Мониторинг системных событий и производительности

- Существенный недостаток средств контроля современного ПО, в т.ч. и системного, состоит в узкой специализации и т.о. затруднениях в сравнительном анализе значений нескольких параметров.
- А также, в невозможности двухстороннего взаимодействия с API управления, например, для установки автоизвещений.

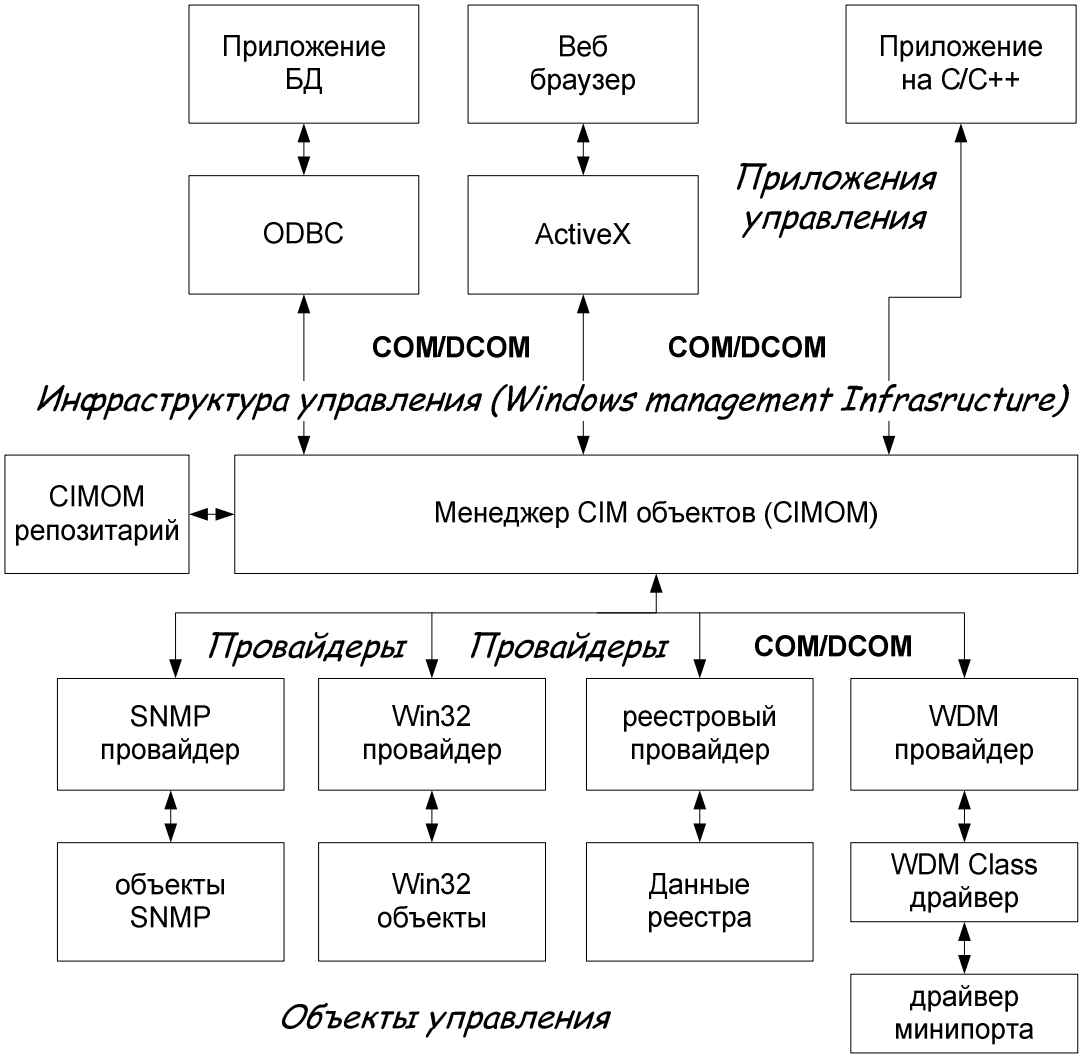
Windows Management Instrumentation (WMI)

- Windows Management Instrumentation (WMI) - разработан на базе т.н. «технологии управления предприятием через Web» - Web-Based Enterprise Management (WBEM)
- WBEM - стандарт, определенный консорциумом Distributed Management Task Force (DMTF): MS, CISCO, HP, Novell, Sun,Intel,Compaq, IBM
- WMI реализован MS в Windows 98 и в Win95 OSR2, в NT 4.0, начиная с Service Pack 4 (SP4) и интегрирован в Windows 2000, 2003/XP

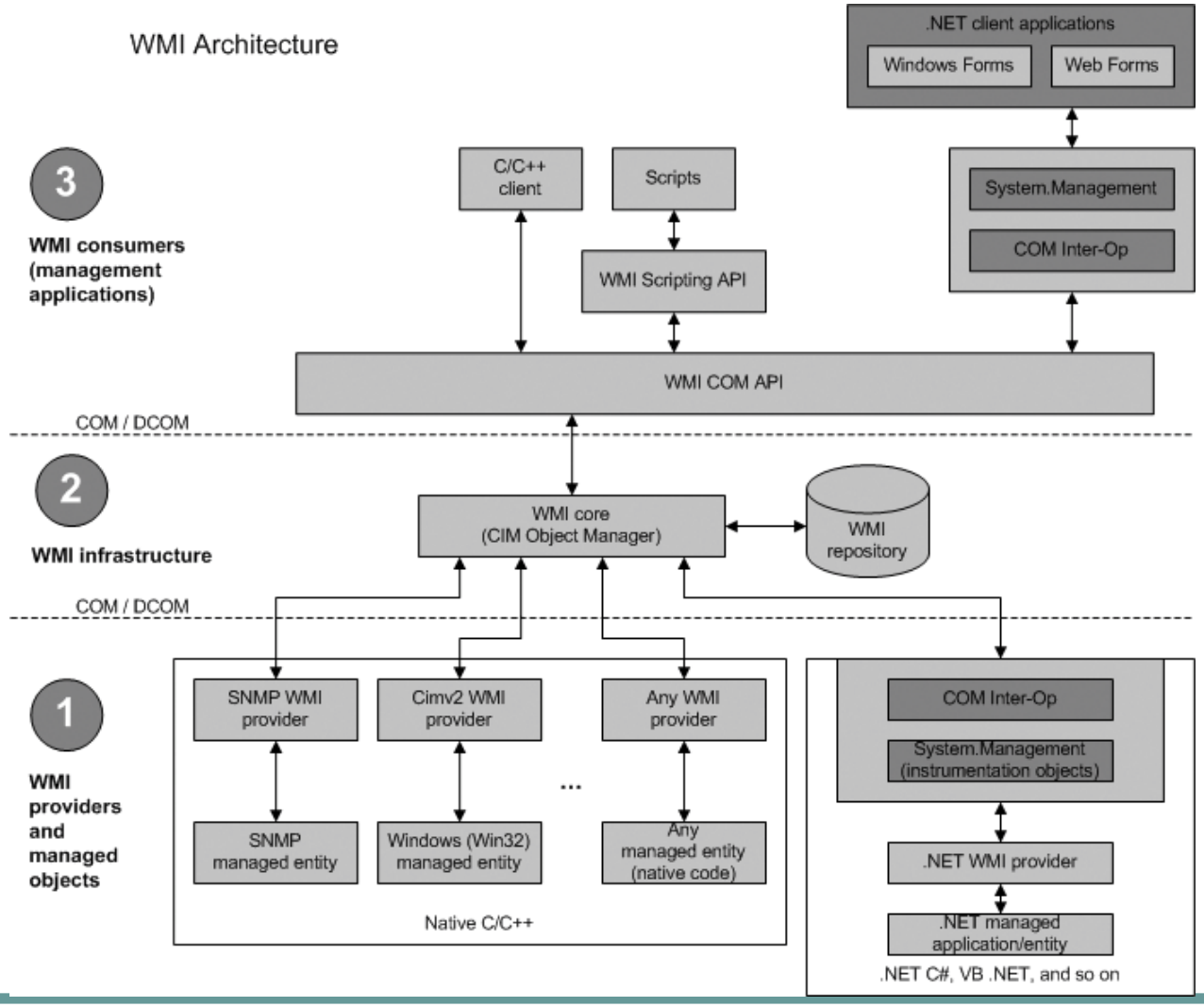
Состав WMI

- управляющие программы (management applications, например, Windows Script Host, MMC)
- ядро WMI (WMI infrastructure)
- провайдеры или поставщики(providers)
- управляемые объекты (managed objects)

Архитектура WMI



Архитектура WMI

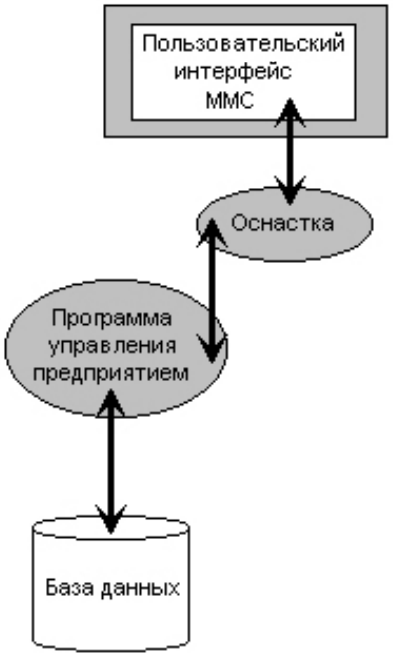


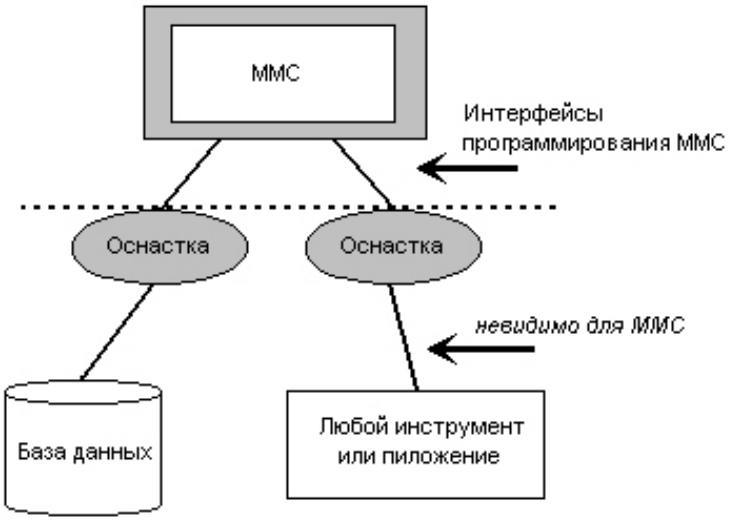
MMC, как интерфейс для инструментов управления. Интеграция оснасток с консолью

Консоль управления Microsoft - Microsoft Management Console, MMC.

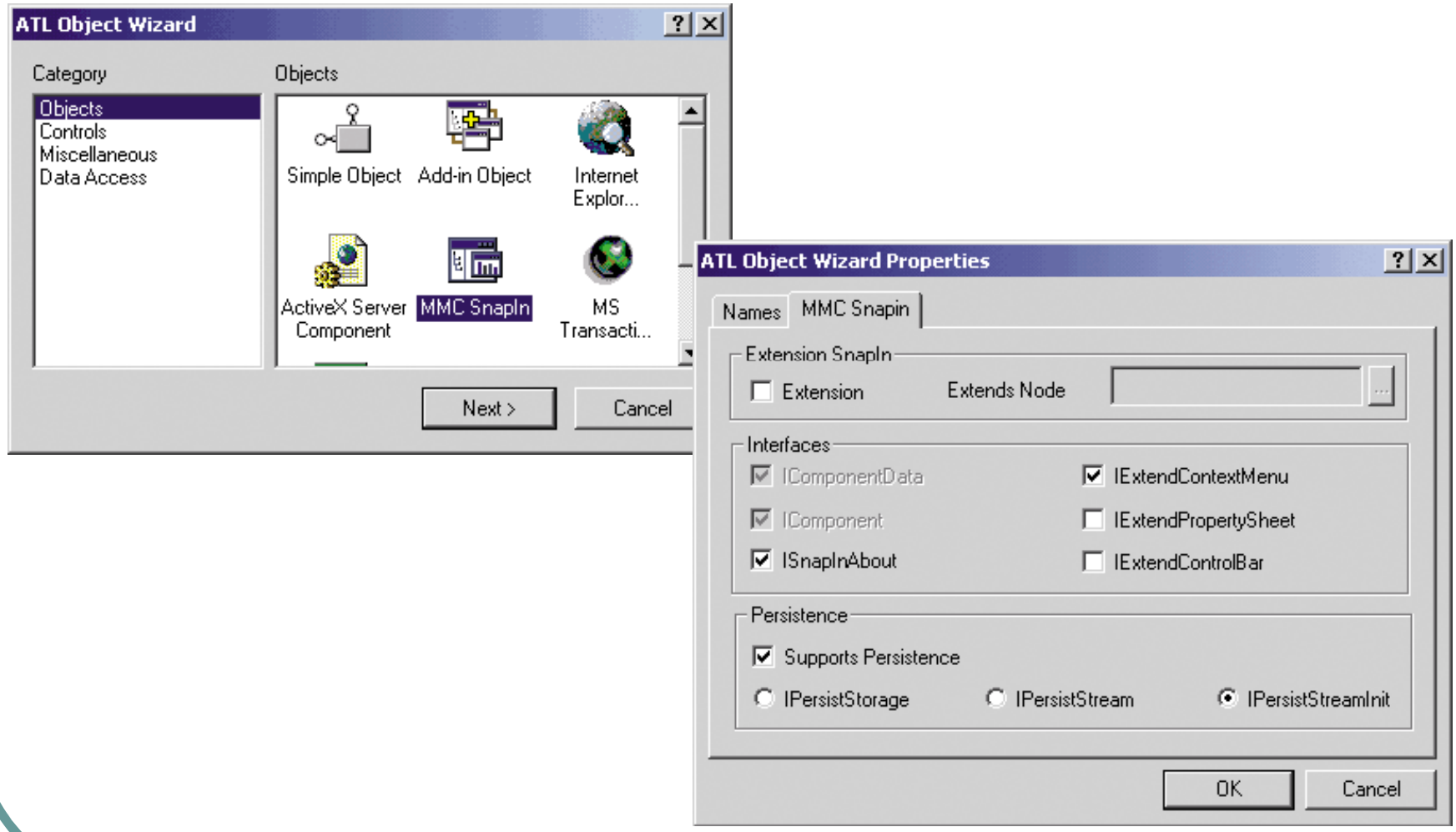
Оснастки - snap-ins – это специальные COM-объекты

Файл конфигурации консоли (*.msc) содержит информацию о модулях, входящих в консоль

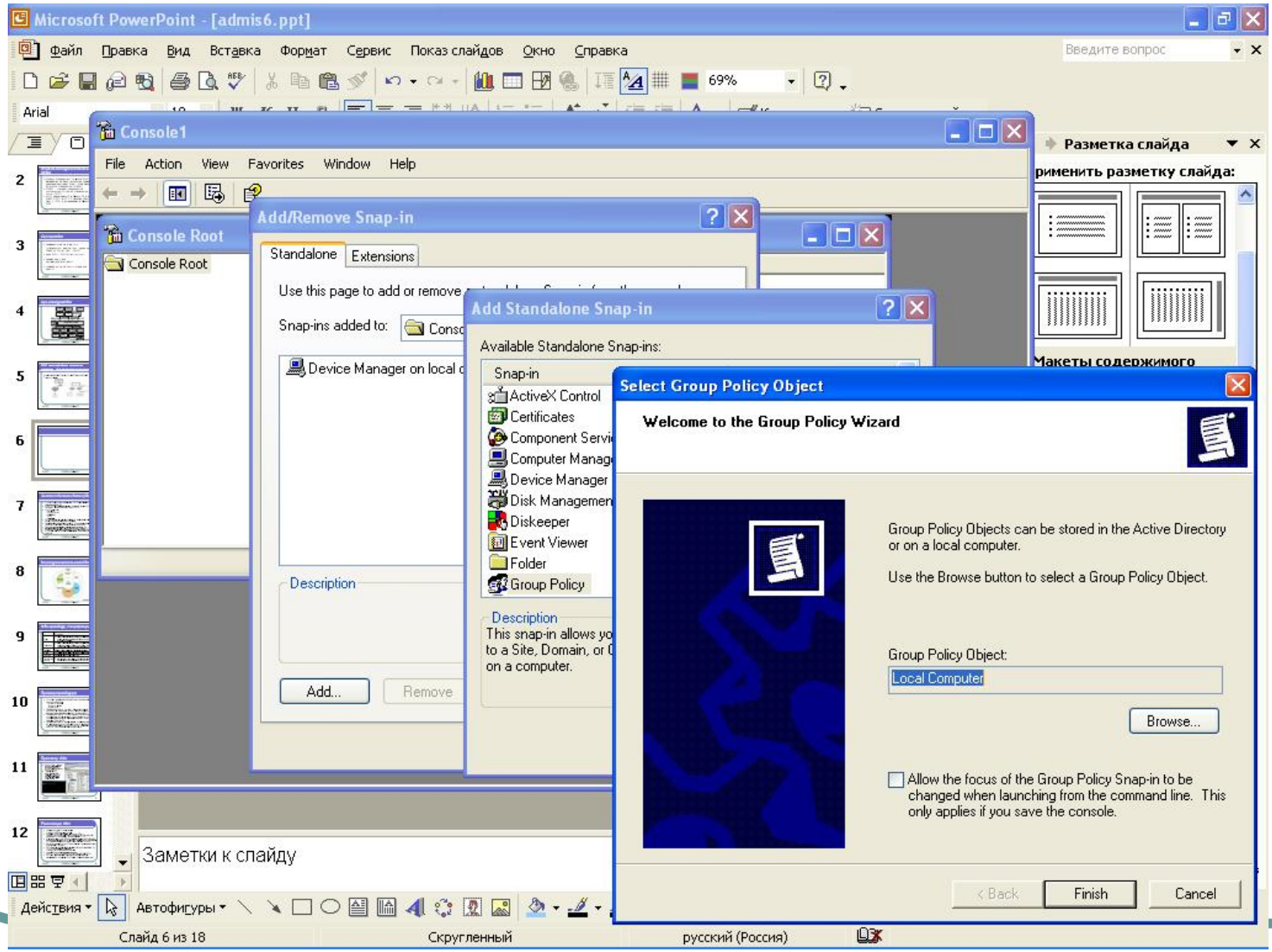




Создание оснастки в MS Visual с помощью мастера ATL COM AppWizard



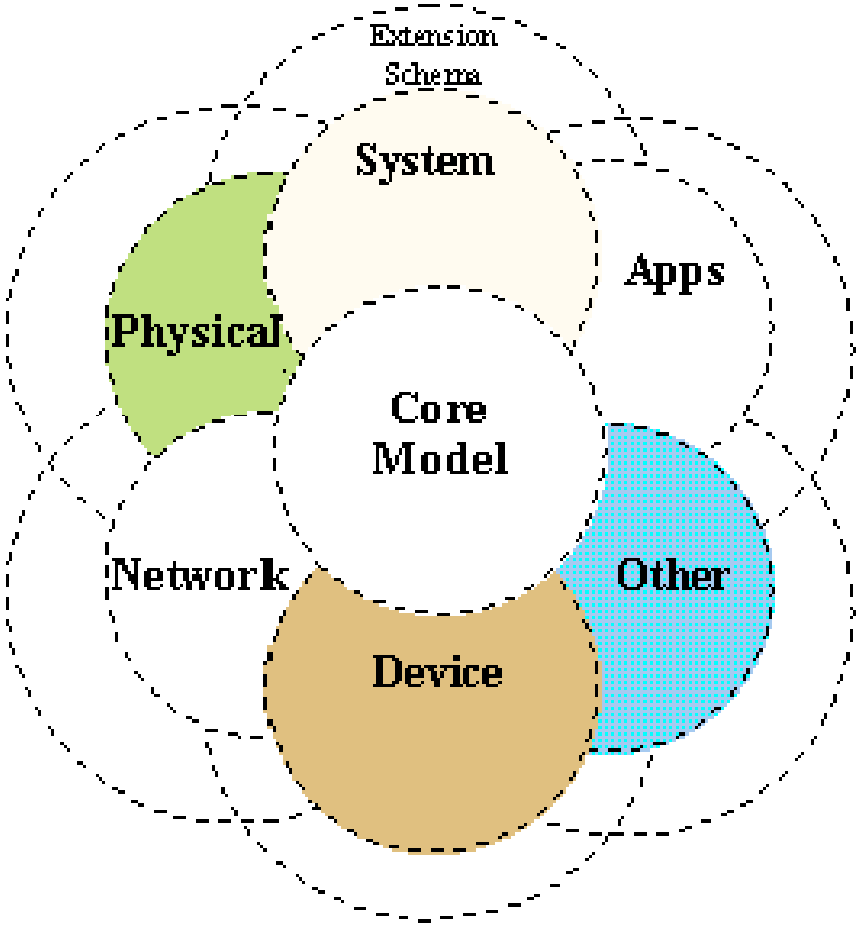
Создание консоли управления



Common Information Model (CIM)

- Основа WBEM - спроектированная в DMTF спецификация Common Information Model (CIM)
- 1996, DMTF сформировал комитет Common Information Model Technology Development Committee (CIM TDC)
- CIM TDC включает рабочие группы: Applications/Metrics, Architecture, Behavior and State, CIM Core Schema, Database, Desktop & Mobile, Networks, Policy, Pre-OS, Security Protection and Management, User and Security, Server Management, Support, System Virtualization, Partitioning, and Clustering, Telecom, Utility, WBEM Infrastructure & Protocols (WS-CIM, WIP-Management, WIP-Messages)
-
- CIM определяет, как системы управления представляют структуру компьютера, приложения или устройства
- Разработчики провайдера используют CIM для представления управляемых компонентов, составляющих приложение.
- Для удобства реализации компонентов в стандарте CIM разработчики применяют язык Managed Object Format (MOF) - основное средство для описания новых элементов модели CIM
- CIM подобен объектно-ориентированным языкам программирования C++ и Java, в которых проектировщик создает представления в виде классов.

Многоуровневая схема CIM



CIM Schema =

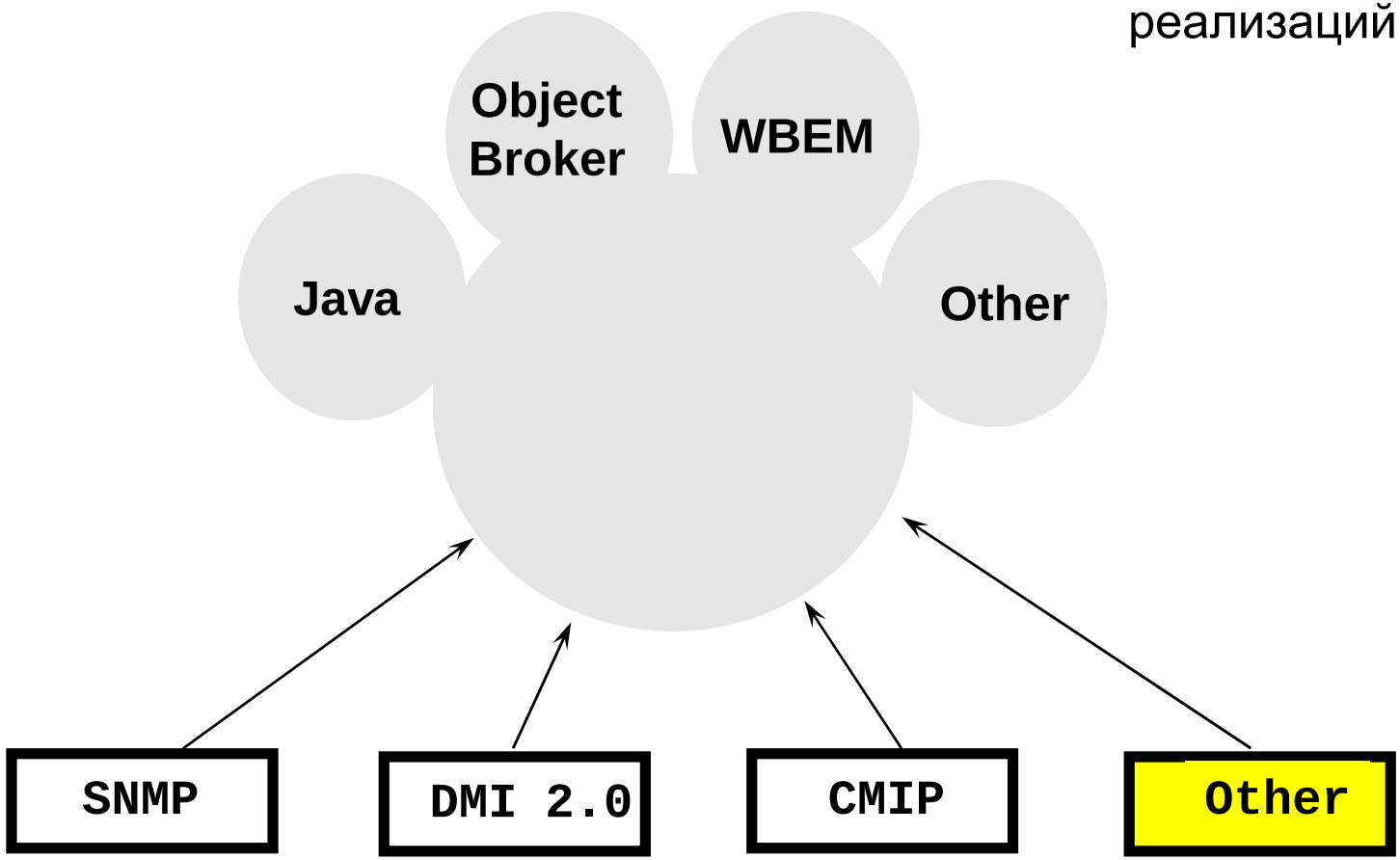
CORE Model + Common Model

Common Model =

Systems + Applications + Networks + Devices + etc

CIM – нейтральная схема для описания управления (как самих данных, так и методов)

WBEM – одна из реализаций



WMI-провайдер, спецификации

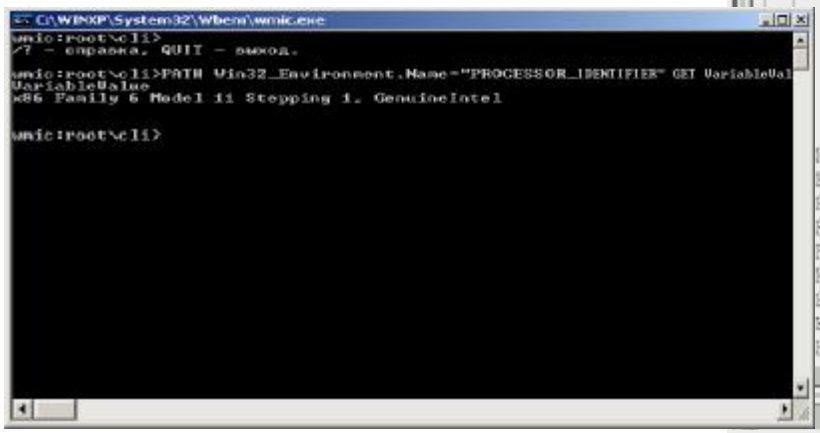
	Описание
Класс	Может вызывать, изменять, удалять, просматривать класс, специфичный для провайдера. Также поддерживает выполнение запросов.
Экземпляр	Может вызывать, изменять, удалять, просматривать экземпляры системы и классы, специфичные для провайдера. Также поддерживает выполнение запросов.
Свойство	Может вызывать и изменять значения индивидуальных свойств.
Метод	Вызывает методы, специфичные для класса провайдера.
Событие	Формирует уведомления о событии.
Потребитель события	Ставит в соответствие физического потребителя событий логическому для передачи уведомлений о событиях.

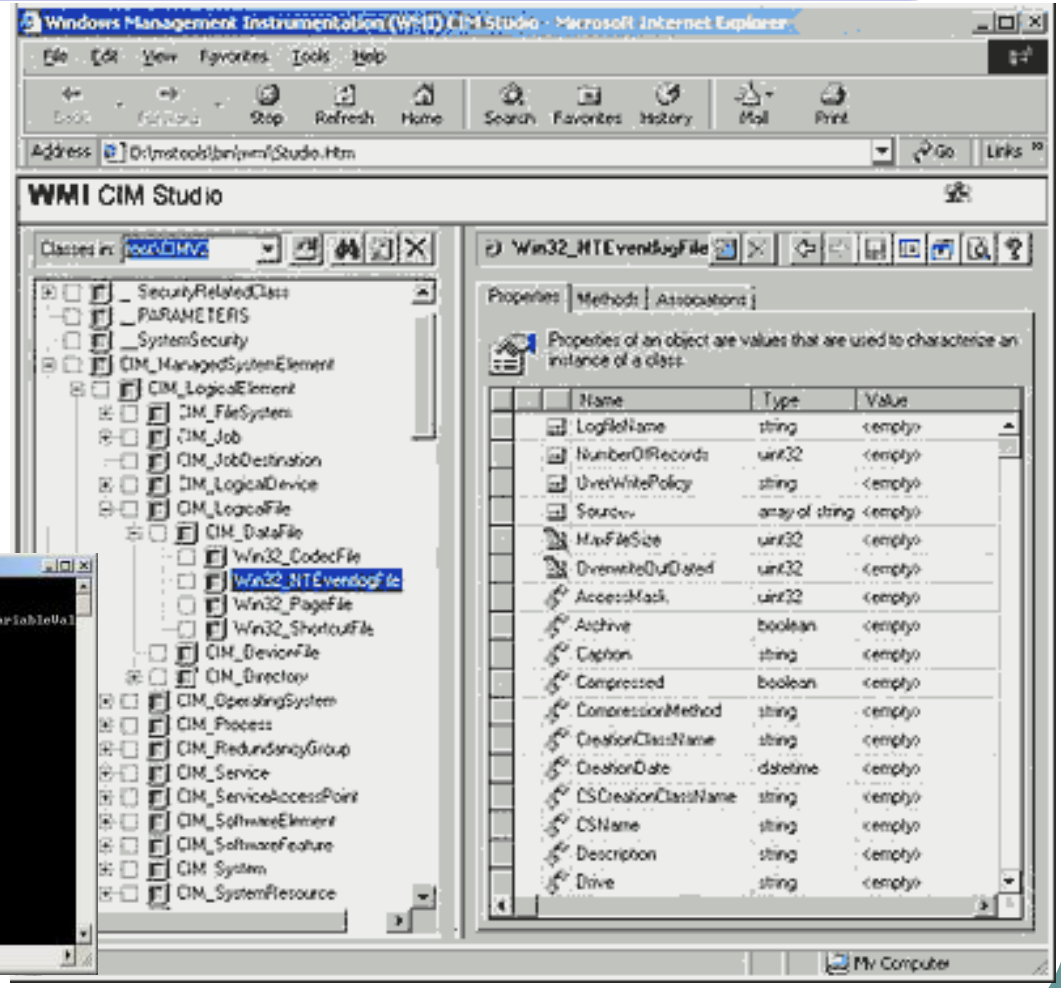
Пример провайдера

- Источник (провайдер) событий EventLog определяет несколько объектов:
  - EventLog Computer
  - EventLog Record
  - EventLog File
- Провайдер EventLog Computer - поставщик классов, поскольку он определяет объекты, используя классы, и должен предоставлять описания этих классов WMI.
- Провайдер EventLog Computer является также поставщиком экземпляров, так как он может предоставить несколько экземпляров для каждого из своих классов. Один из таких классов - EventLog File.
- Провайдер EventLog предоставляет экземпляры для каждого из журналов системных событий (system's event logs) (например, журналы системных событий, прикладных событий, событий в системе безопасности).

Просмотр CIM

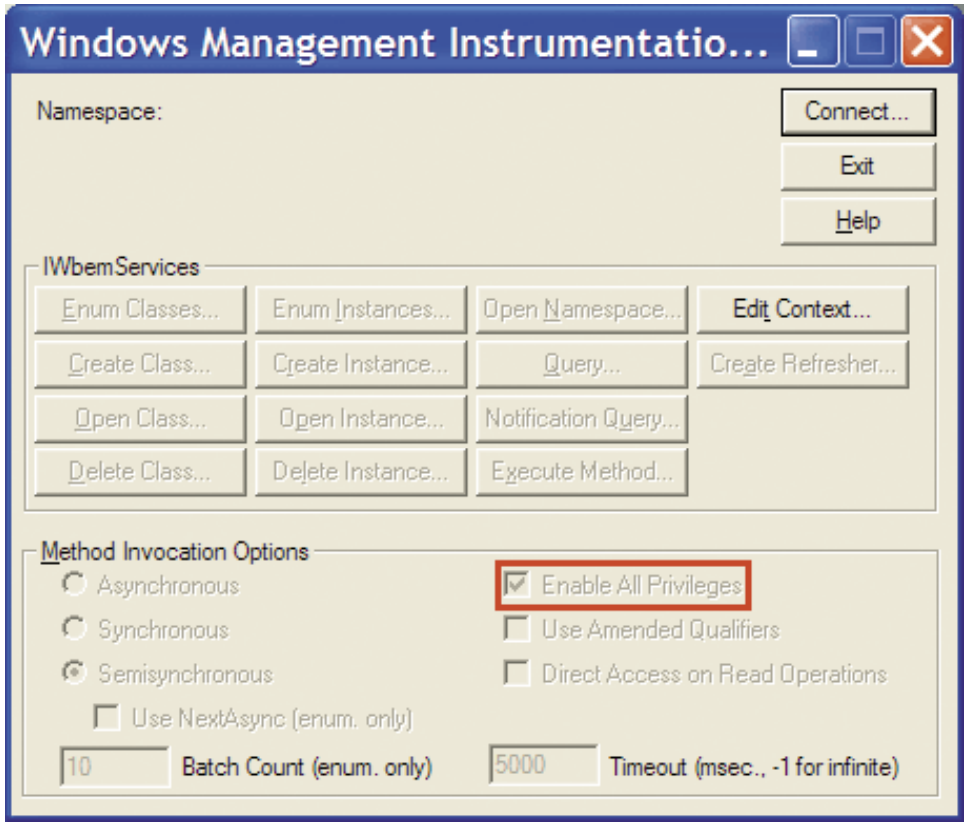
- WMI CIM Studio - браузер для просмотра классов, поставляемого с WMI SDK (Microsoft поставляет WMI SDK с MSDN).
- Программа WMIC представляет собой командную строку WMI, предназначена для просмотра классов, экземпляров CIM.



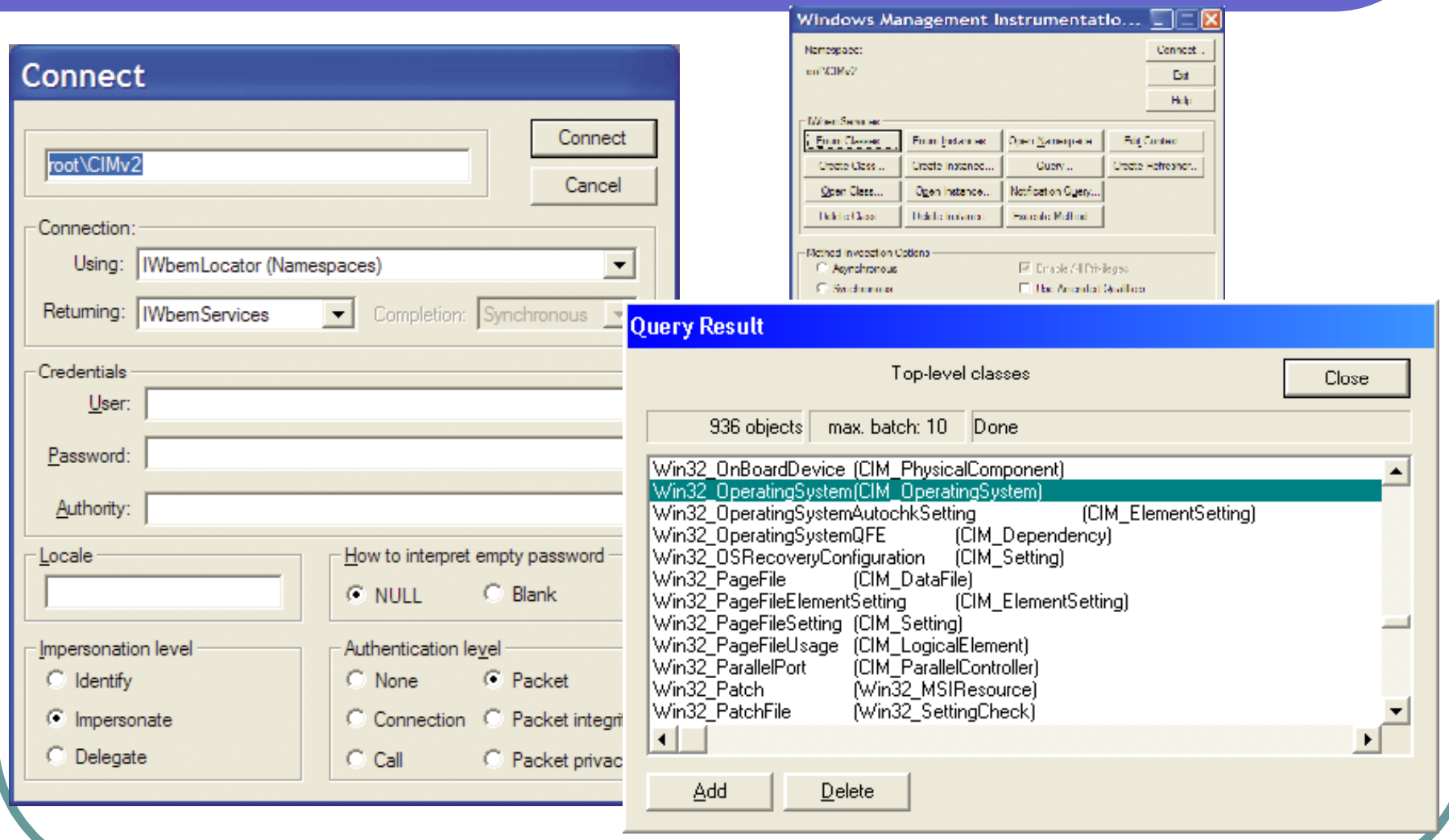


wmic bios, baseboard, cpu, temperature, share, process list brief

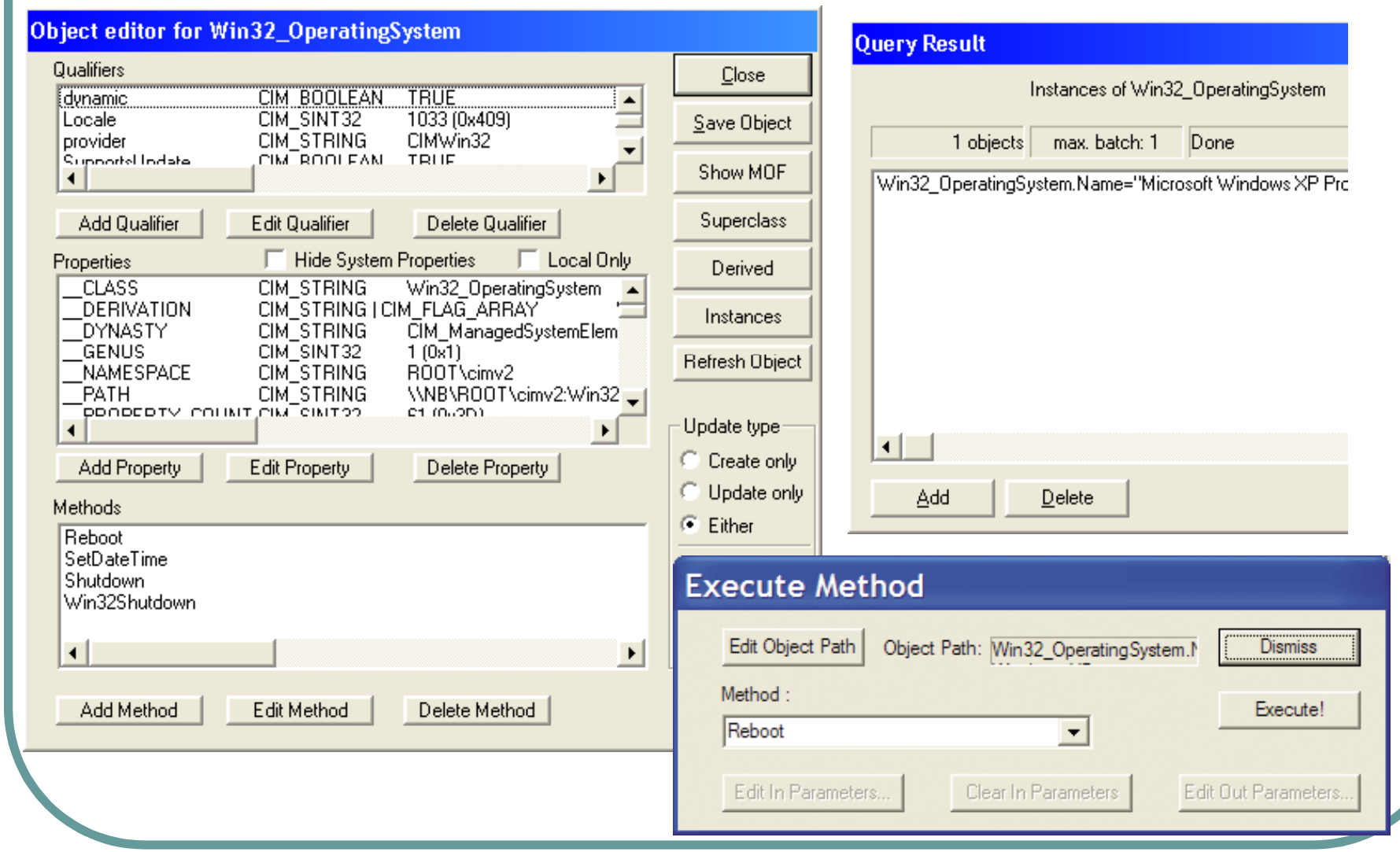
утилита **Wbemtest.exe** для тестирования классов и методов



подключение к репозиторию WMI утилиты WBEMTEST



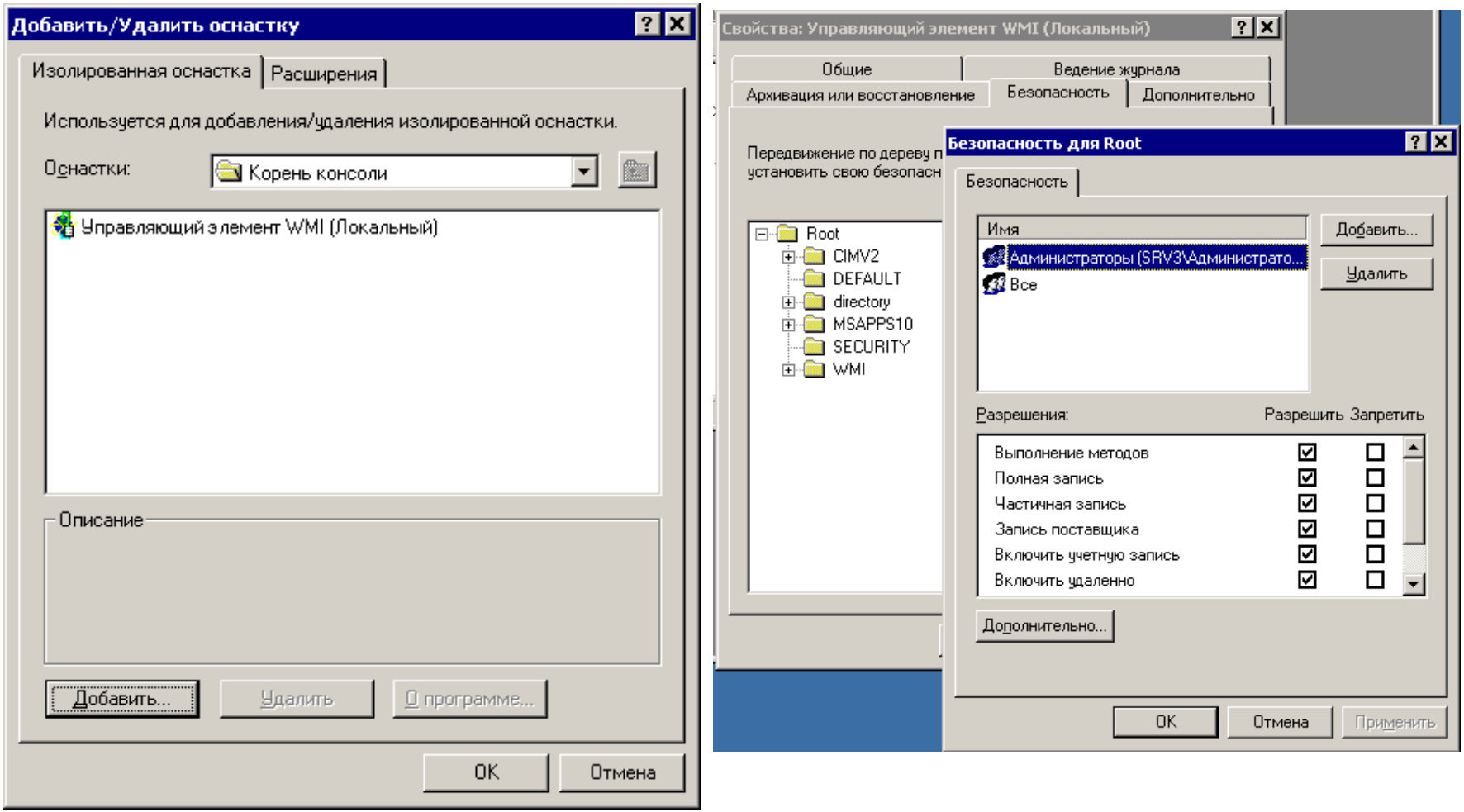
класс Win32_OperatingSystem



Реализация WMI

- Инфраструктура WMI представлена \winnt\system32\wbem\winmgmt.exe
- Компоненты WMI находятся в \winnt\system32 и \winnt\system32\wbem, включая MOF-файлы Win32, встроенный провайдер DLL и управляющее приложение WMI DLL.
- В каталоге \winnt\system32\wbem находится ntevt.mof - MOF-файл провайдера журнала событий EventLog, а также ntevt.dll, библиотека DLL провайдера EventLog, которую загружает winmgmt.exe.
- Каталоги ниже \winnt\system32 \wbem вмещают репозитарий, файлы журналов и MOF-файлы.
- WMI реализует репозитарий, называемый Object Management CIM (CIMOM) репозитарием, как файл \winnt\system32\wbem\repository\cim.rep
- Служба WMI использует раздел реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM
- WMI осуществляет защиту на уровне пространства имен, настраиваемую с помощью WMI Control (Computer Management)

Настройка безопасности WMI в консоли MMC (оснастка wmimgmt)

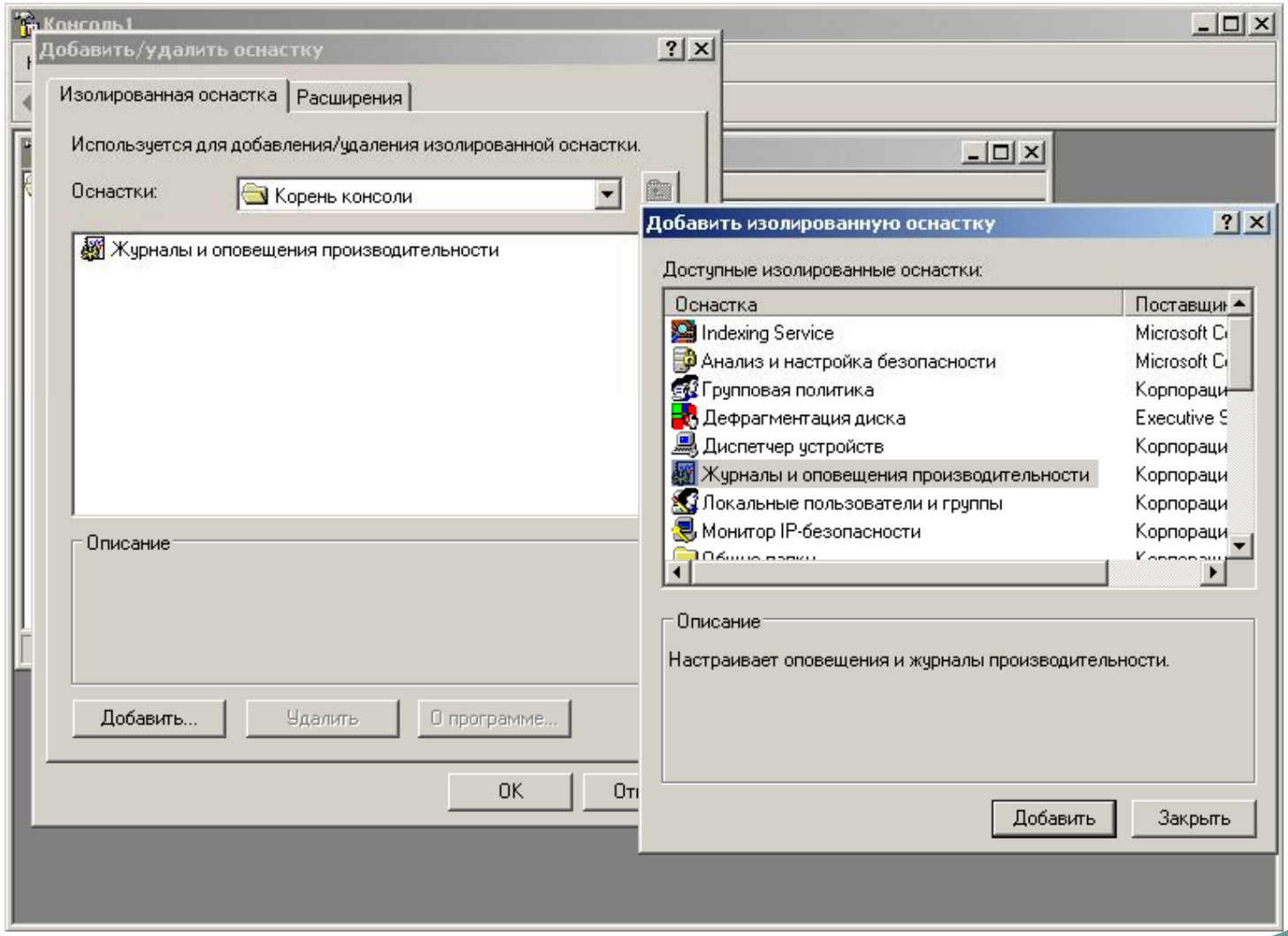


Уровни безопасности WMI

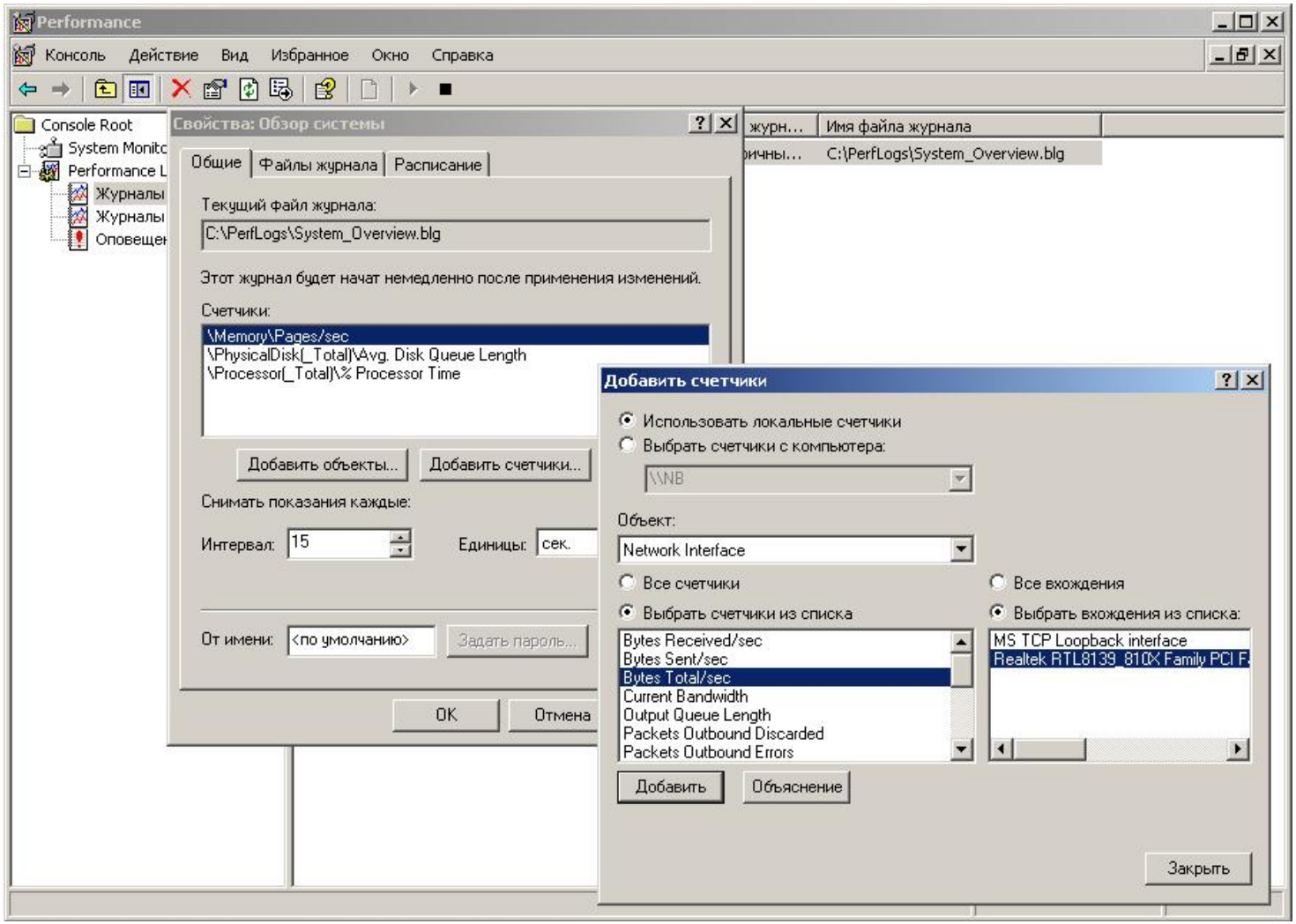
Уровень	Описание
Выполнение методов	Разрешает выполнение методов, экспортированных из классов и экземпляров WMI.
Полная запись	Разрешает полный доступ на чтение, запись и удаление ко всем объектам, классам и экземплярам WMI.
Частичная запись	Разрешает доступ на запись к статическим объектам WMI.
Запись поставщика	Разрешает доступ на запись к объектам, предоставляемым поставщиком.
Включить учетную запись	Разрешает доступ на чтение к объектам WMI.
Включить удаленно	Разрешает удаленный доступ к пространству имен.
Прочесть безопасность	Разрешает доступ на чтение к данным безопасности WMI.
Изменение правил безопасности	Разрешает доступ на чтение и запись к данным безопасности WMI.

Журналы и оповещения производительности

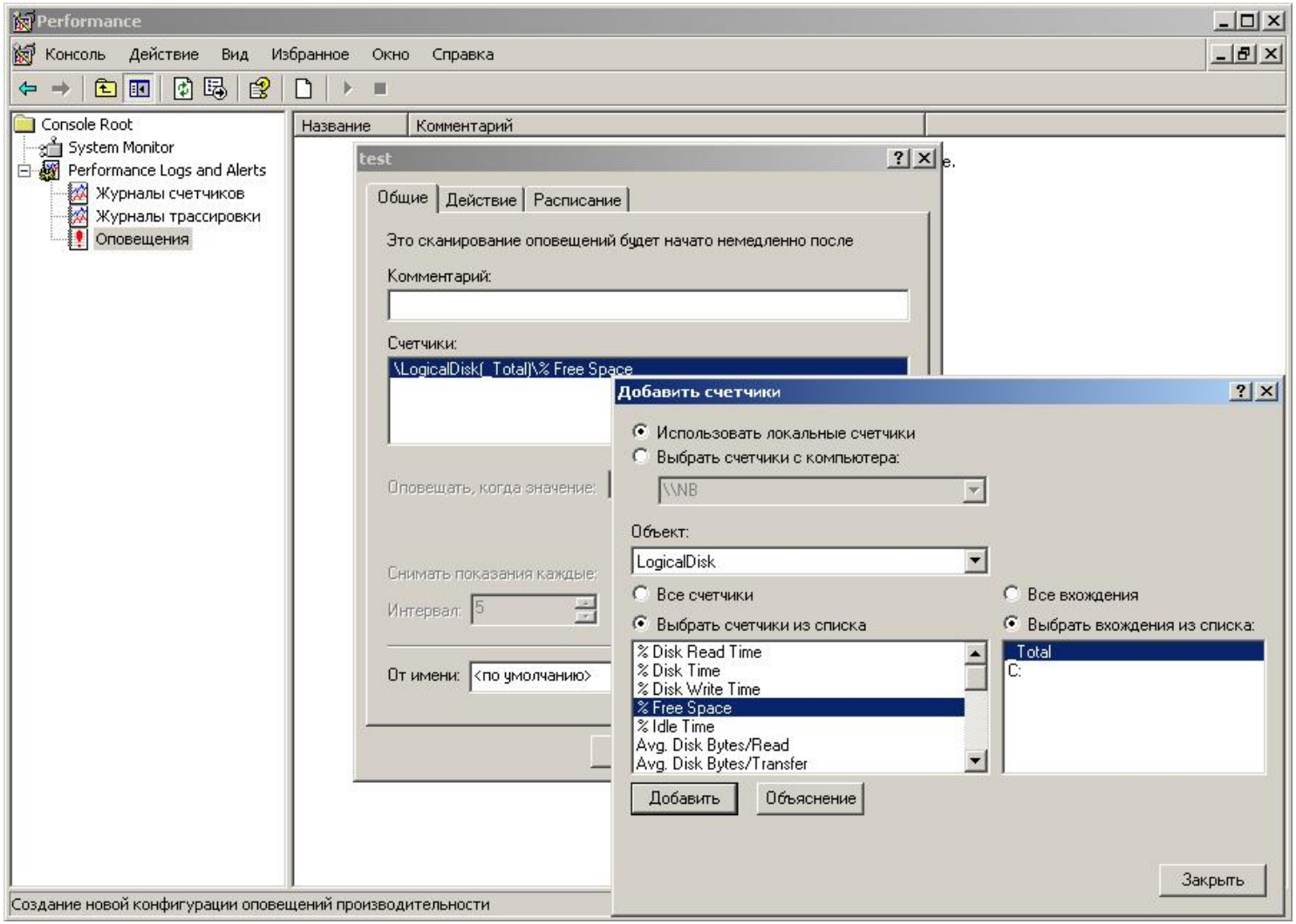
Добавление оснастки журналов WMI в консоль управления MMC

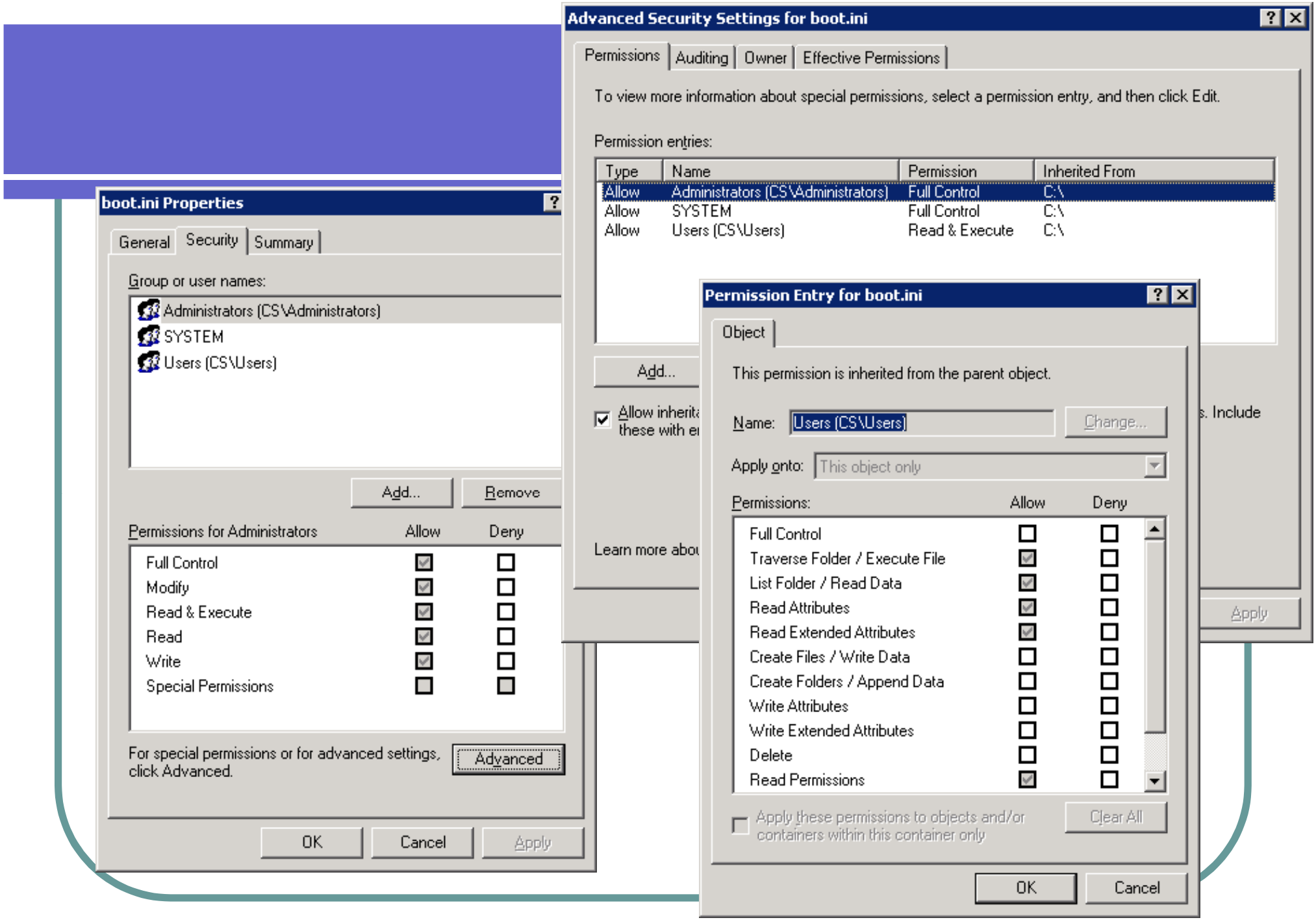


Журналы производительности

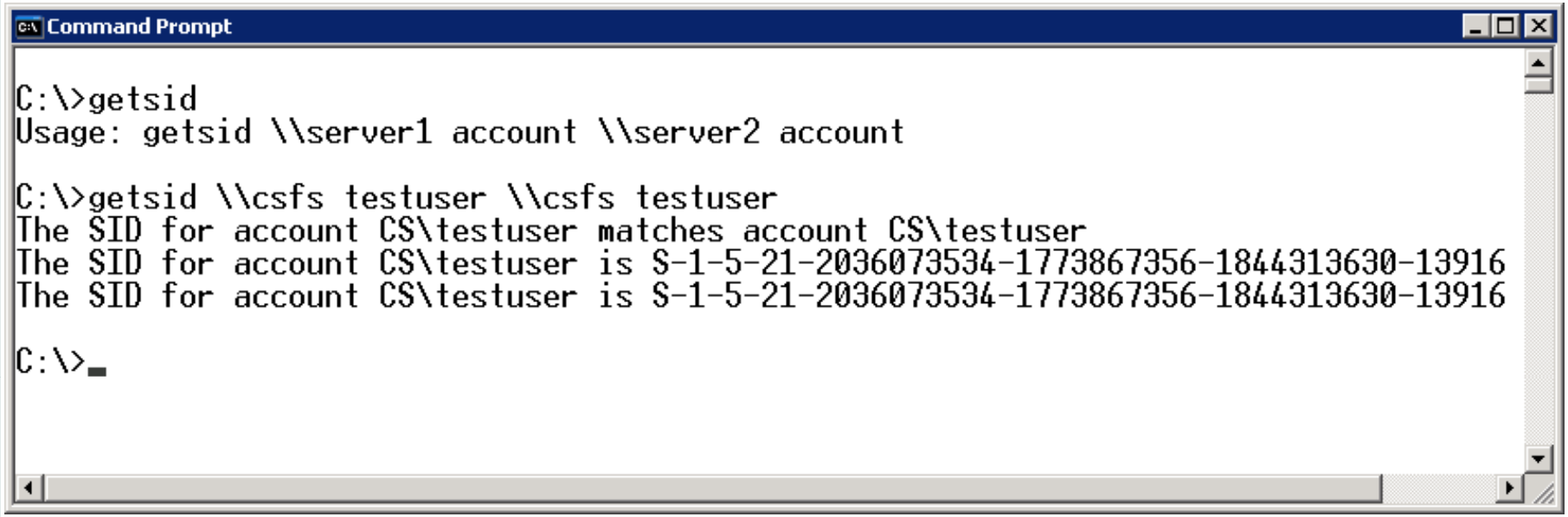


Оповещения WMI




Advanced Security Settings for boot.ini
Permissions
Auditing
Owner
Effective Permissions
To view more information about special permissions, select a permission entry, and then click Edit.
Permission entries:
Type
Name
Permission
Inherited From
Allow
Administrators (CS\Administrators)
Full Control
C:\
Allow
SYSTEM
Full Control
C:\
Allow
Users (CS\Users)
Read & Execute
C:\
Add...
Apply
boot.ini Properties
General
Security
Summary
Group or user names:
Administrators (CS\Administrators)
SYSTEM
Users (CS\Users)
Add...
Remove
Permissions for Administrators
Allow
Deny
Full Control
Modify
Read & Execute
Read
Write
Special Permissions
For special permissions or for advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Permission Entry for boot.ini
Object
This permission is inherited from the parent object.
Name:
Users (CS\Users)
Change...
Apply onto:
This object only
Permissions:
Allow
Deny
Full Control
Traverse Folder / Execute File
List Folder / Read Data
Read Attributes
Read Extended Attributes
Create Files / Write Data
Create Folders / Append Data
Write Attributes
Write Extended Attributes
Delete
Read Permissions
Apply these permissions to objects and/or containers within this container only
Clear All
OK
Cancel

идентификаторы безопасности (Security Identifier – SID)



версия SID – 1, код агента идентификатора – 5 (NT-системы), коды 4-х субагентов, а в конце – RID

Универсальный SID	**Описание**
Null SID (S-1-0-0)	Пустая группа. Часто используется, если **SID** не известен.
World (S-1-1-0)	Все пользователи.
Local (S-1-2-0)	Пользователи, прошедшие локальную аутентификацию.
Creator Owner ID (S-1-3-0)	**SID** создателя объекта.
Creator Group ID (S-1-3-1)	**SID** группы создателя объекта.

ACL – Access Control List.
ACE – Access Control Entry

Тип ACE	**Описание**
Запрещающий **ACE**	Используется в **DACL** для запрета доступа к ресурсу.
Разрешающий **ACE**	Используется в **DACL** для разрешения доступа к ресурсу.
Системный **ACE** аудита	Используется в **SACL** для создания записей аудита.

ACL бывают: DACL – Discretionary Access Control List - определяют права доступа и системные SACL – System Access Control List - определяют аудит событий.