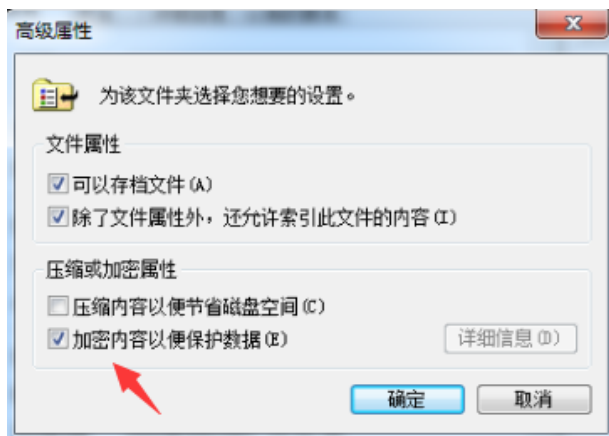


## 0x01 EFS 的使用

(1) 右键要加密的文件或目录，点击“属性”：



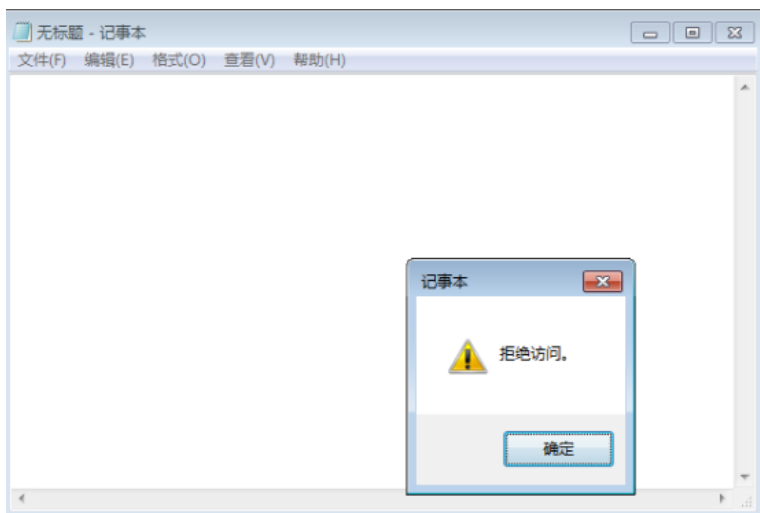
(2) 点击“高级”，勾选“加密内容以保护数据”：



(3) 可以看到文件名显示为绿色，说明成功 EFS 加密：

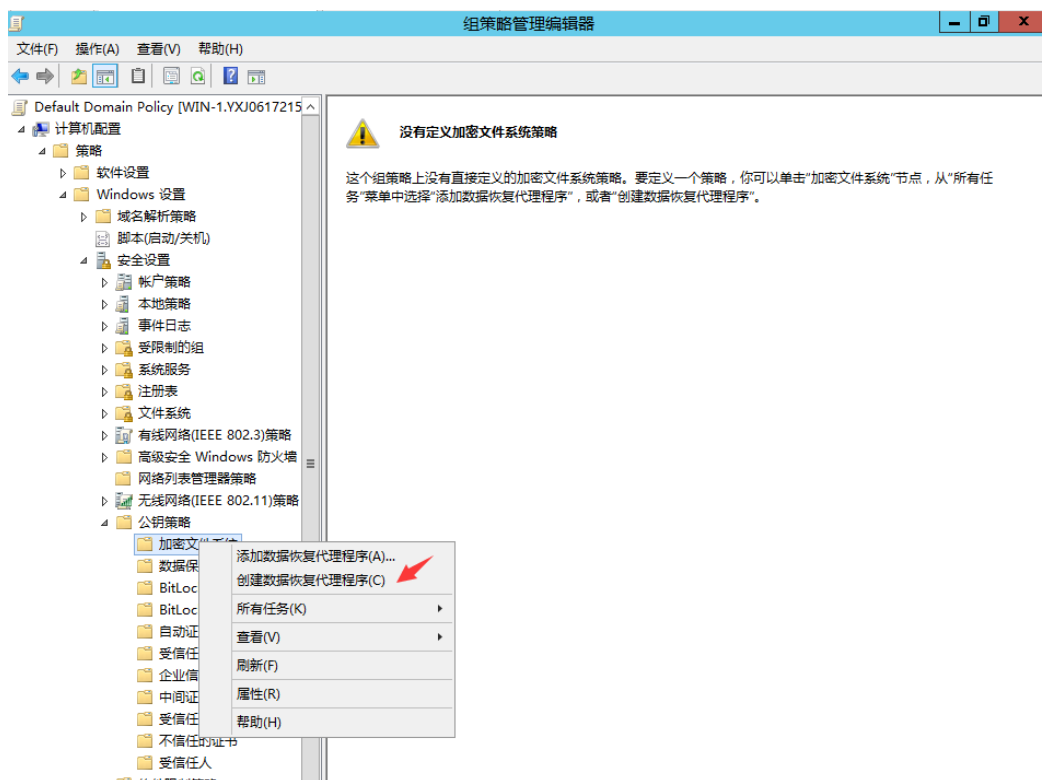


(4) 切换账号再次登录， 尝试访问该文件，发现弹出“拒绝访问”：

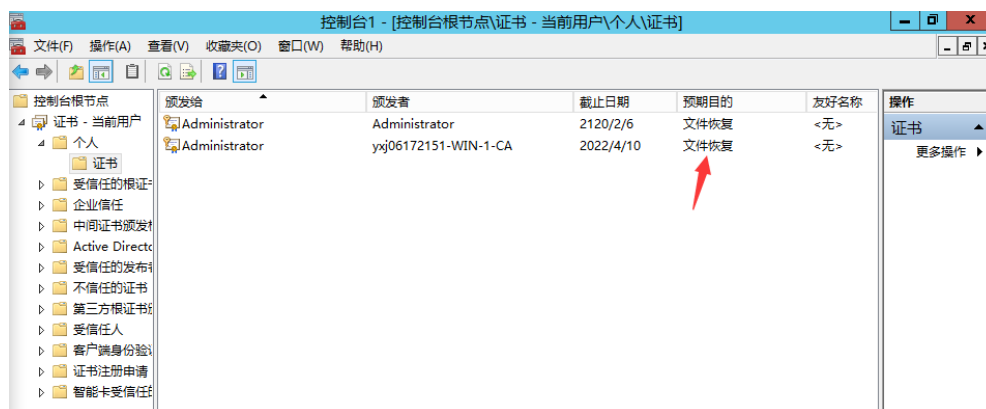


## 0x02 故障恢复代理的设置

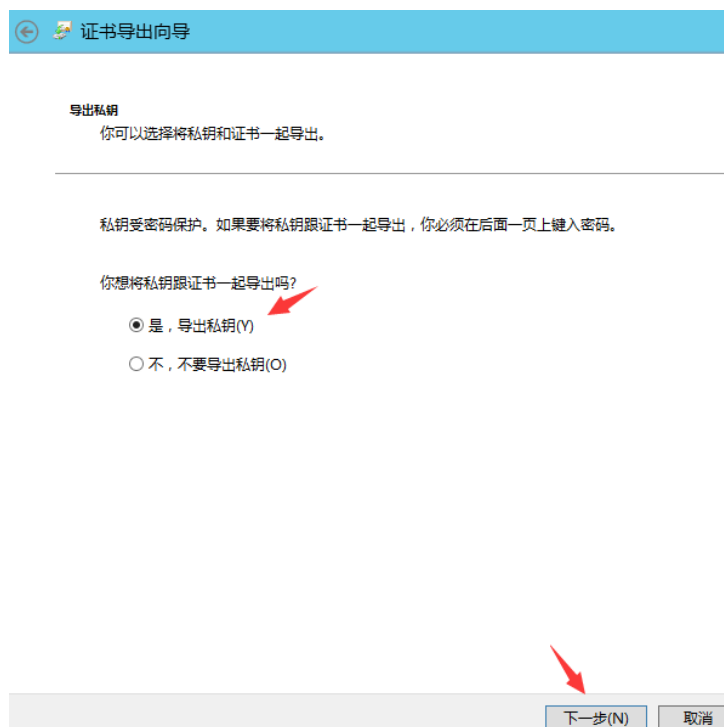
(1) 在域控上打开组策略管理器，找到公钥策略、加密文件系统，然后创建文件恢复代理：



(2) 然后我们导出该证书:



选择导出私钥:



设置密码:

证书导出向导

**安全**  
若要维护安全，必须保护安全主体的私钥或使用密码。

☐ 组或用户名(建议)(G)

添加(A)

移除(R)

☒ 密码(P):  
.....

确认密码(C):  
.....

下一步(N) 取消

证书导出向导

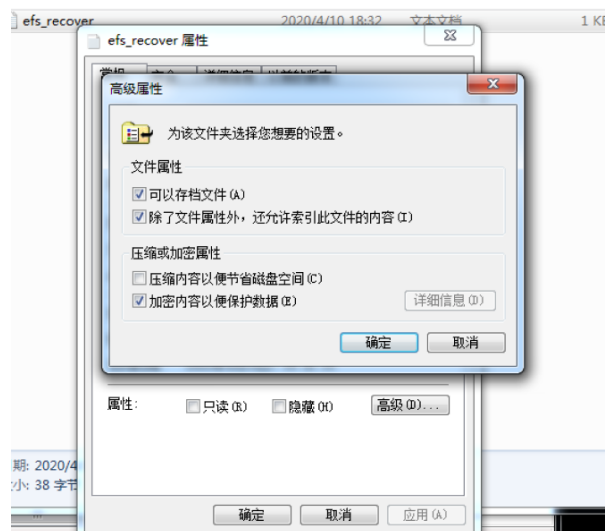
**要导出的文件**  
指定要导出的文件名

文件名(F):  
C:\efs\_recover.pfx

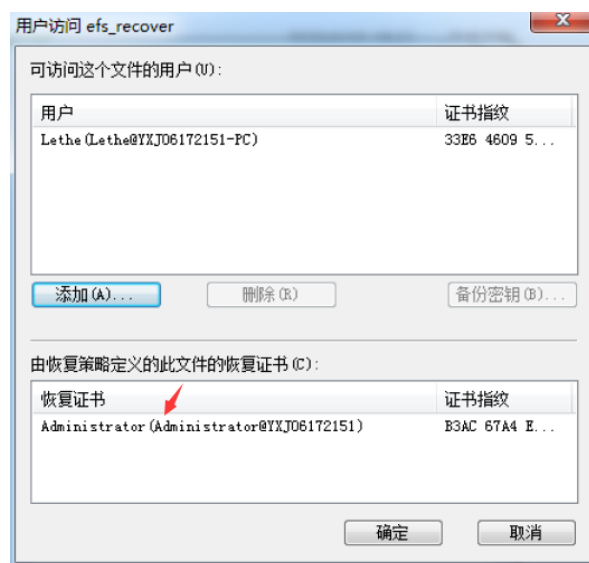
浏览(B)...

下一步(N) 取消

- (3) 使用 `gpupdate /force` 下发组策略。
- (4) 然后我们登录客户机再次创建一个加密文件，因为文件恢复代理只能恢复其创建后加密的文件：



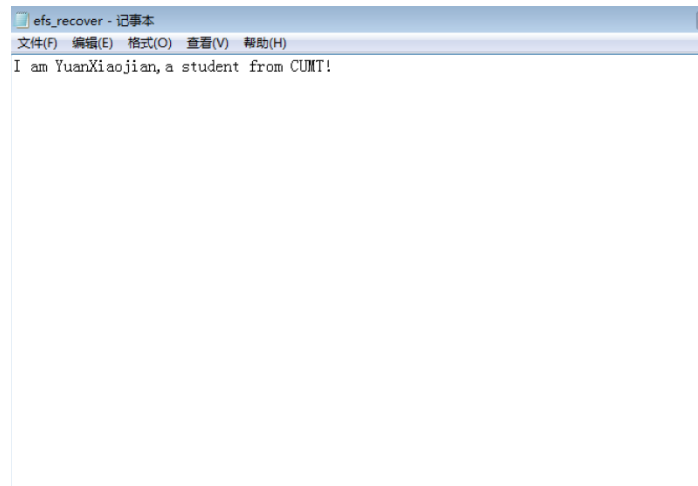
可以看到已经存在恢复代理：



(5) 然后我们用域管理员账号登录客户机，第二步中导出的私钥导入到客户机中，输入导出时设置的密码：

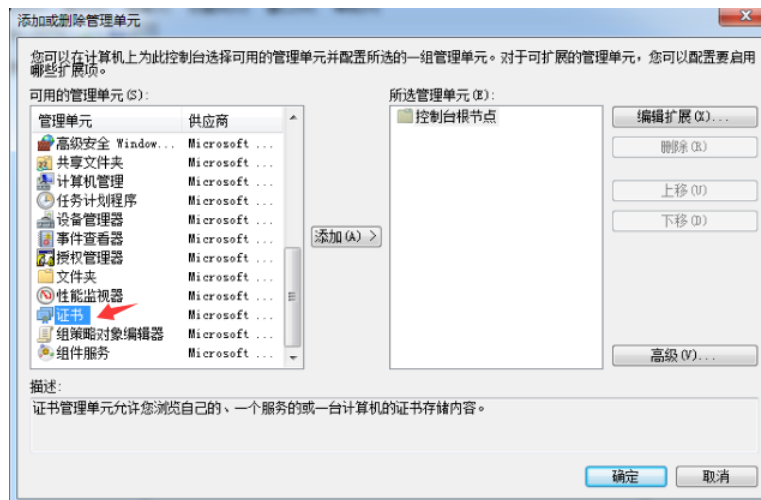


(4) 导入成功后，再次打开加密文件，发现成功打开：

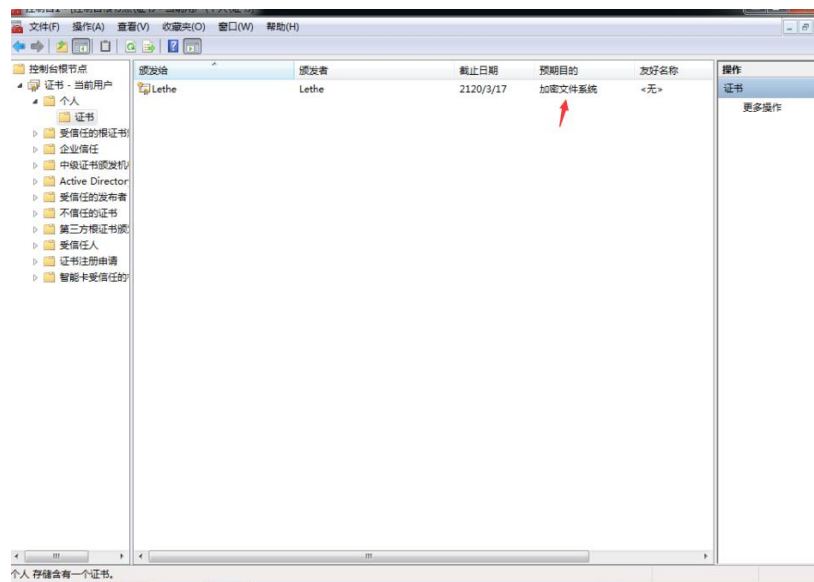


## 0x03 利用备份密钥进行数据恢复

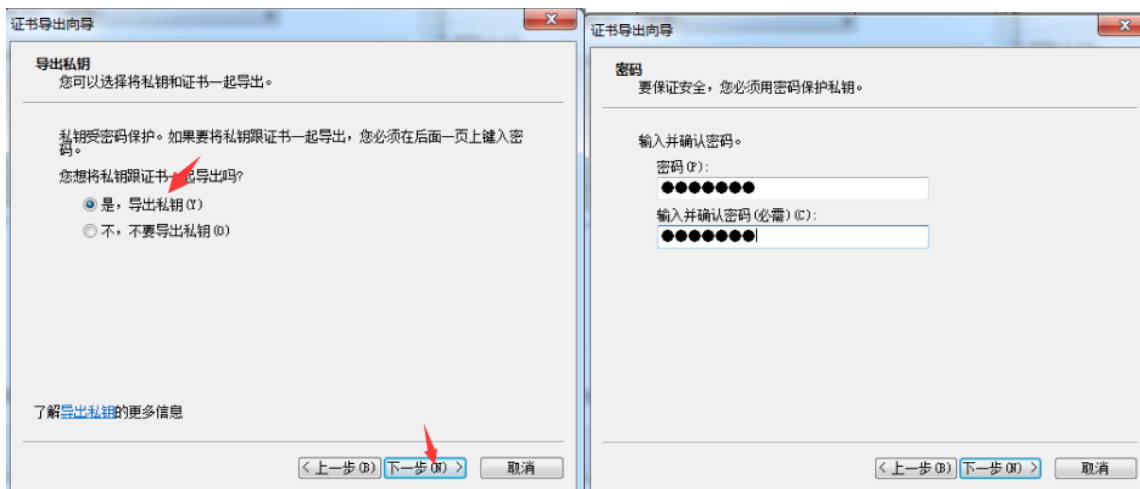
(1) 在控制台中输入 mmc，然后在控制台添加“证书”：



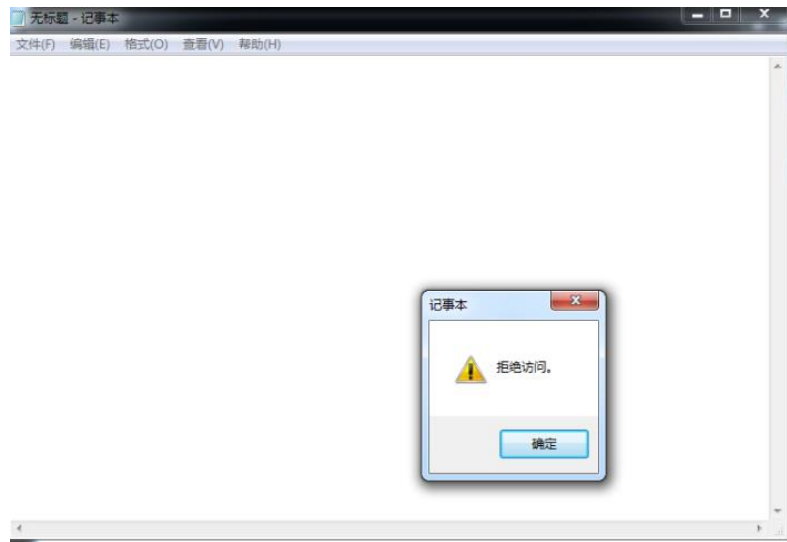
(2) 选择个人证书，可以看到加密文件系统的证书：



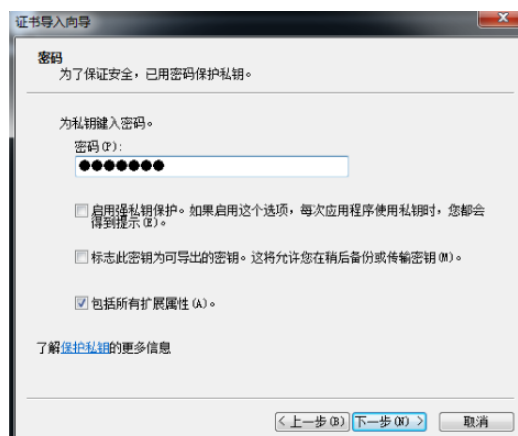
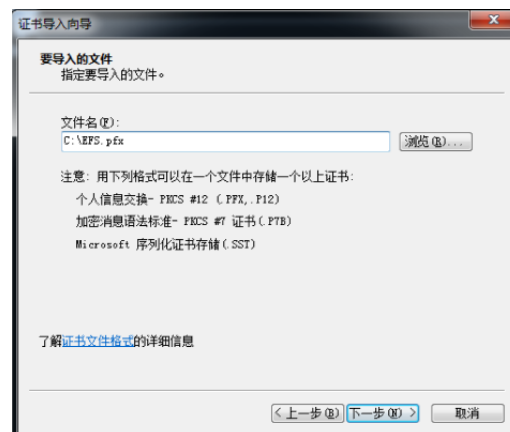
(3) 我们导出该证书，右键打开该证书，选择“复制到文件”，选择“导出私钥”：，并设置密码，然后保存为.pfx 文件：



(4) 导出后，假设我们删除了加密文件系统证书，并重新登录，发现无法打开加密文件了；

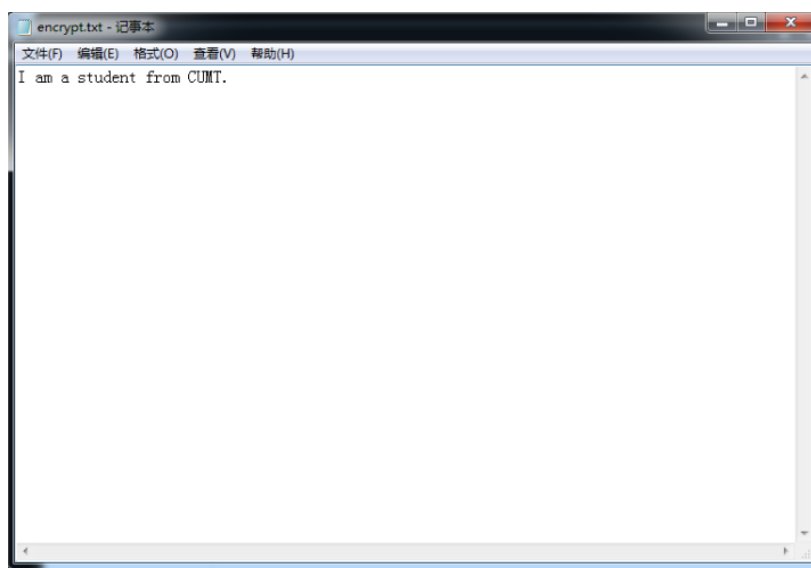


(5) 然后将我们前面导出的私钥文件重新导入：



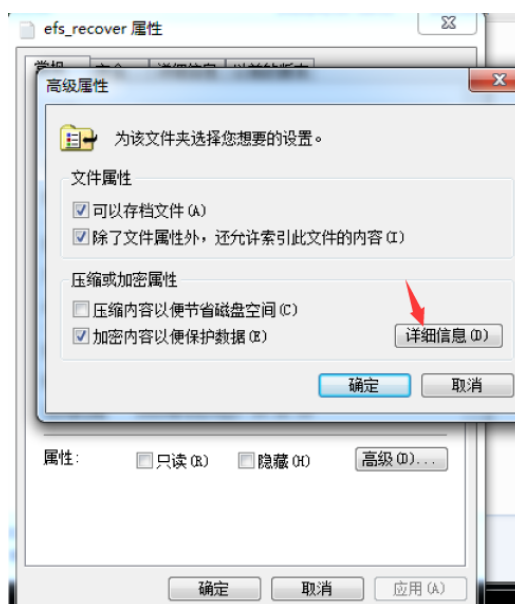


(6) 导入后再次打开，发现再次成功打开：

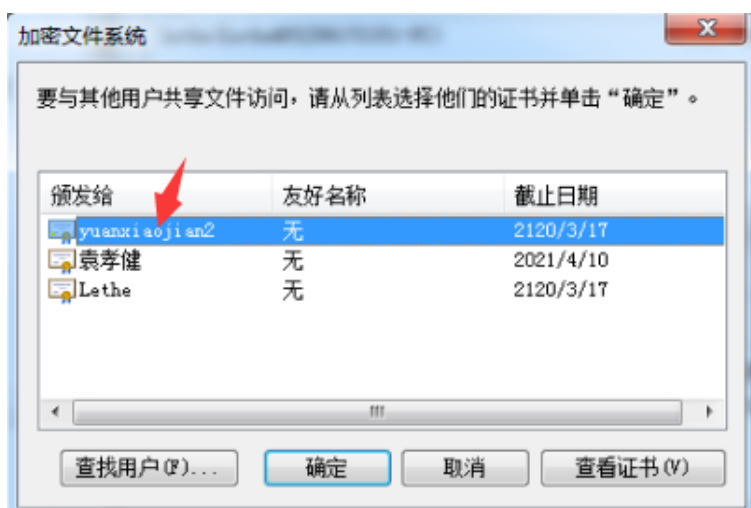


## 0x04 多用户共享加密文件

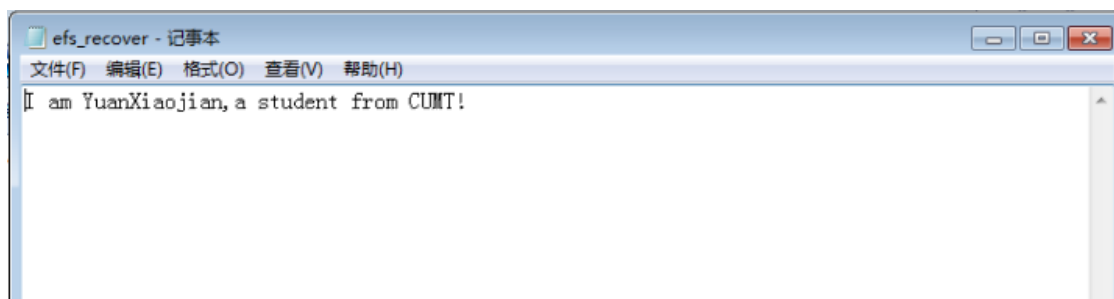
(1) 共享的用户需要也在客户机上进行过 efs 加密操作，才能有公私钥对，我们用加密文件所有者的账户登录客户机，在加密文件上右键“属性”——“高级”——“详细信息”：



(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:

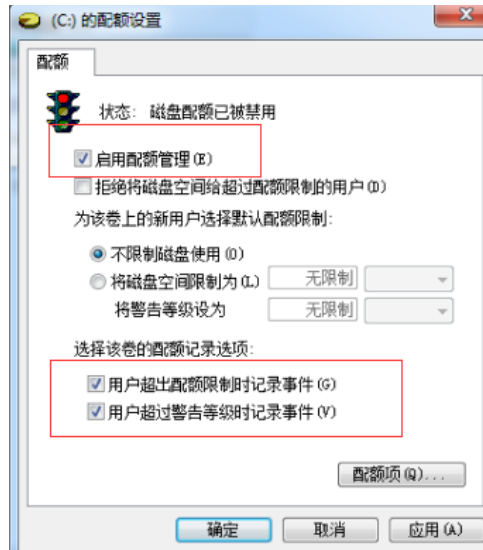


(3) 登录 yuanxiaojian2 用户，成功打开加密文件:

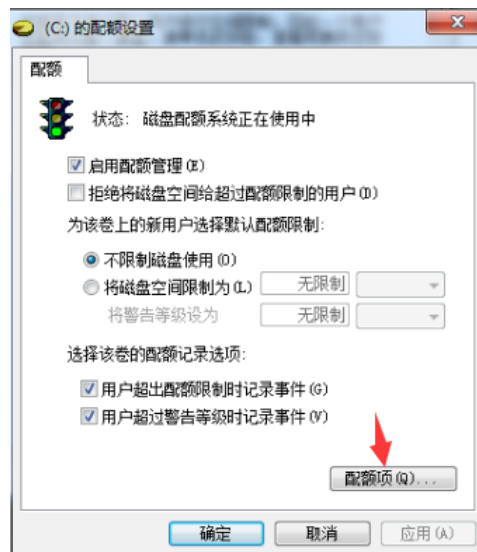


## 0x05 磁盘配额的使用


(1) 磁盘上右键属性—配额—显示配额设置，选择“启用配额管理”：



(2) 选择磁盘配额项：



(3) 查看配额项：



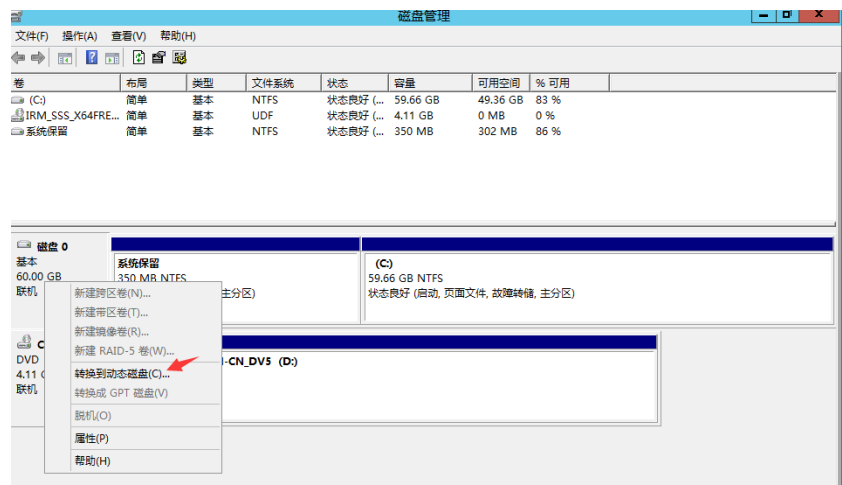
The screenshot shows the 'Quota' tab in Windows File Explorer for drive C:. The table lists various users and their quota settings.

状态	名称	登录名	使用量	配额限制	警告等级	使用...
正常	BUILTIN\Administrators	BUILTIN\Administrators	3.93 GB	无限制	无限制	暂缺
正常	[正在搜索名称]	S-1-5-80-956008885-34185...	4.49 GB	无限制	无限制	暂缺
正常	[正在搜索名称]	S-1-5-18	1.59 GB	无限制	无限制	暂缺
正常	[正在搜索名称]	S-1-5-19	28.82 ...	无限制	无限制	暂缺
正常	[正在搜索名称]	S-1-5-21-3451913502-6674...	26.48 ...	无限制	无限制	暂缺
正常	[正在搜索名称]	S-1-5-80-2620923248-4247...	1 KB	无限制	无限制	暂缺
正常	[正在搜索名称]	S-1-5-20	33.92 ...	无限制	无限制	暂缺
正常	[正在搜索名称]	S-1-5-21-231812040-16181...	26.22 ...	无限制	无限制	暂缺
正常	[正在搜索名称]	S-1-5-21-547972254-33733...	22.56 ...	无限制	无限制	暂缺
正常	[正在搜索名称]	S-1-5-21-3442302922-1636...	20.17 ...	无限制	无限制	暂缺
正常	yuan06172151\yuanxiaojian3	yuan06172151\yuanxiaojian3	15.27 ...	无限制	无限制	暂缺
正常	YXJ06172151\Administrator	YXJ06172151\Administrator	3 KB	无限制	无限制	暂缺

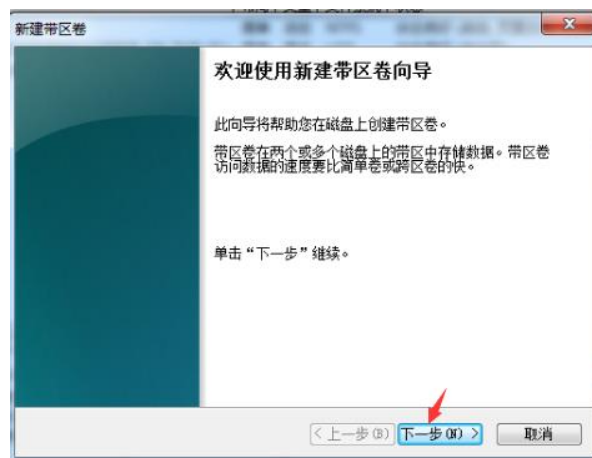
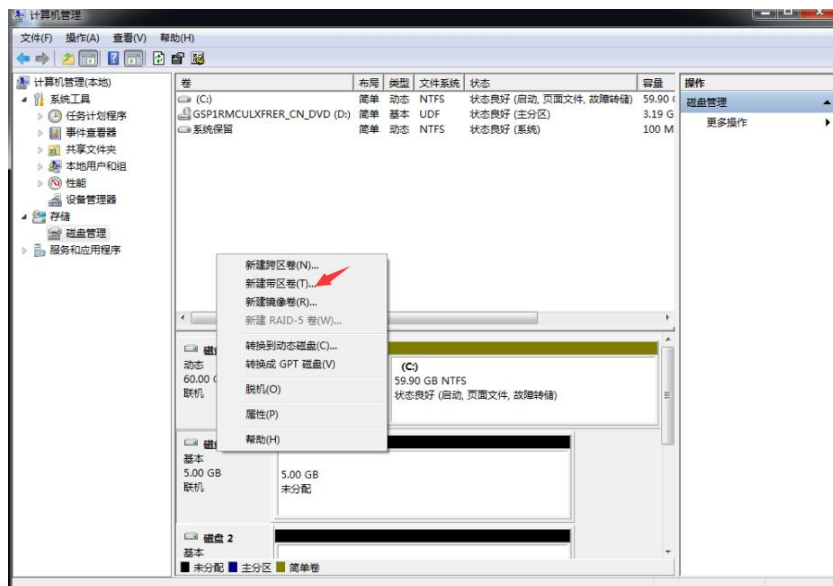
## 0x06 软 RAID 的使用

### 一、RAID0 的使用

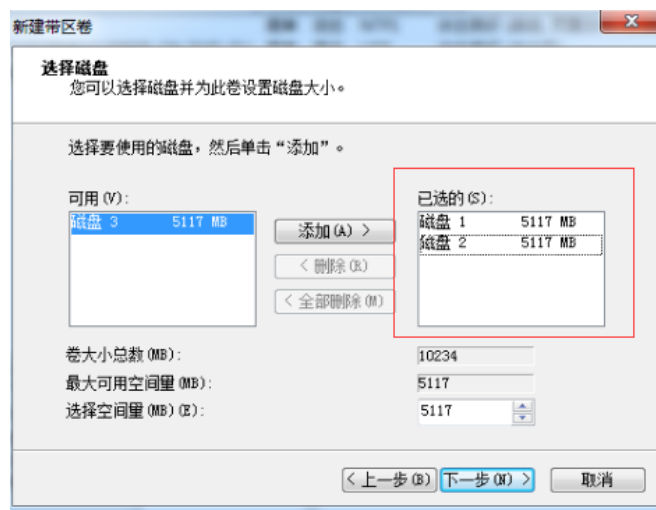
(1) 打开计算机管理—磁盘管理，然后将磁盘转换为动态磁盘：



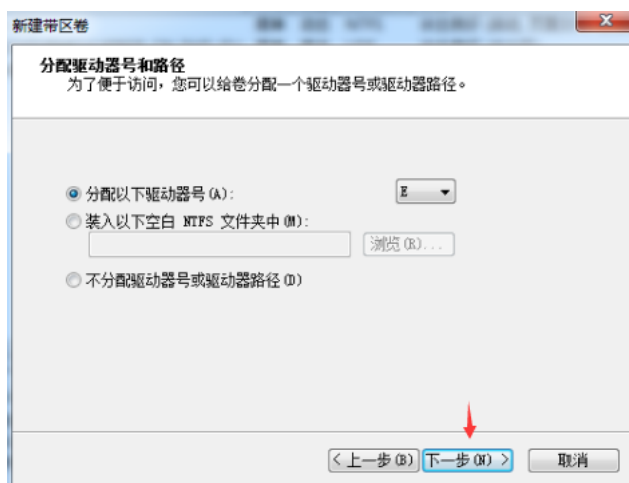
(2) RAID0 至少需要 2 块磁，盘右键“新建带区卷”：



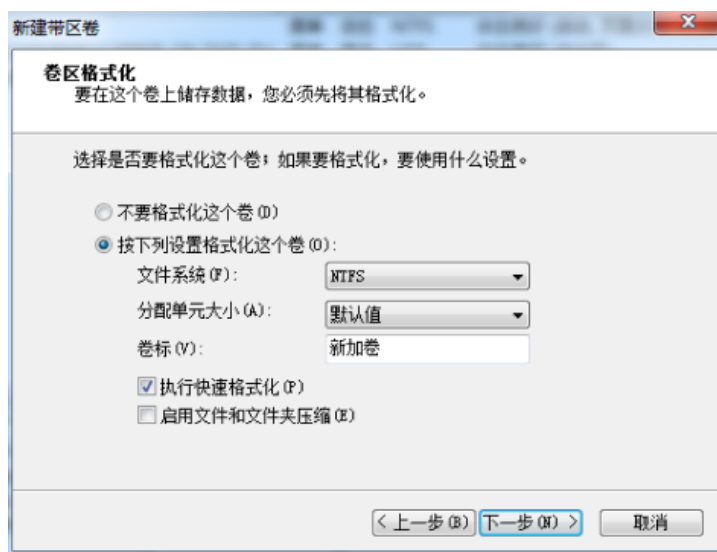
(2) 选择两个磁盘：



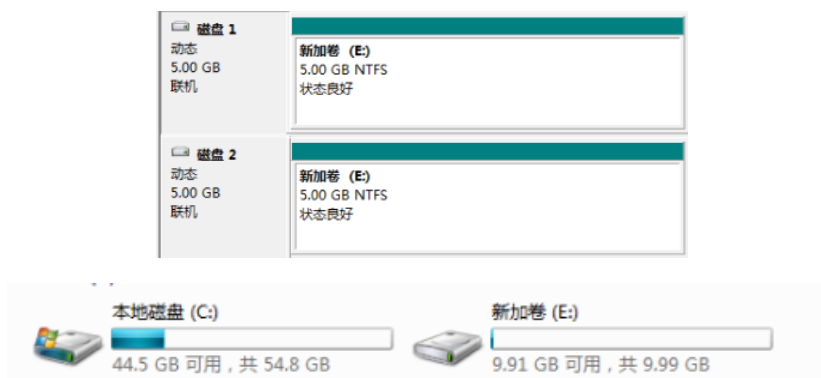
(3) 默认下一步:



默认选项即可，下一步:

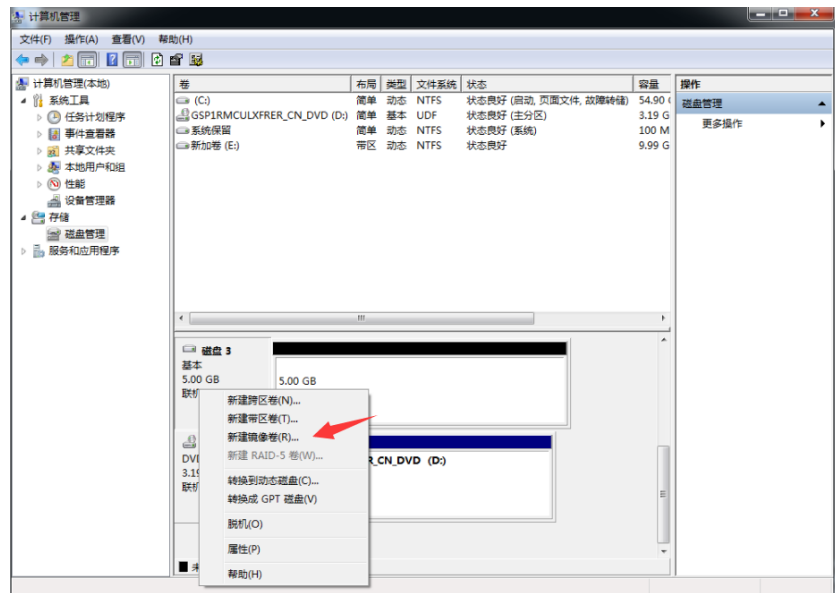


(4) 成功创建了 RAID0:

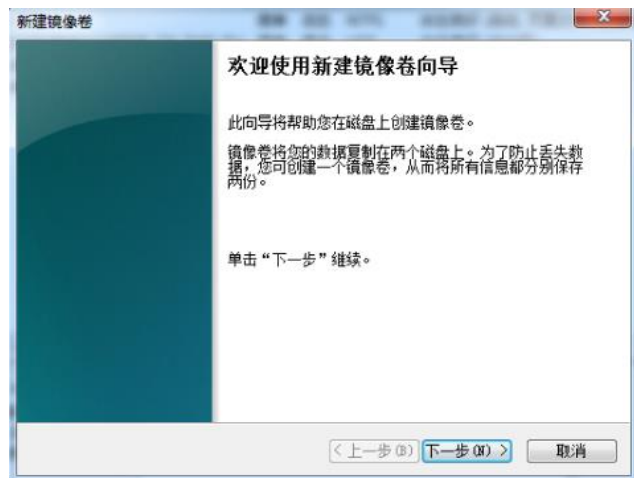


## 二、RAID1 的使用

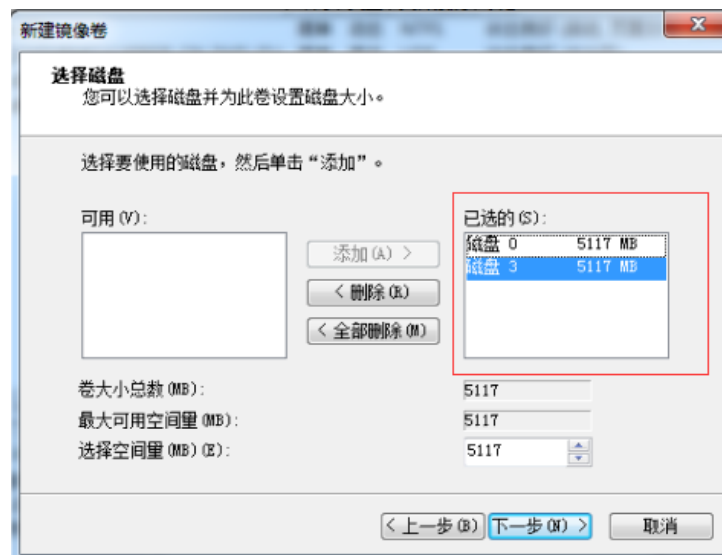
(1) RAID1 至少需要 2 块磁盘，右键选择新建“镜像卷”：



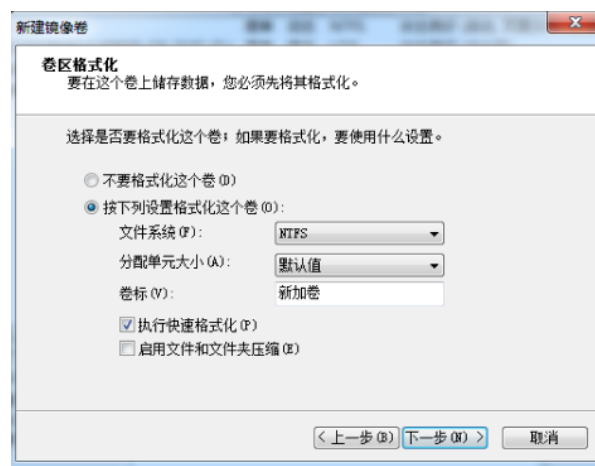
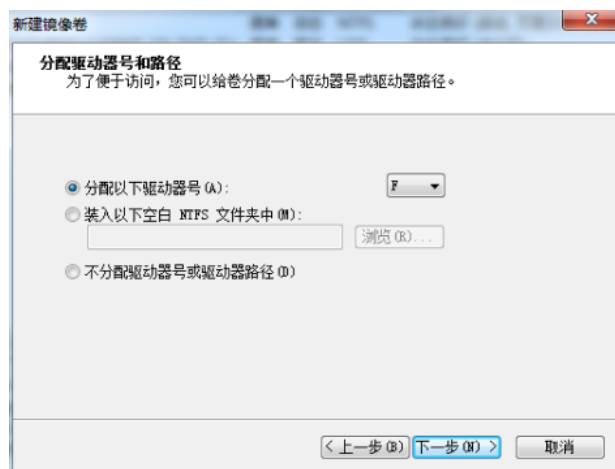
选择下一步：



(2) 选择两个未分配磁盘：

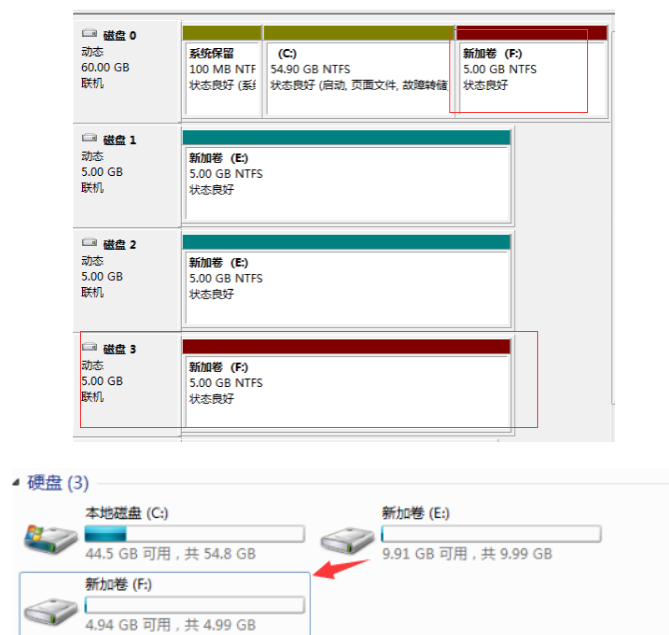


(3) 后续步骤使用默认选项即可：



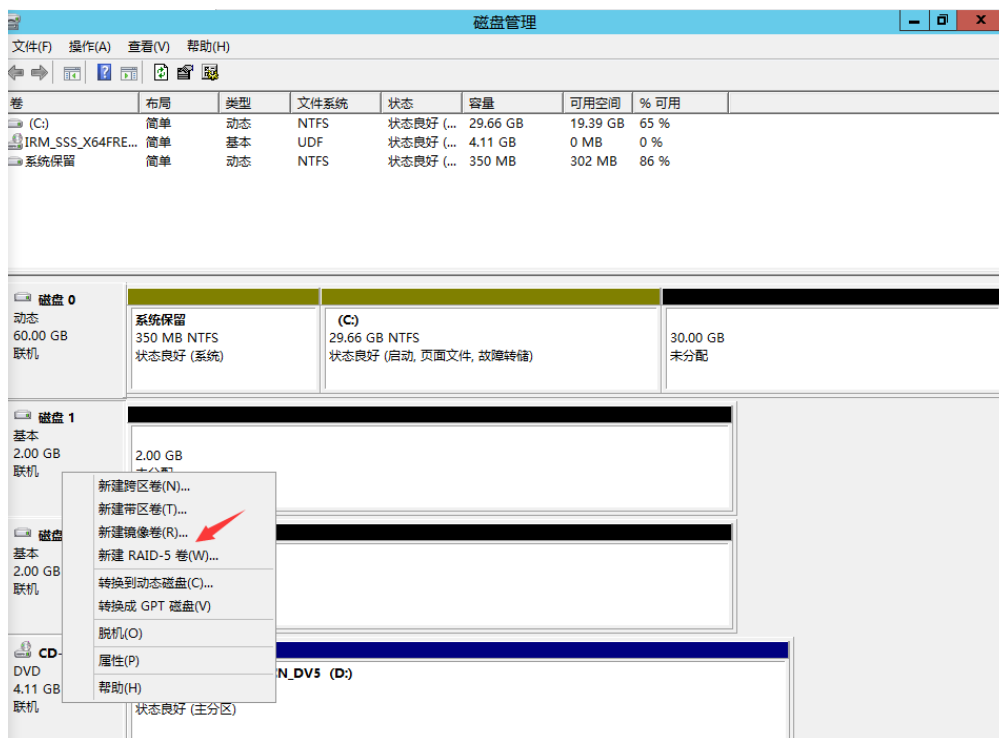


(4) 成功创建 RAID1:



三、RAID5 的使用

(1) RAID5 至少需要 3 块磁盘，由于 win7 某些版本不支持创建 RAID5，因此选择这里换用服务器进行配置，右键选择“新建 RAID-5 卷”：



选择下一步：



(2) 选择 3 个可用的磁盘：



(3) 选项选项默认即可，选择下一步：

新建 RAID-5 卷

**分配驱动器号和路径**  
为了便于访问，你可以给卷分配一个驱动器号或驱动器路径。

☒ 分配以下驱动器号(A): E ▼

☐ 装入以下空白 NTFS 文件夹中(M):  
 浏览(R)...

☐ 不分配驱动器号或驱动器路径(D)

< 上一步(B)   下一步(N) >   取消

新建 RAID-5 卷

**卷区格式化**  
要在这个卷上储存数据，你必须先将其格式化。

选择是否要格式化这个卷；如果要格式化，要使用什么设置。

☐ 不要格式化这个卷(D)

☒ 按下列设置格式化这个卷(O):

文件系统(F): NTFS ▼

分配单元大小(A): 默认值 ▼

卷标(V): 新加卷

☐ 执行快速格式化(Q)

☐ 启用文件和文件夹压缩(E)

< 上一步(B)   下一步(N) >   取消

(4) 成功创建 RAID-5 卷：

磁盘 0 动态 60.00 GB 联机	系统保留 350 MB NTFS 状态良好 (系统)	(C:) 29.66 GB NTFS 状态良好 (启动, 页面文件, 故障转储)	新加卷 (E:) 2.00 GB NTFS 状态良好	28.00 GB 未分配
磁盘 1 动态 2.00 GB 联机	新加卷 (E:) 2.00 GB NTFS 状态良好			
磁盘 2 动态 2.00 GB 联机	新加卷 (E:) 2.00 GB NTFS 状态良好			

设备和驱动器 (3)



本地磁盘 (C:)  
19.3 GB 可用, 共 29.6 GB



新加卷 (E:)  
3.96 GB 可用, 共 3.99 GB