Windows安全原理与技术

— 第十章：组策略

王轶骏， Eric Ericwyj@sjtu.edu.cn

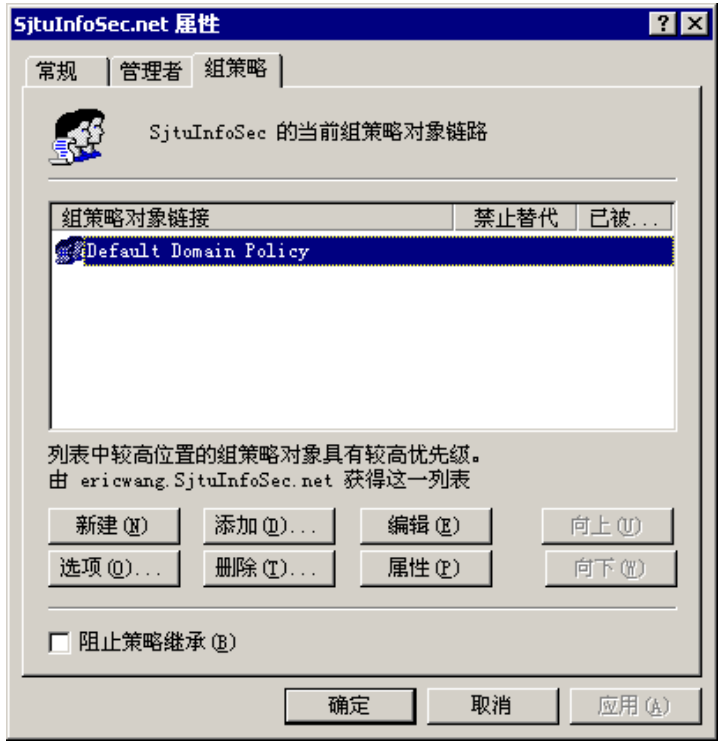
SJTU.INFOSEC.A.D.T, 2008

组策略概述

- 组策略（Group Policy）设置实现了关于特殊桌面或安全配置选项的决策。
- 组策略对象（Group Policy Object, GPO）是大量组策略设置的一个集合，即可以为一组计算机或用户指定特定的设置。
- 通过使用组策略管理单元，可以创建计算机和用户的配置。

组策略与活动目录的结合

- 组策略与活动目录的联合使用实现了策略的集中与分散管理，适应从小到大的各种规模。
- 组策略管理单元提供了管理组策略的集成工具，并提供了对“Active Directory用户和计算机”插件等其他MMC管理工具的扩展。



- 组策略能够从站点、域和最后到的组织单元继承而来。
- 应用组策略对象（把组策略对象链接到它们的目标上）的顺序和级别决定了用户或计算机实际能收到的组策略设置。
- 组策略能够在站点、域、组织单元这些级别上被阻塞。
- 组策略还能够以非覆盖方式来进行强制实施。

组策略的基础结构

- 组策略对象和组策略管理单元
  - 可以把组策略对象想象为关联组策略管理单元的文档。
  - 可以将组策略管理单元作为独立工具或者活动目录管理单元的扩展来使用。
- 组策略对象的链接
  - 可以将组策略对象链接到指定的站点、域或组织单元。
- 组策略管理单元的访问
- 通过安全组成员筛选组策略的效果

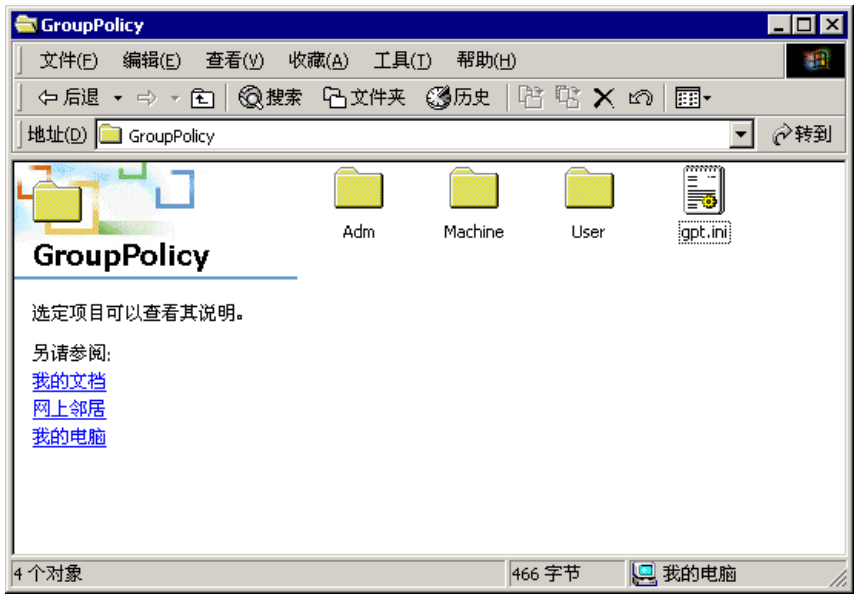
组策略的存储

- 组策略对象的类型
  - 本地组策略对象：存储在每台基于Windows 2000的计算机中。
  - 非本地组策略对象：基于活动目录，用全局惟一标识符确定。

如果两者发生冲突，那么本地组策略对象的设置可被非本地组策略对象所覆盖。

本地组策略对象的存储

- 本地组策略对象存储在%SYSTEMROOT%\System32\GroupPolicy文件夹中。
- 组策略模板的文件夹结构
  - 配置文件：gpt.ini。
  - 模板子目录树：Adm, Machine, User。
  - 注册表设置文件：Registry.pol。
- 权限设置
  - Administrators组：完全控制。
  - SYSTEM：完全控制。
  - 用户：读取。

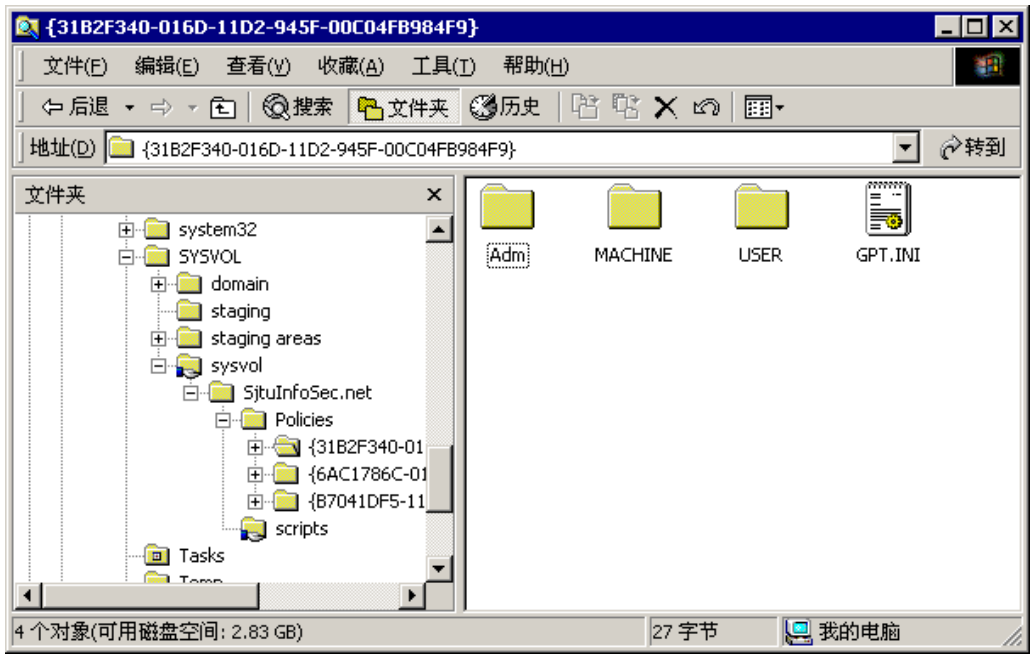


非本地组策略对象的存储

- 组策略容器
  - 是一个关于组策略对象的活动目录存储区域，它包括计算机和用户组策略信息。
  - 具有的属性：
    - 版本信息：用来保证信息与组策略模板信息同步。
    - 状态信息：用来指明GPO是处于开启状态还是关闭状态。
    - 组件列表：指定组策略的哪些扩展在该GPO中具有设置。

组策略模板

- 实际上就是保存组策略信息的文件夹结构。
- 位于域控制器系统卷的%SYSTEMROOT%\Sysvol\SYSVOL\Policies中。
- 模板目录中的文件和子目录结构同“本地组策略对象的存储”。



组策略的配置

- 组策略管理单元的根节点
  - <组策略对象名称> [<域名称>]策略

    如： Default Domain Policy [SjtuInfosec.net] 策略
- 第二层节点
  - 计算机配置
  - 用户配置
- 第三层节点
  - 软件设置
  - Windows设置
  - 管理模板

- **Windows设置：包括由Microsoft所提供的扩展。**
  - 脚本：含有计算机特殊脚本的信息。
    - 启动和关闭脚本存在于计算机配置节点中。
    - 登录和注销脚本存在于用户配置节点中。
  - 安全设置：含有登录到计算机的所有用户的安全设置。
  - 目录重定向：可以重定向My Documents、应用数据、桌面及开始菜单等文件夹到网络上一个可选的位置。
  - Internet Explorer维护。
  - 远程安装服务。

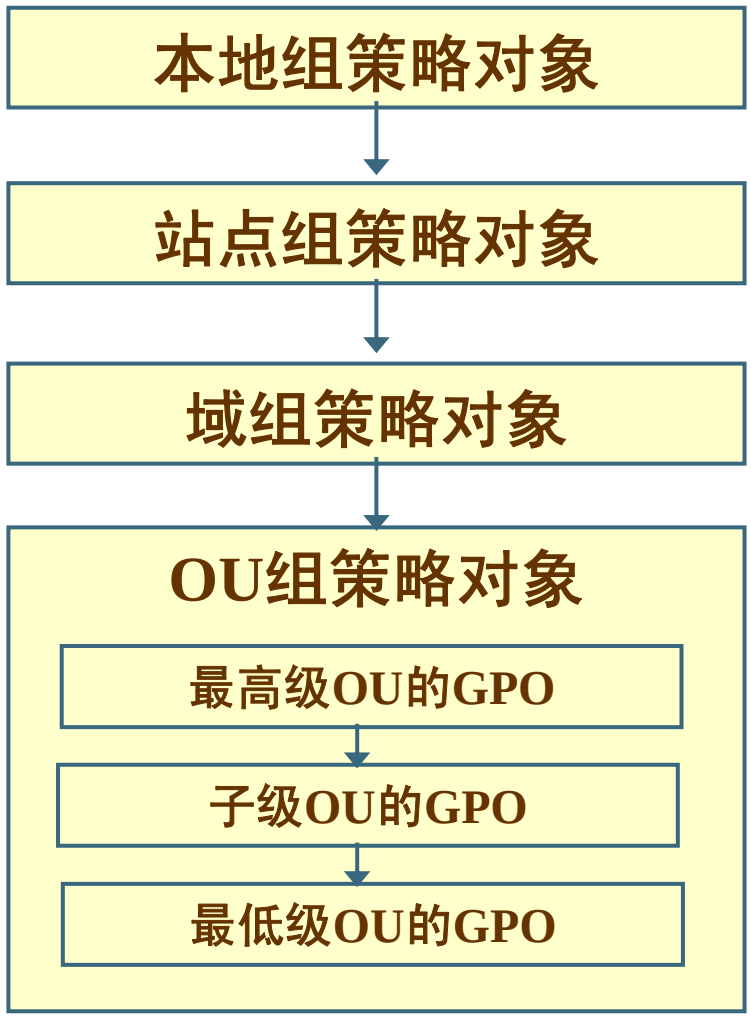
管理模板

- 是供组策略用来生成用户界面设置的文件。
- 这些文件由分层的目录和子目录所组成，目录定义了哪些选项将显示在组策略中，以及显示哪些可由组策略进行修改的注册表设置。
- 这些设置包括基于注册表的可以控制有关桌面行为和外观（以及操作系统组件和应用程序）的注册表设置的组策略配置，它们被写入到注册表数据库中的HKEY_CURRENT_USER以及HKEY_LOCAL_MACHINE部分。

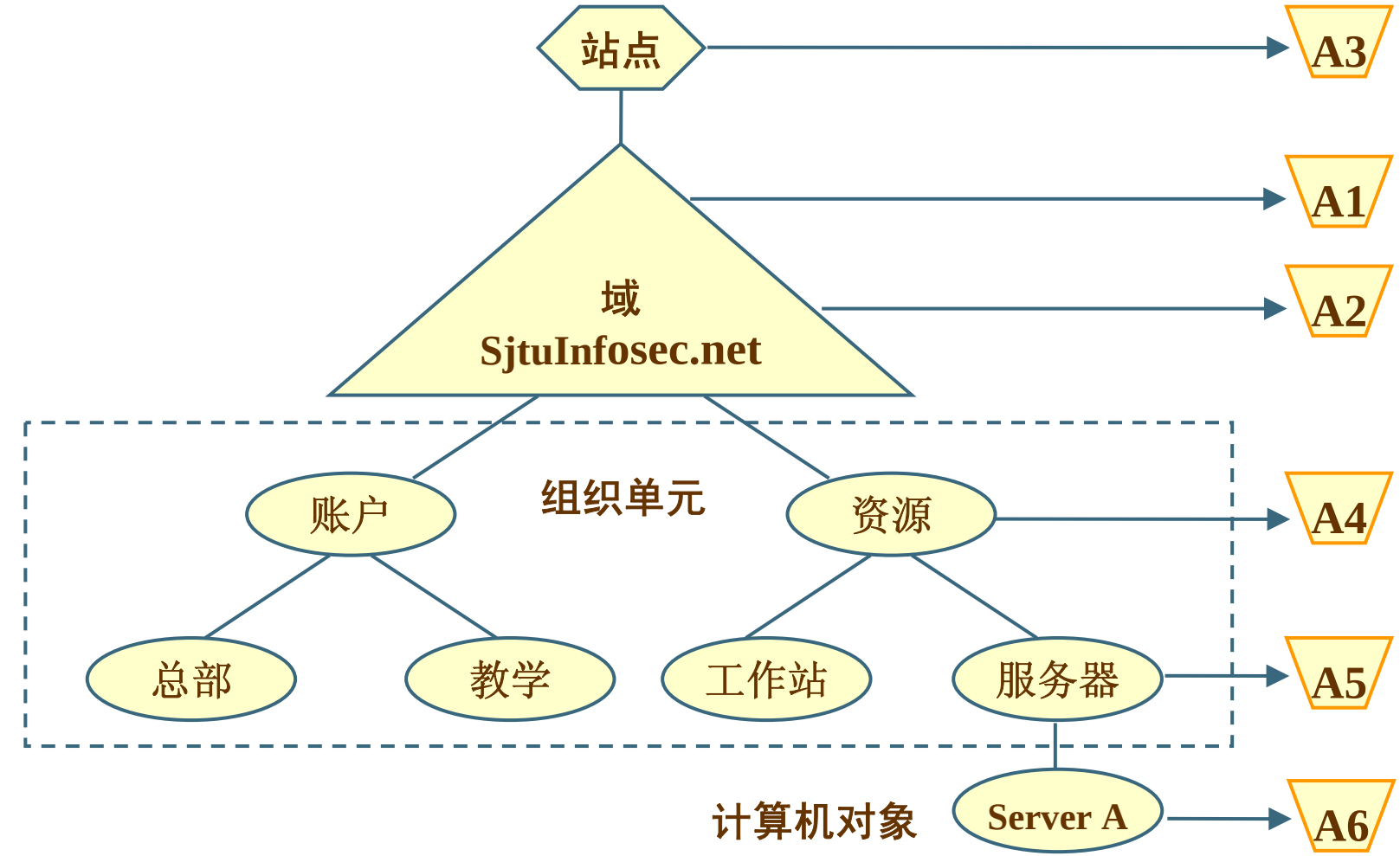
组策略的应用

- 计算机策略是在计算机引导的时候加载，而用户策略是在用户登录的时候加载。
- 计算机和用户是仅有的接收组策略的活动目录对象类型，安全组不需要应用策略。

组策略的应用顺序



后面应用的组策略将覆盖前面应用的组策略。



组策略对象

Server A 的组策略应用顺序：A6, A3, A1, A2, A4, A5

组策略的继承关系

- 总的来说：
  - 组策略具有继承性。
  - 子容器的设置优于与从父容器继承下来的设置。
- 具体来说：
  - 父容器的某个策略未配置，子容器将不继承该设置。
  - 父容器配置了某个策略，子容器将继承该设置。
  - 父容器和子容器都配置了某个策略，但策略兼容，那么子容器将继承父容器的设置，并与自身的设置合并。
  - 父容器和子容器都配置了某个策略，但策略不兼容，那么子容器将不继承父容器的设置。

特殊的应用顺序和继承

- 工作组成员只处理本地组策略对象。
- “禁止替代”（No override）选项
  - 链接到站点、域或组织单元（不包括本地）的任何一个组策略对象都可以使用该选项，来防止随后处理的组策略对象覆盖该组策略对象中的所有策略设置。
  - 如果有多个组策略对象设置为“禁止替代”时，那么就会优先采用在活动目录层次结构中处于更高层的那一个。

- “阻止策略继承”（Block Policy Inheritance）选项
  - 在任何一个站点、域或组织单元上，组策略继承都可以被选择性的标记为“阻止策略继承”，来禁止从父目录容器继承组策略。
  - 但是，设置为“禁止替代”的组策略对象链接将始终都会被采用，且不能阻止。
  - “阻止策略继承”设置直接应用于站点、域或组织单元，而不应用于组策略对象，也不应用于组策略对象链接。

“反向”（Loopback）选项

- “替换”（Replace）模式
  - 用户的GPO列表被在系统启动时被计算机获得的GPO列表完全替代。
- “合并”（Merge）模式
  - 用户的GPO列表添加到在系统启动时被计算机获得的GPO列表之后。
  - 计算机的GPO列表具有更高的优先权。

组策略的实现和管理

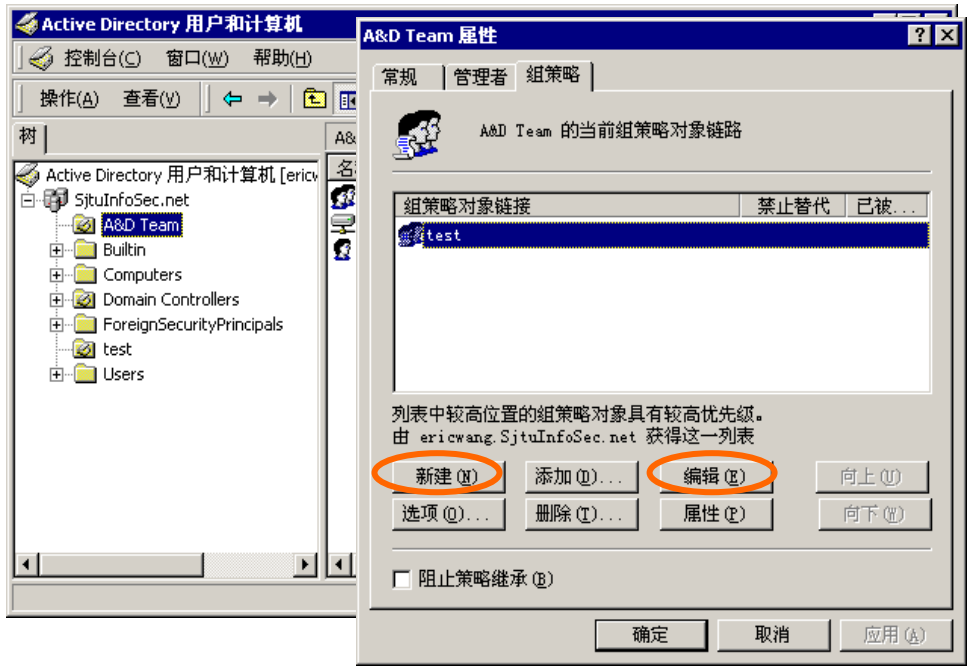
- 访问组策略管理单元（方法1）
  - 在MMC中选择作为独立管理单元的组策略，指定对象或计算机以访问其策略。

“MMC”→“添加组策略管理单元”→“选择组策略对象”

访问组策略管理单元（方法2）

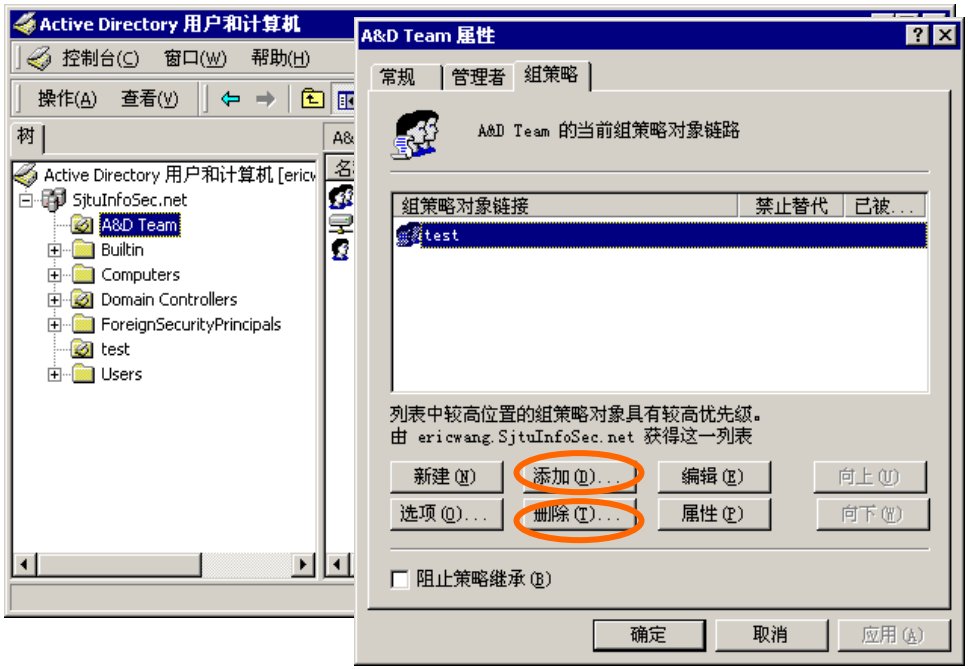
- 在Active Directory管理控制台（“用户和计算机”以及“站点和服务”控制台）中选择对象，并将组策略作为扩展管理单元来访问。

“AD用户和计算机管理控制台”→“选择AD对象”→“属性”→“组策略”→“新建”（选择“组策略对象链接”→“编辑”）



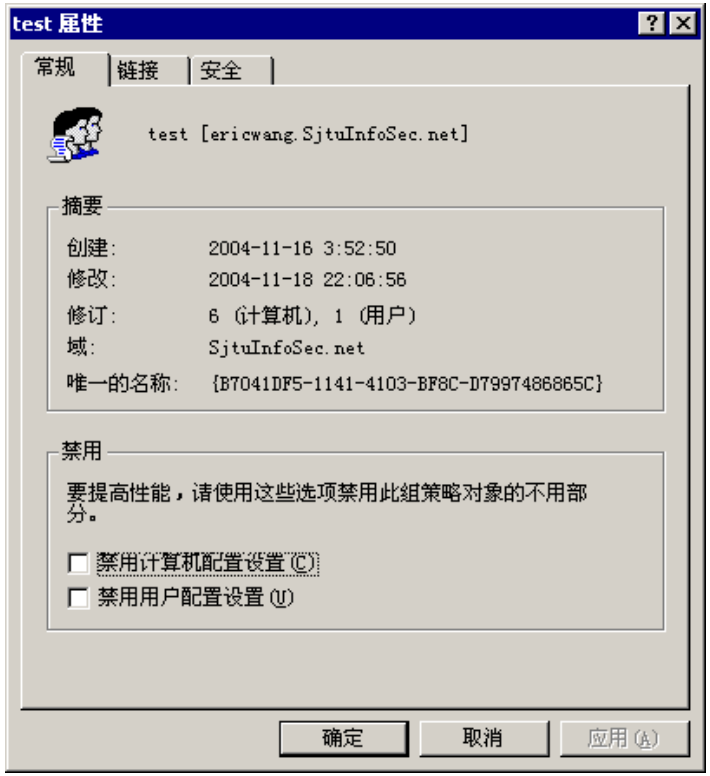
将GPO链接到指定的站点、域或组织单元

“AD用户和计算机管理控制台”→“选择AD对象”→“属性”→“组策略”→“添加”



禁用组策略的计算机配置或用户配置

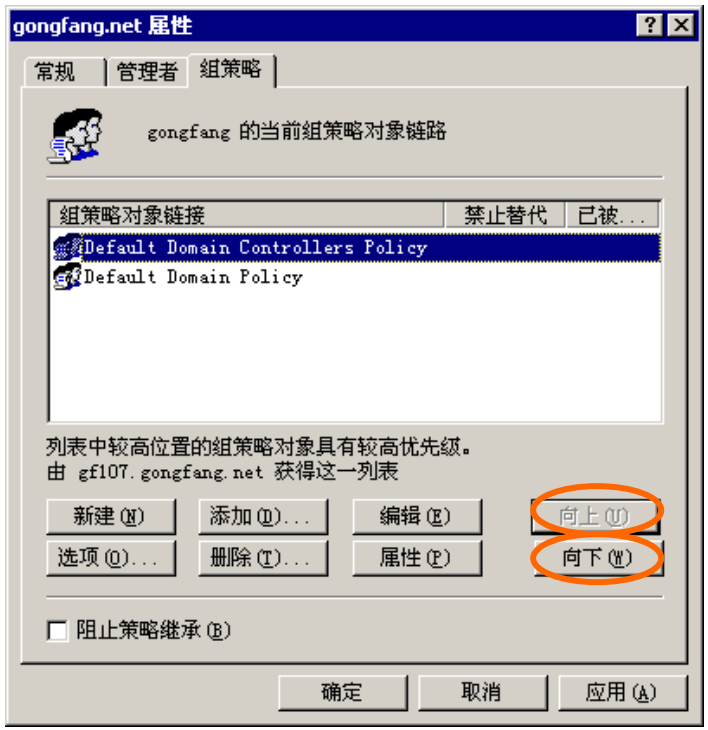
打开“组策略管理单元”→选择组策略对象→“属性”→“常规” →“禁用”



指定组策略对象的特殊应用顺序和继承（1）

- 修改组策略应用顺序

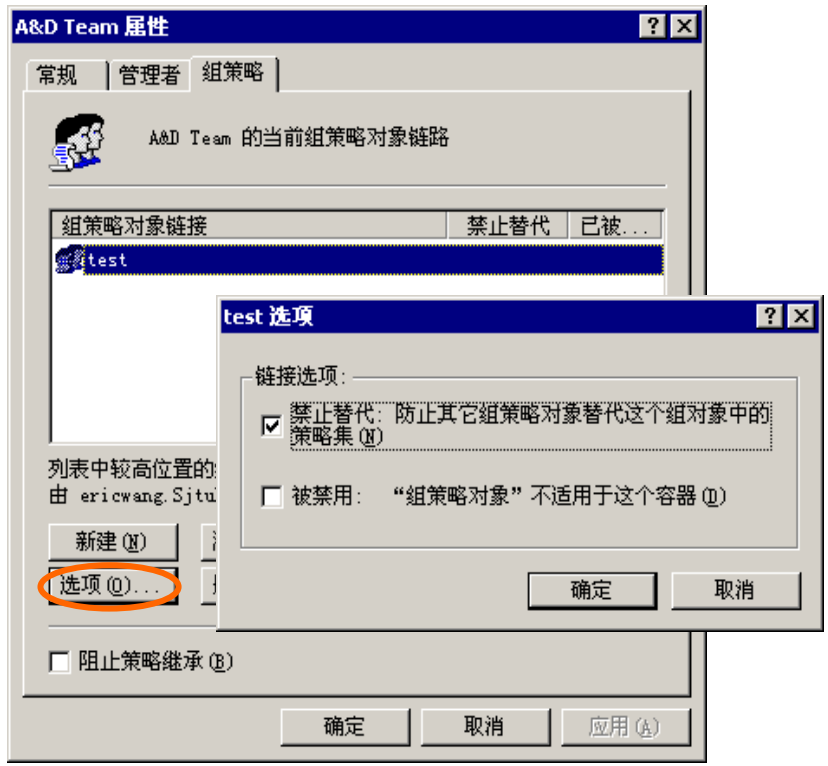
“AD用户和计算机管理控制台”→“选择AD对象”→“属性”→“组策略”→选择“组策略对象链接”→“向上”/“向下”



指定组策略对象的特殊应用顺序和继承（2）

- 使用“禁止替代”选项

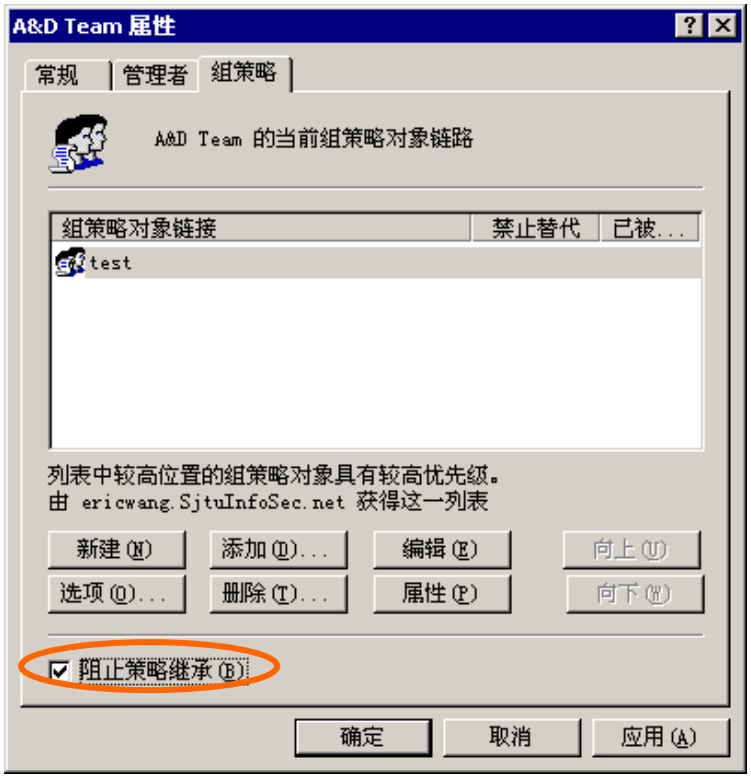
“AD用户和计算机管理控制台”→“选择AD对象”→“属性” →“组策略” →选择“组策略对象链接”→“选项”→ “链接选项”



指定组策略对象的特殊应用顺序和继承（3）

- 阻止策略继承

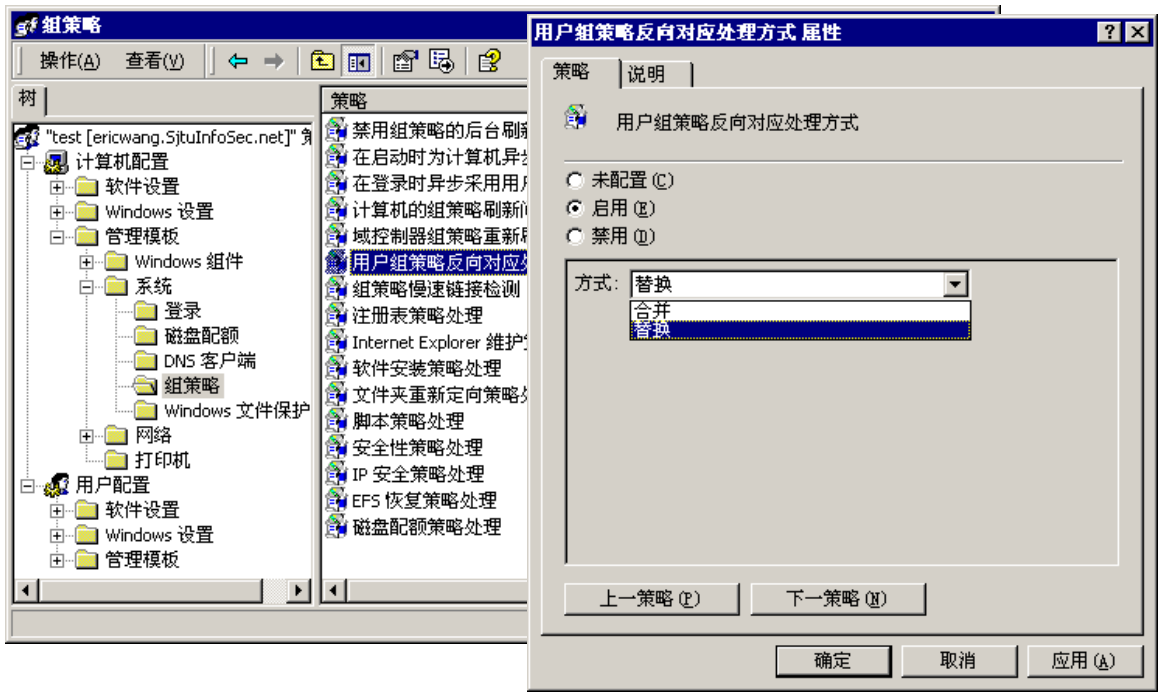
“AD用户和计算机管理控制台”→“选择AD对象”→“属性”→“组策略”→“阻止策略继承”



指定组策略对象的特殊应用顺序和继承（3）

– 启用反向设置

打开“组策略管理单元”→选择组策略对象→“计算机配置”→“管理模板” →“系统” →“组策略” →“用户组策略反向对应处理方式”→“启用”→“合并” / “替换”



SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

Any Questions ?

确定 取消