МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г.Шухова)

Лабораторная работа №3
дисциплина «Администрирование распределенных вычислительных сетей»
по теме «Использование средств инструментария для управления Windows (WMI) в администрировании»

Выполнил: студент группы ВТ-41 Макаров Д.С.
Проверил: Федотов Е.А.

Белгород 2020

Лабораторная работа №3

«Использование средств инструментария для управления Windows (WMI) в администрировании»

Цель работы:познакомиться со структурой объектов WMI, способами доступа к ним, а также научиться работать с WMI через сценарии и утилиты WBEMTEST и WMIC..

Ход работы

1. Просмотр набора классов в репозитории WMI.

Через меню “Выполнить” была вызвана команда wbemtest

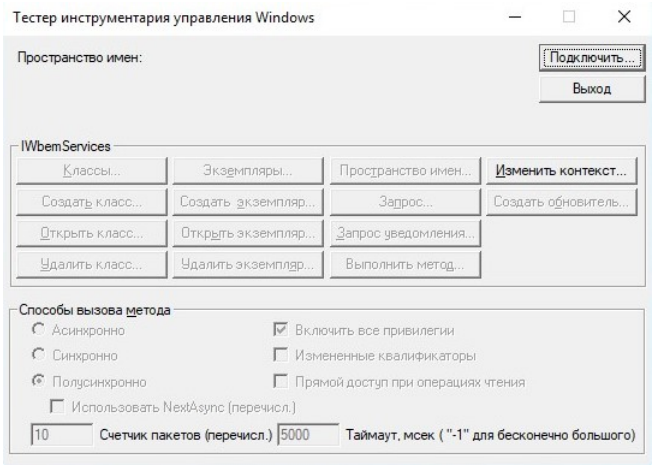

Рис. 1: Окно wbemtest

В списке всех классов WMI был найден класс Win32_NTDomain и получен список всех его экземпляров.

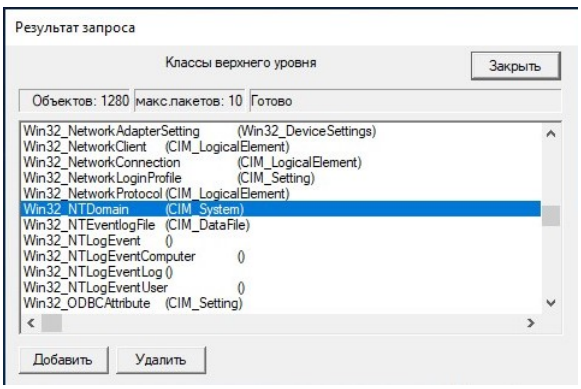

Рис. 2: Список классов

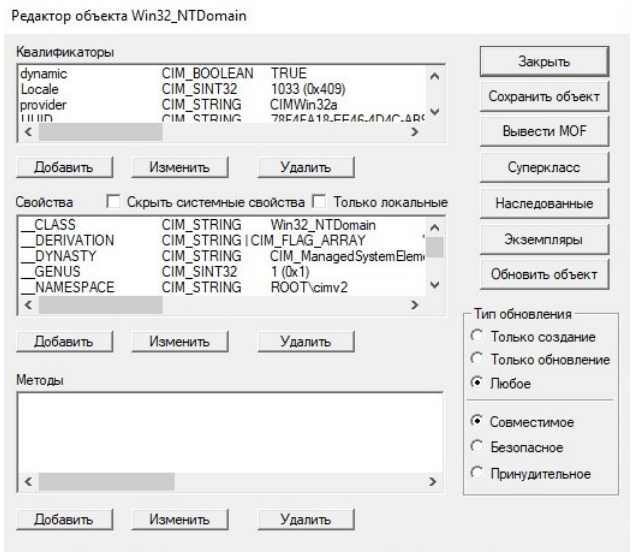

Рис. 3: Редактор объекта Win32_NTDomain

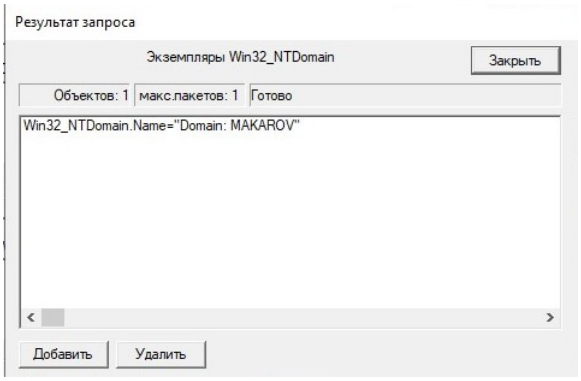

Рис. 4: Экземпляры класса Win32_NTDomain

В окне списка соединителей был получен список групп домена и найдена группа “Sales Representative”.

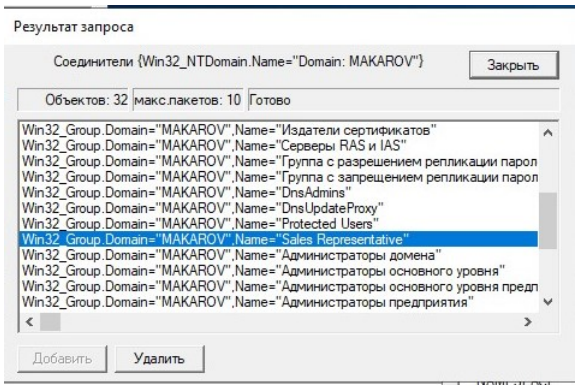

Рис. 5: Список групп

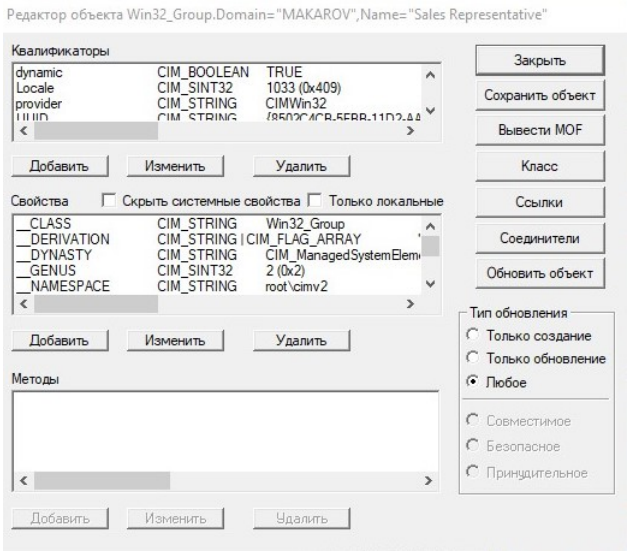

Рис. 6: Окно группы “Sales Representative”

В экземплярах класса учетных записей были найдены указанные пользователи, в атрибут *Disabled* установлены требуемые значения.

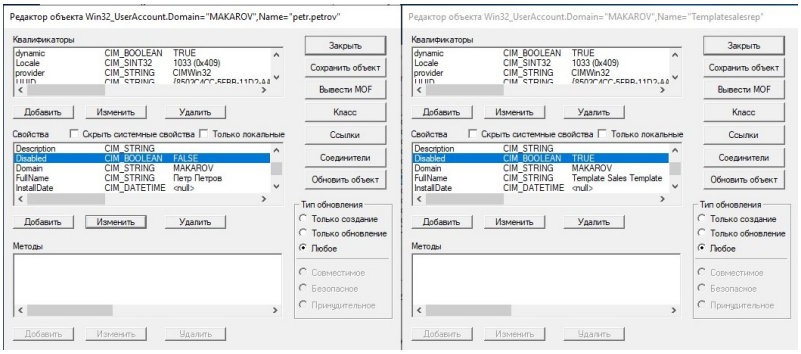

Рис. 7: Окна объектов пользователей

2. Был найден класс Win32_UserAccount.

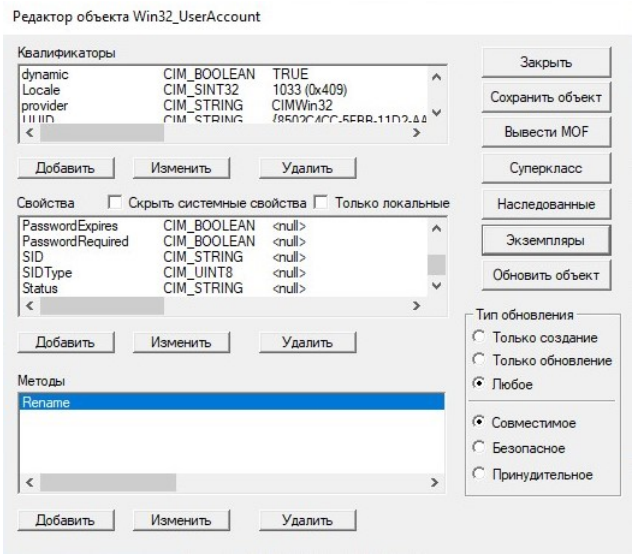

Рис. 8: Объект Win3_UserAccount

В списке экземпляров класса был найден объект “petr.petrov”

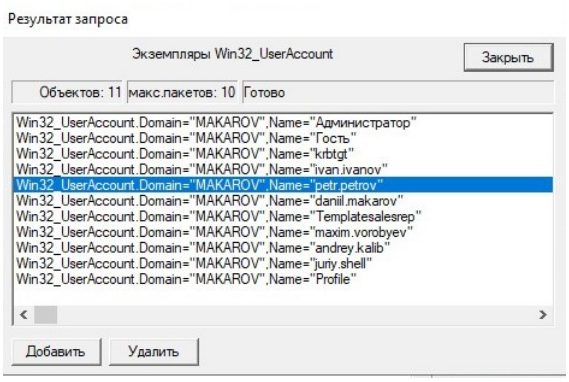

Рис. 9: Список экземпляров класса

В окне вызова метода был выбран метод Rename объекта “petr.petrov”, и установлены требуемые параметры.

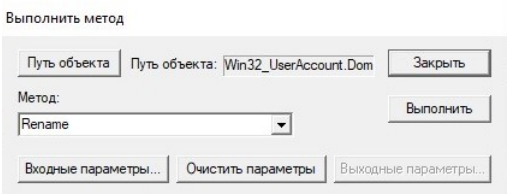

Рис. 10: Окно вызова метода

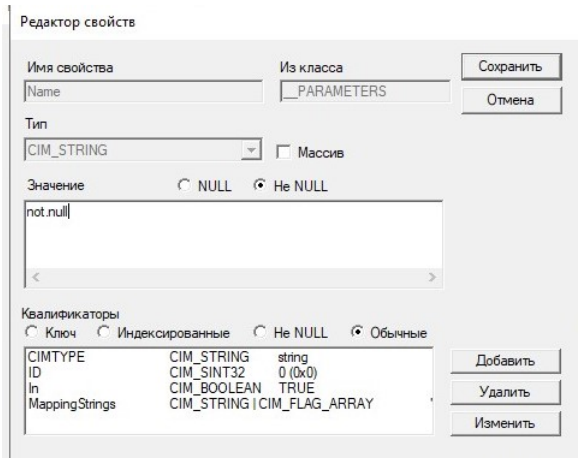

Рис. 11: Окно изменения аргументов метода

Метод был успешно выполнен но изменения не были внесены в поля объекта.

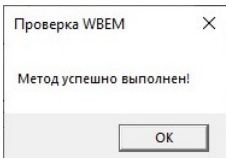

Рис. 12: Сообщение об успехе выполнения метода

3. Запросы WSL

В окне запросы, был выполнен WQL запрос

```
select * from Win32_UserInDomain
```

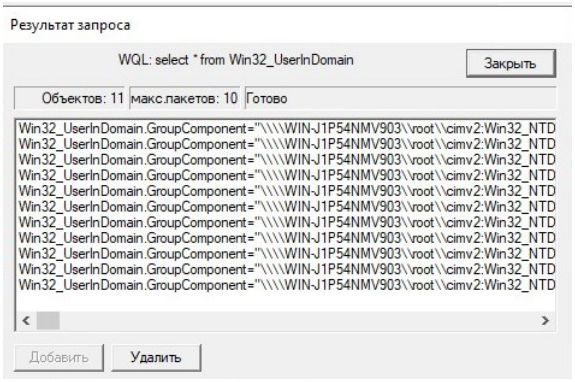

Рис. 13: Результат выполнения запроса

Запрос выводящий пользователей группы “Sales Representative”.

```
   select * from Win32_GroupUser where
      GroupComponent =  '
                           Win32_Group.Domain    =  "makarov",
                           Name                  =  "Sales Representative"
                        '
```

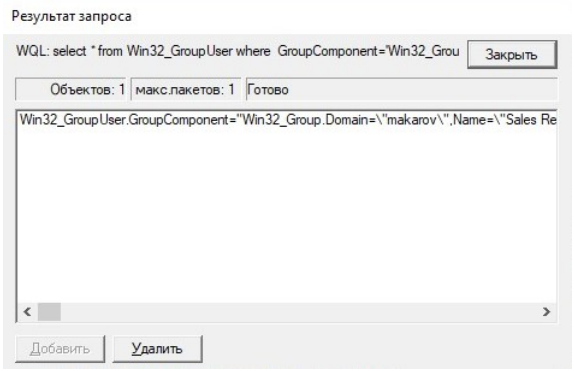

Рис. 14: Результат выполнения запроса

Запрос перечисляющие логические диски:.

```
select * from Win32_LogicalDisk
```

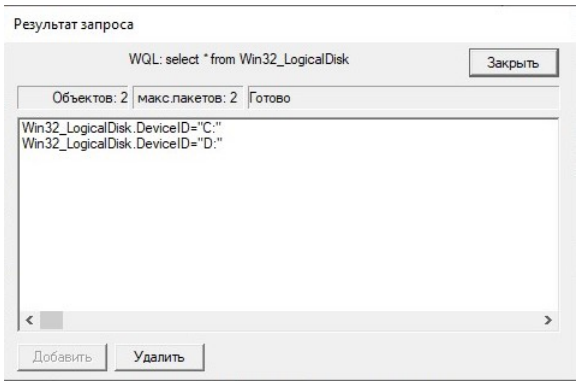

Рис. 15: Результат выполнения запроса

Запрос перечисляющие процессоры:.

```
select * from Win32_PerfRawData_PerfOS_Processor
```

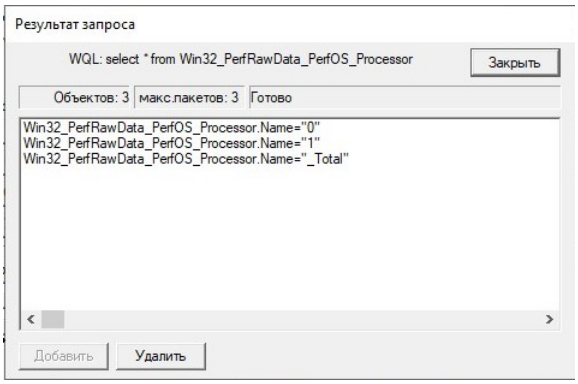

Рис. 16: Результат выполнения запроса

4. Утилита wmic

Был запущена консоль powershell и в ней запущена консоль wmi. При просмотре списка команд, было указано что инструмент WMI является устаревшим и больше не поддерживается.

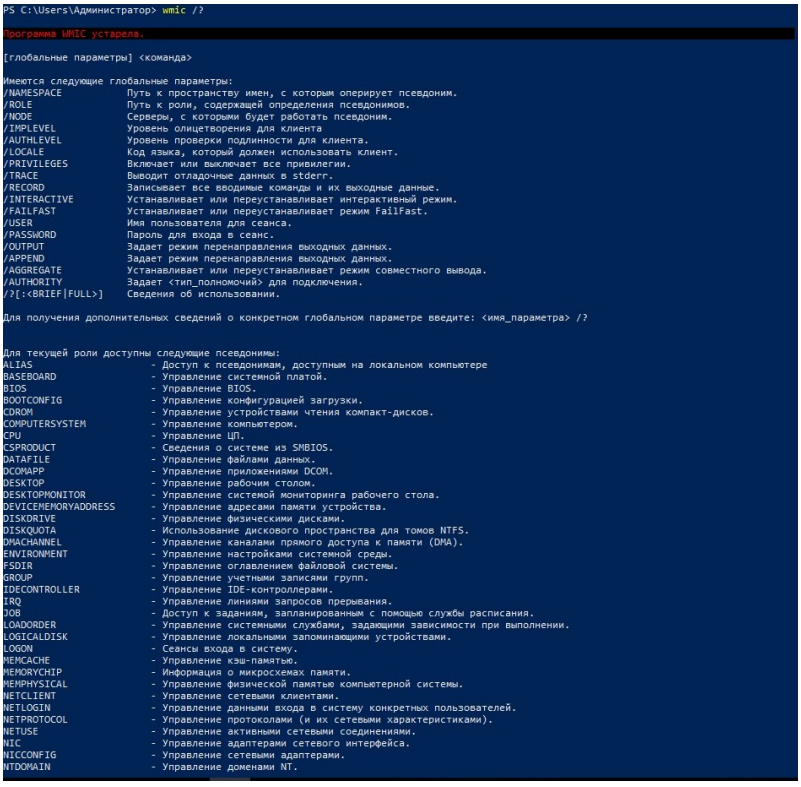

Рис. 17: Список команд WMI

Используя команду `wmic group where domain="makarov"` был выведен список всех групп домена.

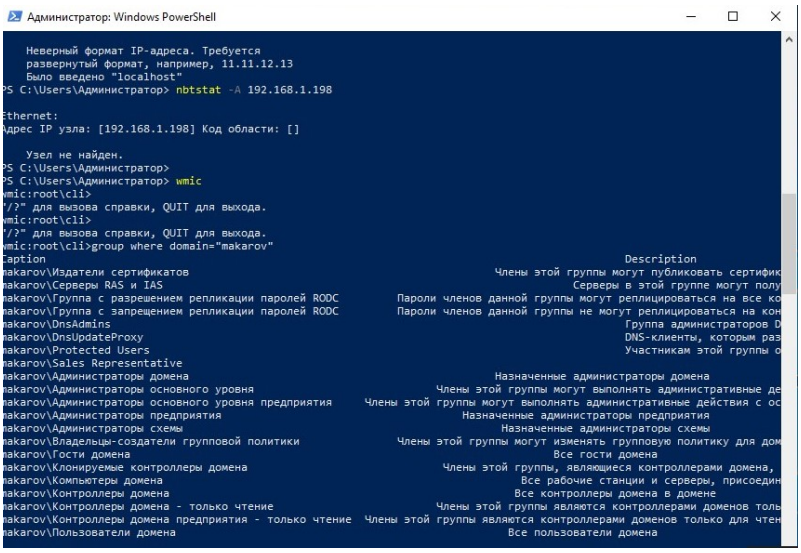

Рис. 18: Результат работы команды

Используя команду `wmic group where domain="makarov"` был выведен список всех пользователей домена.

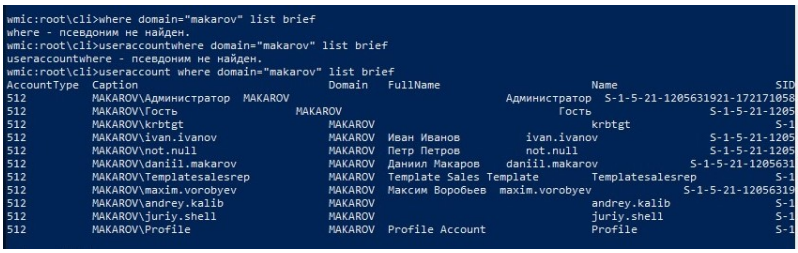

Рис. 19: Результат работы команды

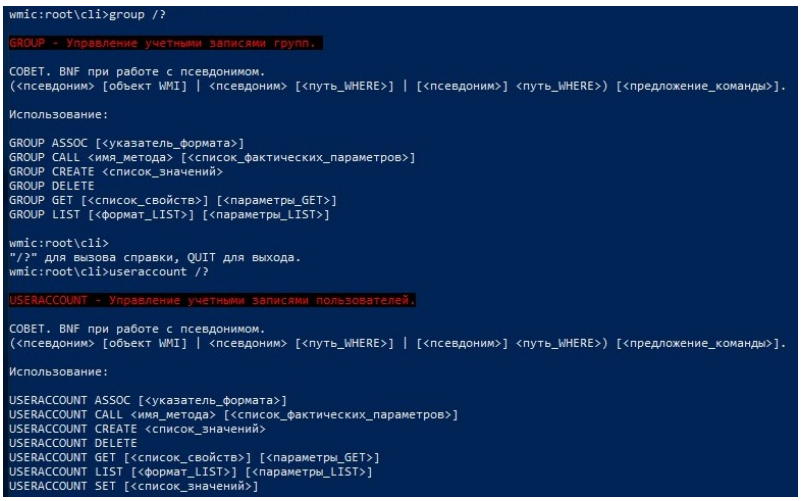

Рис. 20: Список команд для group и useraccount

5. Сценарии с использованием WMI

Был создан сценарий с указанным исходным кодом

```
On error Resume Next
strComputer="server01"
Set objWMIService = GetObject("winmgmts:\\" & strComputer &"\root\cimv2")
Set colItems=objWMIService.ExecQuery("Select * from Win32_UserAccount")
For each objItem in colItems
if ObjItem.domain="makarov" then
   Wscript.echo "Caption "&ObjItem.caption
   Wscript.echo "Name: "&ObjItem.name
   Wscript.echo "Full name: "&ObjItem.fullname
   Wscript.echo "Disabled: "&ObjItem.disabled
   Wscript.echo "---------------------------------"
   end if
Next
```

Сценарий был исполнен при помощи консольной утилиты **cscript**.

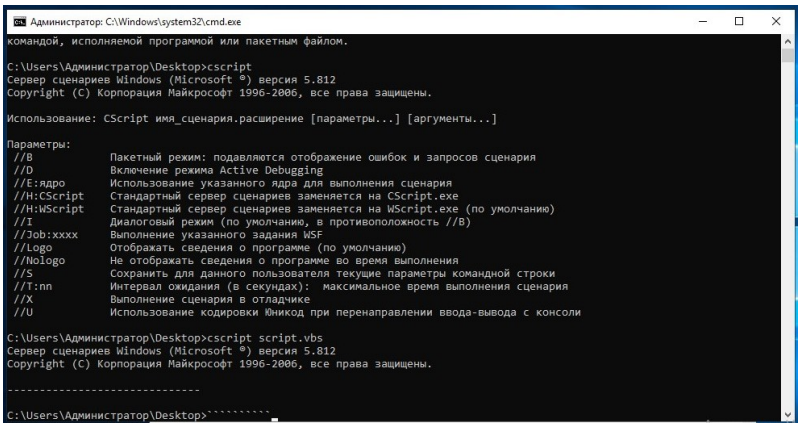

Рис. 21: Результат работы сценария

Вывод

В ходе выполнения данной лабораторной я ознакомился с утилитами использующими WMI, для взаимодействия с объектами домена. Так же я ознакомился с языком запросов WQL позволяющим, создавать SQL-подобные запросы, где вместо строк из таблиц с данными запрос возвращает объекты домена.

Контрольные вопросы

1. Что такое WMI? Для чего она используется?

WMI – Windows Management Instrumentation, он же инструментарий для управления Windows. Представляет из себя набор интерфейсов для управления операционной системой через специальные компоненты, причем как локально, так и по сети. Позволяет использовать различные скриптовые языки для упрощения управления объектами Active Directory.

2. Перечислите средства работы с WMI для администратора.

- mofcomp.exe
- winmgmt.exe
- wmimgmt.msc
- wbemtest.exe
- wmic.exe

3. Общая структура WMI.

Архитектура WMI состоит из 3 частей:

- ядро WMI (WMI infrastructure) - связующее звено архитектуры WMI, отвечающее за связность компонентов.
- управляющие программы (management applications)- потребителями сервисов WMI.
- управляемые объекты/ресурсы (managed resources) — любые логические или физические компоненты информационной системы, доступ к которым может быть получен с помощью WMI.

4. Опишите возможности программы WMIC.

Инструментарий WMI. Используется для получения сведений об оборудовании и системе, управления процессами и их компонентами, а также изменения настроек с использованием возможностей инструментария управления Windows.

5. Опишите возможности программы WBEMTEST.

Утилита предоставляющая графический интерфейс для доступа к ресурсам WMI, позволяющая получить списки классов, экземпляров классов, связи между ними, а так же выполнять методы классов и WQL запросы.

6. Использование WQL-запросов.

WQL запросы используют синтаксис SQL запросов, за исключением того что вместо связных таблиц с данными выборка производится по классам домена, и вместо строк таблиц возвращаются объекты домена.