



# 计算机安全与维护

## Windows系统安全维护与加固进阶



## 本章内容提要

- WMI体系结构
- 提供者
- CIM和可管理对象的格式语言
- WMI名字空间
- 类关联
- WMI实现和安全性
- Windows的环境变量设置



# WMI体系结构

---

- Windows NT一直以来集成了性能监视工具和系统事件监视工具
- 事件管理器报告错误消息和用于诊断的消息
- 事件查看器让管理员检查计算机的事件输出
- 性能监视器报告一些与性能有关的统计信息



# WMI体系结构

- 局限性

- 编程接口各不相同，使得采集数据的应用程序变得非常复杂
- 缺乏扩展性，没有提供十分必要的双向交互能力
- 无法限制只接收某些特定类型的事件通知，或者只接收某些来源的事件通知
- 无法与事件数据或者性能数据的提供者进行通信



## WMI体系结构

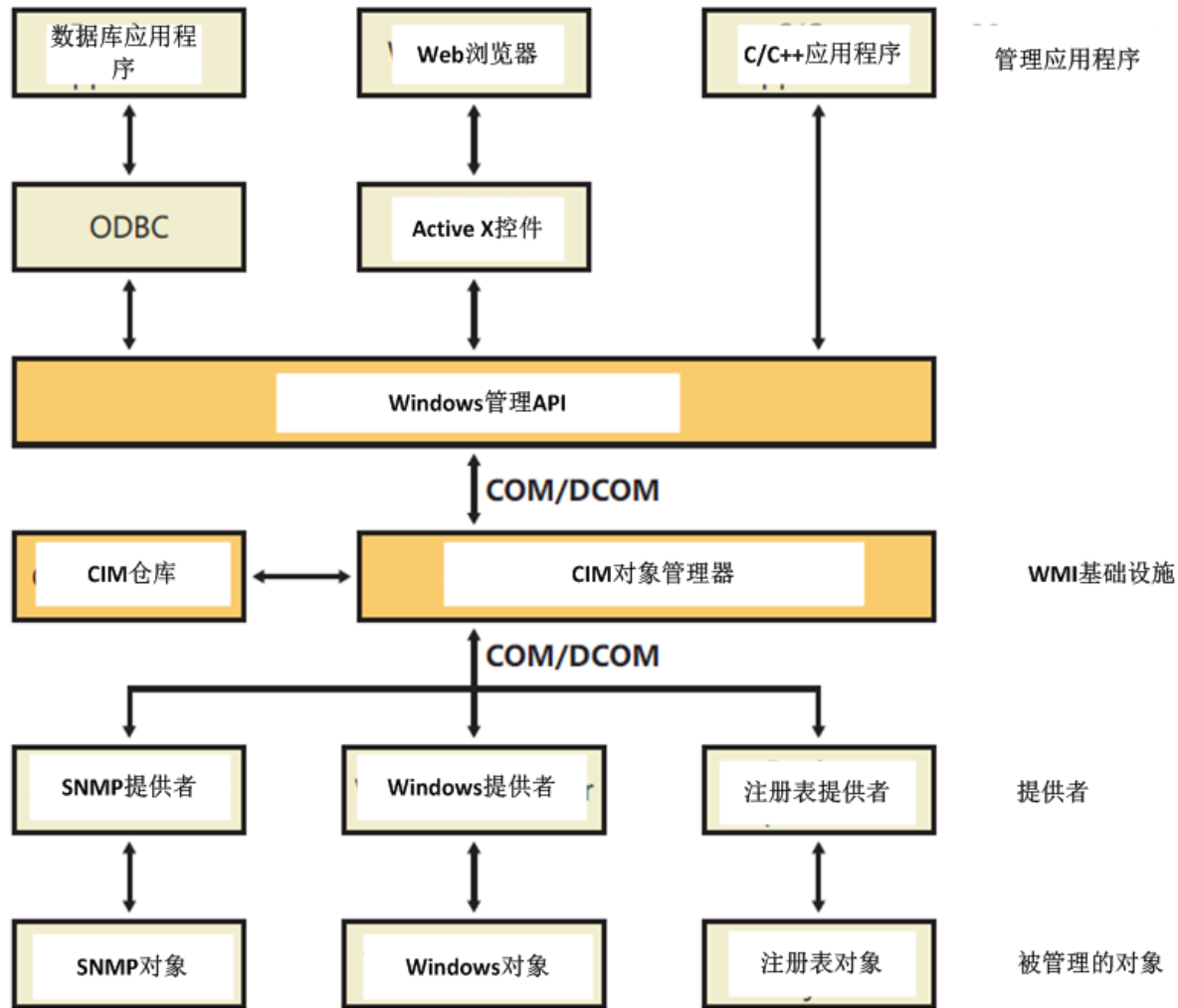
---

- Windows还有一种新的管理机制称为windows管理规范（WMI）
- WMI是WBEM（Web-Based Enterprise Management）的一个实现，而WBEM则是DMTF（工业界联盟）定义的一个标准
- WBEM标准包含了一套可扩展的，针对企业的数据采集和数据管理设施的设计方案，此设计方案具有很强的灵活性和扩展性



# WMI体系结构

## • WMI体系结构示意





# WMI体系结构

---

- WMI由四个主要的部件构成
  - 管理应用程序
  - WMI基础设施
  - 提供者
  - 被管理的对象



## WMI体系结构

- 管理应用程序的目标定义为采集有关特定对象的数据以及管理这些对象
- 提供者需要为管理应用程序可能感兴趣的对象，定义和导出它们的表示形式
- WMI基础设施是把管理应用程序和提供者绑定在一起的粘合剂，其核心是CIM对象管理器（CIMOM），此基础设施被用作对象-类的存储体，实现为磁盘上的数据库





# WMI体系结构

---

- Windows程序使用WMI COM API来直接与WMI打交道，这是最为基本的管理API
- 数据库开发人员使用WMI ODBC接口嵌入对于数据库的对象数据的引用
- WMI ActiveX控件为WMI数据构造出基于WEB的界面
- WMI脚本API，主要为了基于脚本的应用程序和VB程序中使用



## 本章内容提要

---

- WMI体系结构
- 提供者
- CIM和可管理对象的格式语言
- WMI名字空间
- 类关联
- WMI实现和安全性
- Windows的环境变量设置



## 提供者

- 提供者的开发人员使用CIM来表达那些“属于他们想要管理的应用中的各种部件”。开发人员使用“可管理对象的格式” (MOF) 语言来实现CIM表示
- 提供者除了定义一些类来表达对象以外，还必须作为接口将WMI与这些对象连接起来，WMI根据这些提供者所支持的接口特性对它们进行分类
- 每个提供者可以实现一个或者多个特性



# 提供者

---

- 类 (class)
- 实例 (instance)
- 属性 (property)
- 方法 (method)
- 事件 (event)
- 事件消费者 (event consumer)



# 提供者

- 类

——可以提供，修改，删除和枚举一个特定于提供者的类，也可以支持查询处理

- 实例

——可以提供，修改，删除和枚举系统类的实例，或者特定于提供者的类的实例。一个实例代表一个被管理的对象，也可以支持查询处理

- 属性

——可以提供和修改单独的对象属性值



# 提供者

- 方法

- 为一个特定于提供者的类提供方法

- 事件

- 产生事件通知

- 事件消费者

- 将一个物理消费者映射到一个逻辑消费者，以便支持事件通知



## 本章内容提要

- WMI体系结构
- 提供者
- CIM和可管理对象的格式语言
- WMI名字空间
- 类关联
- WMI实现和安全性
- Windows的环境变量设置



# CIM和可管理对象的格式语言

- CIM遵从像C++和Java这样的面向对象语言原理，用类来表示问题中给的数据
- DMTF提供多个类，作为WBEM标准的一部分，是CIM的基本语言，它们表达了可适用于所有管理领域的对象，这些类是CIM核心模型的一部分
- WBEM标准的抽象类是为了让其他的类继承它们，是专门用于为其他类定义属性的模板





# CIM和可管理对象的格式语言

- 第二种类表达了那些特定于管理领域但是与具体实现无关的对象，这些类构成了公共模型（common model）
- 公共模型被认为是核心模型的一个扩展
- 最后一种类别的类是扩展模型（extended model），由一些附加于公共模型之上的，与特定技术相关的类组成的
- Windows定义了很多这种类来表达那些特定于windows环境的对象



# CIM和可管理对象的格式语言

- 事件日志 (Event Log) 提供者大量的使用了继承技术
- WMI提供者的开发人员使用MOF语言来编写它们的类
- 动态 (dynamic) 的类意味着当一个管理应用程序查询该类的对象的属性时，WMI基础设施向WMI提供者询问与该对象相关联的属性的值



## CIM和可管理对象的格式语言

---

- 静态 (static) 的类是指WMI仓库中的类，WMI基础设施仅仅依靠WMI仓库就可以得到这些值，无需向提供者询问这些值
- 对于那些属性频繁变化的对象，动态提供者更加高效
- 在WMI开发人员使用MOF编写了它们的类后，通过不同的方式将这些类定义提供给WMI



- 将一个MOF文件编译成一个二进制MOF文件 (BMF) 并交给WDM基础设施
- 提供者编译该MOF文件，通过WMI COM API，将这些定义交给WMI基础设施
- 提供者可以使用MOF编译器，将一个类编译之后的表示形式直接交给WMI基础设施



## 本章内容提要

---

- WMI体系结构
- 提供者
- CIM和可管理对象的格式语言
- WMI名字空间
- 类关联
- WMI实现和安全性
- Windows的环境变量设置



## WMI名字空间

- WMI使用一个名字空间将对象组织起来，该名字空间包含了几种子名字空间
- WMI按照层次空间安排子命名空间，管理应用程序在访问一个名字空间中的对象之前，必须限于该名字空间建立连接
- WMI将名字空间的根目录命名为root
- 所有安装的WMI都有四个预定义的名字空间，位于root的下面
- 分别为CIMV2， Default， Security， WMI



## WMI名字空间

- 不像文件系统的名字空间是有目录和文件的层次结构构成的，WMI名字空间只有一层的深度
- 不像文件系统那样使用名称来标示文件和目录，WMI使用对象的属性来标示对象把这些属性定义为键（key）
- 管理应用程序指定类名和键名来找到一个名字空间内部的特定对象



## 本章内容提要

---

- WMI体系结构
- 提供者
- CIM和可管理对象的格式语言
- WMI名字空间
- 类关联
- WMI实现和安全性
- Windows的环境变量设置





# 类关联

- WMI允许提供者构造一个关联类 (association class) 来表达两个不同的类之间的逻辑连接
- 关联类将一个类与另一个类关联起来，所以这样的类仅有两个属性：一个类名和Ref修饰符



## 本章内容提要

---

- WMI体系结构
- 提供者
- CIM和可管理对象的格式语言
- WMI名字空间
- 类关联
- WMI实现和安全性
- Windows的环境变量设置



## WMI实现

- WMI服务运行在一个共享的svchost进程中，在本地系统账户下执行
- WMI将提供者加载到一个专门接收提供者的进程wmiprvse.exe中，wmiprvse.exe作为RPC服务进程的一个子进程被启动起来
- WMI在本地系统账户，本地服务账户或者网络服务账户下执行wmiprvse.exe，具体账户取决于代表此提供者的WMI Win32Provider对象实例的HostingModel属性值



# WMI实现

- 大多数WMI组件在默认情况下驻留在  
\\windows\\system32和  
\\windows\\system32\\Wbem下，包括windows  
MOF文件，内置的提供者DLL和管理应用程序  
WMI DLL
- 打开\\windows\\system32\\Wbem目录，你可以  
找到Ntevt.mof,这是事件日志提供者的MOF文  
件
- Ntevt.dll，这是事件日志提供者的DLL文件，  
WMI服务要用到它



# WMI实现

- \windows\system32\Wbem下面的目录存放了仓库文件，日志文件和第三方的MOF文件
- WMI使用一个私有版本的Microsoft JET数据库引擎来实现它的仓库，即CIMOM仓库
- 此数据库驻留在  
\windows\system32\Wbem\Repository\ 中
- WMI用到了大量的注册表设置，存放在该服务的  
HKLM\SOFTWARE\Microsoft\WBEM\CIMOM注册表键中



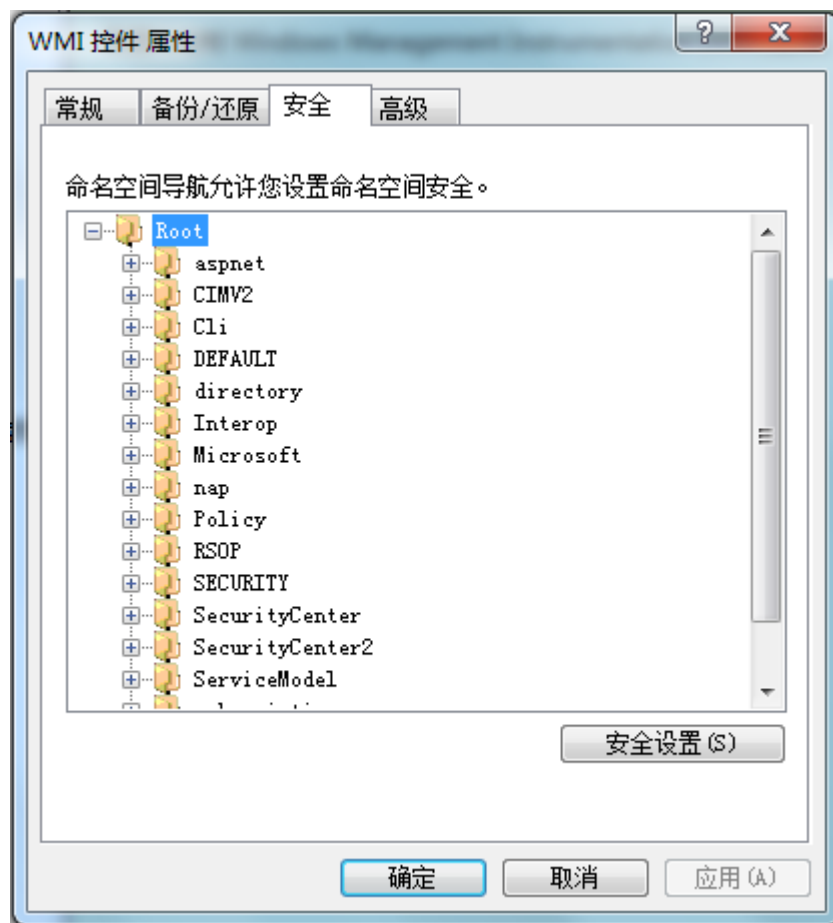
# WMI实现

- 设备驱动程序使用特殊的接口来向WMI提供数据，以及接受来自WMI的命令（WMI系统控制命令）
- 这些接口是WDM的一部分，因为这些接口是跨平台的，所以位于\root\WMI名字空间下面



# WMI安全性

- WMI安全属性





## WMI安全性

---

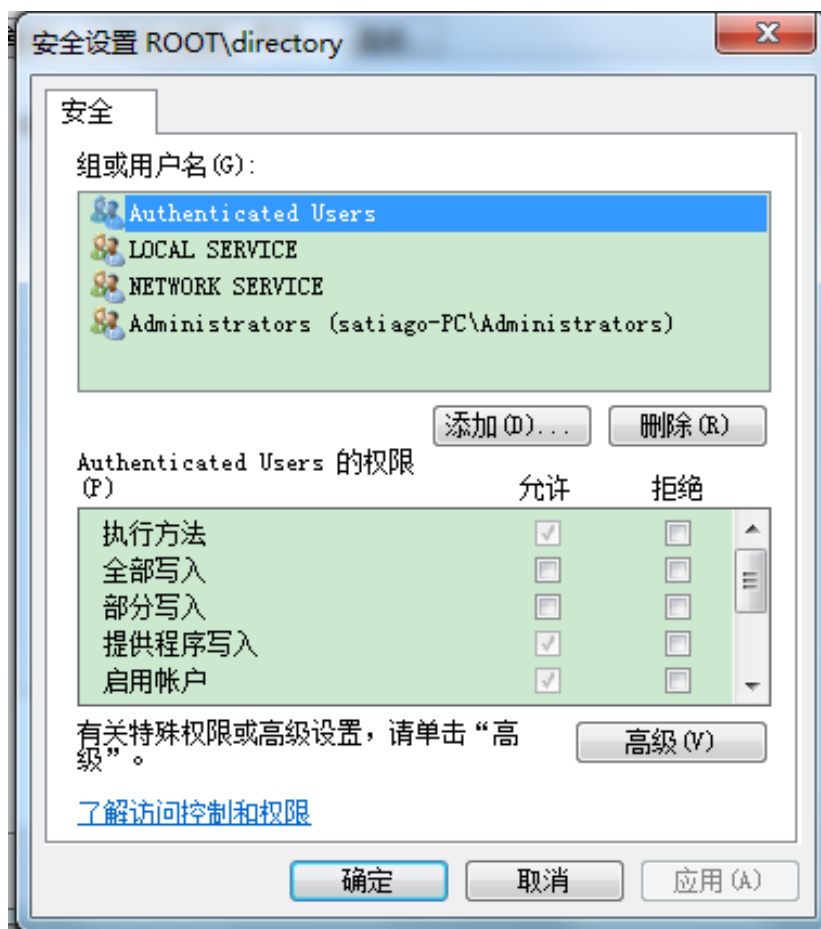
- WMI在名字空间层次上实现了安全性，如果一个管理应用程序成功的连接到一个名字空间，那么此应用程序可以查看和访问该名字空间中所有对象的属性





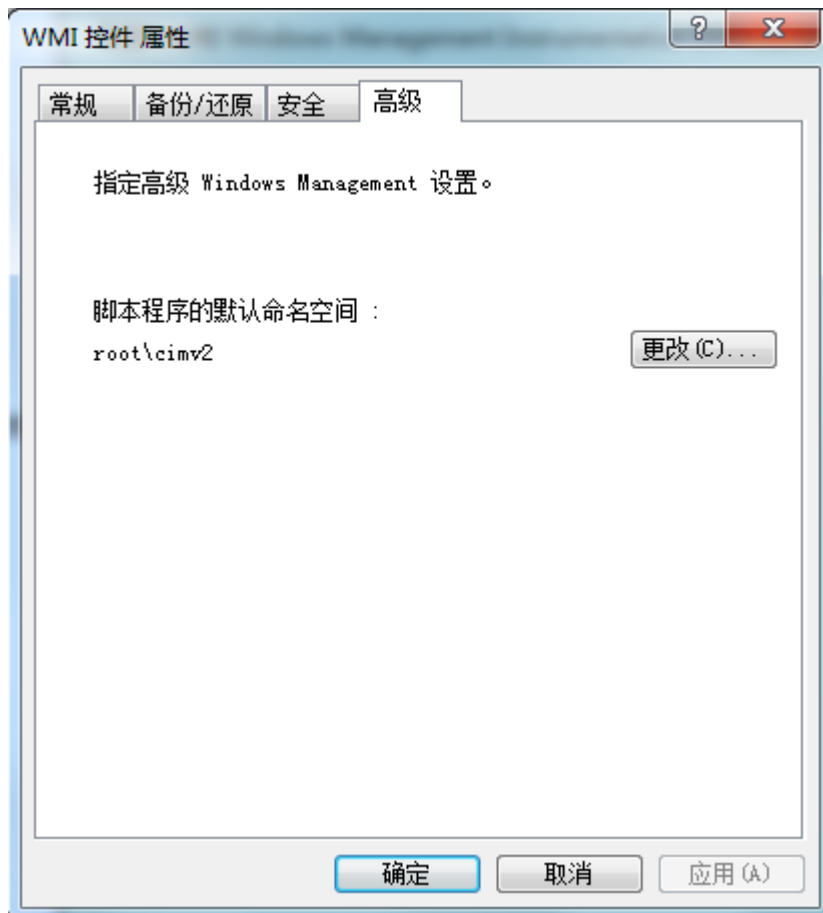
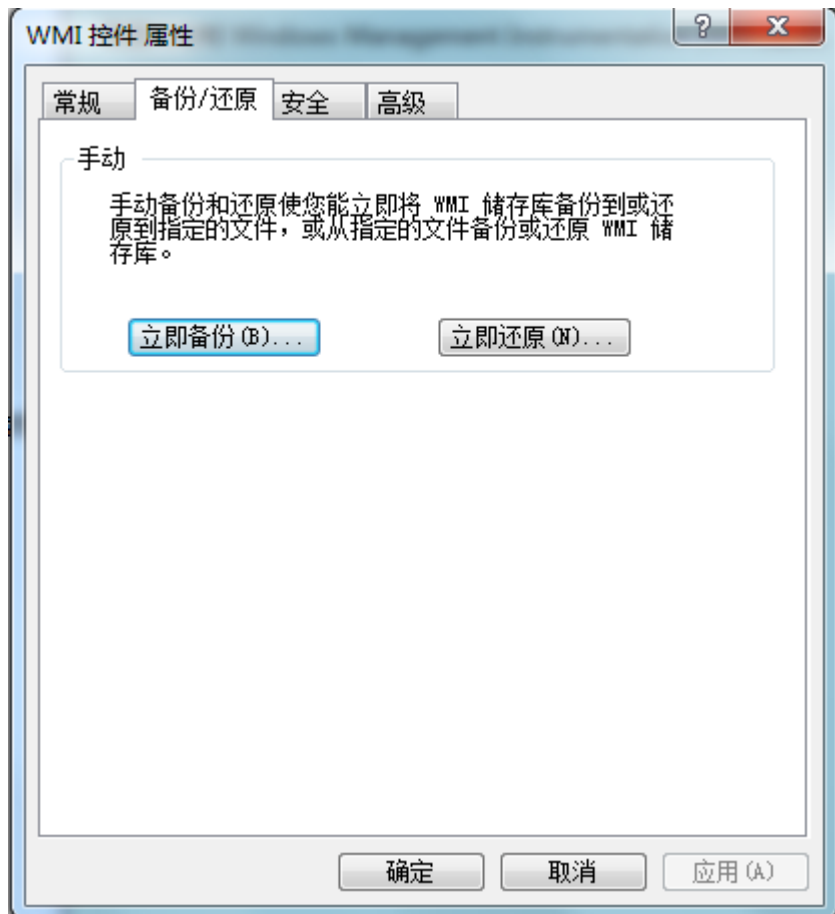
# WMI安全性

- 配置名字空间的安全性





# WMI安全性





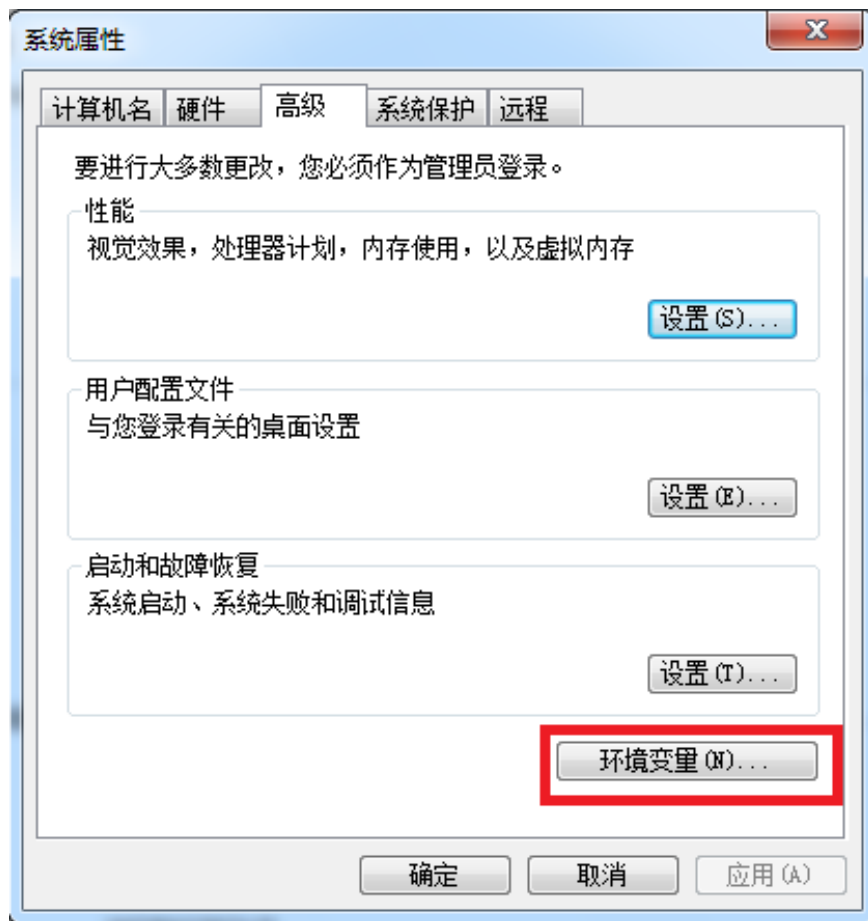
## 本章内容提要

- WMI体系结构
- 提供者
- CIM和可管理对象的格式语言
- WMI名字空间
- 类关联
- WMI实现和安全性
- Windows的环境变量设置



# Windows的环境变量设置

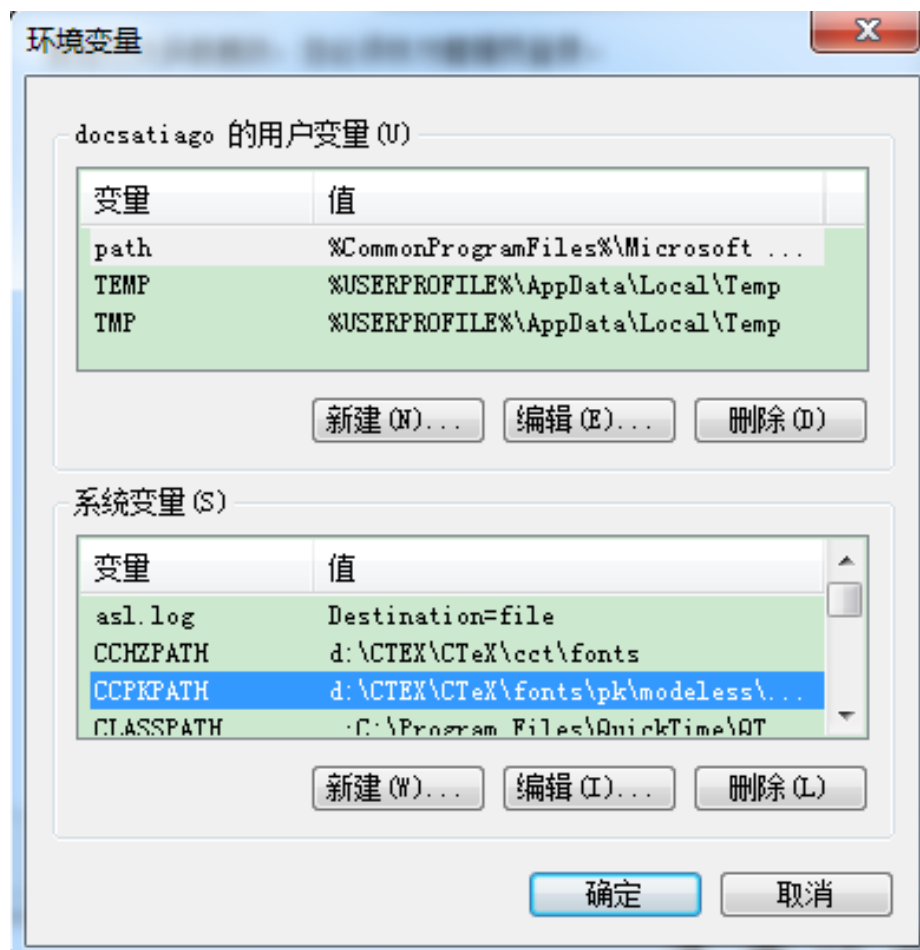
- Windows电脑“系统属性”





# Windows的环境变量设置

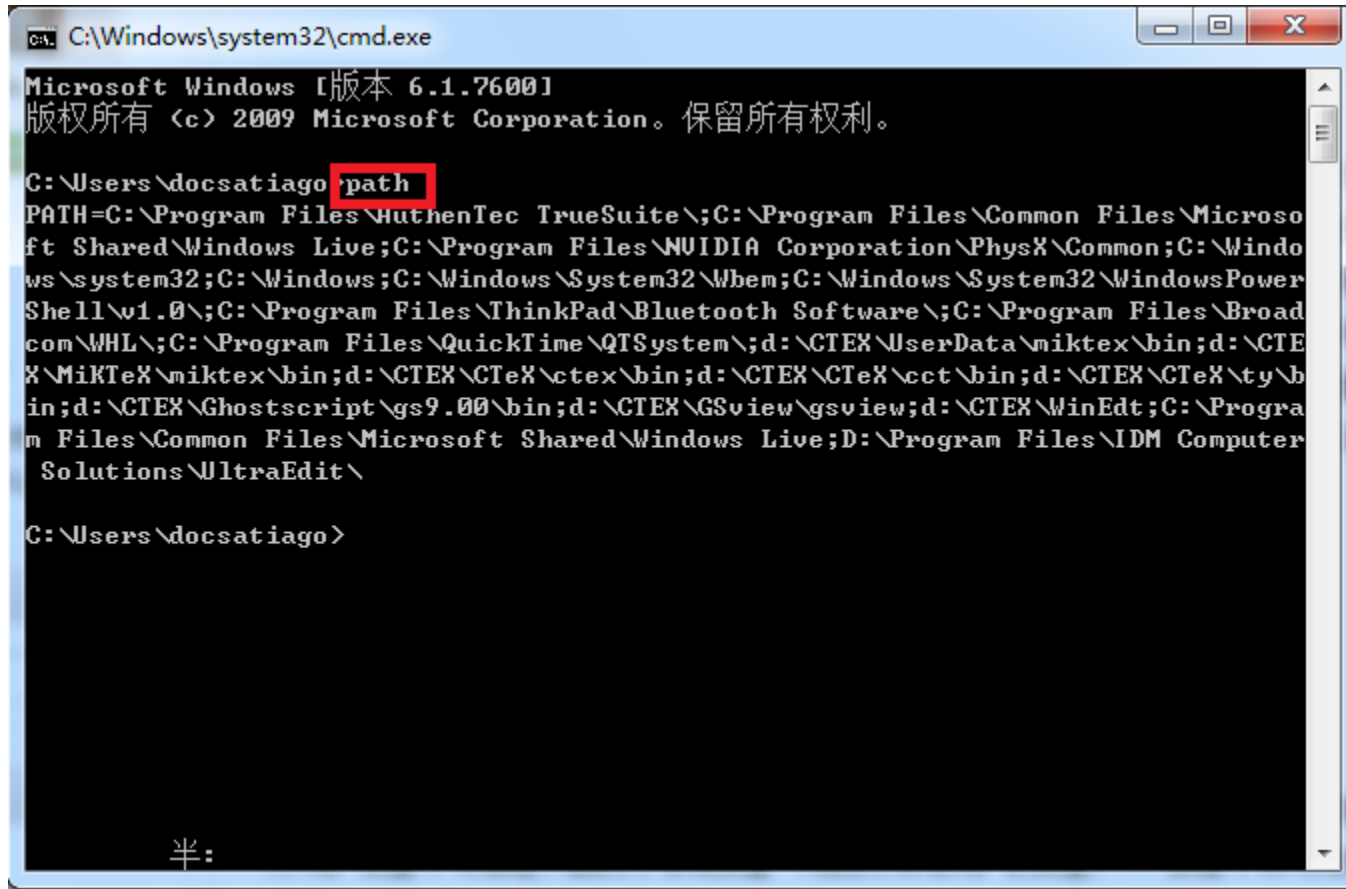
- 环境变量设置界面





# Windows的环境变量设置

- 命令查看环境变量



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\docsatiago> path
PATH=C:\Program Files\HuthenTec TrueSuite\;C:\Program Files\Common Files\Microso
ft Shared\Windows Live;C:\Program Files\NVIDIA Corporation\PhysX\Common;C:\Windo
ws\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPower
Shell\v1.0\;C:\Program Files\ThinkPad\Bluetooth Software\;C:\Program Files\Broad
com\WHL\;C:\Program Files\QuickTime\QTSystem\;d:\CTEX\UserData\miktex\bin;d:\CTE
X\MiKTeX\miktex\bin;d:\CTEX\CTeX\ctex\bin;d:\CTEX\CTeX\cct\bin;d:\CTEX\CTeX\tyb
in;d:\CTEX\Ghostscript\gs9.00\bin;d:\CTEX\GSview\gsview;d:\CTEX\WinEdt;C:\Progra
m Files\Common Files\Microsoft Shared\Windows Live;D:\Program Files\IDM Computer
Solutions\UltraEdit\

C:\Users\docsatiago>
```



# Windows的环境变量设置

- echo %变量名%形式显示环境变量

```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\docsatiago>echo %classpath%
.;C:\Program Files\QuickTime\QTSystem\QTJava.zip

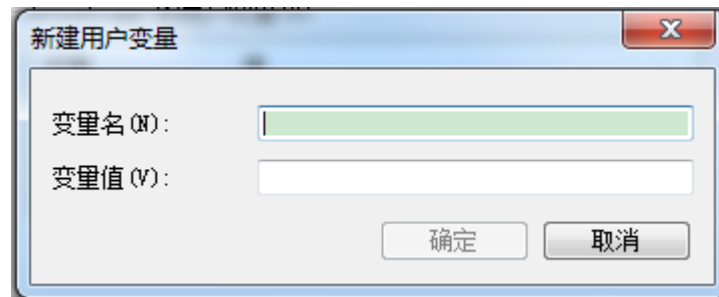
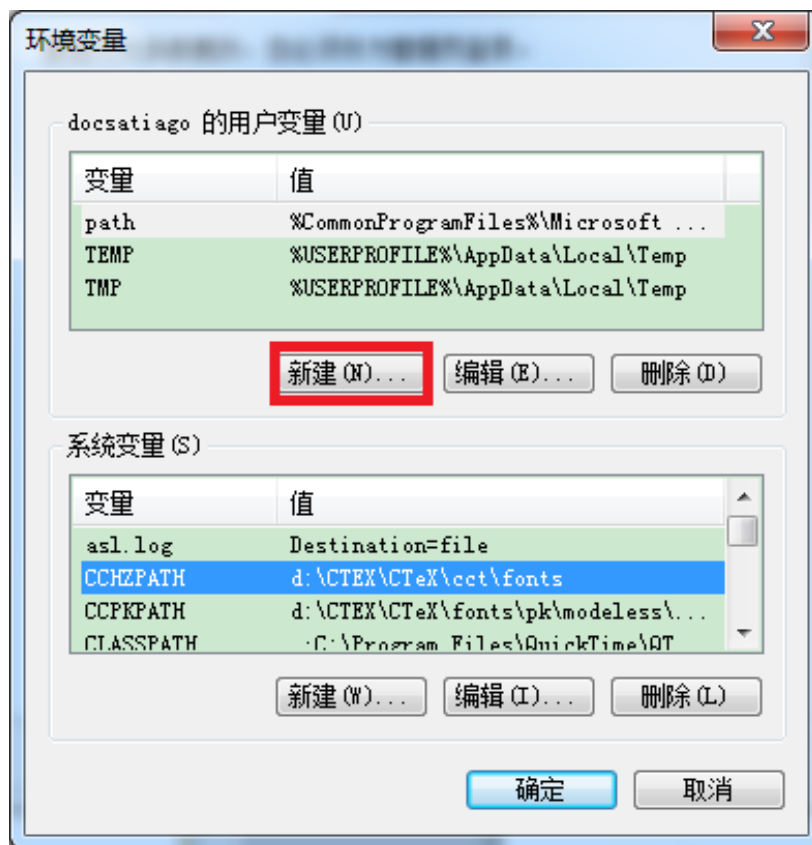
C:\Users\docsatiago>echo %path%
C:\Program Files\AuthenTec\TrueSuite\;C:\Program Files\Common Files\Microsoft Shared\Windows Live;C:\Program Files\NVIDIA Corporation\PhysX\Common;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files\ThinkPad\Bluetooth Software\;C:\Program Files\Broadcom\WiFi\;C:\Program Files\QuickTime\QTSystem\;d:\CTEX\UserData\miktex\bin;d:\CTEX\MikTeX\miktex\bin;d:\CTEX\CTEX\ctex\bin;d:\CTEX\CTEX\cct\bin;d:\CTEX\CTEX\ty\bin;d:\CTEX\Ghostscript\gs9.00\bin;d:\CTEX\GSview\gsview;d:\CTEX\WinEdt;C:\Program Files\Common Files\Microsoft Shared\Windows Live;D:\Program Files\IDM Computer Solutions\UltraEdit\

C:\Users\docsatiago>
```



# Windows的环境变量设置

- 新建环境变量

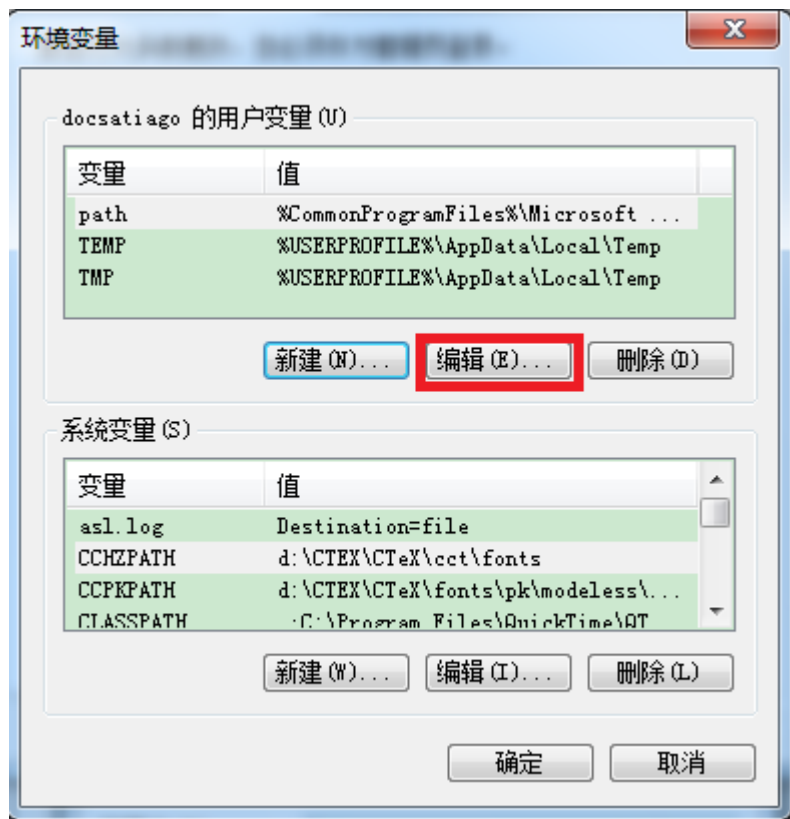






# Windows的环境变量设置

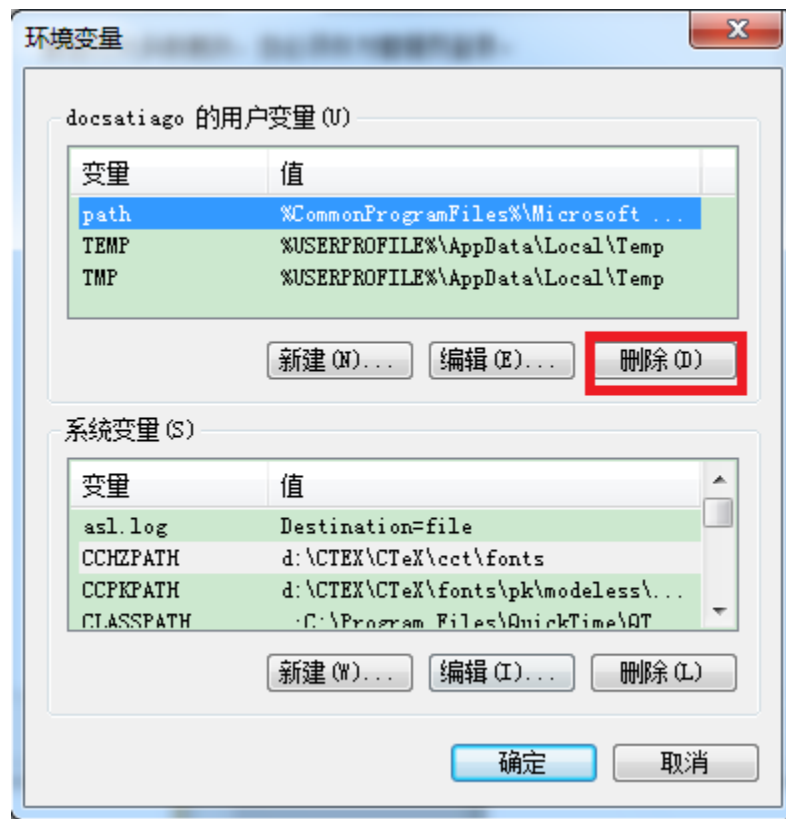
- 编辑环境变量





# Windows的环境变量设置

- 删除环境变量





# Windows的环境变量设置

- 系统变量

- 与windows操作系统包括网络状况有关，由操作系统定义。Administrators组的用户可以添加添加、修改或删除，

- 系统变量的作用域是全局的，对所有用户生效

- 用户变量

- 由操作系统、某些应用程序以及用户建立，任何用户都可以添加、修改或删除

- 用户变量的作用域是当前用户，只对当前用户生效



## Windows的环境变量设置

- %ALLUSERSPROFILE% : 列出所有用户Profile文件位置。
- %APPDATA% : 列出应用程序数据的默认存放位置。
- %CD% : 列出当前目录。
- %CLIENTNAME% : 列出联接到终端服务会话时客户端的NETBIOS名。
- %CMDCMDLINE% : 列出启动当前cmd.exe所使用的命令行。



## Windows的环境变量设置

---

- **%CMDEXTVERSION%**：命令出当前命令处理程序扩展版本号。
- **%CommonProgramFiles%**：列出了常用文件的文件夹路径。
- **%COMPUTERNAME%**：列出了计算机名。
- **%COMSPEC%**：列出了可执行命令外壳（命令处理程序）的路径。
- **%DATE%**：列出当前日期。



## Windows的环境变量设置

---

- **%ERRORLEVEL%**：列出了最近使用的命令的错误代码。
- **%HOMEDRIVE%**：列出与用户主目录所在的驱动器盘符。
- **%HOMEPATH%**：列出用户主目录的完整路径。
- **%HOMESHARE%**：列出用户共享主目录的网络路径。



## Windows的环境变量设置

---

- **%LOGONSERVER%**：列出有效的当前登录会话的域名控制器名。
- **%NUMBER\_OF\_PROCESSORS%**：列出了计算机安装的处理器数。
- **%OS%**：列出操作系统的名字。(Windows XP 和 Windows 2000 列为 Windows\_NT.)
- **%Path%**：列出了可执行文件的搜索路径。
- **%PATHEXT%**：列出操作系统认为可被执行的文件扩展名。



## Windows的环境变量设置

---

- %PROCESSOR\_ARCHITECTURE%：列出了处理器的芯片架构。
- %PROCESSOR\_IDENTIFIER%：列出了处理器的描述。
- %PROCESSOR\_LEVEL%：列出了计算机的处理器型号。
- %PROCESSOR\_REVISION%：列出了处理器的修订号。





## Windows的环境变量设置

---

- %ProgramFiles%：列出了Program Files文件夹的路径。
- %PROMPT%：列出了当前命令解释器的命令提示设置。
- %RANDOM%：列出界于0 和 32767之间的随机十进制数。



## Windows的环境变量设置

- %SESSIONNAME%：列出连接到终端服务会话时的连接和会话名。
- %SYSTEMDRIVE%：列出了Windows启动目录所在驱动器。
- %SYSTEMROOT%：列出了Windows启动目录的位置。
- %TEMP% and %TMP%：列出了当前登录的用户可用应用程序的默认临时目录。
- %TIME%：列出当前时间。



## Windows的环境变量设置

---

- %USERDOMAIN%：列出了包含用户帐号的域的名字。
- %USERNAME%：列出当前登录的用户的名字。
- %USERPROFILE%：列出当前用户Profile文件位置。
- %WINDIR%：列出操作系统目录的位置。



# 课后实验

---

- 实验一 WMI管理工具的配置和使用
  - WMI Tools工具的安裝和使用
  - 使用wbemtest工具查看WMI类的MOF定义
  - 查看WMI的安全属性



# 课后实验

- 实验二 windows环境变量查看和设置
  - 在用户配置界面查看环境变量和设置环境变量
  - 在命令行界面查看环境变量和设置环境变量