WCI321
组策略在 Windows Vista 中的新特性

议程

- 今天的组策略现状
- Windows Vista 中的组策略
  - 全新的功能
  - 更多被使用的策略集

今天的组策略现状
被广泛的应用在中大型企业

- 组策路的应用情况：
  - 超过90%的大型企业和组织采用组策路
  - 超过60%的中小企业采用组策管理企业环境
- 策略的覆盖面非常大
  - 超过1800项的策略设置
  - 比如在安全方面或者IE等方面都有很多的策略

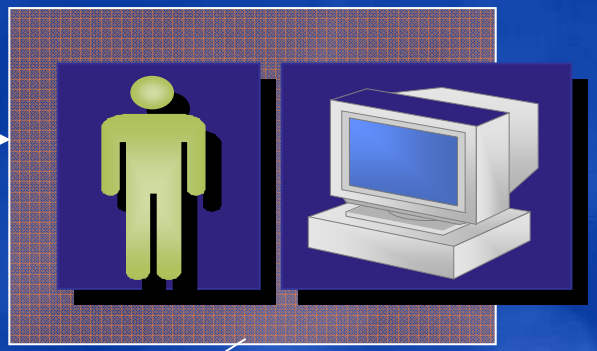
Group Policy Object (GPO) 基础结构: 客户的痛

ADM file format & Sysvol bloat

AD

Policy Targeting

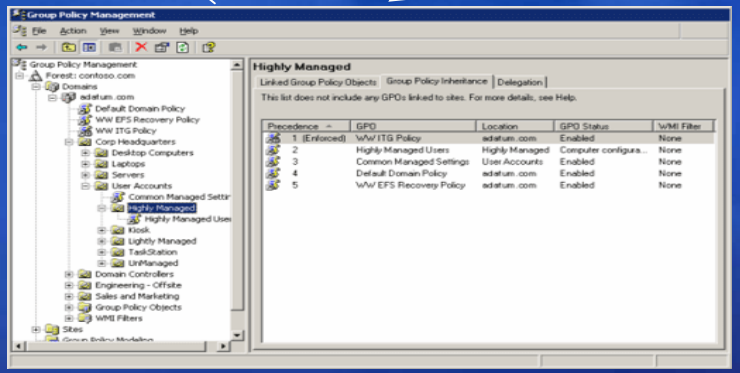
Policy Enforcement



Ping issues,
VPN scenarios
Non-AD scenarios

Policy Troubleshooting

Policy Definition



GPO Management and Operations
(GPMC/GPEdit)

Error messages
Complicated diagnostic log (Userenv)

Difficult to locate settings
Lack of best practice knowledge

What and where is GPMC?
Change management, auditing and workflow

Windows Vista 中组策略的改变

更多的设置，更可靠，容易使用

类别	关键特性和增强
扩展	可控策略从1，800 到3,000条 增加策略－针对Windows Vista的新特性 主要区域的改进
应用组词策略 可靠性和性能	更安全可靠的基础结构 全新的网络感知技术 支持多本地策略 组策略多语言支持
易用性	GPMC的集成 更强大的模版支持 sysvol bloat 的解决方案 搜索/分类/过滤/模板

议程

- 今天的组策略现状
- Windows Vista 中的组策略
  - 全新的功能
  - 更多使用的策略集

Group Policy Client Service

- 可靠性– Windows Vista的基础
  - 在从前组策略进程是通过Winlogon进程实现的
  - 在Vista中组策略的引擎是运行在一个共享的服务主机
- 增强的服务
  - 管理员也需要通过权限提升才能停止服务
  - 在遇到不可预料的情况下，服务将重新启动
  - 第三方客户端的支持

GPMC 集成

- GPMC推出已经三年
- 为什么要集成GPMC到系统中？ The perception is:
  - GPMC是一个很有用的小工具集吗？
  - 非常正确，但它不是操作系统的一部分
  - 什么是GPMC
- 不在需要下载/安装，它将默认集成到Windows Vista &Longhorn Server中。

单一的本地安全策略

- 本地安全策略主要被应用在:
  - 没有活动目录的情况下
  - 共享计算机 (比如：展台)
- 客户需要更加有效的安全策略
  - 比如：管理员和普通用户应该有不同策略设置
  - 没有目的的策略应用

Windows Vista：多本地安全策略

- 域组策略的优先级依然高于本地安全策略
- 本地策略可以应用到:
  - 计算机 新: 管理员或者管理员组
  - 新: 单独的本地用户
- 应用的顺序是最后应用的生效
- 一个用户只能接收一种策略（针对管理员或针对非管理员）
- 新的策略设置: Exclude processing of all local GPOs

Demo

Multiple Local GPOs

今天：网络感知

- 策略的应用不是网络敏感的，比如：
  - VPN 会话
  - 笔记本待机/休眠
- 慢速连接检测错误
  - ICMP Ping数据包不能通过路由器
  - 带宽高延迟很高的场合

Windows Vista: 网络感知

- 适应网络改变
  - 策略应用不再局限在90分钟
  - 如果从前应用的策略出现问题，而没能成功应用，网络感知将在下一次网络可用时自动应用
- 网络感知应用
  - 组策路可以订阅服务器边的改变
  - 不再依靠ICMP (没有更多的ping!)
  - 准确的带宽检测

今天: 组策略故障排除

- 含糊的错误消息
  - 不一致的排错和解决信息
  - 错误帮助连接部可用
  - 难以识别
- Userenv.log
  - 许多用户不清楚这个选项
  - 界面不友好
- 每个组策略扩展都有不同的模版和不同的日志位置
- 不支持事件合并

Windows Vista: 组策略日志增强

- 新的 ‘Crimson’ 事件管理特性
  - 基于XML的事件日志
  - 支持应用程序 ‘channels’
  - 使用 ‘Subscription’实现事件合并
  - 支持事件触发器
- 两个不同的日志级别
  - Admin events
  - Operational events

Windows Vista: 组策略增强

- Admin events
  - Actionable set of events in ‘System’ log (source = ‘Group Policy Service’ not ‘Userenv’)
  - Linked to Microsoft Web site with more information including troubleshooting steps, related KBs
- Operational events
  - Step-by-step policy processing events in ‘Group Policy’ Application channel
  - Admin friendly replacement of Userenv.log
  - Unique Activity ID enables grouping of events occurring in a single policy refresh
  - Provides valuable data like Username, GPO list, policy processing metrics (total time, individual extension processing time, etc.)

Why ADMX Files?

- ADM文件的挑战…
  - 不支持多语言环境
  - Sysvol的膨胀(4Mb+ per GPO）
  - 难以理解和使用的语法
- ADMX 文件的优点
  - 内建多言支持
  - 通过集中存储，解决Sysvol膨胀的问题
  - 支持集中存储或本地存储
  - 更多的扩展语言支持

ADMX 中心存储

- 默认是不启用中心存储的
  - 管理员可以使用GPMC/GPEdit来编辑本地的ADMX
- 启用中心存储
  - 在域中ADMX的存储位置是 – [sysvol]\policies\policydefinitions
  - 一次性创建中心存储
    - Windows Vista: 通过 Internet Explorer
    - Windows Server “Longhorn” Timeframe*: Additional tools
  - 最后，管理员可以使用Windows Vista 中的GPMC/GPEdit 工具管理中心存储的ADMX files (忽略本地存储)

rrent plan is to make available in this timeframe – will NOT require Windows Server “Longhorn”

ADMX/ADM 共存

- Windows Vista 不会装载任何的ADM文件
- ADMX和ADM文件可以并存，可以通过添加删除模版来添加ADM文件
- 提示：没有计划推出从ADM到ADMX的装换工具

ADM 和 ADMX 文件 对比

Behavior	ADMX (Windows Vista and later)	ADM (Windows 2000, Windows Server 2003 and Windows XP)
Can Manage Windows 2000, Windows Server 2003, Windows XP	√	√
Can Manage Windows Vista, Longhorn Server	√	X
Multilingual Support	√ (ADML Files)	X
Can Consume Custom ADM Files	√	√
Default Location of Files	ADMX files read locally	ADM files copied to GPO
Can Use Central Store	√	X
Avoids Duplicated Files in the GPO (Sysvol Bloat)	√	X
Option to Add GPO-Specific Files (Add/Remove Templates)	ADM Files Only	ADM Files Only
File Comparisons	Version Numbers	Timestamp

议程

- 今天的组策略现状
- Windows Vista 中的组策略
  - 全新的功能
  - 更多使用的策略集

新的、更合理的策路设置

更多的策略且实用的策略。。。。。。

Removable Storage Devices	IPSec / Windows Firewall	Power Management	Printer Management	Troubleshooting & Diagnostics
Windows Defender	Network Access Protection	Internet Explorer	Tablet PC	Windows Error Reporting
User Account Control	Wired and Wireless Policy	Desktop Shell	Globalization	Remote Assistance

Instant Cost Savings With Power Management Policy Settings

Power Management Can Lower Operational Costs[1]

Energy management features (sleep and display blanking) translate into savings

- Compare system on 24x365 with one with energy saving features enabled
- Display blanking alone
  - 17” LCD up to $17/monitor per year
  - 17” CRT up to $31/monitor per year
- System sleep and display blanking together
  - Up to $63/system per year

Savings Multiply with Group Policy Management of Energy Features

Assume $63 system idle and display blanking savings per PC

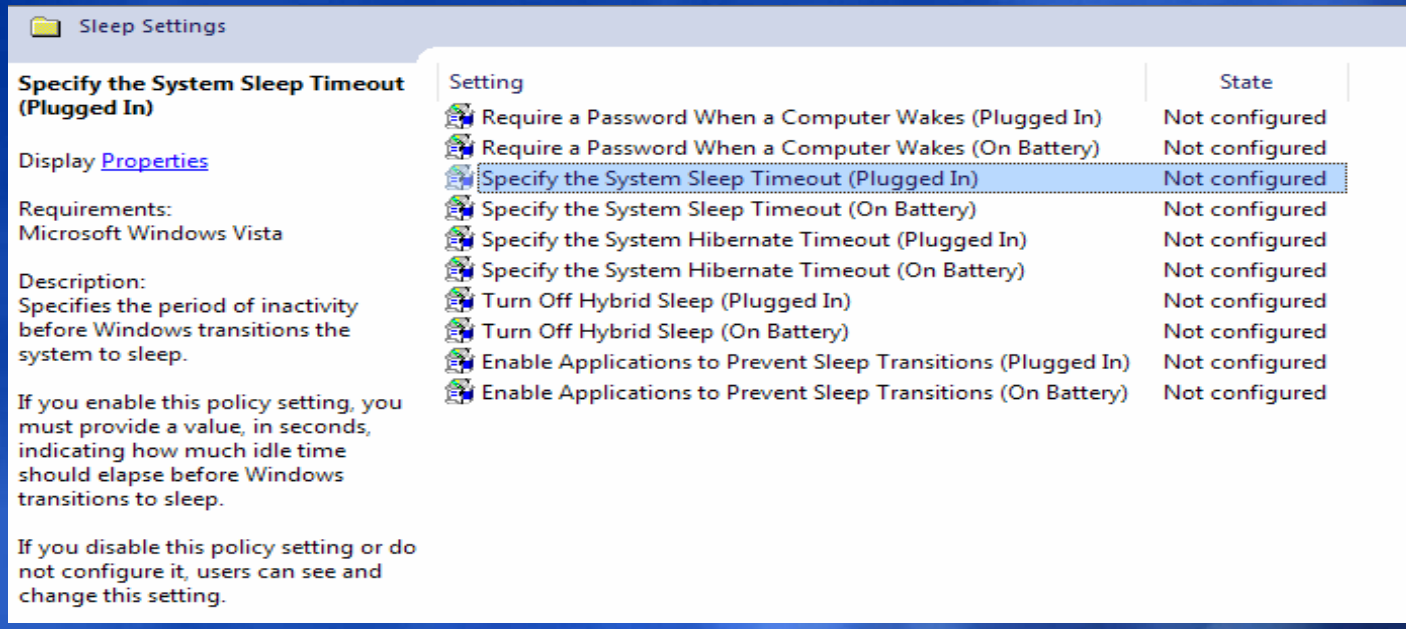
- 1 PC $63
- 1,000 PCs $63,000
- 10,000 PCs $630,000

Other value

- Heating / cooling savings (HVAC)
- Reduction in environmental impact

电源管理

通过组策略控制电源管理为企业节省电源开销



全面的电源管理

Windows Vista 包括全面的电源管理

- 针对不同用户的电源设置
- 通过组策略完全控制
- Separate power plan for when no user is logged into the system

默认省电模式

默认在所有的PC上启用省电模式

- Sleep作为默认的“关机”动作
- 支持系统Sleep空闲时间
- 支持关闭显示器空闲时间

移动存储设备导致的问题

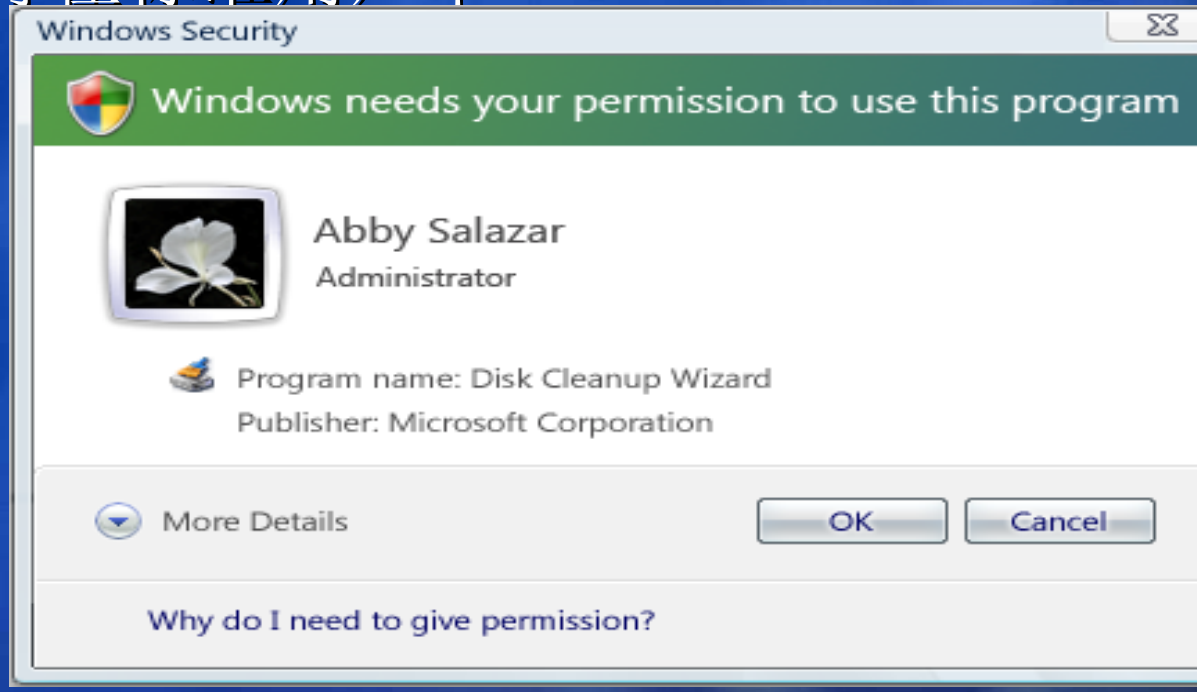
- 数据保护
  - USB设备
  - MP3 播放器
  - CD/DVD 刻录
- 攻击:
  - 恶意软件与病毒
  - 主要数据泄露 (销售数据，产品计划和价格等）
- 客户非常想对移动设备进行控制

移动设备控制

- 控制设备的读写权限
- 移动设备类别
  - CD/DVD
  - Tapes
  - USB plug-in devices
  - Windows Portable Devices (WPD)
  - All other external removable storage devices
- Only computer settings are applicable on Terminal Server

用户账号控制

- 了解 = UAC = LUA = UAP!
- 默认情况下，任何用户将运行在标准用户下
- Administrator始终
  有全部的管理权限
- 针对管理员使用赞成模式
- 标准用户使用全新的
  权限提升方式工作



用户账号访问策略

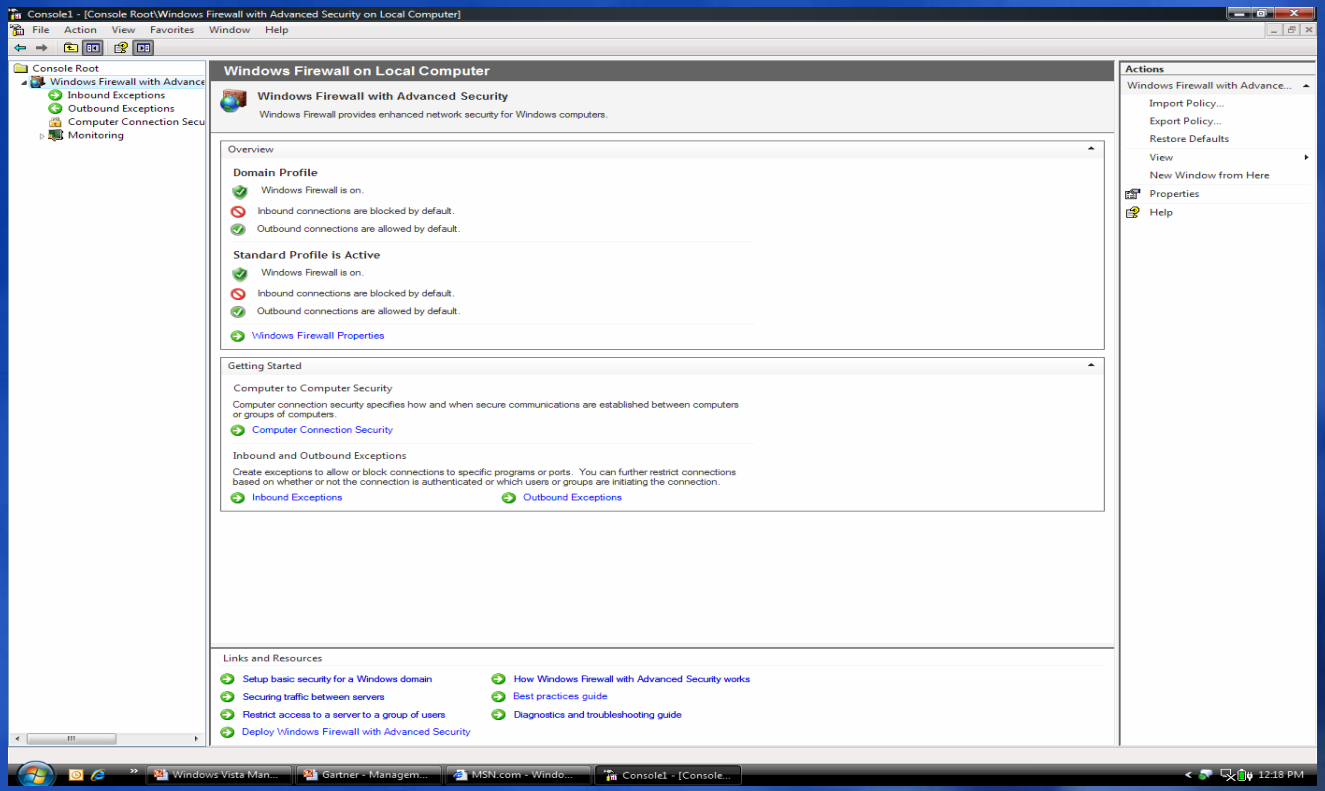
- 用户账号策略位置:
  Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options
- 管理UAC的用户体验
  - 权限提升行为 (没有提示, 赞成模式, 权限提升)
  - 应用程序安装提示
  - 通过支持Virtualizes file和registry 写入失败的支持，减少应用程序兼容的问题

Demo

User Account Contral

Windows 防火墙和IPsec

Windows防火墙和IPsec



更加智能的防火墙

- 特定应用程序和端口允许
- 只允许安全连接
- 只允许AD中的某个组进行连接

强制隔离

- Restrict network resource access to domain-joined computers
- 只允许健康计算机访问网络资源

简化管理

- 单点、统一的管理
- 无缝的管理

Microsoft Tech·Ed 2006 中国

安全特性: 更多的新策略

- Windows Defender (反间谍软件)
  - 即时扫描与监控
  - 有效管理签名下载
- 设备安装控制
  - 有效控制移动设备的使用
- 无线网络安全
  - 更安全的无线网络策略
- 网络访问保护
  - 安全隔离控制
- 增强的公钥配置
  - 更多的认证设置
- 增强的IE安全控制
  - IE 7新增加更多的安全策略

Q & A

- Windows Vista组策略的全新的组策略模板格式是什么？答出至少两个优点
- Windows Vista组策略在客户端增加了一个新的服务，它是什么？
- Windows Vista对移动设备采取的管理措施是什么？
- 多本地策略对于用户的好处是什么？
- Windows Vista如何解决组策略远程应用的问题？

Resources

- What's new in GP in Widows Vista
  - http://www.microsoft.com/technet/windowsvista/library/a8366c42-6373-48cd-9d11-2510580e4817.mspx
- New categories of Policy settings
  - http://www.microsoft.com/technet/windowsvista/library/2b8dc2fd-eafe-4c74-914c-ec101133feb4.mspx
- Managing the new ADMX files: A step by step guide
  - http://www.microsoft.com/technet/windowsvista/library/02633470-396c-4e34-971a-0c5b090dc4fd.mspx

Microsoft®

您的潜力，我们的动力

Microsoft Tech·Ed 2006 中国