Windows安全原理与技术

— 第七章：文件系统安全

王轶骏， Eric Ericwyj@sjtu.edu.cn

SJTU.INFOSEC.A.D.T, 2008

文件系统基础

- 基本磁盘
  - 分区
  - 主分区
  - 扩展分区
  - 逻辑驱动器
- 动态磁盘
  - 卷
  - 卷集

Windows 2000的NTFS文件系统

- **NTFS的特性**
  - 访问控制
  - 加密
  - 压缩
  - 磁盘配额
  - 多数据流
  - 重新解析点
  - 改动日志
  - 稀疏文件支持
- **NTFS的版本**
  - NTFS v5

NTFS文件属性

- 主文件表（MFT, Master File Table）
  - NTFS卷格式化时将创建并初始化MFT。
  - MFT是文件系统的索引。每个文件和目录都在MFT中具有一个对应的1KB大小的条目。
- 文件属性
  - 标准信息：时间（创建、修改和访问），属性（隐藏、系统、存档和只读），链接数等。
  - 文件名称。
  - 安全性描述。
  - 数据：未命名流，命名流。
  - 对象标识符。

NTFS的数据流（Data Stream）

- 建立一个普通文件
  - echo This is an test file > testfile.txt
- 创建（命名）数据流
  - echo This is an ADS > testfile.txt:hidden
  - echo This is an ADS txt > testfile.txt:hidden.txt
  - type c:\windows\system32\calc.exe > testfile.txt:calc2.exe
- 查看/运行（命名）数据流
  - more < testfile.txt:hidden
  - notepad testfile.txt:hidden.txt
  - start .\testfile.txt:calc2.exe
- 检测
  - Lads.exe

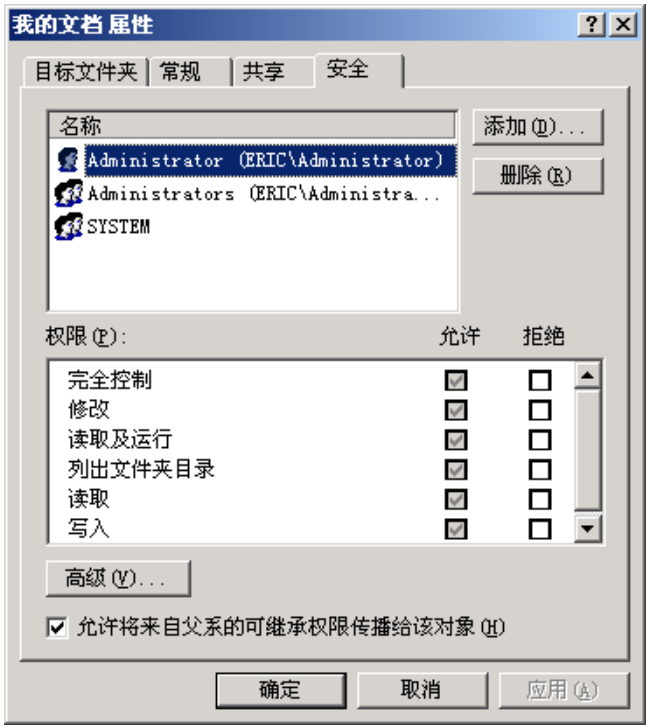
文件系统的转换 FAT→NTFS

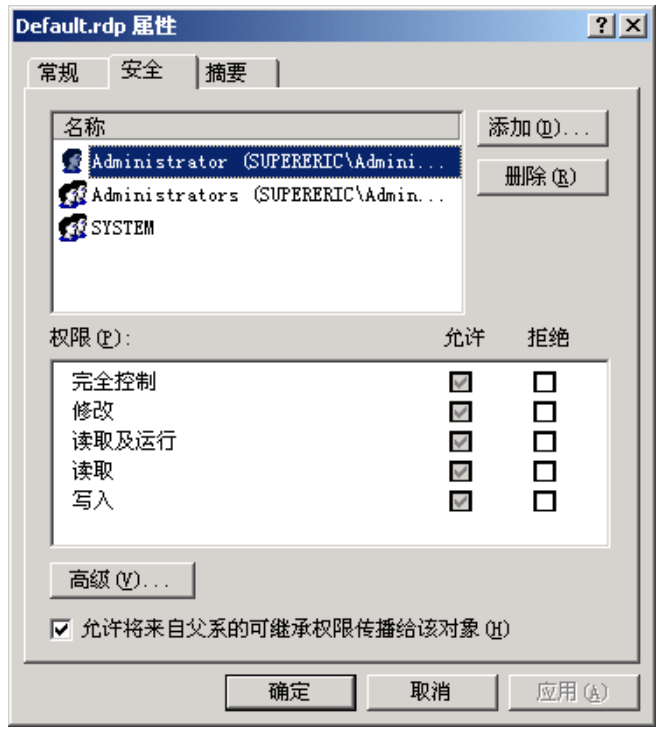
- 使用convert.exe
  - 无需备份原有的文件系统
  - 转换过程不可逆向
  - 转换的NTFS文件系统性能没有初始就格式化为NTFS的文件系统好

CONVERT volume /FS:NTFS [/V]

NTFS的权限控制

- Windows 2000系统的NTFS标准权限控制与Windows NT系统中几乎完全一样。



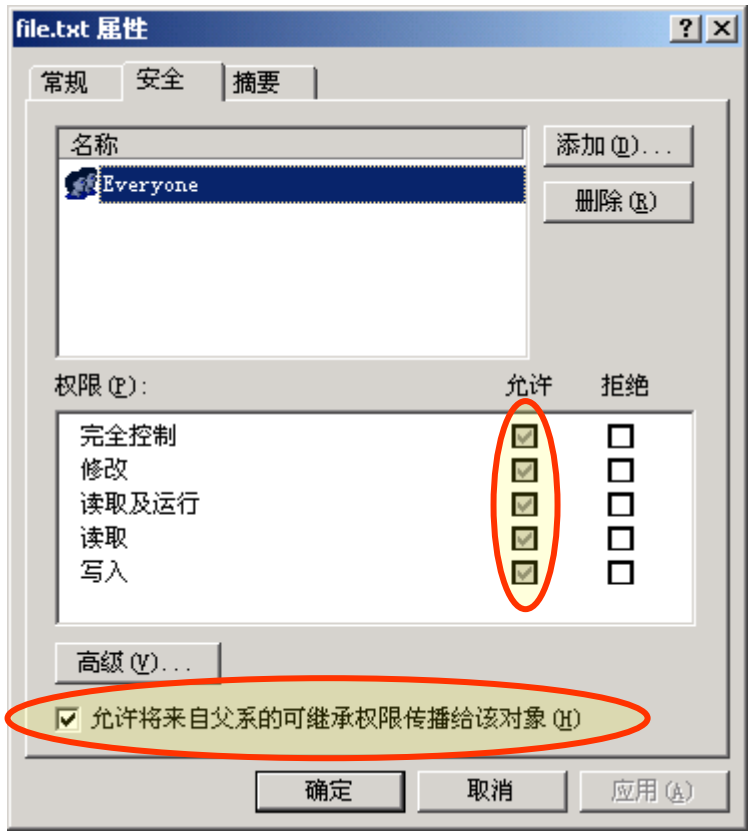


NTFS权限控制的原则

- 权限积累
- 文件权限优先于文件夹权限
- “拒绝”权限优先于其他权限

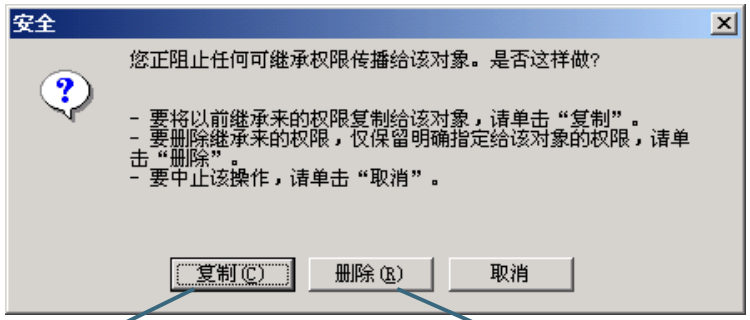
NTFS权限继承

- “允许将来自父系的可继承权限传播给该对象”复选框表明是否允许从父文件夹中继承权限。
- 颜色为灰色的权限表明是从父文件夹中继承下来的权限

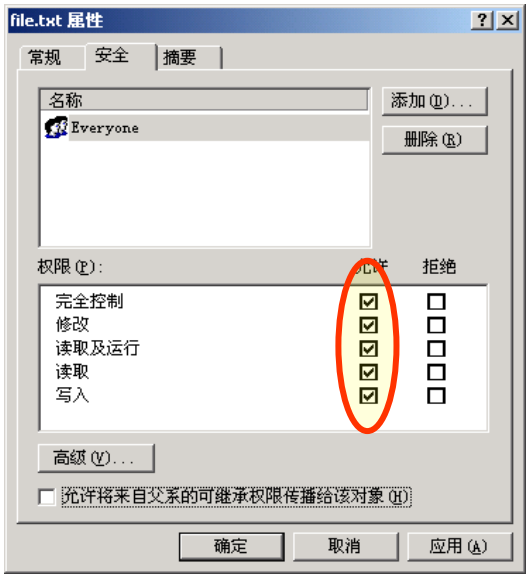


不选中则将阻止权限继承 ←

阻止权限继承

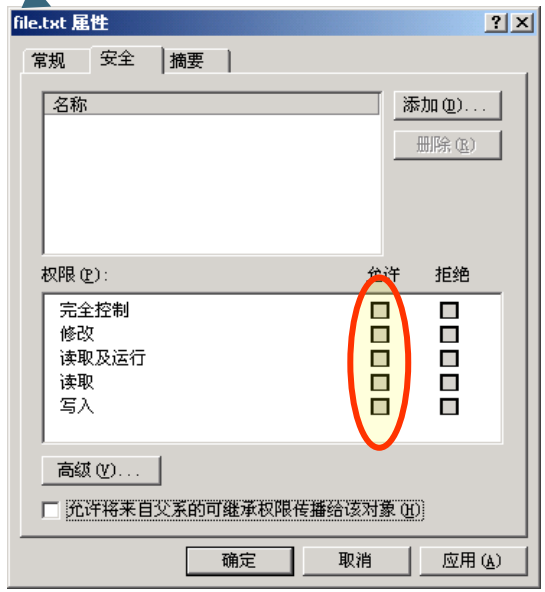


复制继承的权限



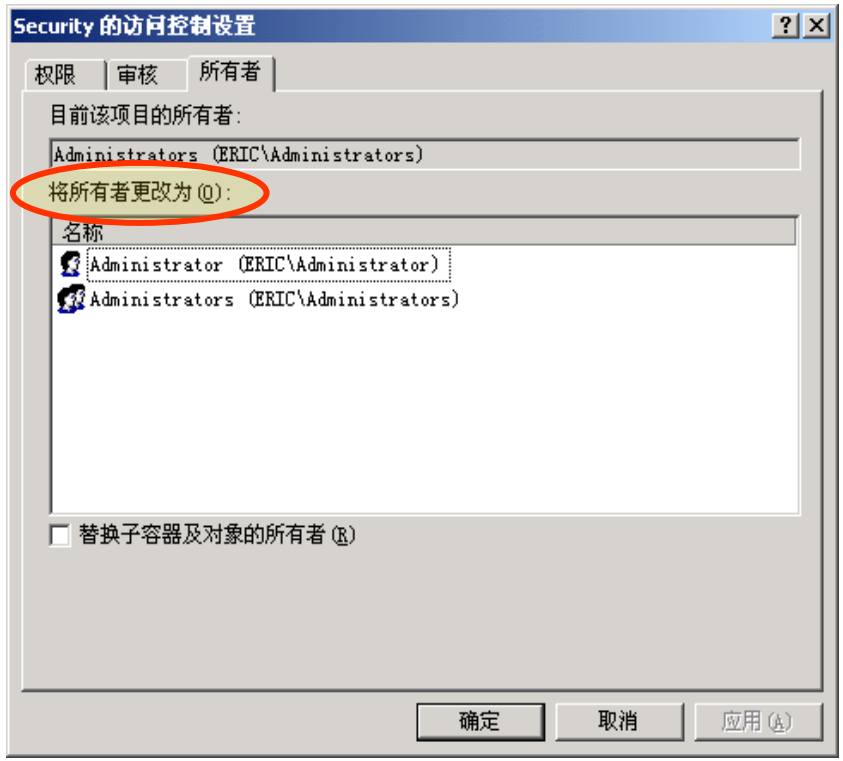
均阻止以后继承的权限

删除继承的权限



特殊的NTFS权限

- 更改权限的权限
- 更改所有者的权限
  - Administrators组的成员始终都能够获取一个文件或文件夹的所有权。



Cacls命令行工具

- 作用：显示和修改文件和文件夹的访问控制列表。
- 语法：cacls filename [Options]

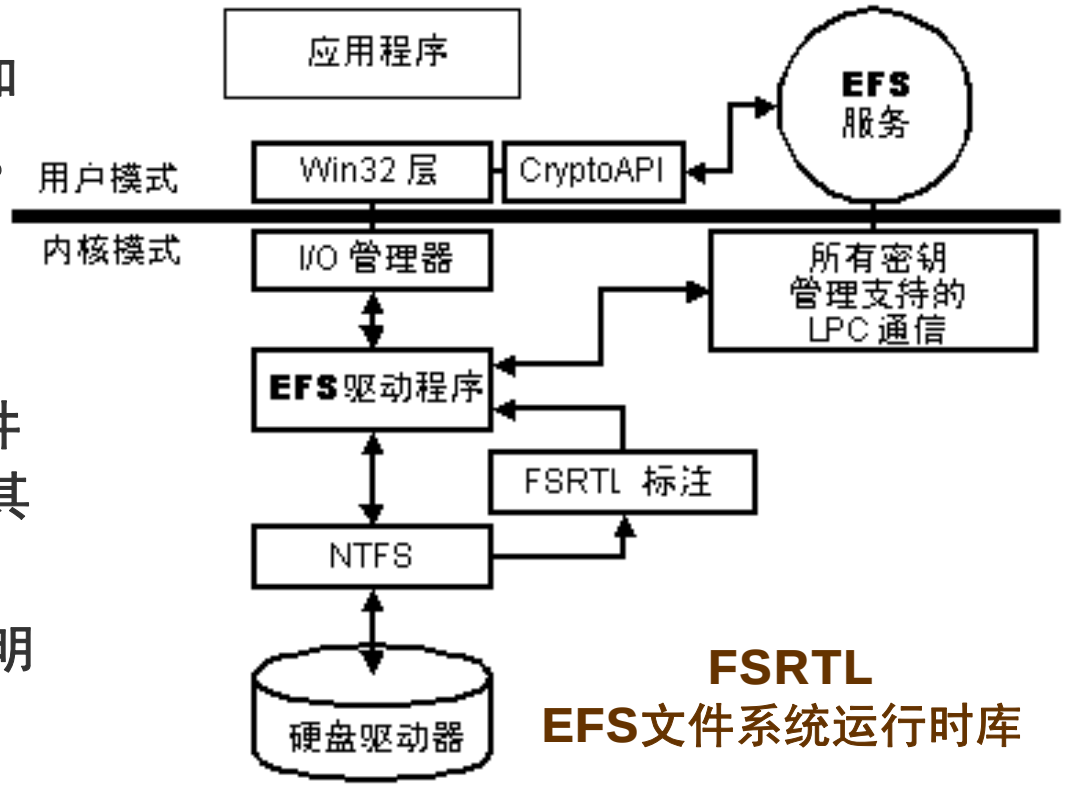
选项	描述
/ t	改变当前目录及所有子目录
/ e	编辑ACL而不替换
/ c	在出现拒绝访问错误时继续
/g user:perm	赋予指定用户的访问权限，perm可为：R（读取）；C（更改）；F（完全控制）
/r user	撤销指定用户的访问权限（必须与/e一起使用）
/p user:perm	替换指定用户的访问权限，perm可为：N（无）；R（读取）；C（更改）；F（完全控制）
/d user	拒绝指定用户的访问

加密文件系统（EFS）

- NTFS文件系统的访问控制能够被绕过。
  - 物理途径接触系统
  - 使用特殊的工具
- 数据加密是唯一解决方案 —— EFS
  - 基于公私钥机制，安全性强。
  - 作为综合系统服务运行，防止内存泄密。
  - 提供数据恢复功能。
  - 对于用户透明，无需手工加解密。

EFS的结构

- **Win32 API函数**
  - 提供编程接口，如EncryptFile, DecryptFile函数。
- **EFS服务（用户态）**
  - 针对CryptoAPI提供文件加密密钥并生成DDF和DRF。
  - 安全子系统的一部分。
- **EFS驱动程序（内核态）**
  - 与EFS服务通信，请求文件加密密钥、DDF、DRF和其他密钥管理服务。
  - 将信息送到FSRTL，以透明地执行各种文件系统操作。

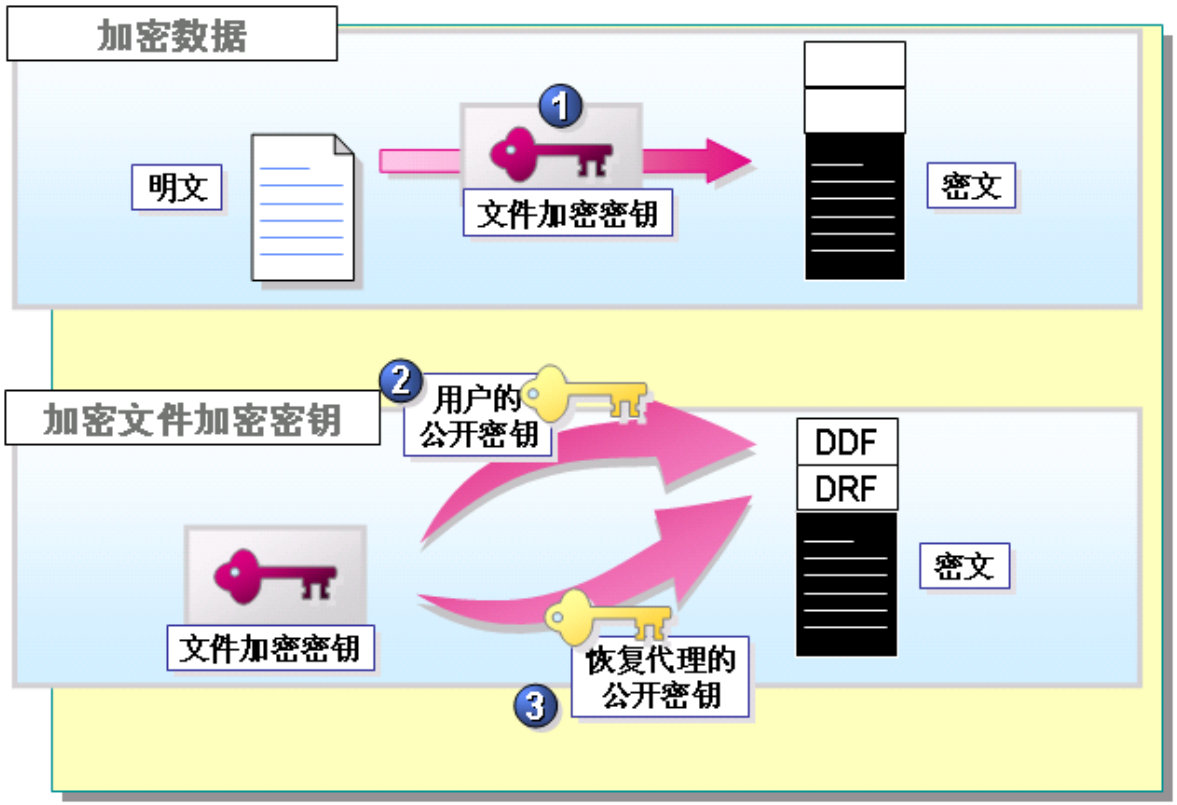


FSRTL
EFS文件系统运行时库

EFS的数据加解密过程

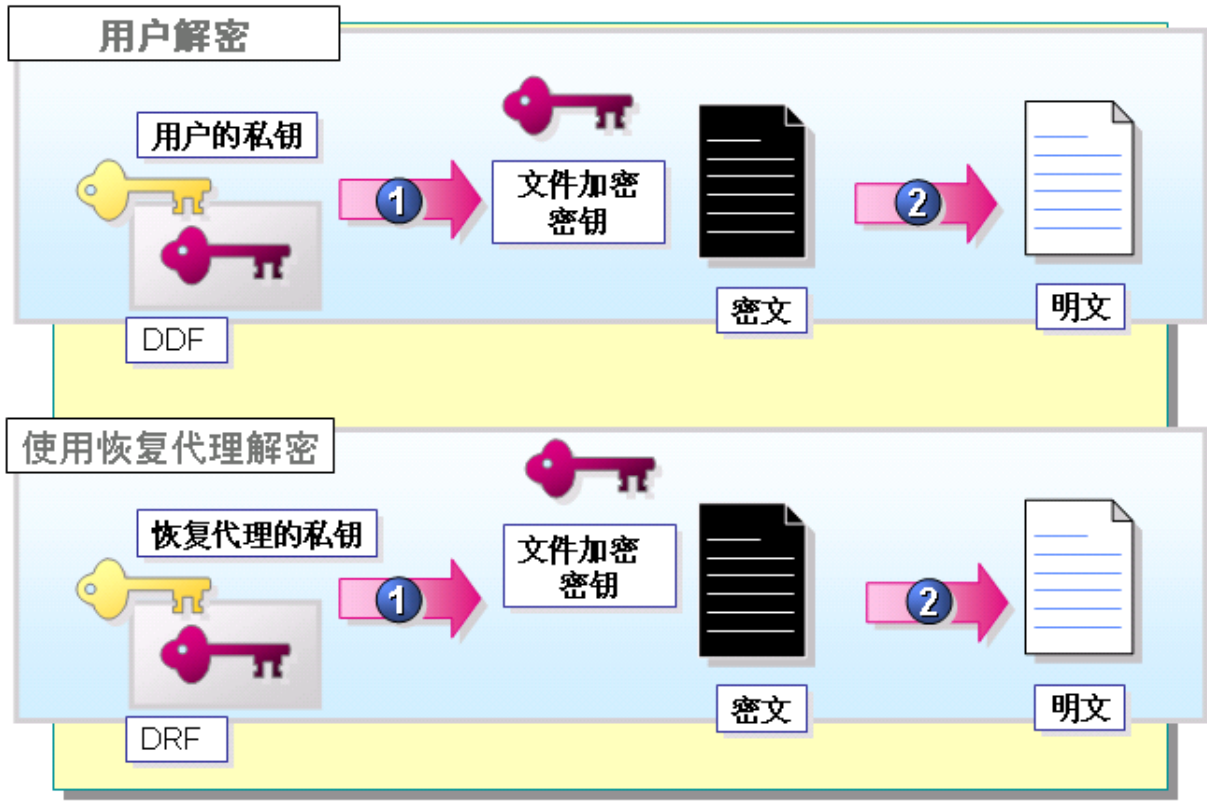
- 加密过程
  - 文件被拷贝到临时文本文件。
  - 文件被一个随机产生的Key（FEK）所加密。
  - 数据加密区域（DDF）产生，使用用户的公钥对FEK加密。
  - 数据恢复区域（DRF）产生，使用恢复代理的公钥对FEK加密。
  - 包含加密数据、DDF及所有DRF的加密文件被写入磁盘。
  - 在第一步中创建的文本文件被删除。
- 解密过程
  - 使用DDF以及用户的私钥（或者恢复代理的私钥）解密FEK。
  - 使用FEK解密文件。

EFS的数据加密过程



- 文件加密密钥（FEK）
- 数据加密区域（DDF）
- 数据恢复区域（DRF）

EFS的数据解密过程

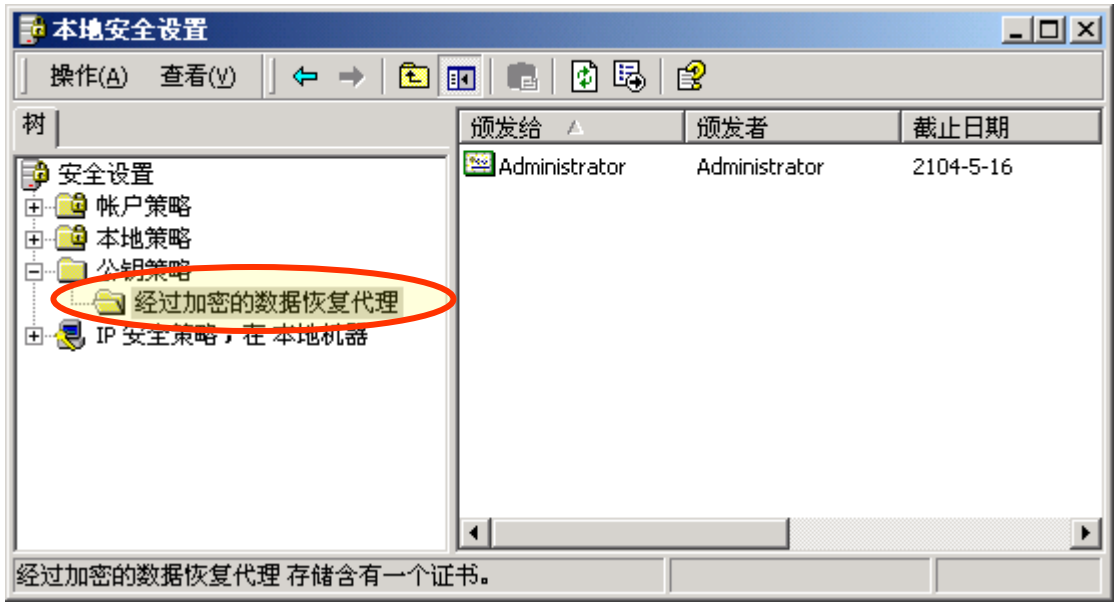

用户解密
用户的私钥
1
文件加密
密钥
2
密文
明文
DDF
使用恢复代理解密
恢复代理的私钥
1
文件加密
密钥
2
密文
明文
DRF

EFS的故障恢复

- 用处
  - 加密数据的用户离开了
  - 加密数据的用户帐号被管理员不小心删除了
  - 加密数据的用户安全密钥/证书被不小心删除了
  - 操作系统崩溃，需要重新安装系统了
- EFS通过实施故障恢复策略来提供内置的数据故障恢复。
  - 故障恢复代理拥有特殊证书和相关私钥，允许在故障恢复策略的影响范围内恢复数据。

配置数据恢复代理策略

- “组策略”/ “本地安全策略” → “安全设置”→ “公钥策略”→“经过加密的数据恢复代理”
- 域管理员是默认的恢复代理；本地系统的管理员是单机系统的恢复代理。



EFS的优势

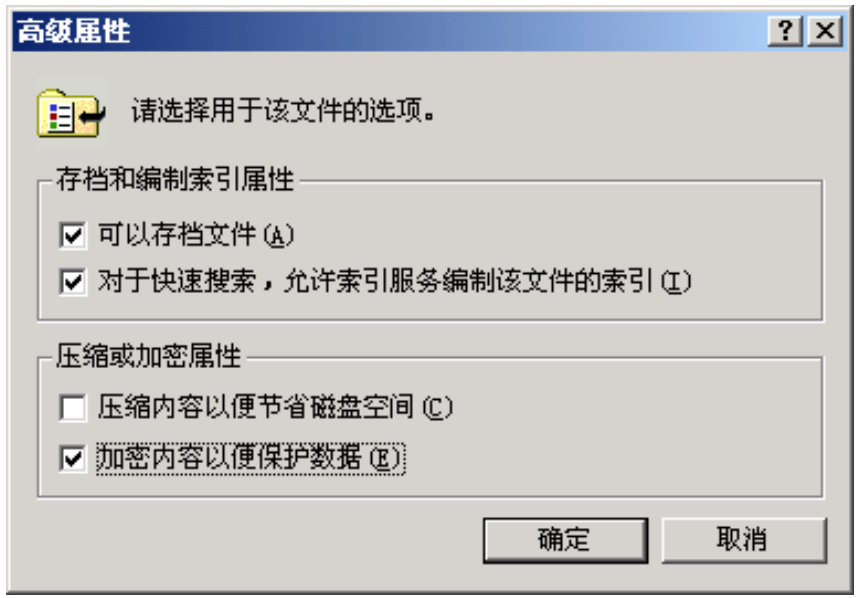
- 基于公钥的加密技术。
  - 使用了Windows的CryptoAPI结构
  - 结合了对称加密和非对称加密的优点
- 与文件系统紧密结合，防止恶意攻击。
- 无须管理上的设置即可使用，在操作上对用户完全透明。
- 既支持对单个文件，也支持对完整目录的加解密。
- 提供内置的数据恢复支持。

EFS的局限

- 增加花费、降低性能。
- 仅对磁盘上的文件进行加密，不包括网络上的传输加密。
- 病毒监测程序无法起到作用。
- 物理失窃可能导致数据被解密。
- 其他：
  - DESX加密算法不够强壮。
  - 系统文件不能被加密。
  - 太多的恢复代理将影响性能。
  - 不支持文件共享，仅创建DDF的用户能访问。

EFS的用户操作

- 通过Windows 2000的资源管理器



- 通过命令行下的Cipher.exe

加密文件的复制

一般情况下，Windows 2000将事先解密文件，然后复制解密后的文件到磁盘上。复制过去的文件属性将根据其目的文件夹的属性而变化。

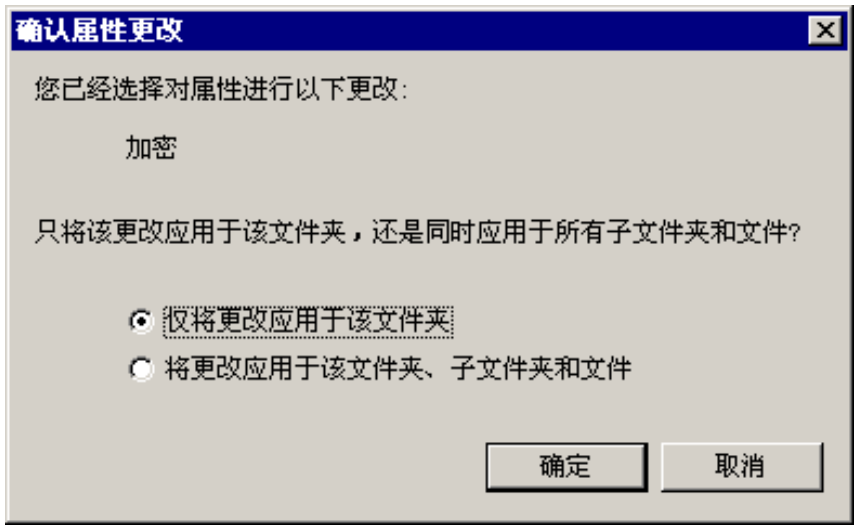
开始加密	复制到	新文件
目录和文件都加密	目录未加密	加密
目录和文件都加密	目录加密	加密
目录加密，文件未加密	目录加密	加密
目录加密，文件未加密	目录未加密	未加密
目录和文件都未加密	目录加密	加密
目录和文件都未加密	目录未加密	未加密

加密文件的移动

- 在同一磁盘里移动加密文件，那么只改变文件分配表，所以文件属性不变。
- 在不同磁盘里移动加密文件，其实是把旧文件删除，在另外的磁盘里复制新的文件，所以新的文件属性将根据目的文件夹的属性而变化。

对文件夹的加密

- 加密操作的选择
  - “仅将更改应用于该文件夹”
  - “将更改应用于该文件夹、子文件夹和文件”



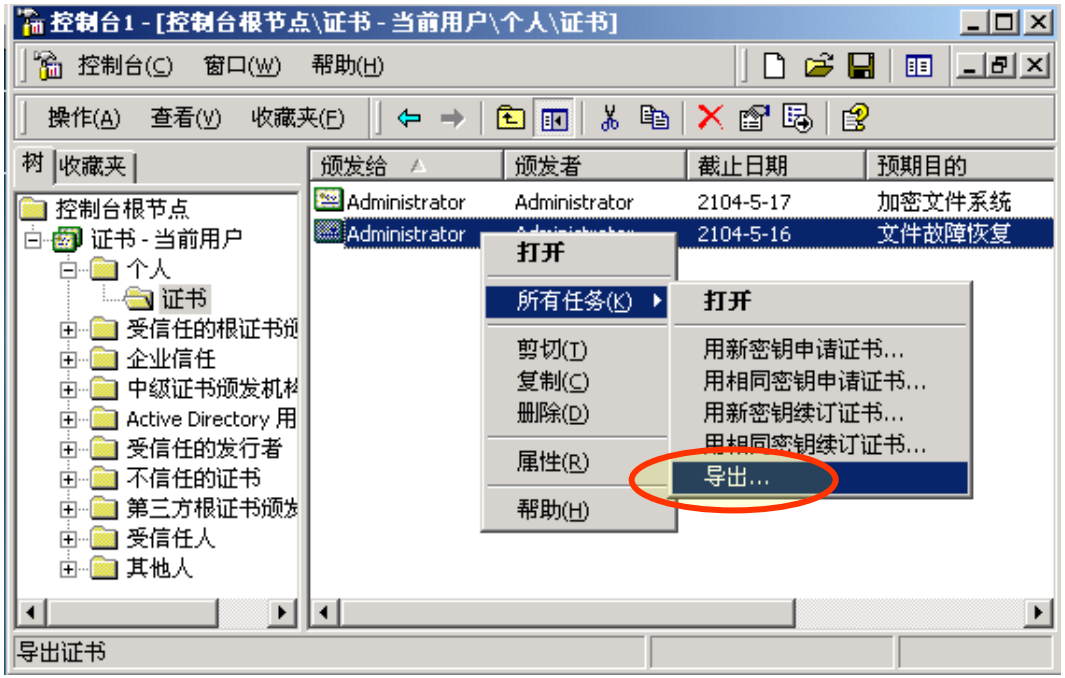
Cipher命令行工具

- 作用：查看EFS的状态，也用来进行文件夹的加解密。
- 语法：cipher [Options] pathname

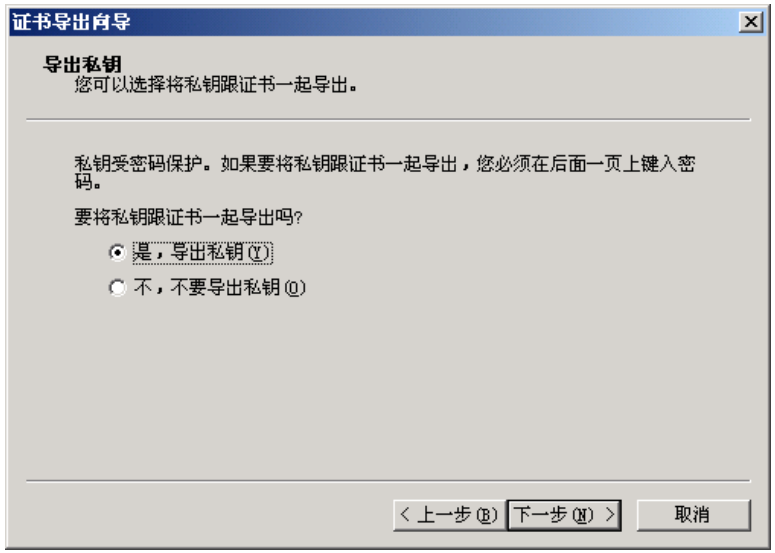
选项	含义
/e	加密指定的目录。目录将被标记，所以之后加进目录中的文件将被加密
/d	解密指定的目录。目录将被标记，所以之后加进目录中的文件将不被加密
/s	在给定的目录和其所有子目录执行指定的操作
/i	即使发生错误仍然继续指定的操作。默认发生错误时Cipher停止
/f	强制对所有指定的对象加密，即使它们已经被加密。 默认为跳过已经加密的对象
/q	只报告最基本的信息
/k	为运行 Cipher的用户创建新的文件密钥。如果选择了此选项，则忽略所有其他选项

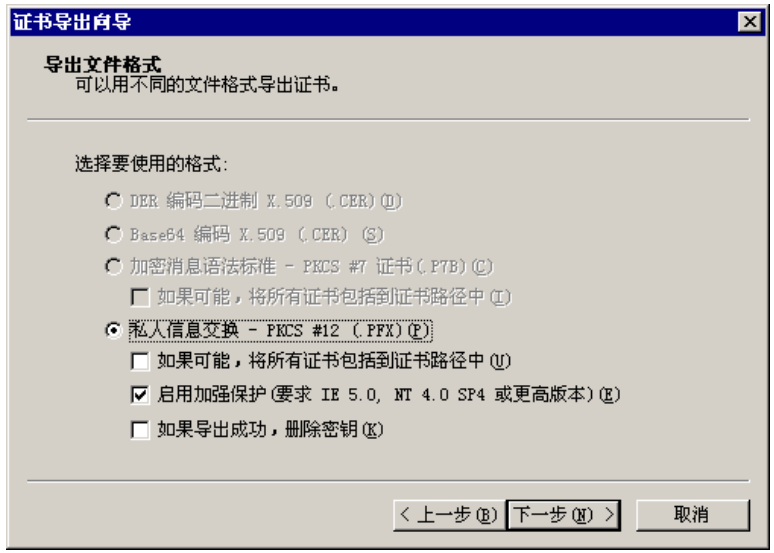
备份默认的恢复代理

- “MMC”→“证书管理单元”→“个人证书存储区”→选择文件故障恢复证书→“导出”。
- 备份介质
  - 软盘、USB等可移动存储设备。
  - 其他主机。



[快捷方式] 在“开始”→“运行”中键入“certmgr.msc”，



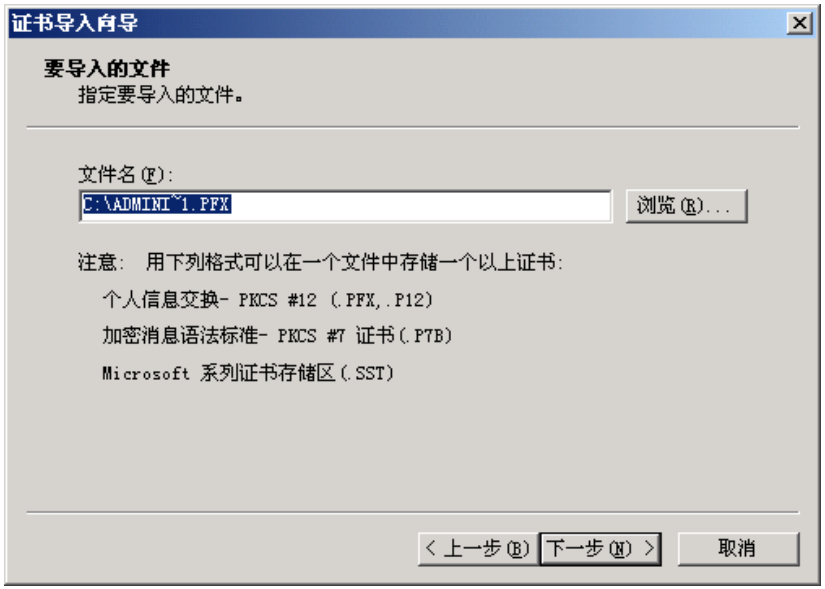


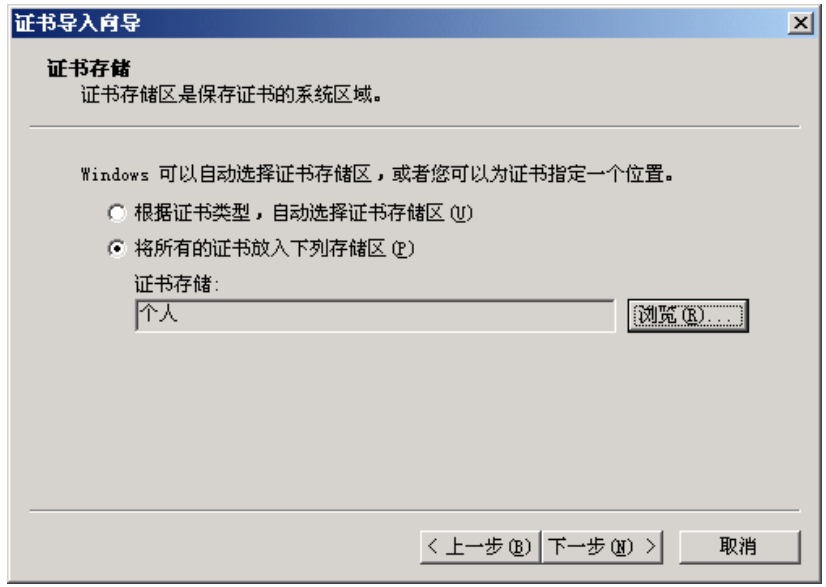
需要导出私钥

后缀名为.pfx

恢复加密文件系统的私钥（方法1）

- 双击.pfx私钥文件
- 导入到个人证书存储区中





恢复加密文件系统的私钥（方法2）

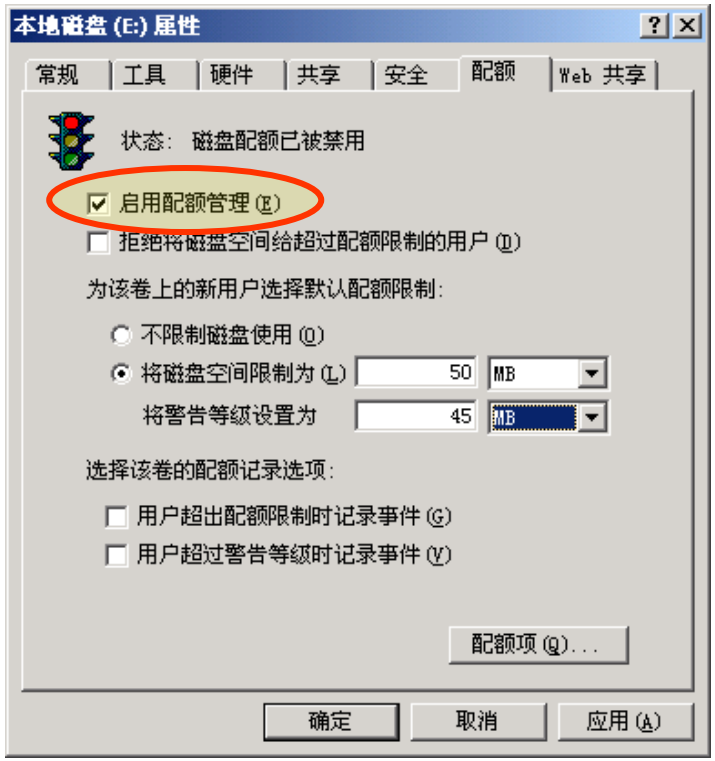
- “MMC” → “证书管理单元”→ “个人证书存储区”→“导入”

磁盘配额

- 作用：
  - 管理员可以方便合理地分配存储资源，避免由于磁盘空间使用的失控可能造成的系统崩溃，从而提高了系统的安全性 。
  - 适用场合：文件服务器、FTP服务器、邮件服务器等。
- 系统管理员可以将Windows配置为：
  - 当用户超过所指定的磁盘空间配额时，阻止进一步使用磁盘空间，并记录事件。
  - 当用户超过指定的磁盘空间警告级别时，记录事件。
- 磁盘配额是以文件所有权为基础的，并且不受卷中用户文件的文件夹位置的限制。
- 磁盘配额只适用于卷，且不受卷的文件夹结构及物理磁盘上的布局的限制。

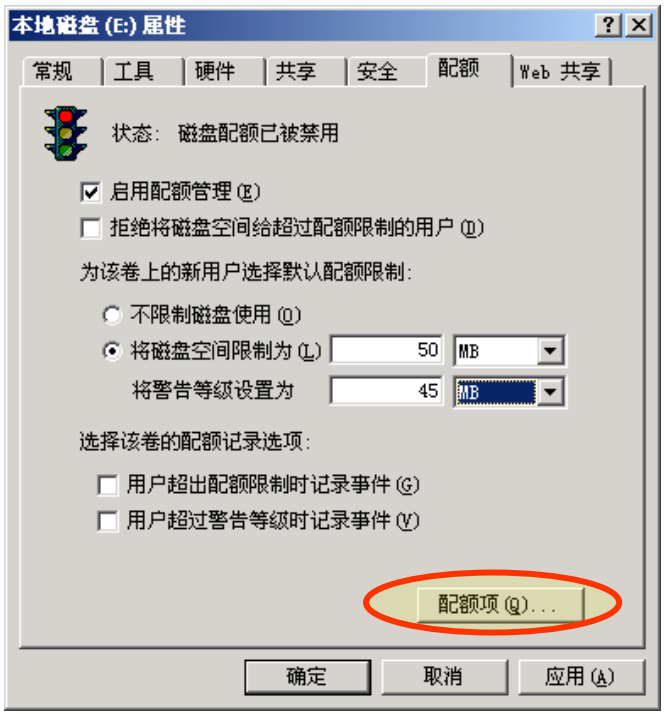
磁盘配额的管理

- 启用磁盘配额
  - “我的电脑”→ 选择磁盘卷 →“属性” →“配额” →“启用配额管理”



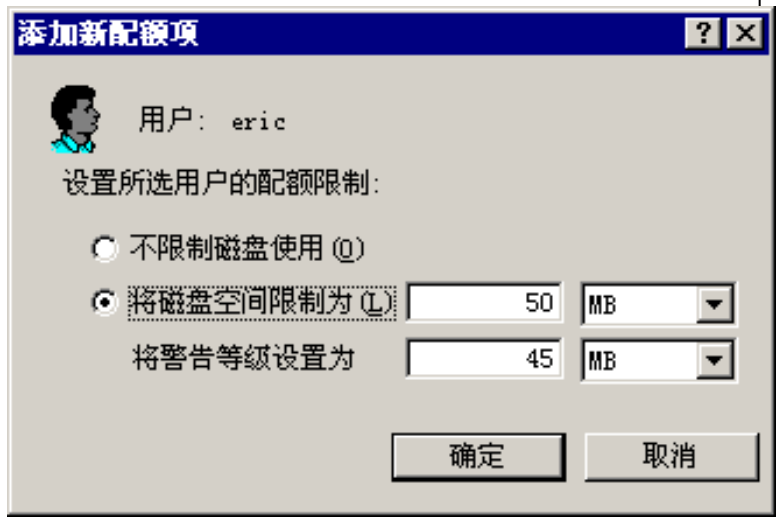
察看配额项目

- “我的电脑”→ 选择磁盘卷 →“属性” →“配额” →“配额项”



新建配额项

- “配额项目”窗口→“配额”菜单→“新建配额项”。



管理配额项

- 查看用户的磁盘配额信息。
- 删除配额项目。
- 修改用户磁盘空间限制和警告级别。
- …

网络共享的安全

- 网络共享
  - 文件夹共享
  - 默认管理共享
    - Dirve$
    - Admin$
    - IPC$
  - 域控制器上的共享
    - SYSVOL
    - NETLOGON

- 共享协议
  - SMB（Server Message Block）是Windows系统中进行文件共享的协议。
- SMB可运行于NBT（Netbios over TCP/IP）上，也可直接运行于TCP/IP上。
  - 137/UDP，139/UDP，139/TCP
  - 445/TCP

Windows的空会话漏洞

- 漏洞存在的前提
  - 开放139/TCP或445/TCP端口
  - 开放IPC$共享
- 危害
  - 泄露系统敏感信息
- 防御措施
  - 在安全策略中，选择“对匿名连接的额外限制”项，对其进行设置，将值设为“没有显式匿名权限就无法访问”项。
  - 修改注册表键值:

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RestrictAnonymous = 2

数据备份

数据备份类型

1 常规备份（完全备份，Full Backup）

- 对整个系统进行备份，包括操作系统和应用程序生成的数据。
- 优点：当发生数据丢失的灾难时，只要用一盘磁带（即灾难发生前一天的备份磁带），就可以恢复全部的数据。
- 缺点：数据量非常大，占用备份的存储设备比较多，备份时间比较长。

数据备份类型

2 增量备份 （Incremental Backup）

- 每次备份的数据只是上一次备份后增加的和修改过的数据。
- 优点：没有重复的备份数据，节省存储空间，又缩短了备份时间。
- 缺点：当发生灾难时，恢复数据比较麻烦，因为需要环环相套的所有备份。

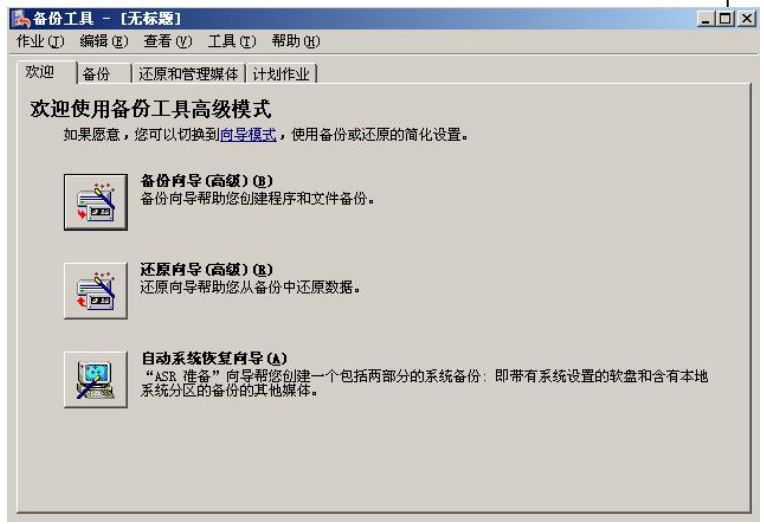
3 差异备份（Differential Backup）

- 每次备份的数据是相对于上一次全备份之后新增加的和修改过的数据。
- 优点：备份所需时间短，并节省磁带空间，灾难恢复也很方便，因为系统管理员只需两盘磁带，即系统全备份与发生灾难前一天的备份。

- **Windows 2000的备份工具**
  - “开始”→“程序”→“附件”→“系统工具”→“备份”
- **备份向导**
  - 要备份的内容
    - 整个系统
    - 选定的文件、驱动器或网络数据
    - 仅系统状态数据
  - 备份保存的位置
    - 媒体类型
    - 媒体或文件名称

Windows系统的文件备份

- 在命令行中输入ntbackup命令，进入“备份工具”界面。
  - 单击 “备份”选项卡。
  - 选择需要备份的驱动器、文件|或文件夹旁的复选框。
  - 为备份选择目的地。
  - 为备份选择相应的选项。
  - 计划备份。
  - 检查已完成的备份是否成功。
  - 验证备份的数据。



SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

Any Questions ?

确定 取消