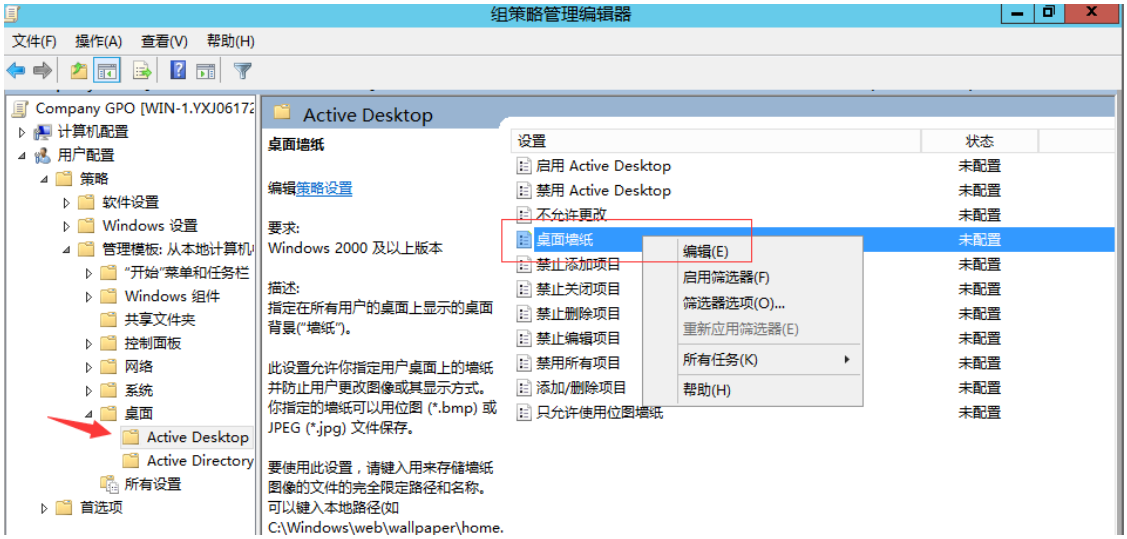
（4）设置域中的 IE 默认主页为 www.baidu.com，并禁止用户更改。

4.2 实施方案

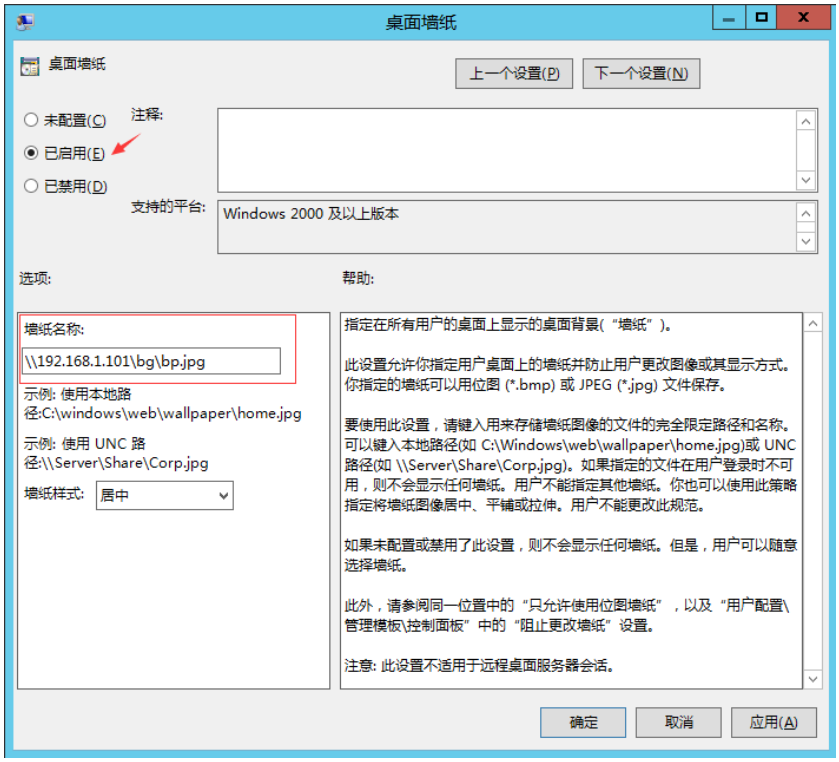
（1）新建共享文件夹“桌面背景”用来存放桌面背景图片，权限设置为 Everyone 完全控制：



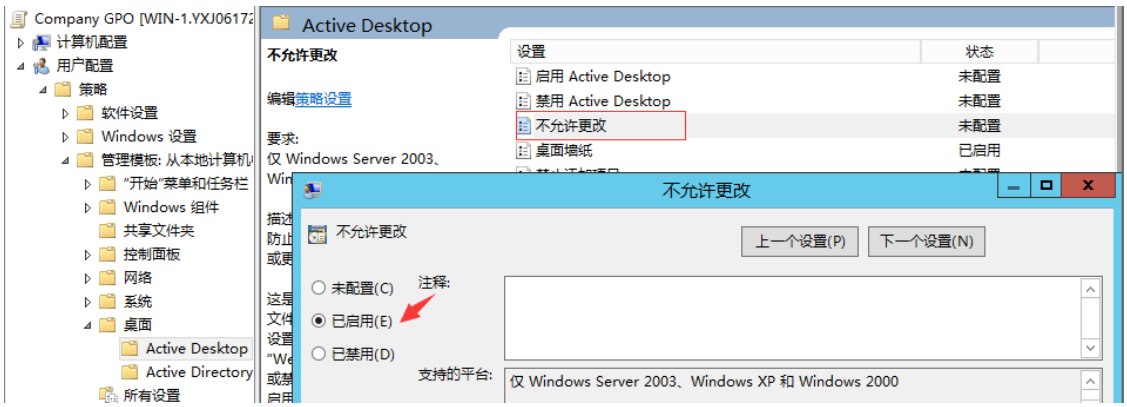
（2）在组策略管理编辑器—用户设置中设置桌面墙纸：



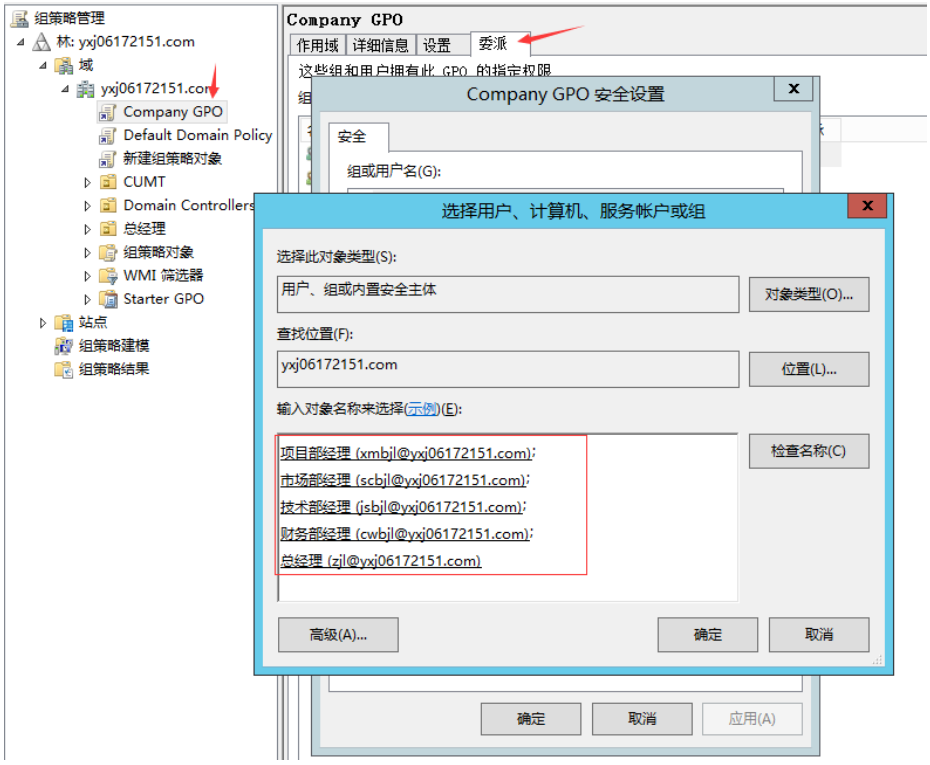
选择刚才存放桌面壁纸的共享文件夹：



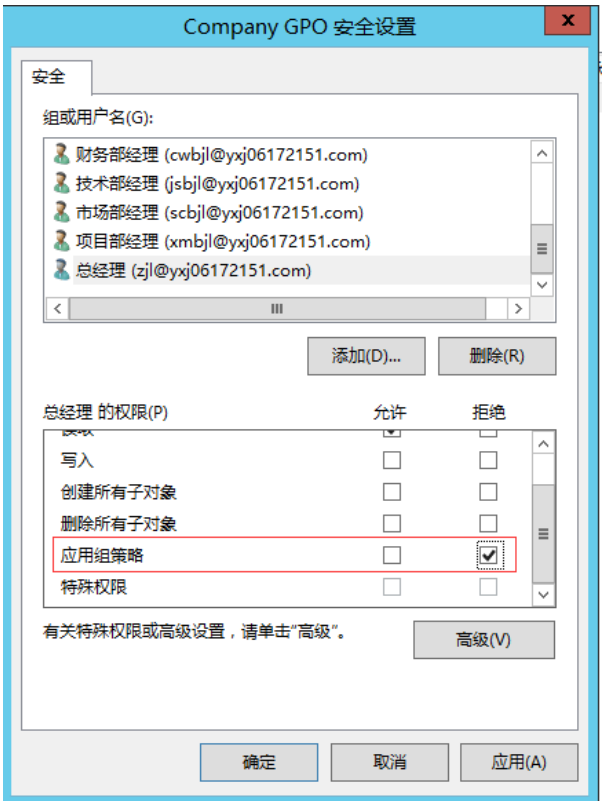
设置不允许用户更改：



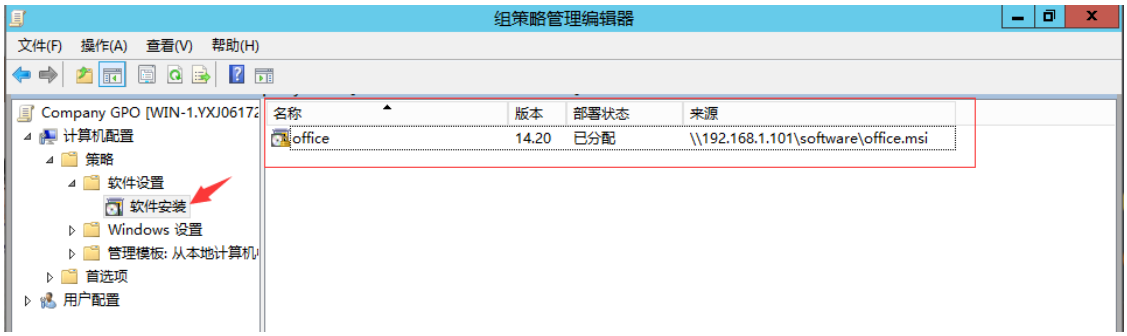
（3）因为个部门经理需要不受此限制，所以需要将其筛选出来，点击域策略GPO—委派—高级—添加，将各经理加进去：



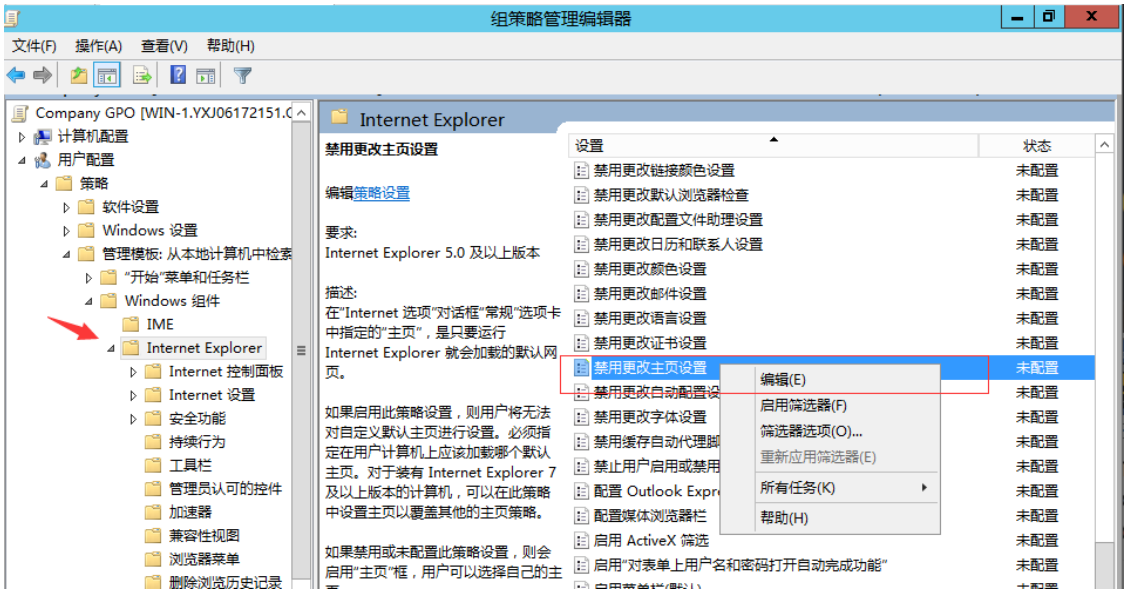
将他们的“应用组策略”权限设置为拒绝：

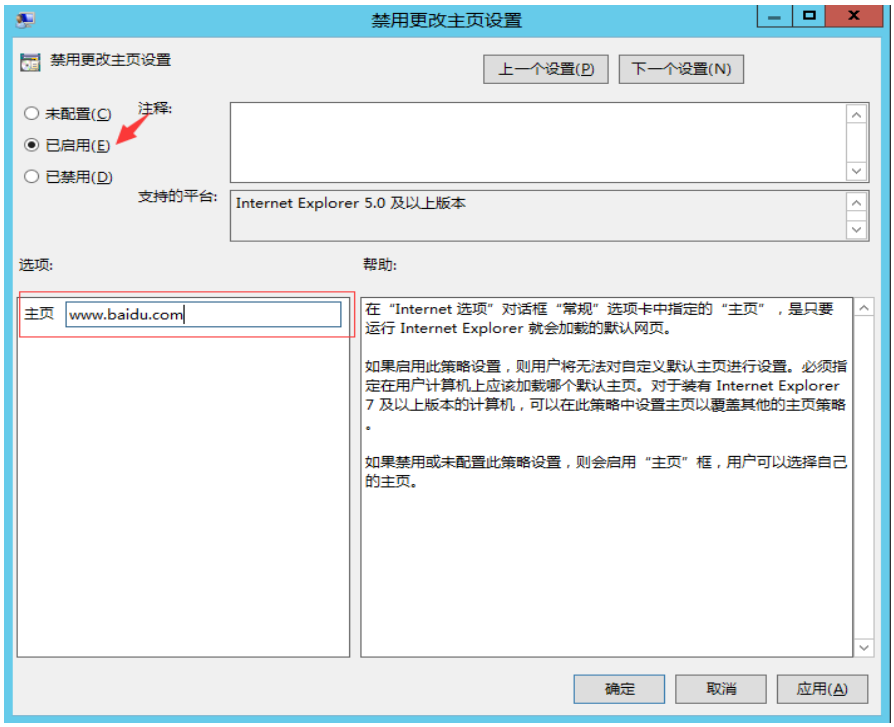


（4）统一指派office软件，先创建一个共享文件夹software，并将要发布的.msi，然后在组策略管理编辑器中，选择“用户配置—软件设置”中的软件安装：



（5）设置域中的IE默认主页为www.baidu.com，并禁止用户更改。





5 需求四：打印服务

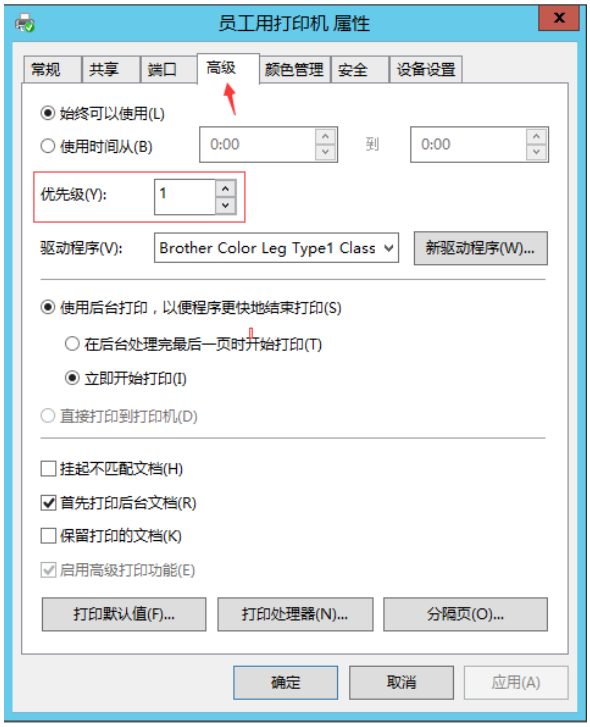
5.1 需求细则

公司所有用户均可使用打印机服务，但总经理、部门经理有优先打印权。

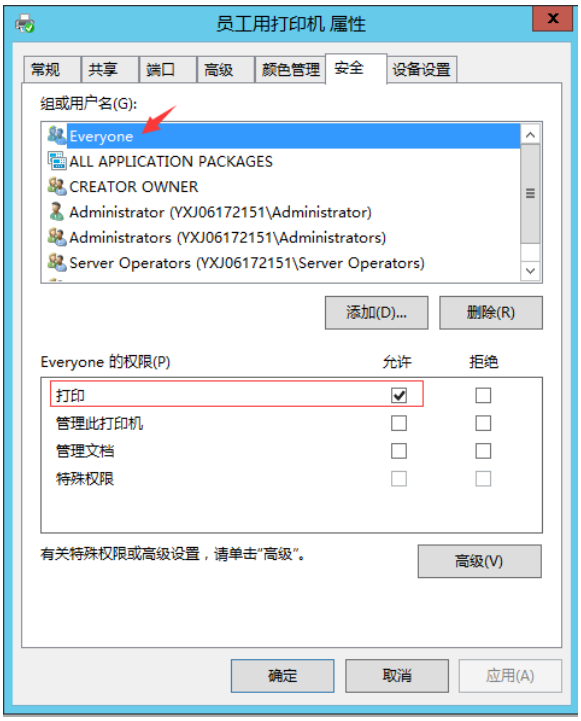
5.2 实施方案

（1）首先在需要添加两台打印机设备：

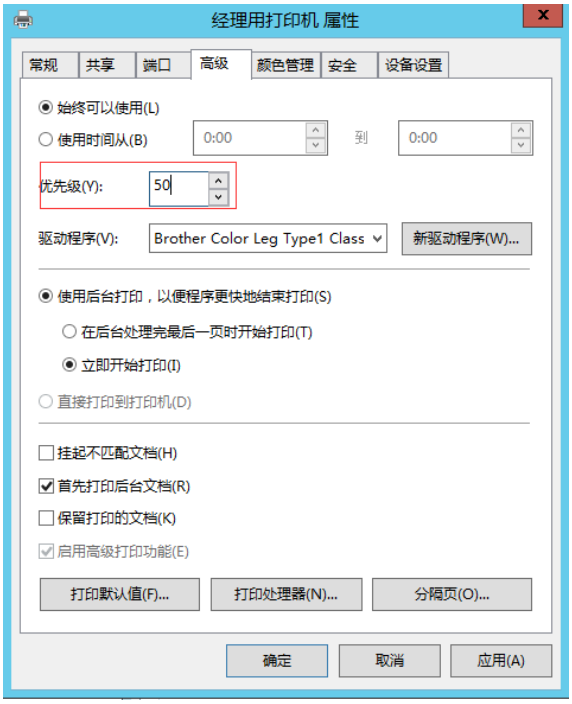
（2）然后将两个打印机设置为共享，并其中一台打印机对优先级进行设定：设置员工使用打印机时的优先级最低：



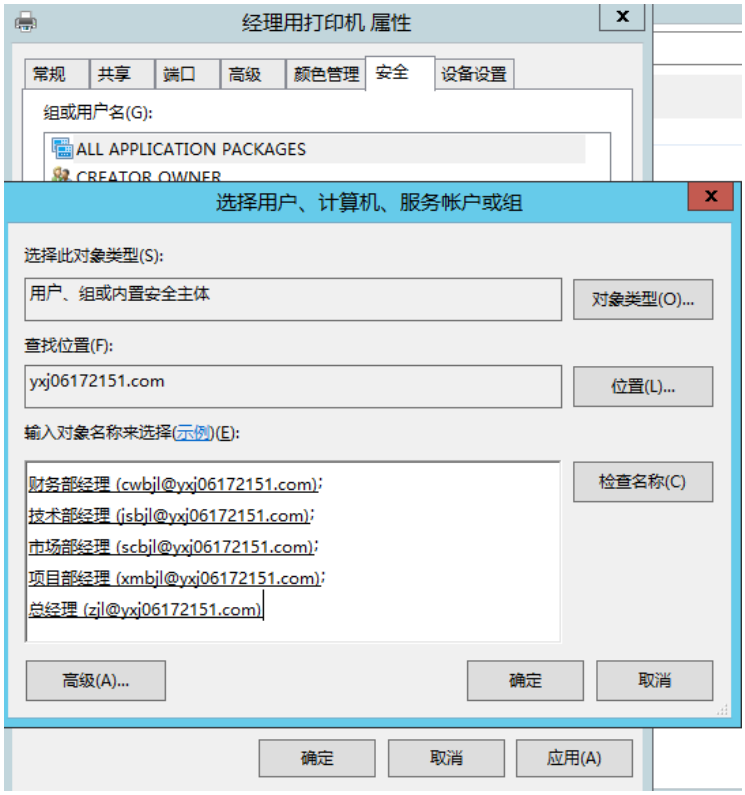
并设置所有用户有打印权限：



（3）设置经理可用的打印机优先级大于员工的：



在安全中删除 Everyone 用户，并将各经理用户添加进来赋予打印权限：



6 需求五：安全共享

6.1 需求细则

（1）公司一些公用文件可以被所有用户所共享。

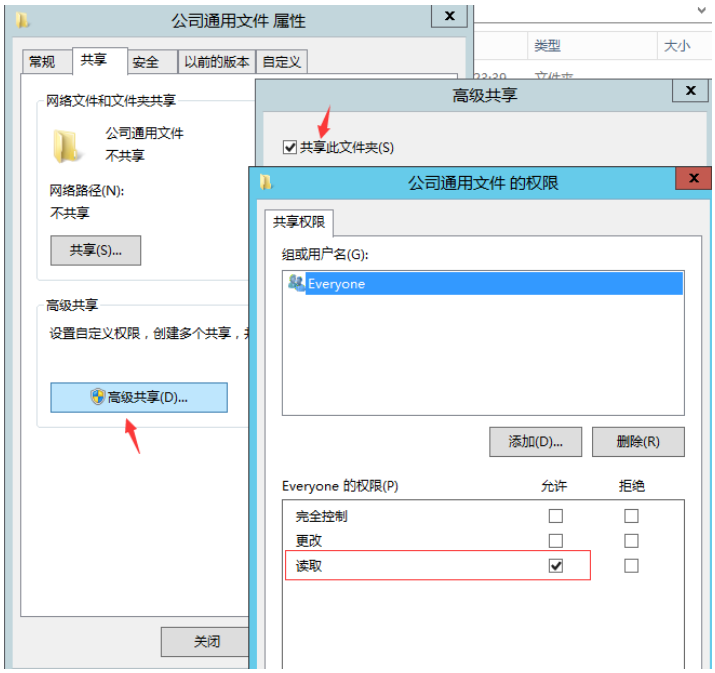
（2）每个用户有自己的文件夹、员工账户配置资料这些都要求保存在服务器上，同时需要进行一定的权限控制。

（3）对数据的安全可靠性有一定的考虑，创建 RAID-5 卷，并将公司数据及员工资料放入 RAID-5 新加卷中。

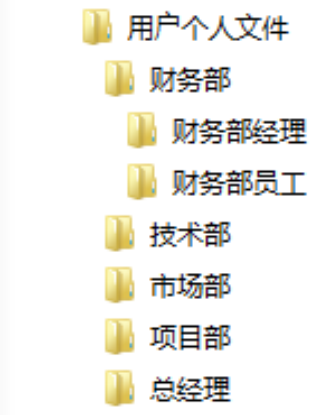
6.2 实施方案

（1）为有效保证资料的安全需创建 RAID-5 卷，将公司文件、员工文件及重要数据放入此新加卷里，可有效保证资料的安全。

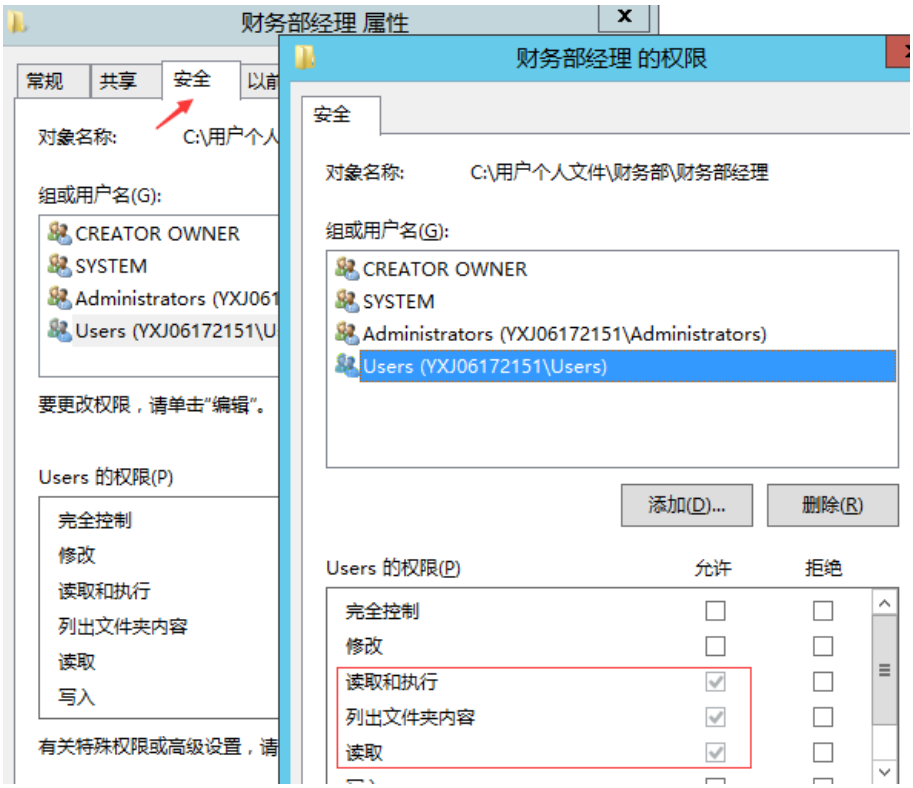
（2）在新加卷中创建“公司通用文件”文件夹，并设置为共享，权限分配为 Everyone 可读：



（3）然后创建“用户个人文件”共享目录，结构如下：



对所有个人文件夹如下进行一定的权限控制，使得文件所有者具有完全控制权限，其他用户仅具有可读权限：



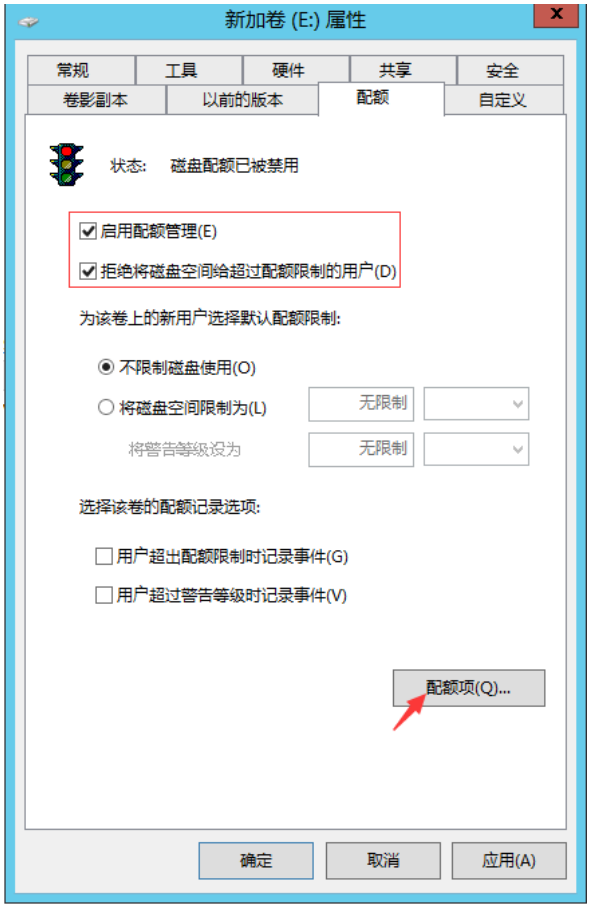
7 需求六：磁盘配额

7.1 需求细则

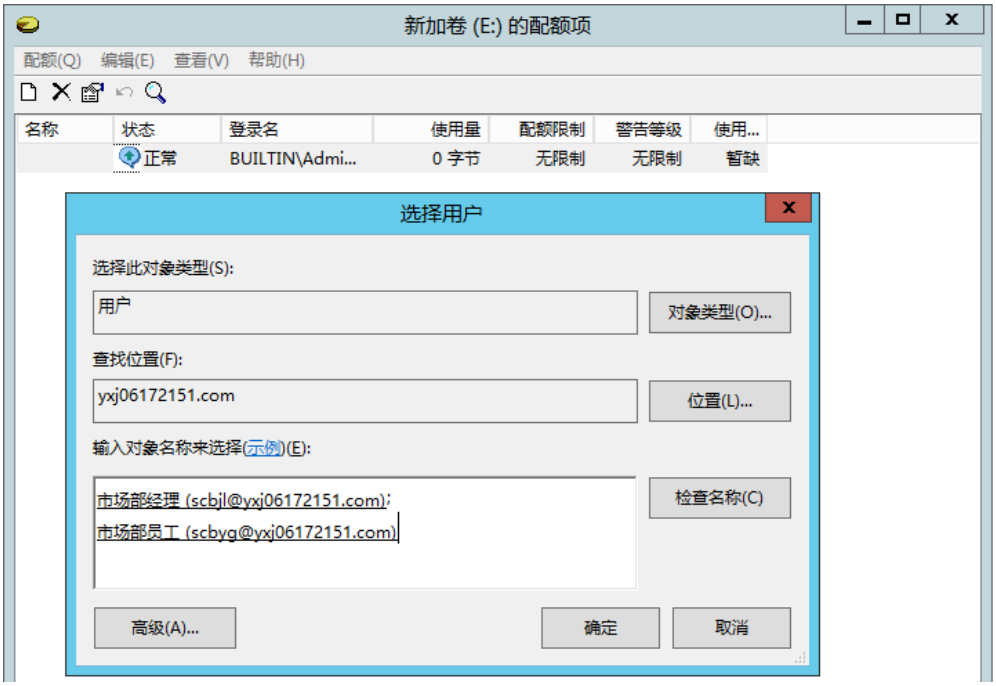
对磁盘配额进行一定的设置，限制员工的对磁盘空间使用的容量大小，这样限制的账户在其个人文件夹中写入大于限制的文件，则会提示无法创建。

7.2 实施方案

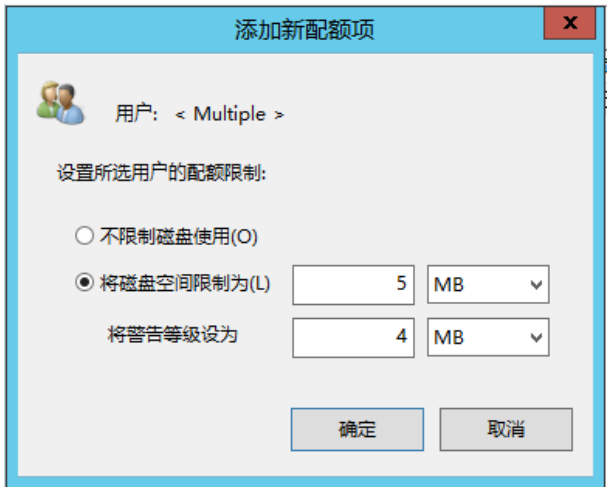
（1）右击放有员工文件夹的磁盘选择属性并选择配额，勾选启用配额管理和拒绝将磁盘空间给超过配额限制的用户，并点击配额项：



（2）新建配额项并添加需要限制的用户：



（3）填写空间限制大小，这样限制的账户在其个人文件夹中写入大于限制的文件，则会提示无法创建：



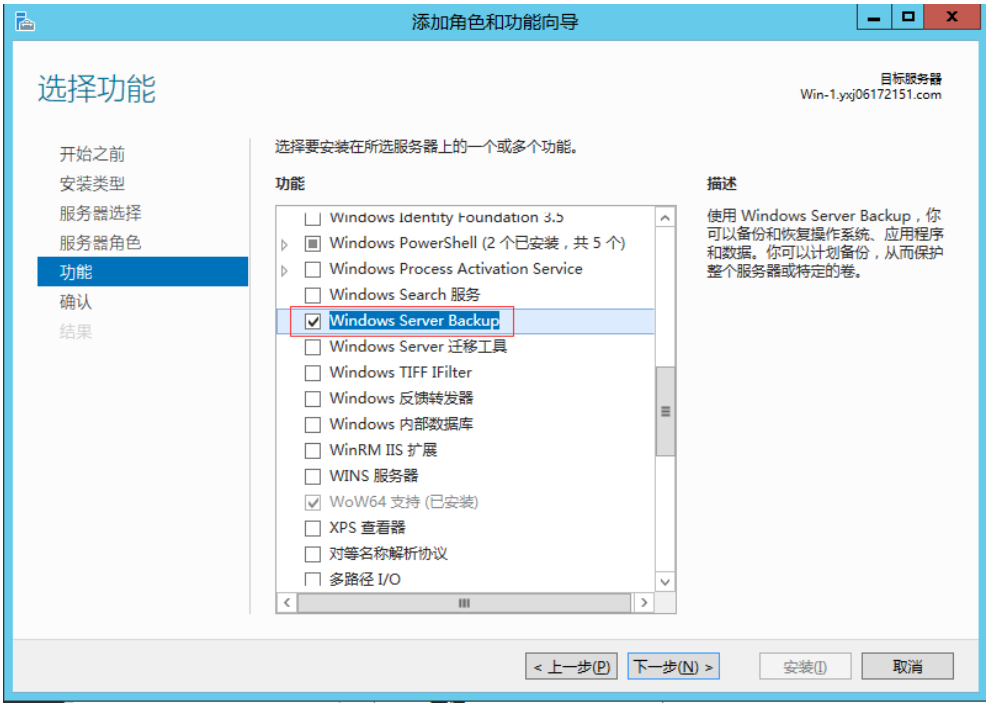
8 需求七：定期备份

8.1 需求细则

保证员工账号信息的安全性，对活动目录数据库定期备份。

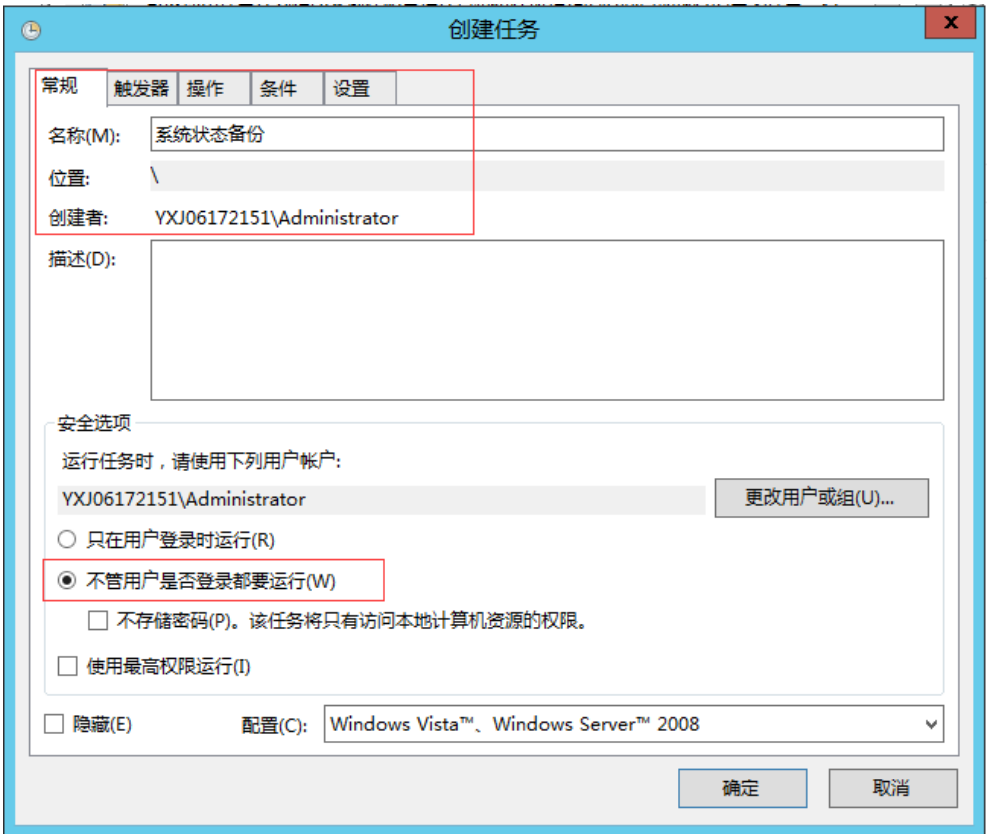
8.2 实施方案

（1）首先需要在服务器上按照 Windows Server Backup 功能：

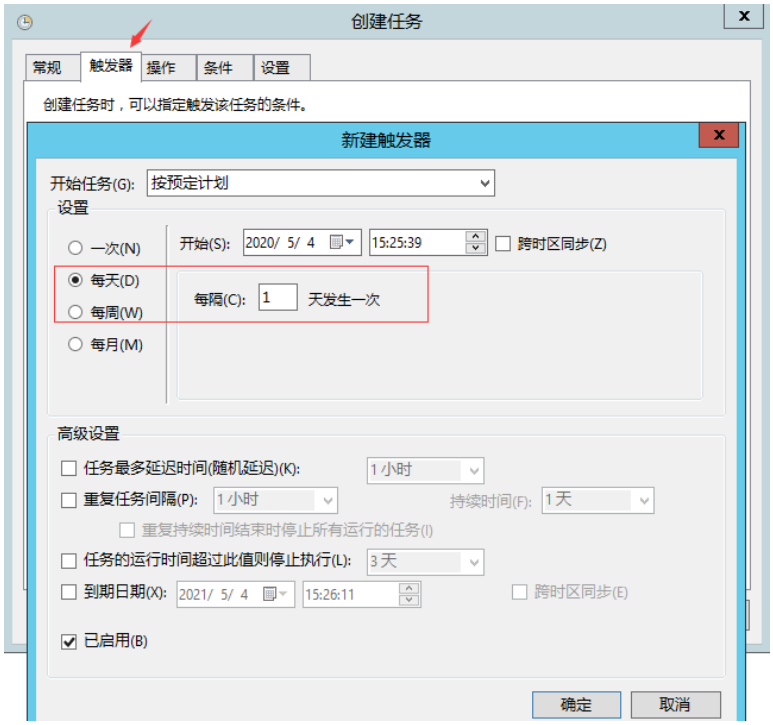


（2）安装成功后，打开“任务计划程序”，点击创建任务：

进行如下设置：

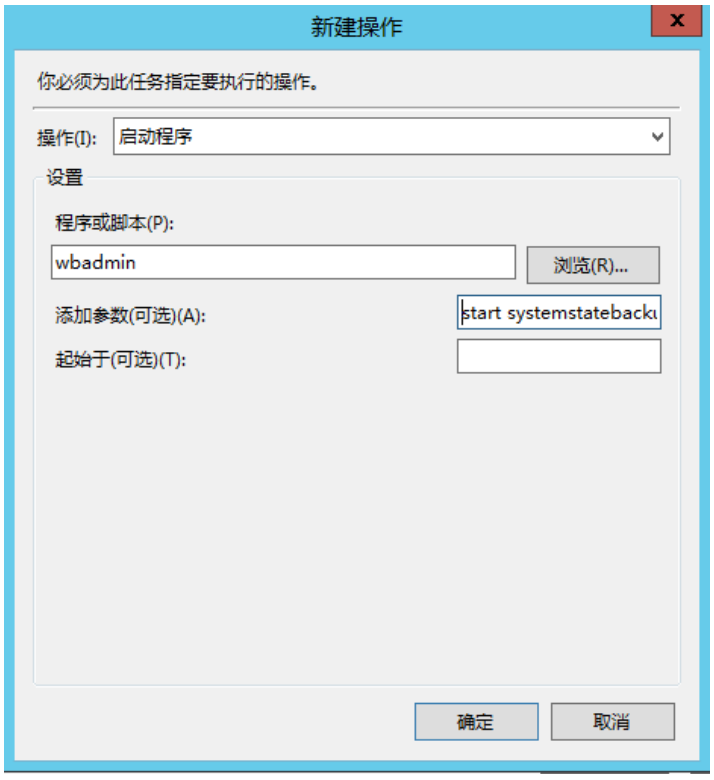


（3）新建触发条件：

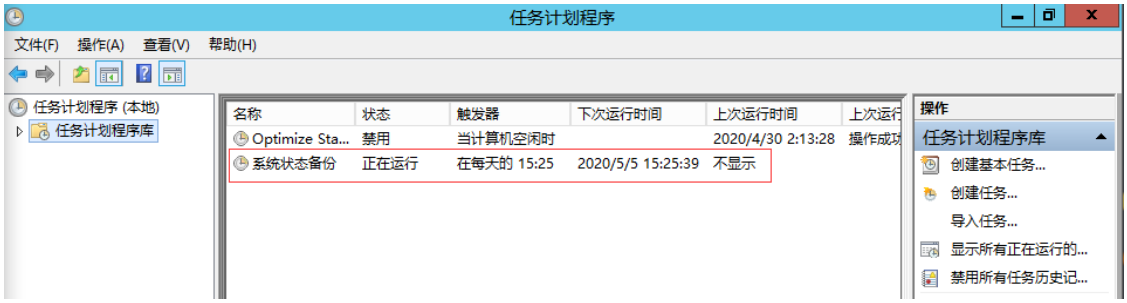


（4）新建操作，在操作中输入：

- 程序名：wbadmin
- 参数：start systemstatebackup -backuptarget:f: -quiet：



（5）成功设置对活动目录数据库进行定期备份：



9 需求八：安全通信

9.1 需求细则

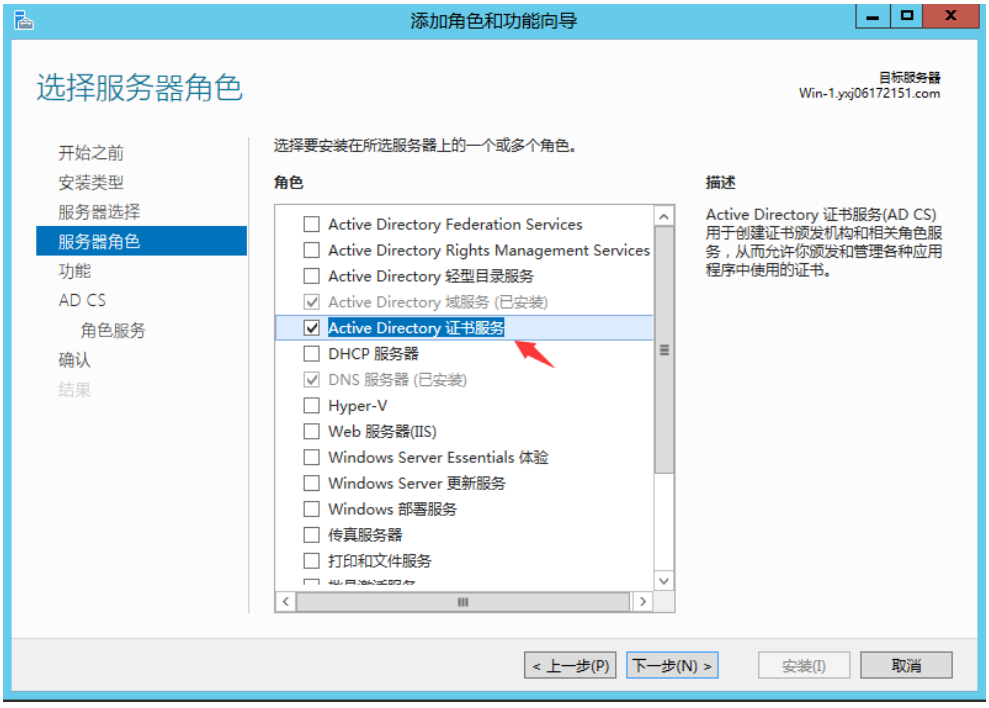
（1）企业内部提供证书申请服务，域中用户可以从域控申请数字证书，从而进行故障恢复代理等需要认证服务的使用。

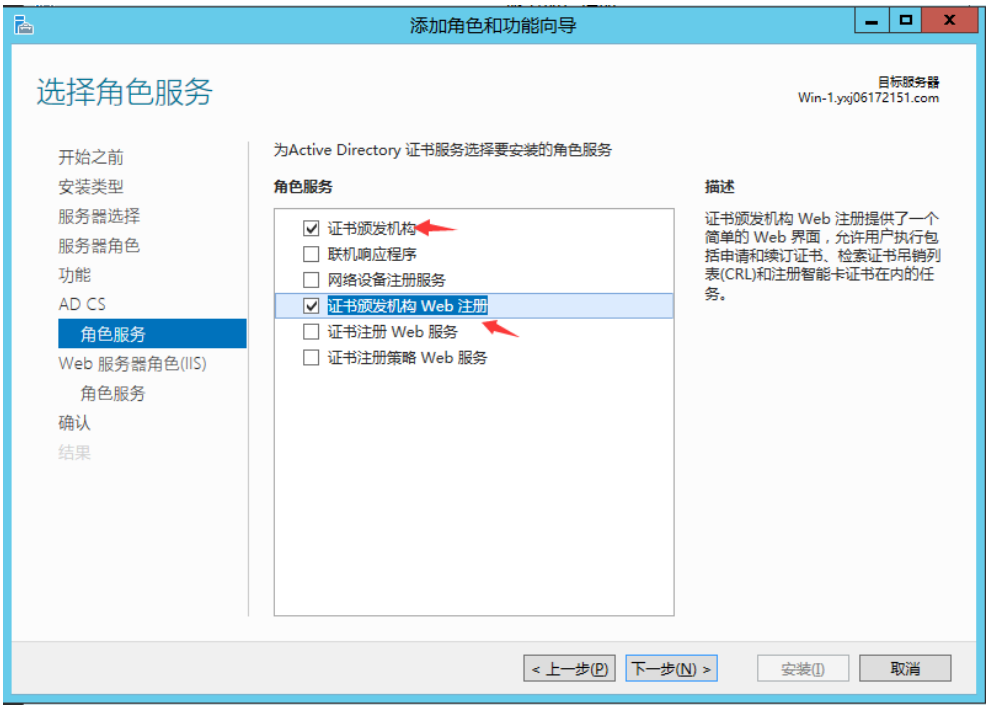
（2）通过数字证书实现域内 Web 服务的 HTTPS 通信。

9.2 实施方案

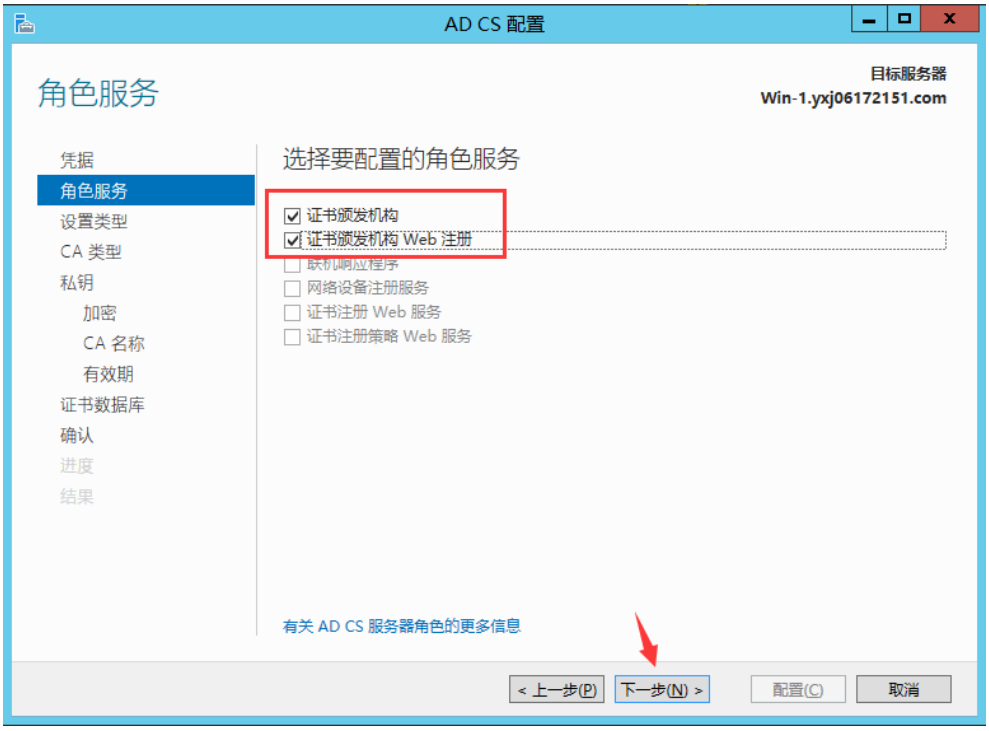
9.2.1 证书服务

（1）首先安装证书服务：

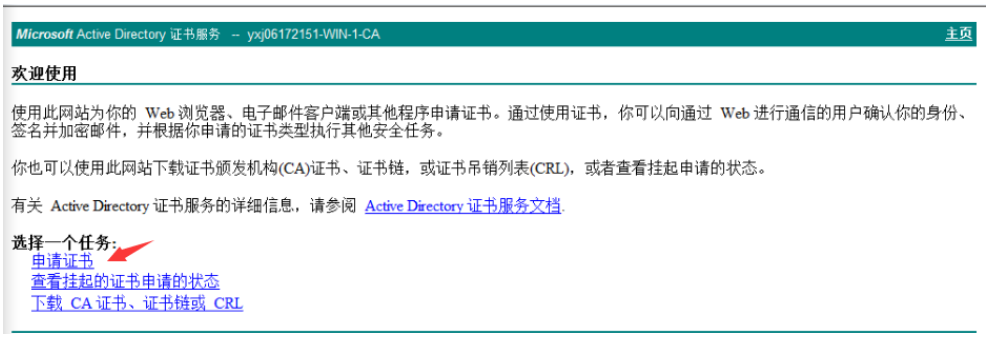




（2）然后对证书服务进行配置：



（3）域内用户即可以通过 Web 方式进行证书申请：



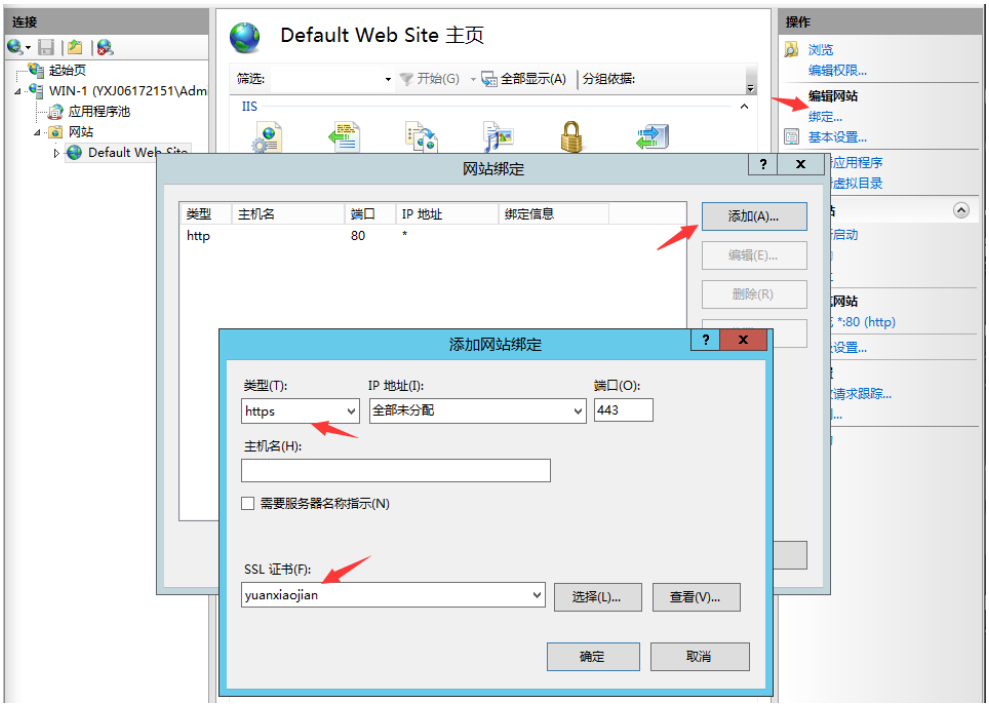
9.2.2 HTTPS 通信

（具体配置过程可参考之前实验）

（1）打开 IIS 服务器，并选择“服务器证书功能”—“创建证书申请”，然后填写相应信息，将申请的证书内容复制，再通过 base64 编码申请服务进行申请，将得到的证书进行下载：

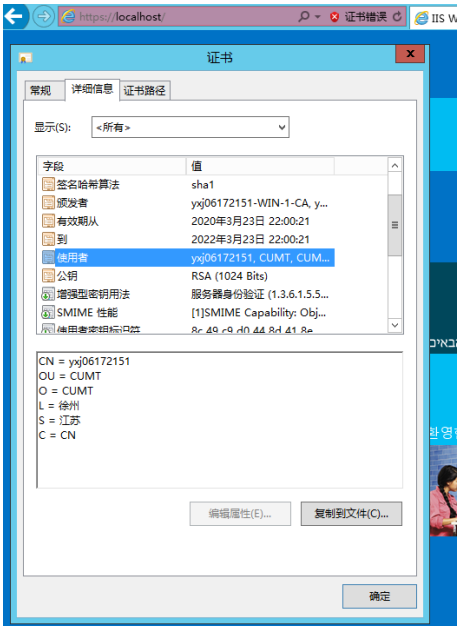
（2）然后再打开 IIS 管理器，选择完成证书申请，导入刚才下载下来的证书，确定后可以看到证书服务器中多了一个证书：

（3）然后选择“绑定”，然后“添加”，选择 https 类型，并将 SSL 证书选择为我们刚才创建的证书：



（4）然后我们尝试访问 https://localhost 如下

（5）可以看到使用的证书即为我们刚才创建的证书



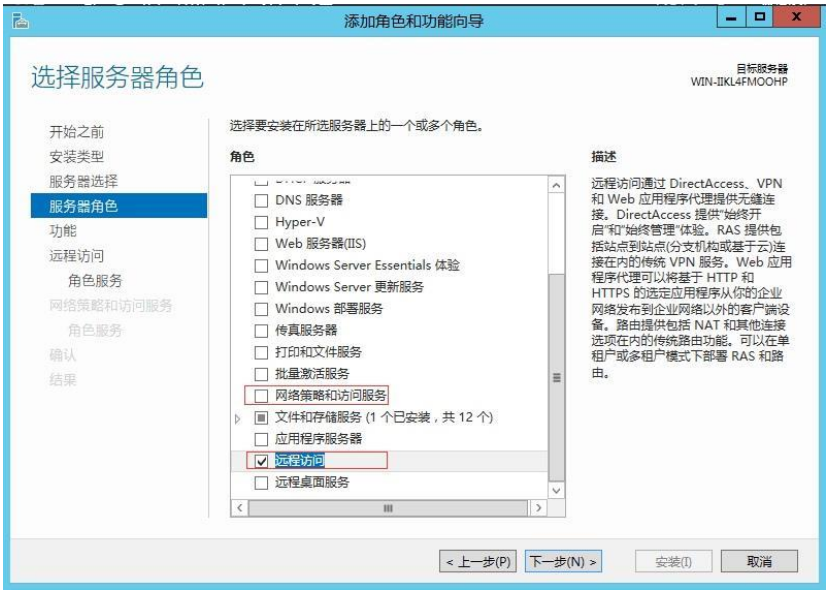
10 需求九：远程访问

10.1 需求细则

企业员工有时候需要外出办公，因此需要设置远程用户访问通过 VPN 进行对企业服务器的访问。

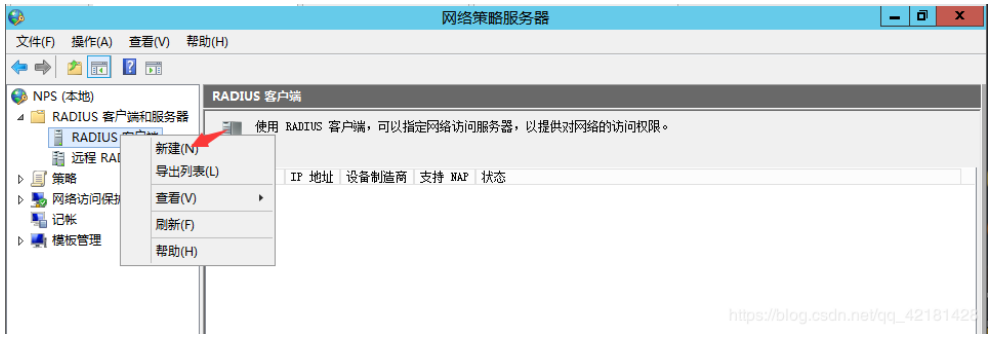
10.2 实施方案

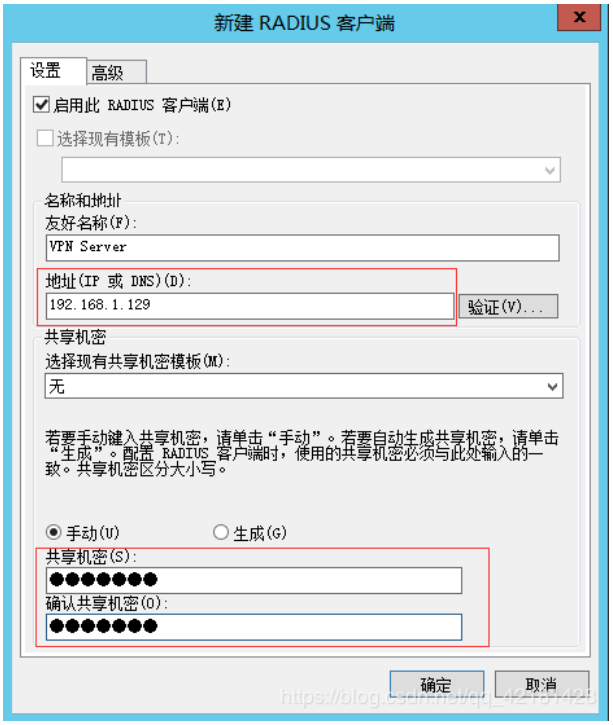
（1）如果需要启用 VPN 功能，则还需要一台服务器作为网关，并且安装远程访问功能：



（2）安装完成后，需要对路由和远程访问”服务进行配置（具体配置过程可参考之前实验）：

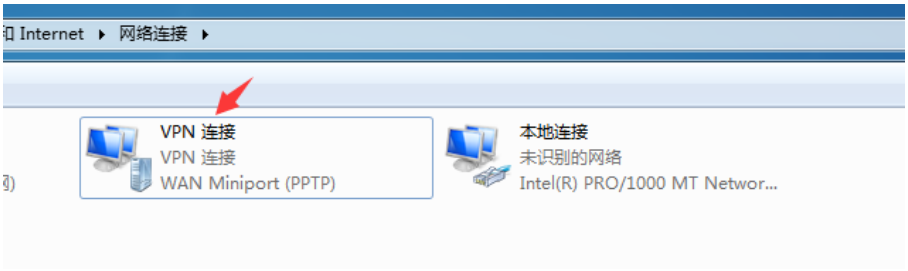
（3）然后在域控服务器上还需要安装 RADIUS 服务器作为认证功能：





（4）然后将运行远程 VPN 登录的员工账户的“网络访问权限”设置为运行：

（5）这样就可以通过创建 VPN 连接对企业内部服务进行访问：



11 需求十：性能监视

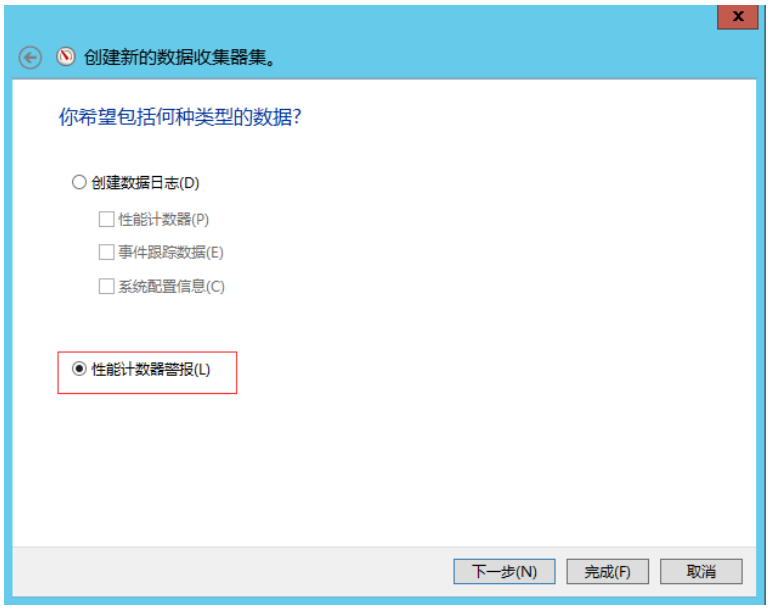
11.1 需求细则

由于企业服务器长时间运作并且内含关键数据，所以需要能够监视服务器的性能，对于可能出现的性能故障要有所警告。

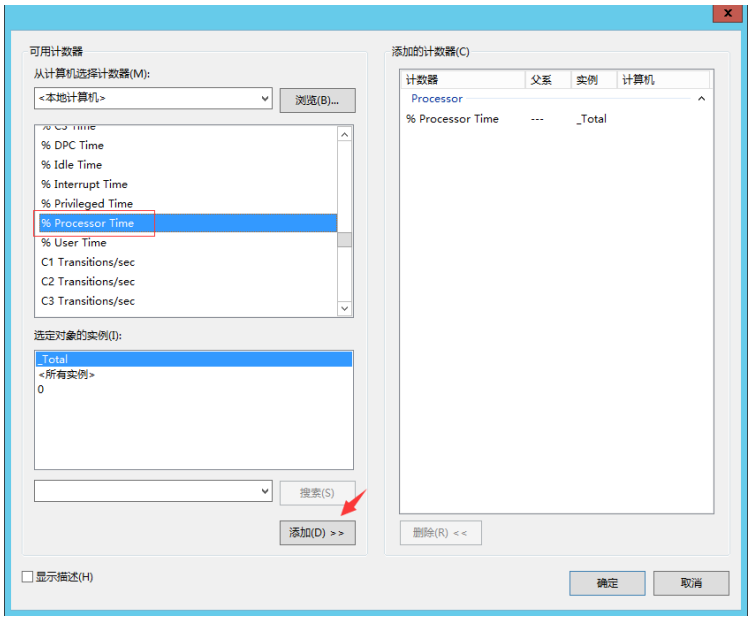
11.2 实施方案

（1）打开性能监视器，在数据收集器集用户定义中新建数据收集器集：

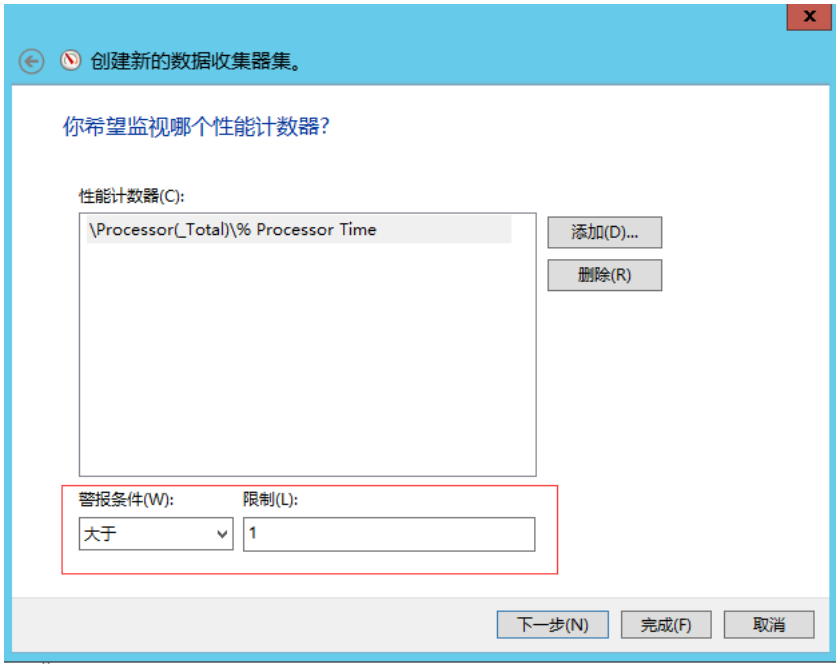
（2）选择手动创建，然后勾选性能计数器警报：



（3）添加需要监视的对象：



（4）设置警报条件：



（5）然后运行监视器，则可以对服务器的性能进行监视：