Windows安全原理与技术

— 第十一章：安全配置与分析

王轶骏， Eric Ericwyj@sjtu.edu.cn

SJTU.INFOSEC.A.D.T, 2008

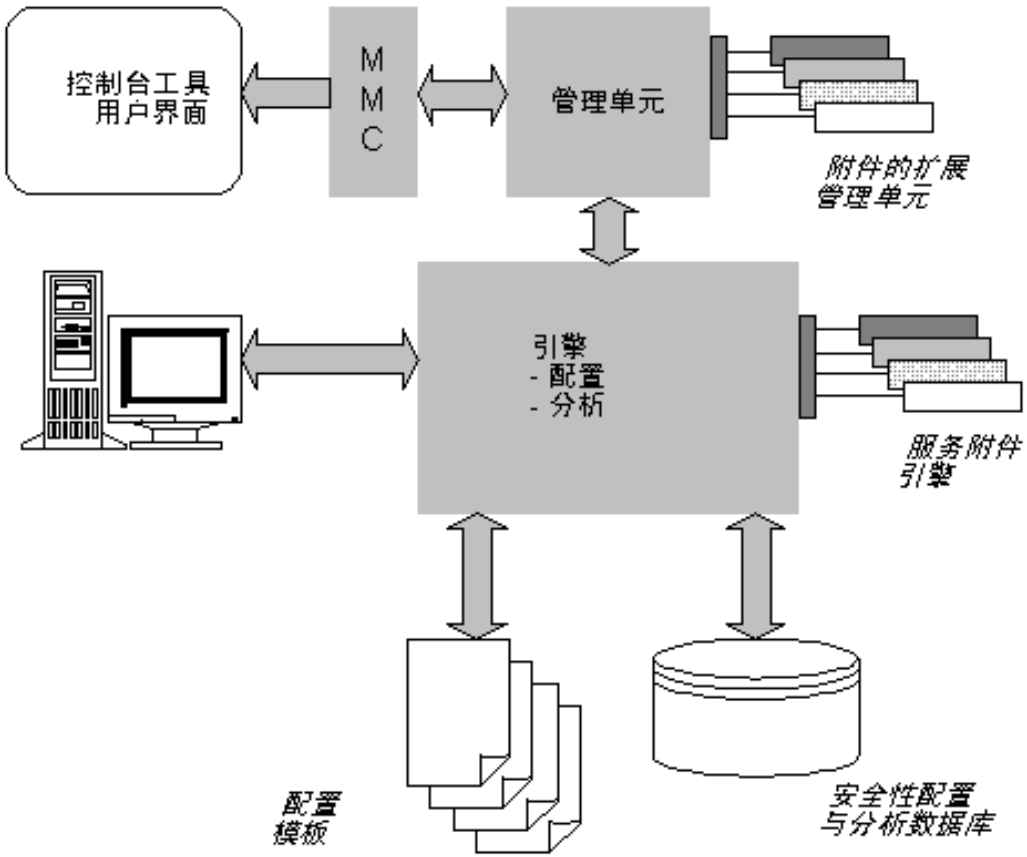
安全配置工具集

- 目的
  - 为配置和分析系统的安全性提供一个全面、灵活、可扩展而且简单的工具集。
    - 集中式的进行安全配置和安全分析。
    - 减小安全配置与分析方面的开销。
- 组件
  - 安全模板
  - 安全配置和分析工具

安全配置工具集的特性

- 全面性
- 灵活性
- 可扩展性
- 简便性

安全配置工具集的体系结构



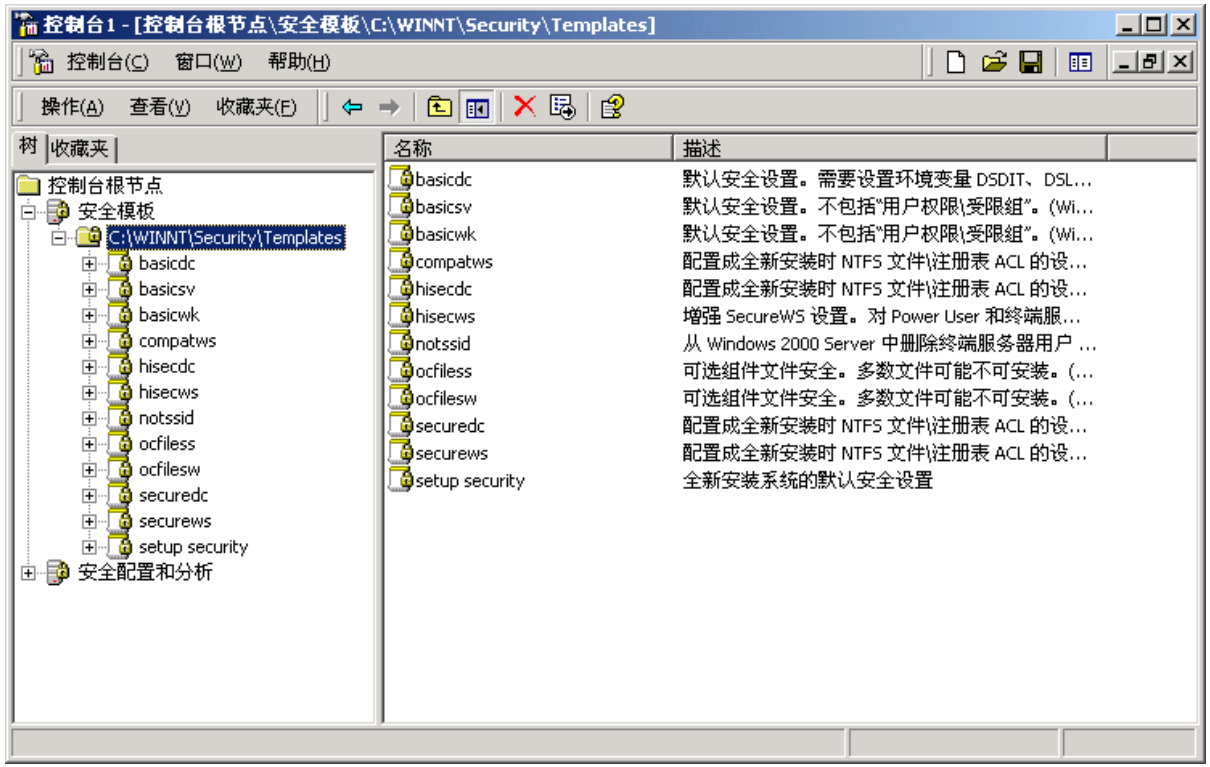
安全配置工具集的组件

- 安全模板管理单元
  - 向一个安全模板创建、编辑和保存安全设置。
- 安全配置和分析管理单元
  - 允许把一个或多个安全模板导入数据库，然后就可以把这一数据库应用到计算机上，并对照保存在其中的合成配置来分析当前的系统配置。
- 组策略编辑器的安全设置扩展
  - 允许把安全配置定义成GPO的一部分，然后可以将组策略对象分配给特定计算机，或者在AD中的域或组织单元范围内进行分配。
- Secedit.exe
  - 命令行工具，执行安全配置和分析功能。

安全模板管理单元

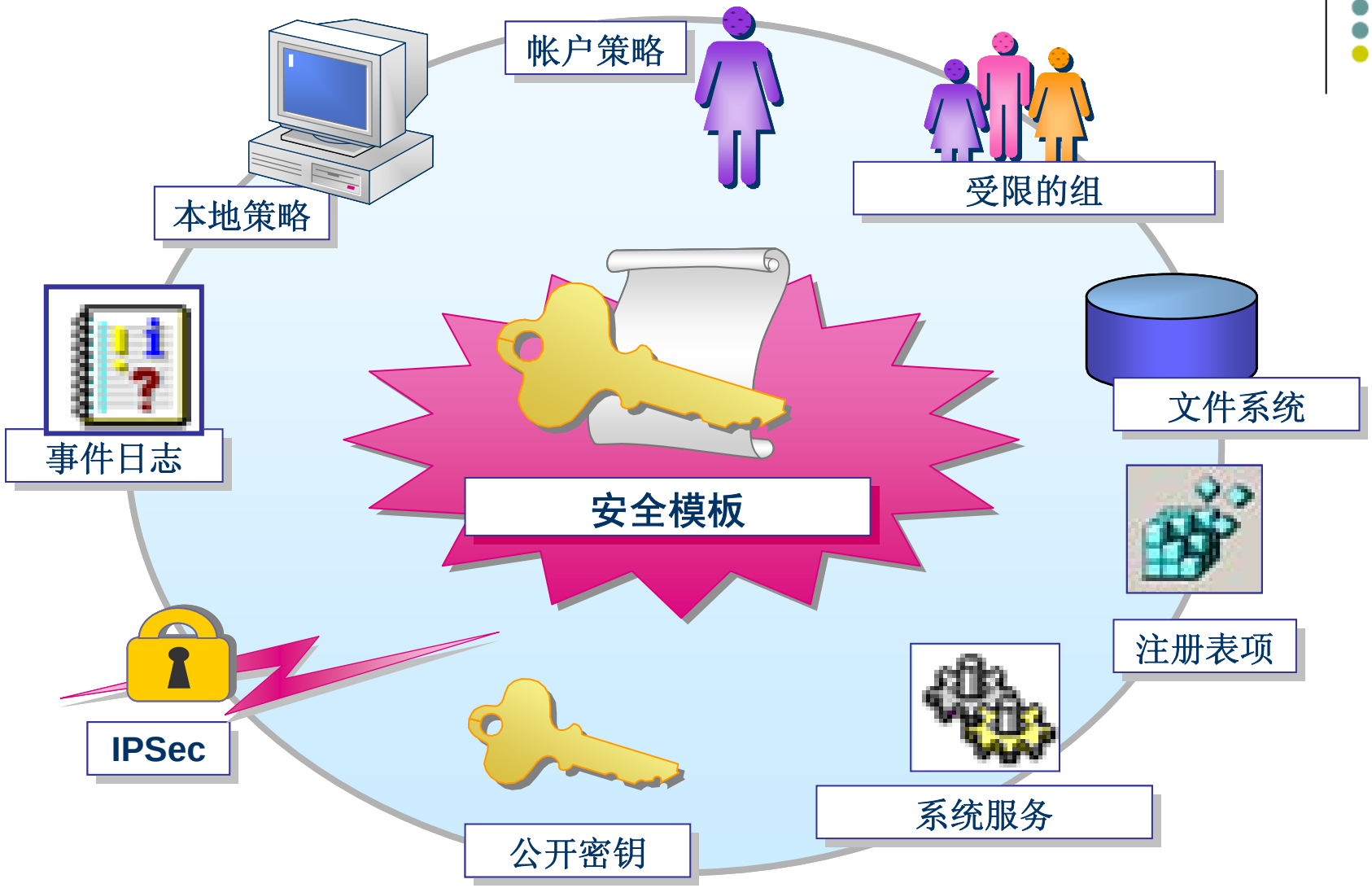
功能

- 定义、编辑和保存安全模板



"MMC"→添加"安全模板"管理单元

支持的安全区域内容



预定义的安全模板

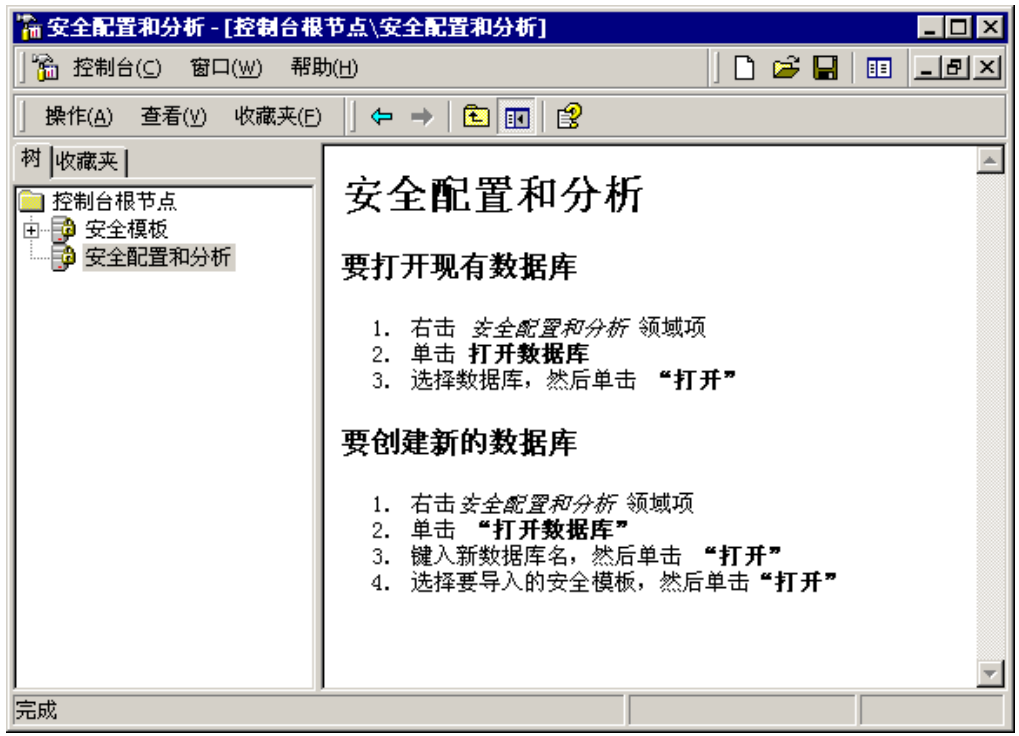
- 存放位置
  - %SystemRoot%\Security\Templates
- 种类
  - 默认工作站（basicwk.inf)
  - 默认服务器（basicsv.inf)
  - 默认域控制器（basicdc.inf)
  - 兼容工作站或服务器（compatws.inf)
  - 安全工作站或服务器（securews.inf)
  - 高度安全工作站或服务器（hisecws.inf)
  - 专用域控制器（dedicadc.inf)
  - 安全域控制器（securedc.inf)
  - 高度安全域控制器（hisecdc.inf)

预定义安全模板的安全等级

- 基本
  - basic*.inf
- 兼容
  - compat*.inf
- 安全
  - secure*.inf
- 高度安全
  - hisec*.inf
- 专用域控制器
  - dedica*.inf

安全配置和分析管理单元

- 功能
  - 分析系统安全性
  - 查看安全性分析数据
  - 配置系统安全性



“MMC”→添加“安全配置和分析”管理单元

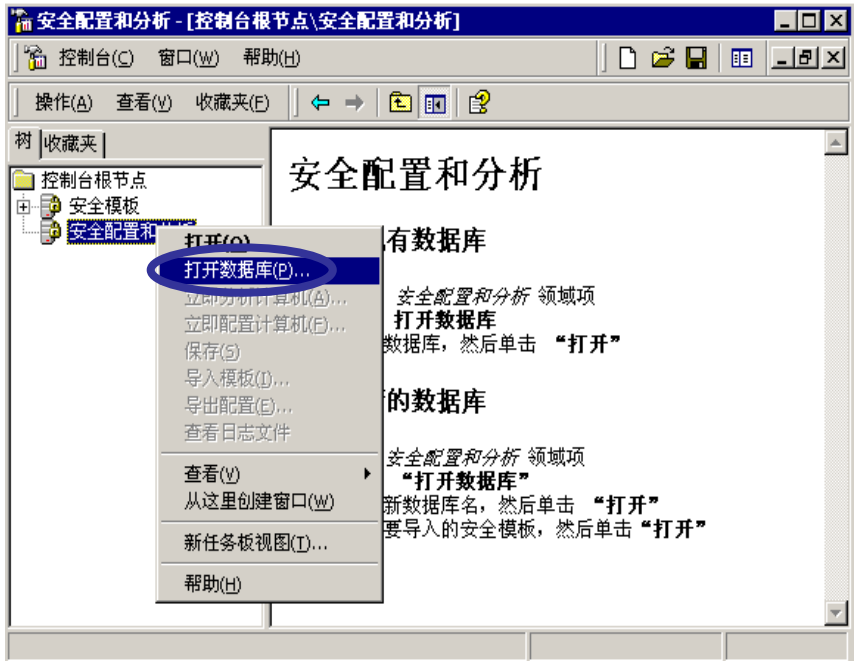
安全配置和分析数据库

- 安全配置和分析是由数据库驱动的，而无需知道安全模板的存在。
- 安全分析时是对当前系统的配置与在数据库中存储的配置做比较。
- 安全配置时是根据数据库中存储的配置来对系统进行设置。

初始化数据库

- 在对系统进行安全性配置和分析之前，首先需要打开一个安全数据库，如果没有则首先创建一个。

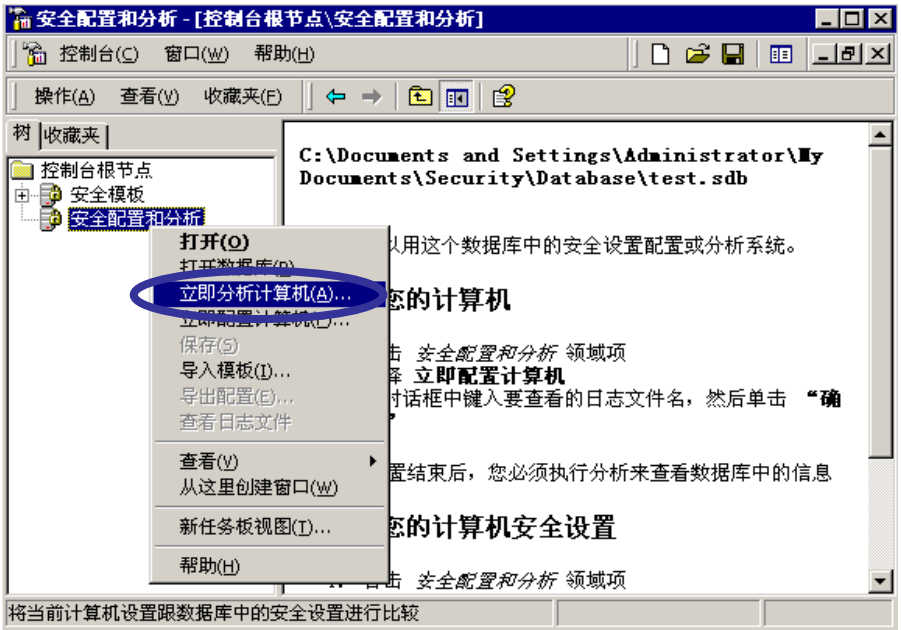
打开“安全配置和分析管理单元”→弹出右键菜单→“打开数据库”→“选择/新建数据库文件（*.sdb）”→“导入模板”

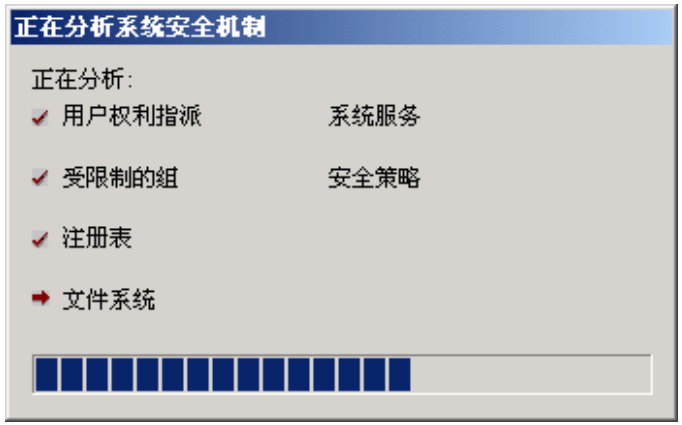


分析系统安全性

- 把系统的当前状态与所导入的安全模板进行比较。如果当前的系统设置与基本设置匹配，则被认为是正确的；否则，那些不匹配的设置都会被标记出来。

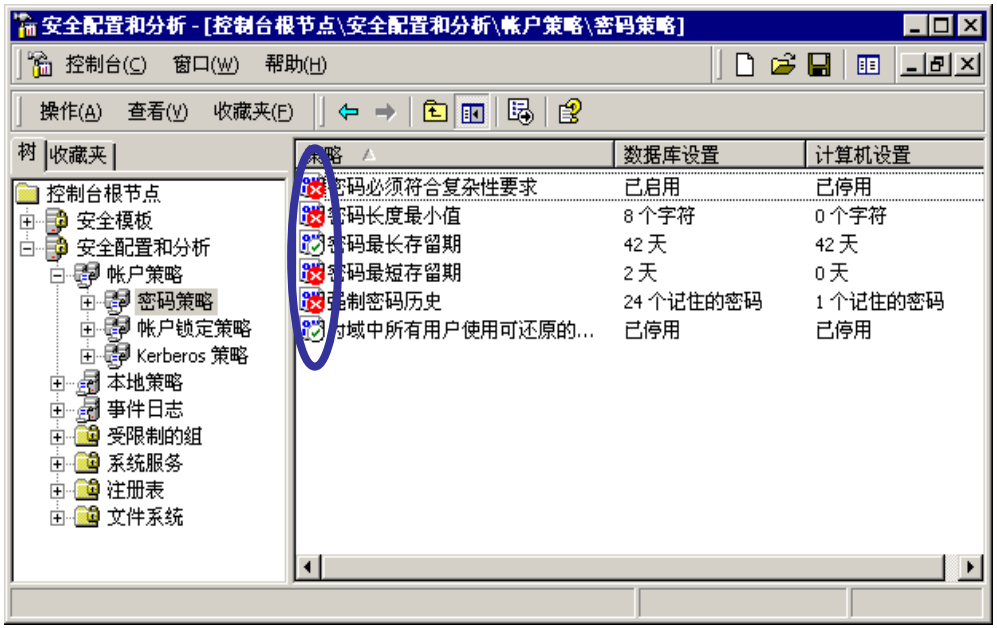
打开“安全配置和分析管理单元”→弹出右键菜单→“立即分析计算机”

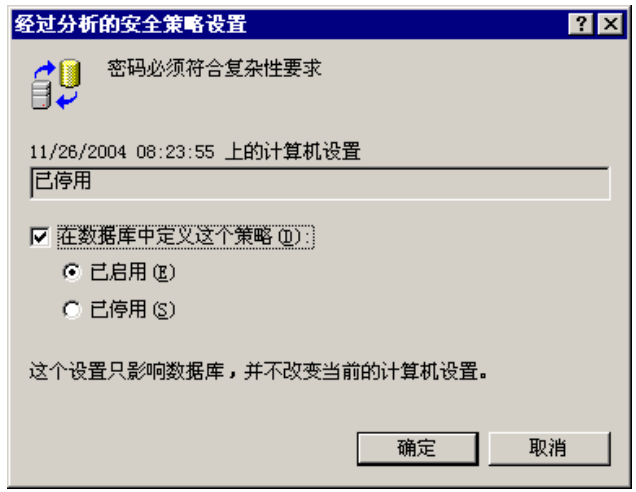




查看安全分析结果

- 展开“安全配置和分析”节点，选中其中具体的某个安全区域。
- 双击右边窗格中的条目来进一步查看不一致的地方。





当前配置与基准线不符合

当前配置与基准线符合或较之更好

配置系统安全性

- 在根据模板分析了当前的系统设置之后，如果对该模板所指示的安全性变化（标记为不匹配的地方）认可的话，就可使用这些新的安全设置来配置系统。

打开“安全配置和分析管理单元”→弹出右键菜单→“立即配置计算机”

“组策略”管理单元的“安全设置”扩展

- 允许管理员用客户-服务器模型配置大量客户
  - 在服务器上进行设置，然后自动传播给客户
- 额外提供的安全区域
  - IPSec策略
  - 公钥策略
  - 加密密钥恢复代理
  - 根证书
  - 证书信任列表（CTL）

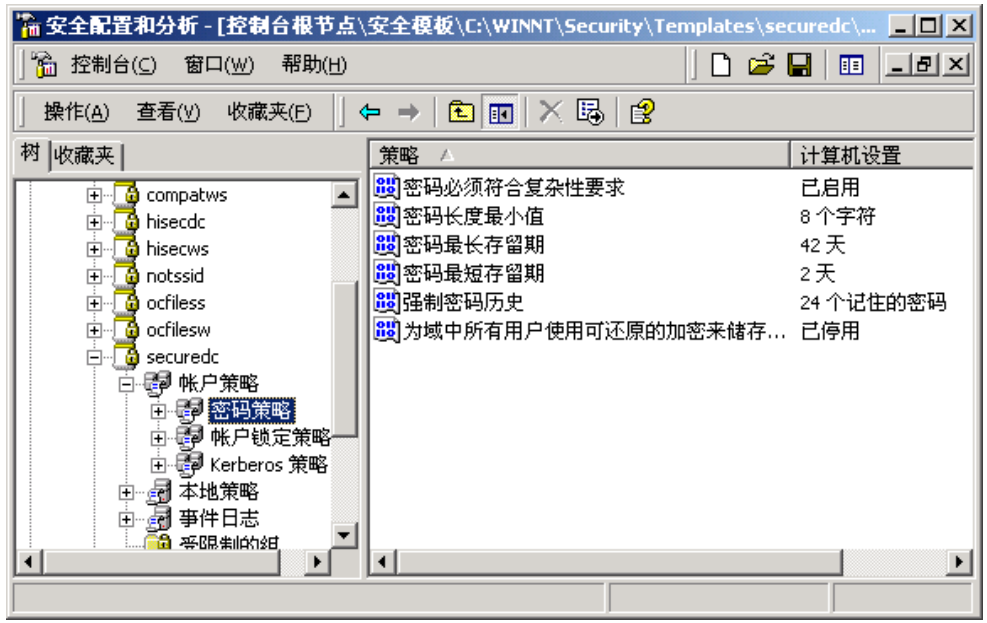
导入自定义的安全模板

打开“组策略管理单元”→选择组策略对象
→“Windows设置”→“安全设置” →弹出右键菜单
→“导入策略” →选择“安全模板文件”（*.inf）

账户策略

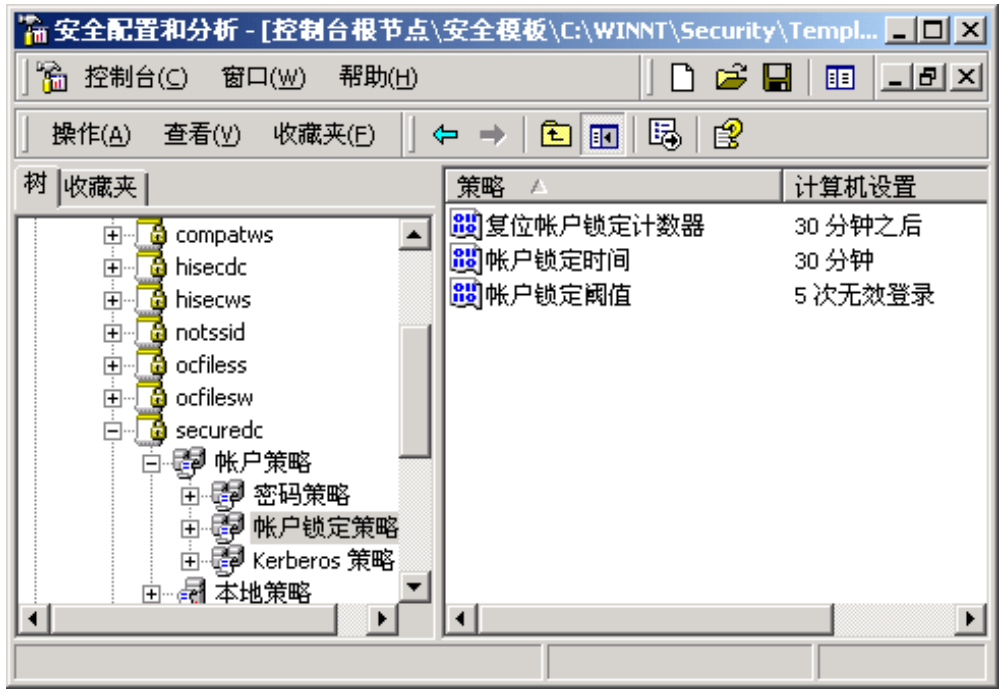
密码策略

- 包含用来限制用户密码的策略。
- 包含的内容：
  - 密码必须符合复杂性要求
  - 密码长度最小值
  - 密码最长存留期
  - 密码最短存留期
  - 强制密码历史
  - 为域中所有用户使用可还原的加密来储存密码



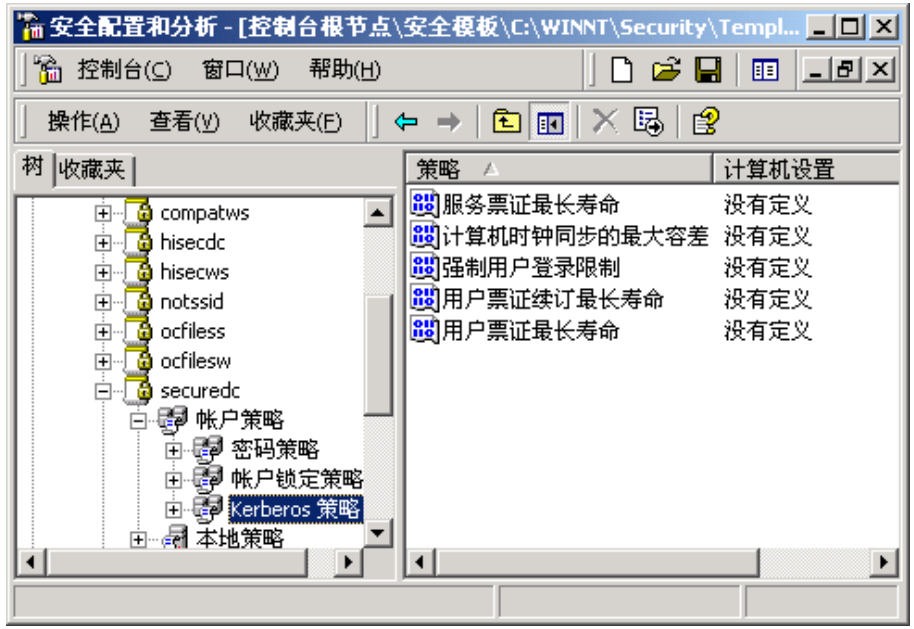
账户锁定策略

- 通过在规定的失败登录尝试次数之后锁定用户账户来防止暴力猜解用户密码。
- 包含的内容：
  - 复位账户锁定计数器
  - 账户锁定时间
  - 账户锁定阀值



Kerberos策略

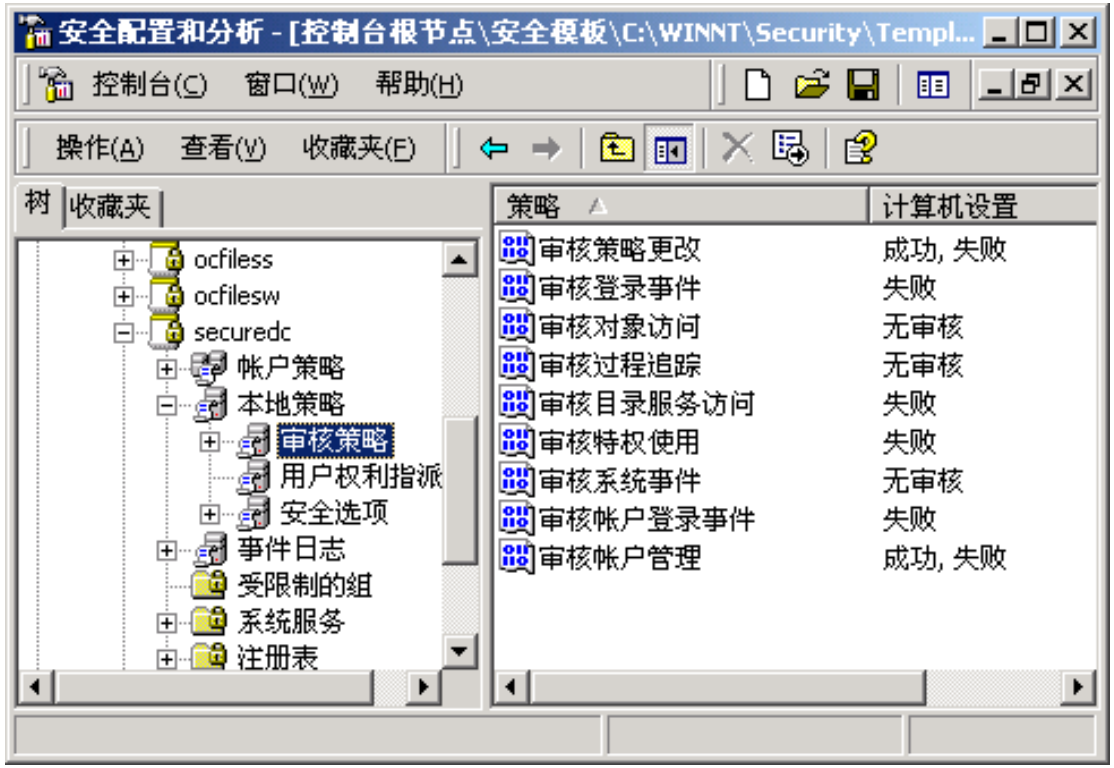
- 决定与Kerberos有关的设置。
- 包含的内容：
  - 服务票证最长寿命
  - 计算机时钟同步的最大容差
  - 强制用户登录限制
  - 用户票证续订最长寿命
  - 用户票证最长寿命



本地策略

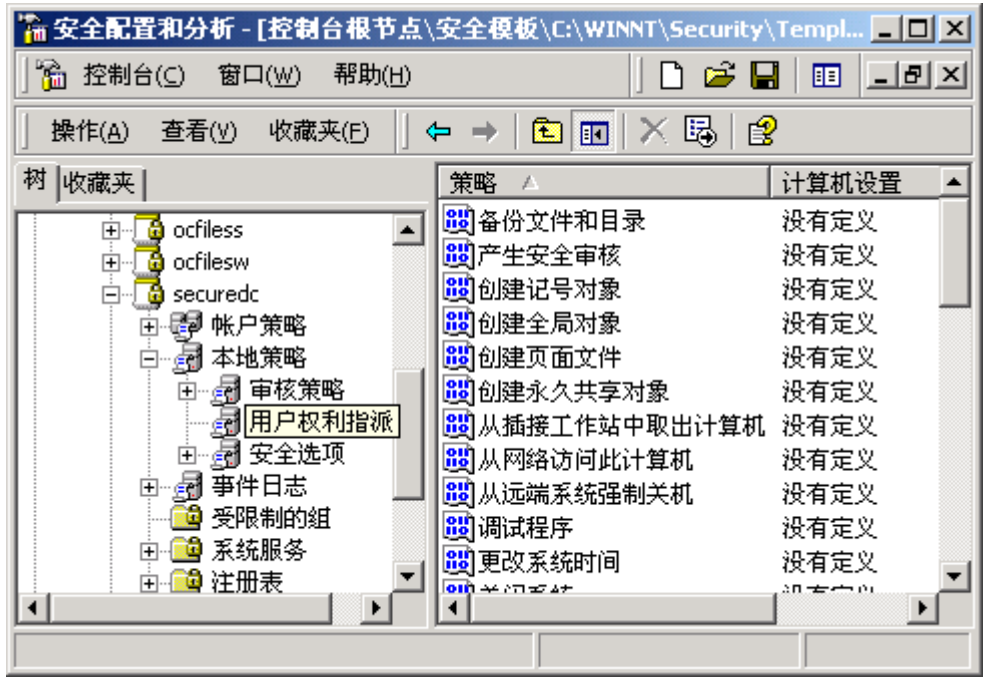
审核策略

- 决定记录计算机需要捕获到安全日志中的安全事件，以便日后在事件查看器中显示。
- 包含的内容：
  - 策略更改
  - 登录事件
  - 对象访问
  - 过程追踪
  - 目录服务访问
  - 特权使用
  - 系统事件
  - 账户登录事件
  - 审核账户管理



用户权利指派

- 用来决定在计算机上有登录或任务特权的用户或组。
- 包含的内容：
  - 取得文件或其他对象的所有权
  - 拒绝从网络访问这台计算机
  - 从网络访问此计算机
  - 从远端系统强制关机
  - 调试程序
  - 更改系统时间
  - 关闭系统
  - 管理审核和安全日志
  - 拒绝本地登录
  - 域中添加工作站
  - …

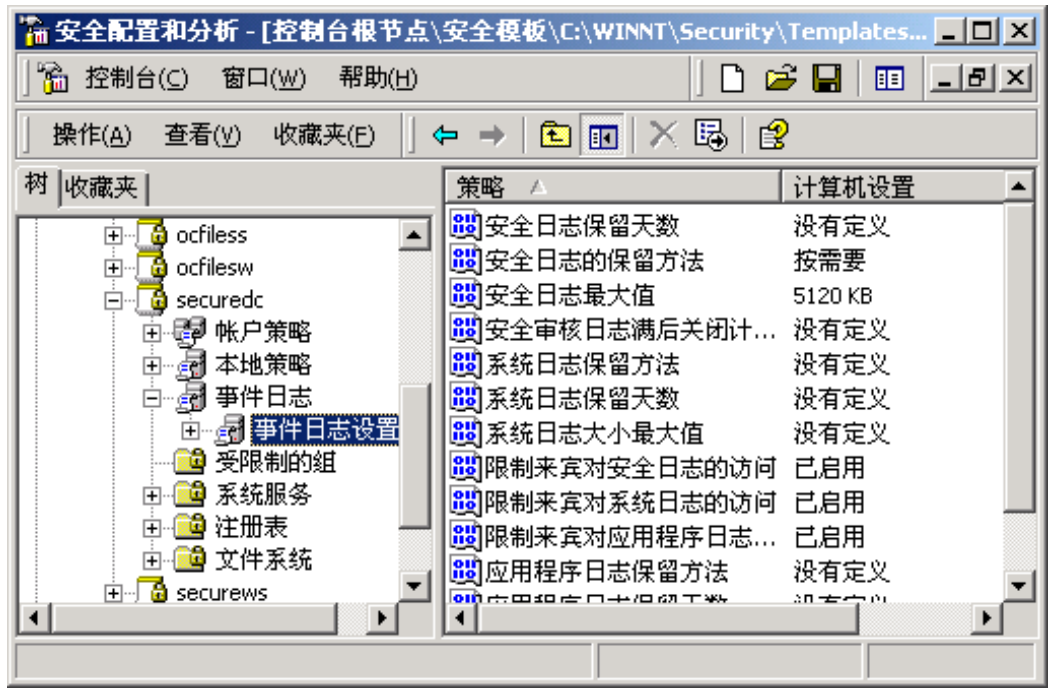


安全选项

- 用来启用或禁用计算机的安全设置
- 包含的内容：
  - LAN Manager身份验证级别
  - 登录屏幕上不要显示上次登录的用户名
  - 对匿名连接的额外限制
  - …

事件日志

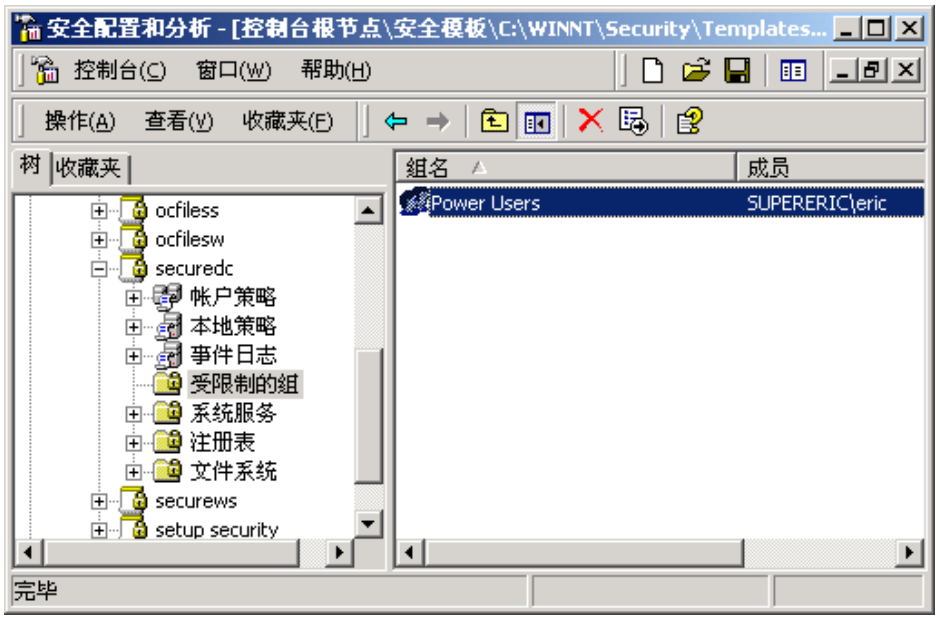
- 事件日志设置
  - 可以用来定义与应用程序、安全性和系统日志相关的属性。
  - 包含的内容：
    - 日志的最大值
    - 日志的保留天数
    - 日志的保留方法
    - 限制来宾对日志的访问



受限制的组

受限制的组

- 允许管理员定义谁应该属于某个组，谁应该不属于某个组。
- 当安全模板被配置到系统上去时，就会在该组内添加或删除用户，以保证实际的组成员身份符合模板



受限制组的应用

假设Power Users组包含两个用户：A和B。后来由于B临时有事，所以它添加了用户C到该组中，以便暂时取代B执行职务。但是，当B回来之后却忘记了将C从组中删除。在实际管理工作中，这种情况时有可能发生，导致不应再拥有相关特权的用户仍然拥有额外的组成员资格。为了避免这种情况，就可以通过“受限制的组”来进行配置。如果设置只有A和B在受限组中被列为Power Users组的成员，那么当管理员下一次应用组策略设置时，C就会被自动从组中删除了。

Secedit命令

- /analyze
  - 分析
- /configure
  - 配置
- /generate
  - 生成
- /RefreshPolicy
  - 刷新
- /validate
  - 验证

分析系统安全性的语法：

secedit /analyze [/DB *filename*] [/CFG *filename*] [/log *logpath*] [/verbose] [/quiet]

配置系统安全性的语法：

secedit /configure [/DB *filename*] [/CFG *filename*] [/overwrite][/areas *area1 area2...*] [/log *logpath*] [/verbose] [/quiet]

安全配置向导

- 安全配置向导（Security Configuration Wizard，SCW）
  - SCW是Windows Server 2003 操作系统在安装SP1或者SP2补丁包后提供的新功能。
  - 管理员使用此配置向导可以非常轻松地完成服务器角色的指定，禁用不需要的服务和端口，配置服务器的网络安全，配置审核策略、注册表和IIS服务器等工作，对提高服务器安全有极大帮助。
  - 由于整个配置过程在向导中完成，无需烦琐的手工设置，因此极大提高了方便性。

安全配置向导的安装

“控制面板“→”添加或删除程序“→”添加/删除Windows组件“→”选择‘安全配置向导’复选框”

安全配置向导的使用

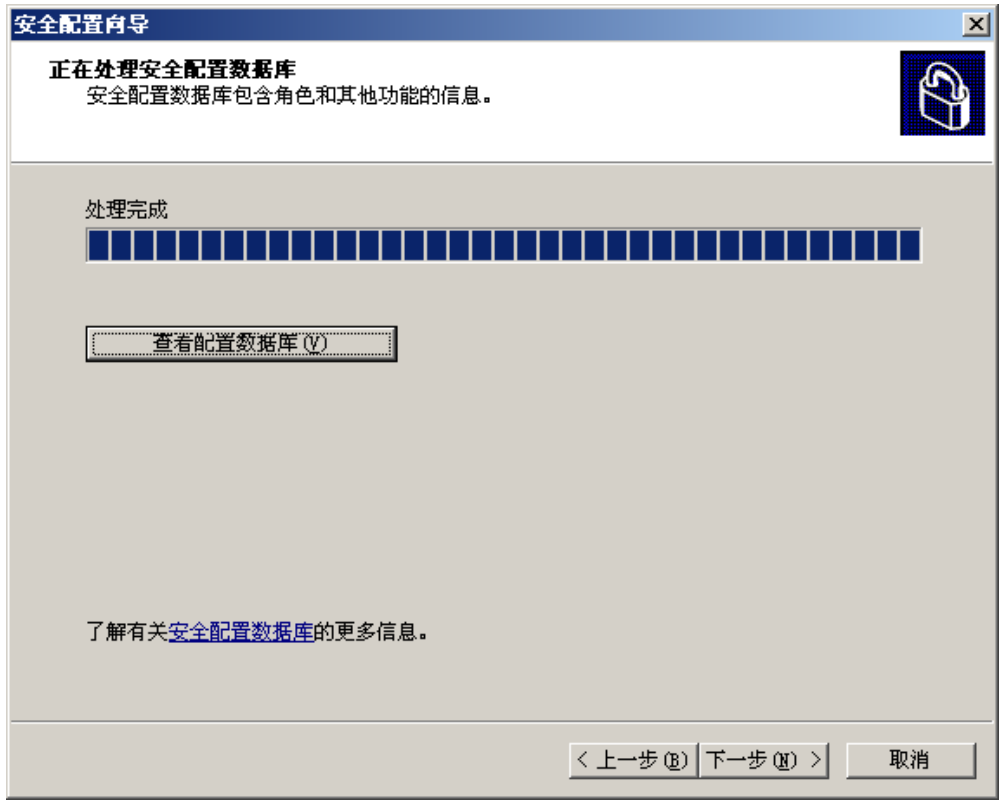
- 配置操作
  - 创建新的安全策略
  - 编辑现有安全策略
  - 应用现有安全策略
  - 回滚上一次应用的安全策略

安全配置向导的使用（续）

- 选择服务器

安全配置向导的使用（续）

- 处理安全配置数据库



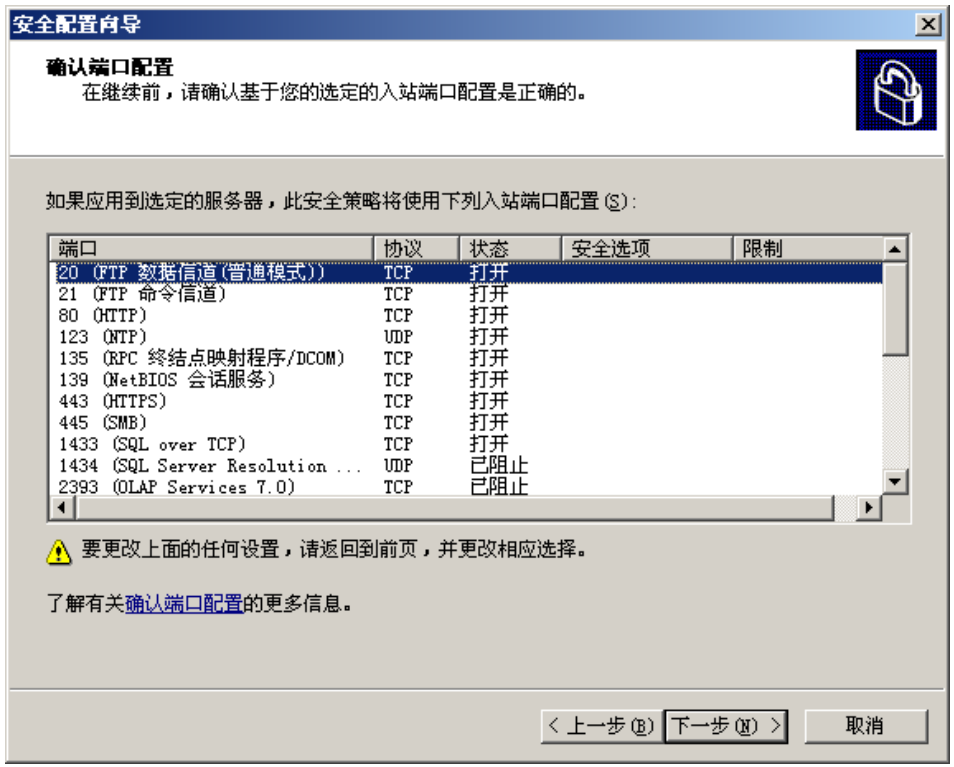
安全配置向导的使用（续）

- 基于角色的服务配置
  - 选择服务器角色
  - 选择客户端功能
  - 选择管理和其他选项
  - 选择其他服务
  - 处理未指定的服务

“确认服务更改”对话框

安全配置向导的使用（续）

- 网络安全
  - 打开端口并允许应用程序



“确认端口更改”对话框

安全配置向导的使用（续）

- 注册表设置
  - 要求SMS安全签名
  - 出站身份验证方法
  - 入站身份验证方法

“注册表设置摘要”对话框

安全配置向导的使用（续）

- 审核策略
  - 系统审核策略

“审核策略摘要”对话框

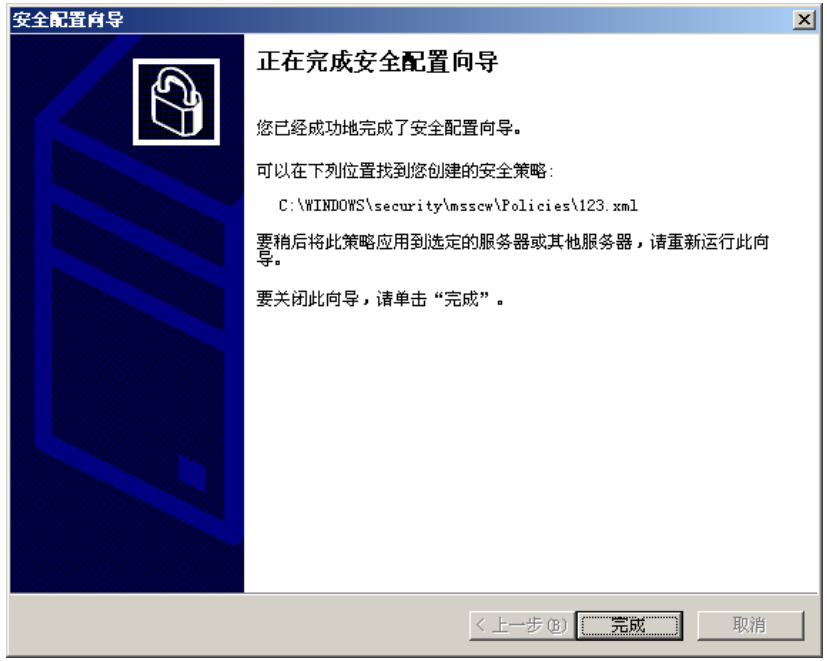
安全配置向导的使用（续）

- **Internet信息服务**
  - 选择动态内容的Web服务扩展
  - 选择一个要保留的虚拟路径
  - 防止匿名用户访问内容文件

“IIS设置摘要”对话框

安全配置向导的使用（续）

- 保存安全策略
- 应用安全策略
- 完成安全配置向导



SJTU Information Security Institute
Network Attack & Defence Technology Research Studio

Any Questions ?

确定 取消