ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»

(БГТУ им. В.Г.Шухова)

**Лабораторная работа №3**

**Использование средств инструментария для управления Windows (WMI) в администрировании**

Выполнил:

студент группы ВТ-41

Сидорова А.С.

Проверил:

Федотов Е.А.

Белгород 2020

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

**Задания к работе**

1. Просмотр набора классов в репозитории WMI.

Щелкните Пуск\Выполнить, введите wbemtest.

Установите флажок «Включить все привилегии».

Нажмите Подключить.

В окне подключения введите в поле Пространство имен \\Server01\root\cimv2 и нажмите Подключить.

Затем нажмите кнопку «Классы…», выберите «Рекурсивно», не заполняйте поле суперкласса и нажмите «Ok». В результате вы получите список классов, определенный в вашем репозитории WMI, в пространстве имен CIMv2.

Найдите класс Win32\_NTDomain и щелкните на нем дважды левой кнопкой мыши.

В открывшемся окне редактора нажмите кнопку Экземпляры, чтобы увидеть список экземпляров.

Найдите свой домен и зайдите в окно свойств для данного экземпляра.

Нажмите кнопку Соединители.

Используя утилиту wbemtest, получите список экземпляров групп домена.

Найдите в списке группу «Sales Representatives» и ознакомьтесь со значениями параметров этой группы.

Найдите в экземплярах класса учетных записей пользователей Templatesalesrep и petr.petrov. Убедитесь, что свойство Disabled у первого установлено в True, а у второго – в False. Измените значение Disabled у petr.petrov.

2. Найдите класс Win32\_UserAccount.

В окне методов этого класса значится метод Rename.

Найдите экземпляр petr.petrov, скопируйте в буфер обмена значение его свойства \_RELPATH.

В главном окне wbemtest нажмите кнопку Выполнить метод (Execute Method).

В появившемся окне введите в поле Object Path содержимое буфера обмена и нажмите ОК.

Вы получили доступ к методу Rename для этого экземпляра. Задайте входные параметры для метода (свойство Name) и выполните метод.

Убедитесь в Active Directory Users and Computers, что в свойствах аккаунта изменилось имя. Измените его обратно на petr.petrov. С помощью выполнения соответствующего метода осуществите перезагрузку системы (класс Win32\_OperatingSystem).

3. Запросы WQL.

Нажмите на кнопку Query в окне утилиты wbemtest.

Убедитесь, что в качестве типа запроса выбран WQL.

В поле ввода напишите запрос.

select \* from Win32\_UserInDomain

Результатом выполнения запроса будет список пользователей.  Составьте и выполните запрос, выводящий список пользователей своего домена, являющихся членами группы Sales Representative. Составьте и выполните запрос, выводящий список заблокированных учетных записей пользователей.

Составьте и выполните запросы, перечисляющие логические диски, процессоры, видеокарты, принтеры в составе системы, а также выполняющиеся на сервере в данный момент процессы. Ознакомьтесь со свойствами экземпляров классов.

4. Утилита Wmic.

Запустите интерпретатор командной строки cmd.exe и в строке приглашения наберите WMIC. После этого появится приглашение консоли WMI.

Просмотрите весь список команд и псевдонимов при помощи команды wmic /? (wmic:root\cli>/?).

Используя команду wmic group where domain=”<Имя\_домена>”, получите список групп домена.

Выполните команду:

Просмотрите возможные команды для useraccount и group. Создайте новую группу в своем домене.

Создайте в этой группе пользователя, задав его имя, полное имя, и требование изменения пароля при следующем заходе в систему. Убедитесь, что группа и пользователь созданы при помощи утилиты wmic.

Удалите группу и пользователя в ней, используя команду Delete. Запросите параметры домена (ntdomain).

Разблокируйте аккаунт Templatesalesrep.

Убедитесь в том, что аккаунт был разблокирован, при помощи соответствующего запроса.

5. Сценарии с использованием WMI

5.1. Просмотр списка процессов при помощи сценария Откройте блокнот и наберите следующий текст:

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="POVTAS" 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

Сохраните файл, сменив расширение на \*.vbs.

Запустить сценарий на выполнение можно просто двойным щелчком на файле, тогда результаты будут выводиться в виде сообщений.

Однако, в данном случае это неудобно, поэтому воспользуйтесь возможностью запуска сценариев в режиме консоли.

Запустите командную строку и выполните команду cscript <имя\_файла\_сценария.vbs>.

Просмотрите полученную информацию.

Разберите текст сценария, чтобы уяснить принцип его составления.

5.2. Управление объектами с помощью сценариев WMI

Выведите список групп, присутствующих в домене.

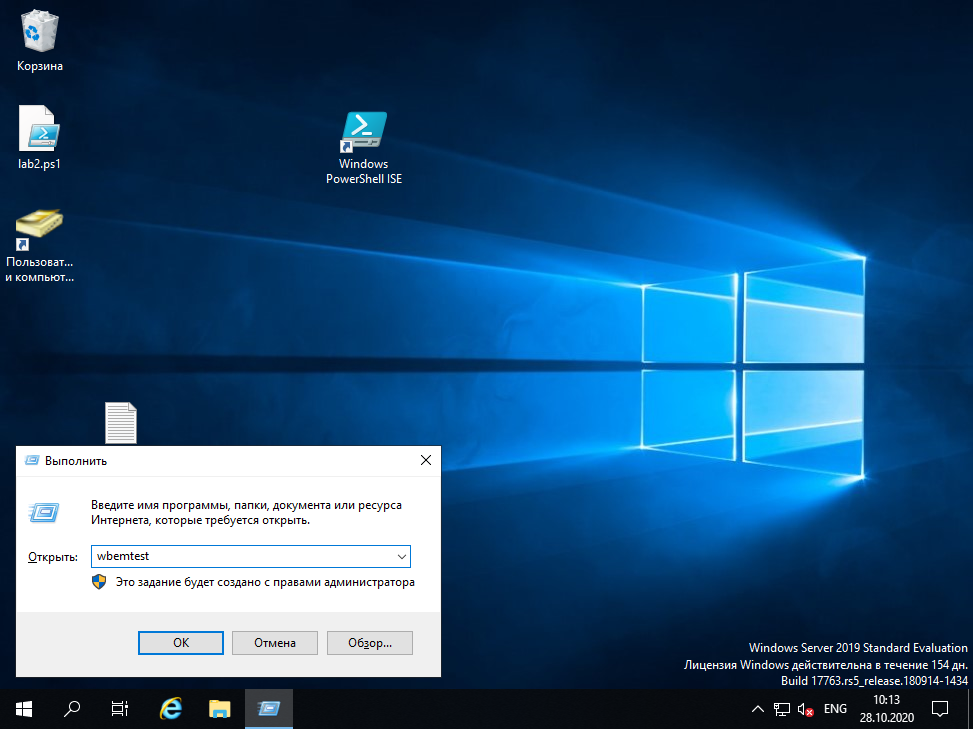
Напишите сценарий, при помощи которого объект пользователя будет перемещен из одной группы в другую.

Создайте сценарий, выводящий список групп и учетных записей пользователей, входящих в эти группы с основными параметрами по каждому объекту в текстовый файл.

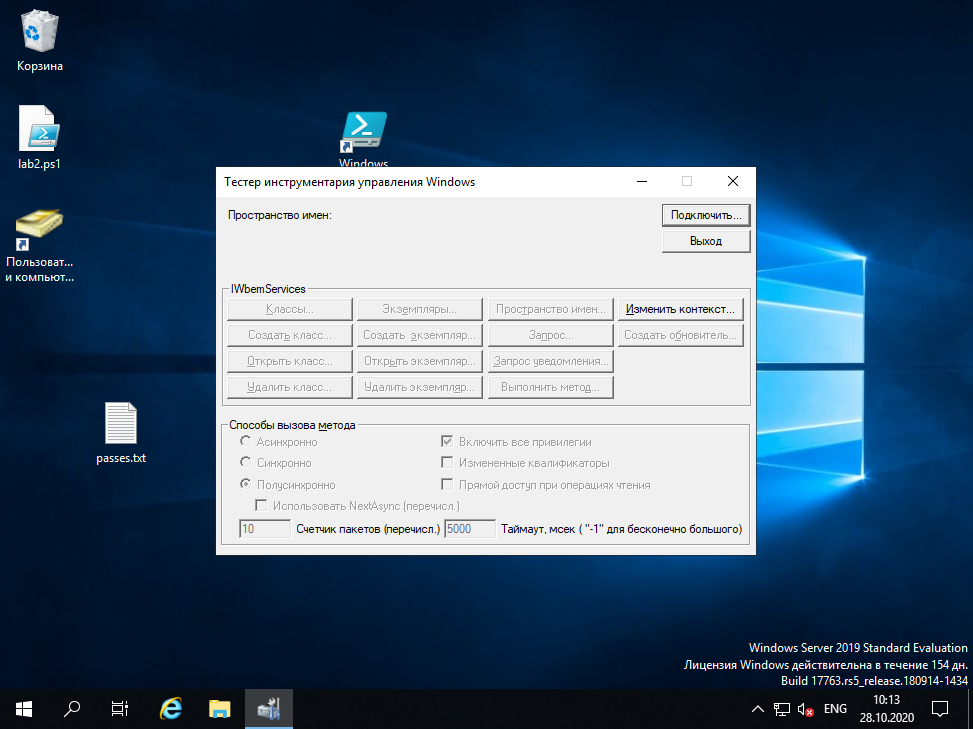
Создайте сценарии синхронного и асинхронного отслеживания подключений пользователей домена.

**Выполнение**

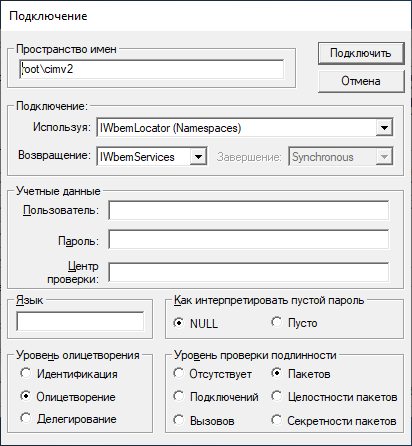
Задание 1



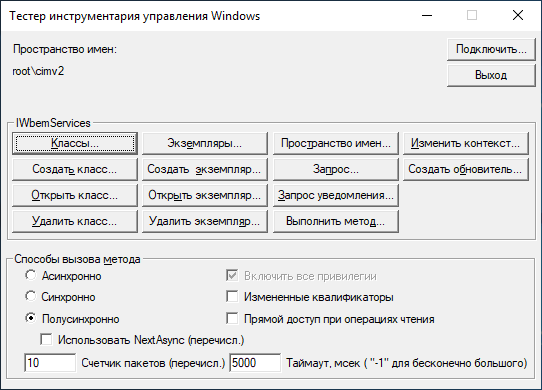
Установили флажок «Включить все привилегии».



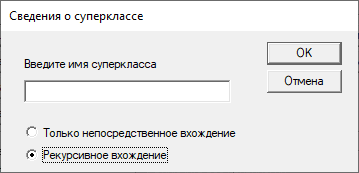
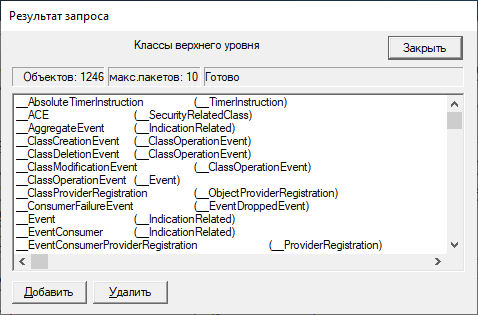
Нажали «Подключить»



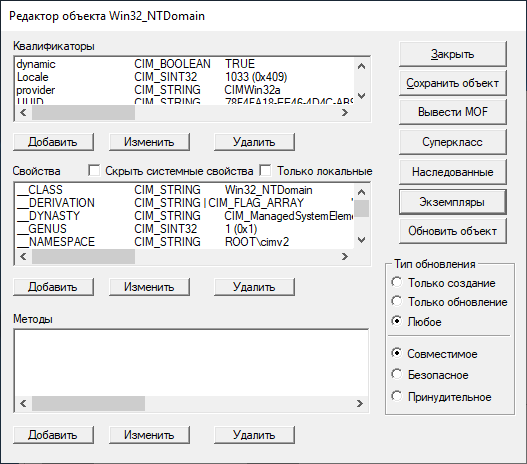
Появились кнопки:



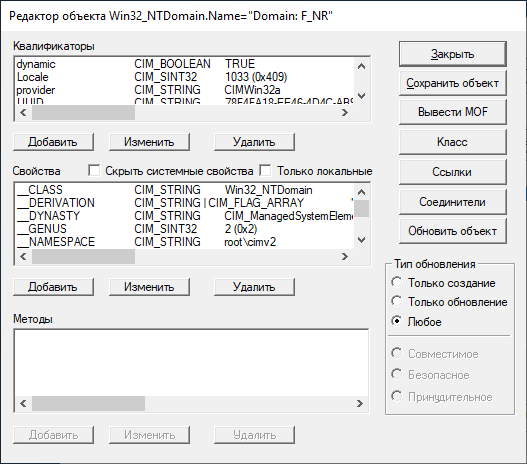
Получили рекурсивно список всех классов:



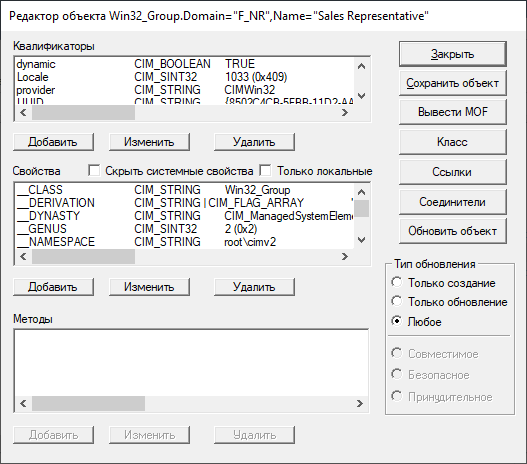
Открыли свойства:



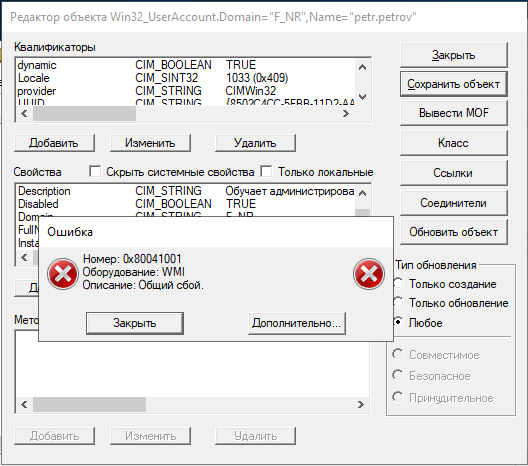
Нашли объект:



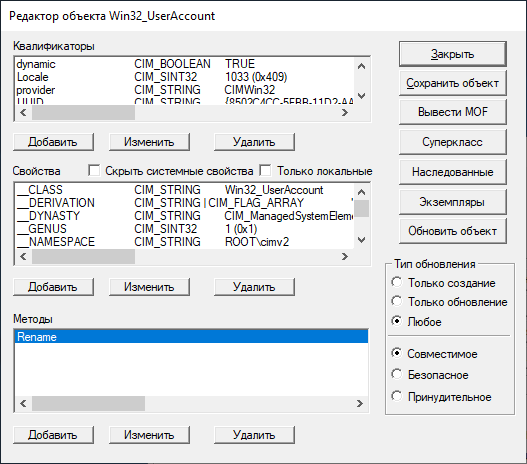
Свойства группы:



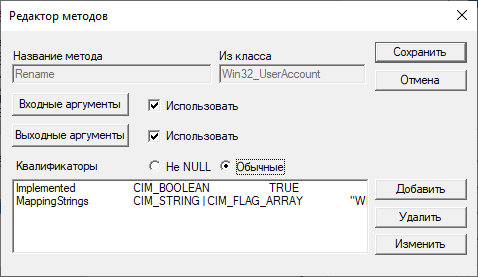
Инструмент WMI имеет проблемы с сохранением объектов.



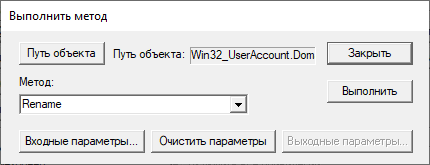
В объекте Win32\_UserAccount обнаружили метод Rename:

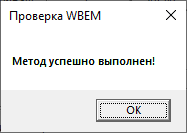


Скопировали в буфер обмена:

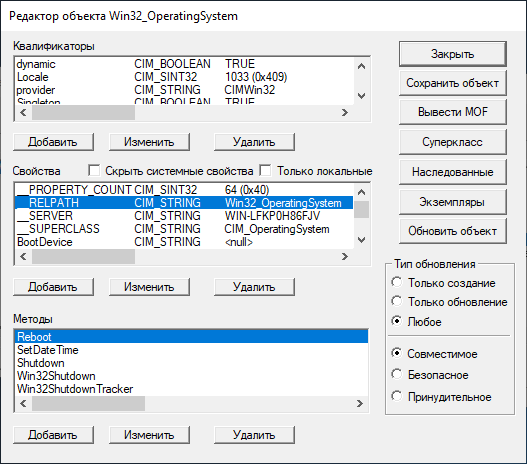


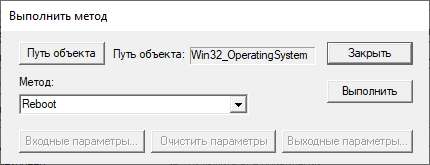
Воспользовались кнопкой «Выполнить метод»



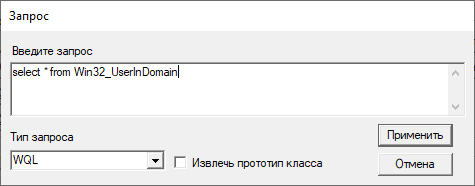


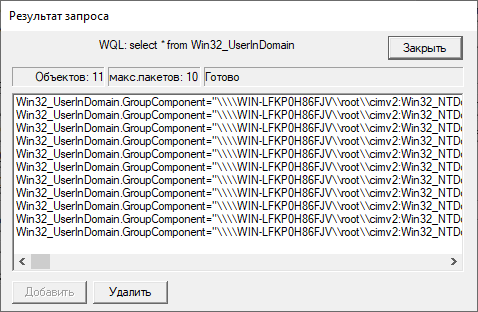
Аналогично воспользуемся методом Reboot у объекта Win32\_OperatingSystem для перезагрузки системы.



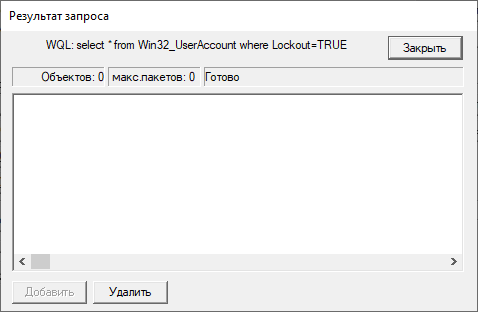


Воспользовались кнопкой «Запрос» в главном меню.

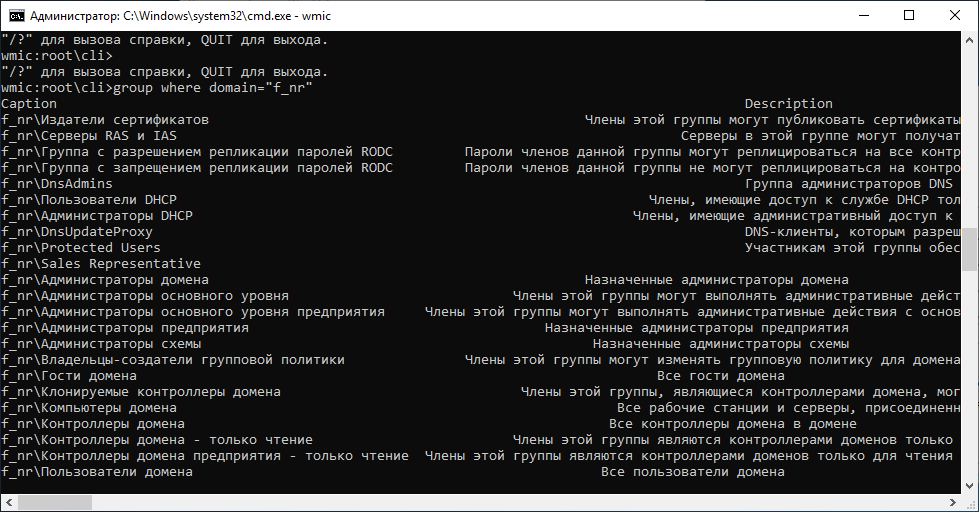




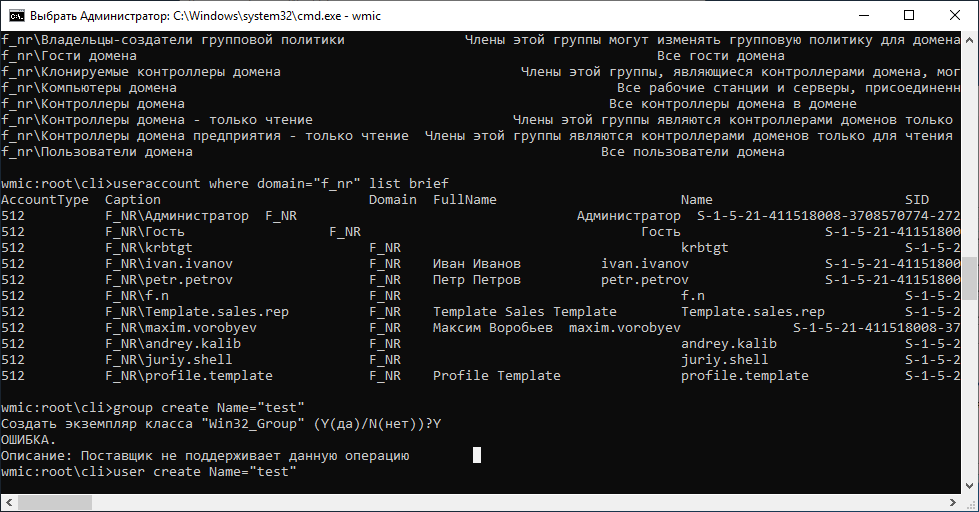
Создали и выполнили запрос на получение всех пользователей с заблокированным аккаунтом.



С помощью инструмента WMIC получили список групп в домене.



С помощью WMIC получили список пользователей в домене.



Используя возможности cscript, записали скрипт на VBS для вывода на экран объектов пользователей. Создали скрипт, выводящий на экран список групп.

**Вывод**

В ходе лабораторной работы мы изучили со структуру объектов WMI, способы доступа к ним, а также научилисьработать с WMI через сценарии и утилиты WBEMTEST и WMIC.

**Контрольные вопросы**

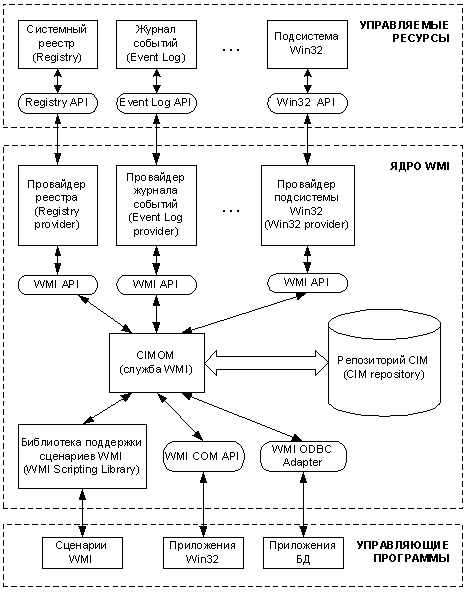
1. Что такое WMI? Для чего она используется?

Windows Management Instrumentation (WMI) в дословном переводе — инструментарий управления Windows. WMI — это одна из базовых технологий для централизованного управления и слежения за работой различных частей компьютерной инфраструктуры под управлением платформы Windows.

2. Перечислите средства работы с WMI для администратора.

* wmimgmt.msc – Позволяет управлять ММС для настройки WMI на локальном ПК.
* winmgmt.exe – Позволяет управлять WMI локального компьютера
* wbemtest.exe – Позволяет взаимодействовать со структурой WMI на локальном или удаленном ПК.
* wmic.exe – Аналогично, но без графического интерфейса.
* mofcomp.exe - компилятор MOF-файлов для расширения структуры WMI, управления библиотекой классов WMI и восстановления репозитория.

3. Общая структура WMI.



4. Опишите возможности программы WMIC.

Команда WMIC (Windows Management Instrumentation Command) используется для получения сведений об оборудовании и системе, управления процессами и их компонентами, а также изменения настроек с использованием возможностей инструментария управления Windows (Windows Management Instrumentation или WMI) .

Инструментарий управления Windows (WMI) – это набор программных средств, обеспечивающий управление системой с использованием сценариев, выполняемых в среде Windows Script Host ( ранее - Windows Scripting Host ) или в командной строке с помощью утилиты WMIC.EXE. Windows Script Host или сокращенно WSH - это компонент Microsoft Windows, предназначенный для запуска сценариев на скриптовых языках JScript и VBScript. Сценарии WSH обычно используются в тех случаях, когда требуется выполнить набор каких-либо действий, требующих написания относительно сложного исходного кода, но нередко в повседневной практике администрирования, удобнее воспользоваться возможностями командной строки WMIC.

Технология WMI — это расширенная и адаптированная под Windows реализация стандарта Web-Based Enterprise Management ( WBEM ), принятого многими крупными компаниями в качестве универсального интерфейса мониторинга и управления различными системами и компонентами распределенной информационной среды предприятия с использованием объектно-ориентированных идеологий и протоколов HTML и XML. В основе структуры данных в WBEM лежит Common Information Model (CIM), реализующая объектно-ориентированный подход к представлению компонентов системы. Практически, WMI, основанный на CIM, является открытой унифицированной системой интерфейсов доступа к любым параметрам операционной системы, устройствам и приложениям, которые функционируют в ней.

6. Использование WQL-запросов.

Запросы WQL (SQL for WMI) очень похожи на запросы SQL с тем отличием, что в WQL производится выборка не записей таблиц, а экземпляров классов.