**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ  
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 систем»

тема: «Использование средств инструментария для управления

Windows (WMI) в администрировании»

Выполнил: ст. группы ВТ-42   
Воскобойников И. С.  
Проверил: Федотов Е.А.

**Белгород 2021**

**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.

**Краткие сведения**

Windows Management Instrumentation (Инструментарий для Управления Windows) — набор интерфейсов для управления операционной системой через специальные компоненты, причем как локально, так и по сети.

WMI позволяет использовать скриптовые языки, такие как VBScript или Windows PowerShell для управления персональными компьютерами и серверами, работающими под управлением Microsoft Windows.

По своей сути WMI – это расширенная и адаптированная компанией Microsoft реализация стандарта WBEM, в основе которого лежит идея создания универсального интерфейса мониторинга и управления к различным системам и компонентам распределенной информационной среды предприятия с использованием объектно-ориентированной идеологии и широко распространенных веб-технологий представления информации: протоколов XML и HTTP.

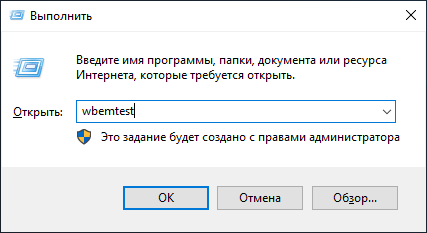
В основе структуры представления данных в стандарте WBEM лежит CIM (Common Information Model – модель информации общего типа), реализующая объектно-ориентированный подход к представлению компонентов систем как классов со своим набором свойств и методов, а также принципов наследования. Основное средство для описания новых элементов модели CIM – это синтаксис языка Managed Object Format (MOF), который является текстовым и легко понятным человеку.

Любое приложение или драйвер в операционной системе может добавить к системной модели CIM свой набор классов. Такое расширение модели позволяет легко интегрировать в единую систему мониторинга и управления новые приложения. Для этого приложение должно зарегистрировать свои классы в существующей модели CIM и обеспечить стандартные вызовы встроенных процедур для создания объектов этих классов и наполнения их свойствами и методами. Набор этих процедур оформляется как WMI Provider – специальная библиотека, являющаяся мостом между любым приложением и ядром службы WMI.

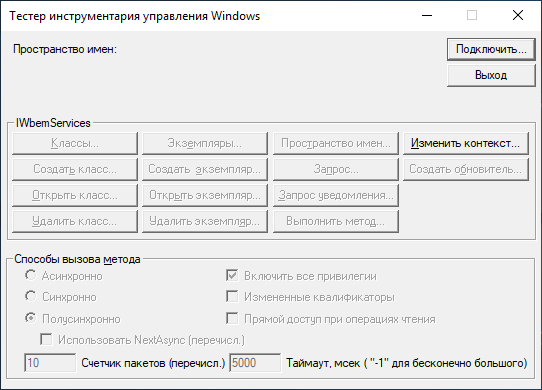
* *Провайдеры WMI* скрывают детали внутренней реализации управляемых объектов, позволяя Менеджеру объектов обращаться к ним, используя API-функции.
* *Менеджер объектов CIM* (Common Information Model Object Manager, CIMOM) обеспечивает обработку всех запросов конечных приложений к WMI и доставку информации от WMI к конечным приложениям.
* *Репозиторий (хранилище классов) CIM*, объекты-экземпляры которых создаются провайдером WMI по запросу потребителя.
* *Библиотека поддержки сценариев* (WMI scripting library), которая располагается в файле *wbemdisp.dll* в каталоге %SystemRoot%\System32\Wbem\.

**Выполнение работы:**

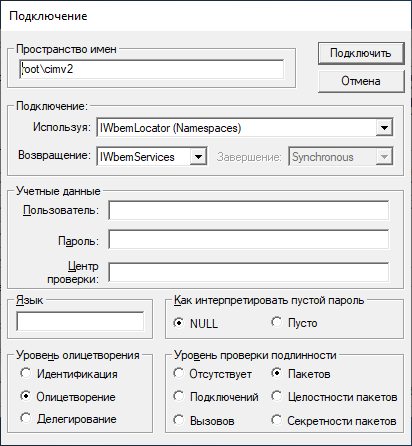
Запустил утилиту wbemtest:



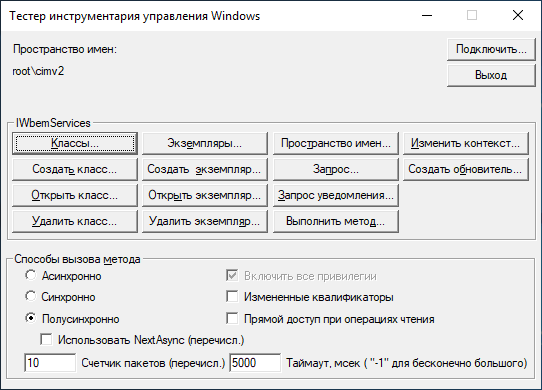
Стартовое окно утилиты:



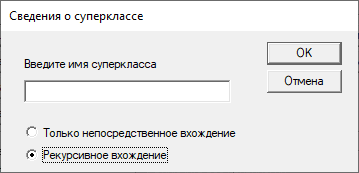
Подключил пространство имен:

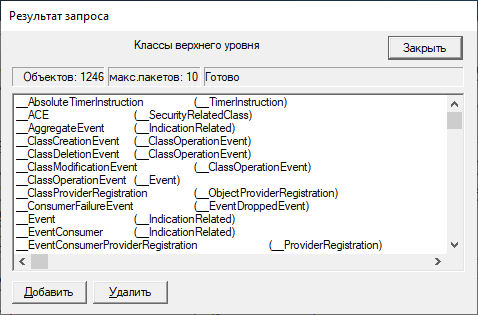


После подключения стали активными кнопки действий в главном окне.

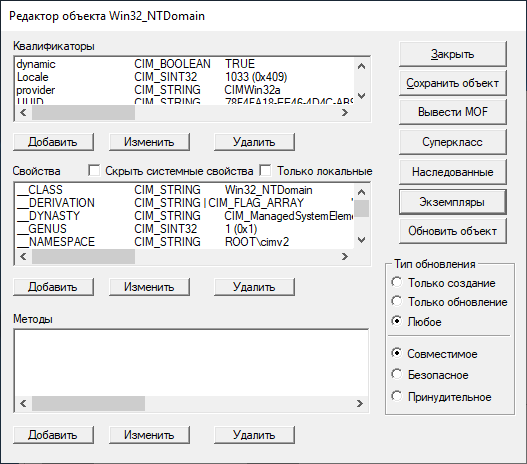


Получил рекурсивно список всех классов.

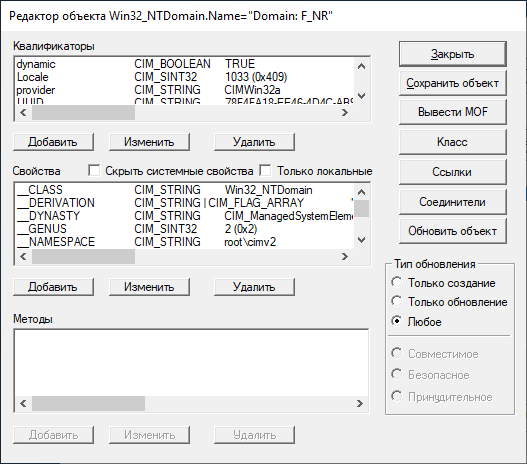




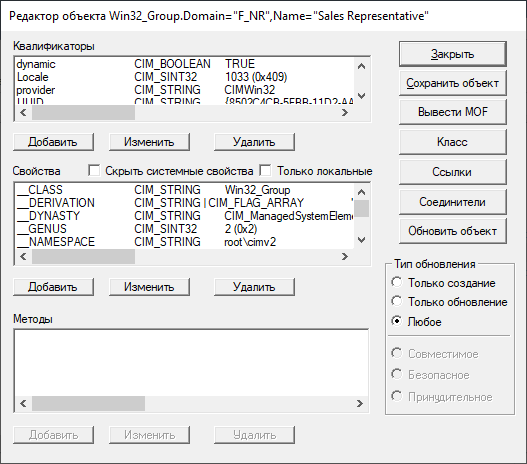
Открыл свойства объекта Win32\_NTDomain



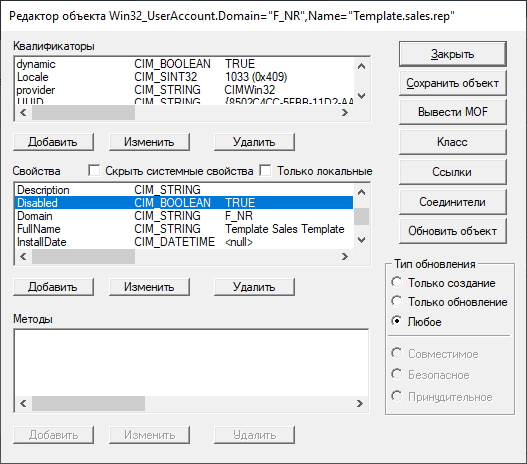
Среди экземпляров класса нашел объект, соответствующий созданному ранее домену.

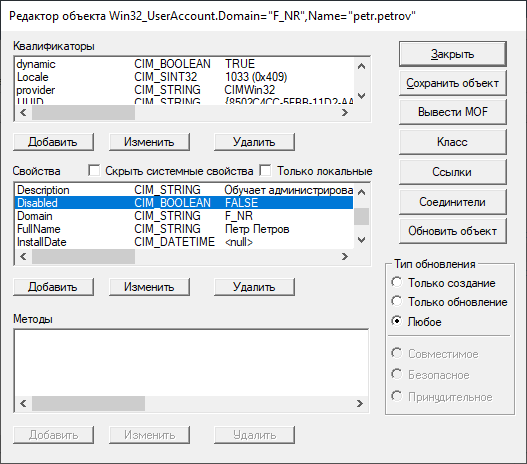


Через список соединителей нашел группу Sales Representative. На снимке экрана – свойства группы.

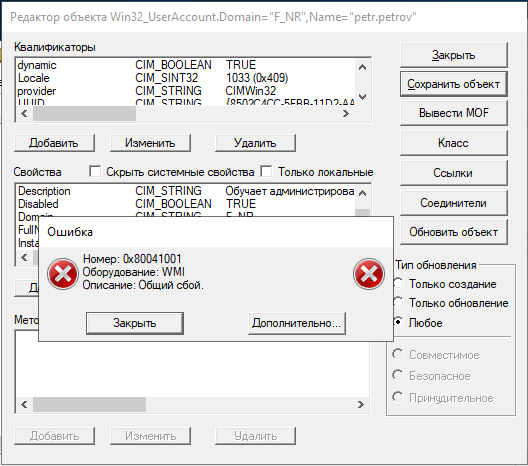


Нашел объект пользователя Template.sales.rep и объект пользователя petr.petrov. Изменил свойство Disabled с TRUE на FALSE.

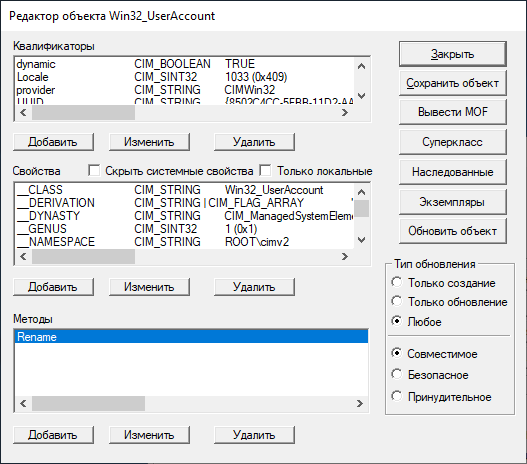




Инструмент WMI имеет проблемы с сохранением объектов.

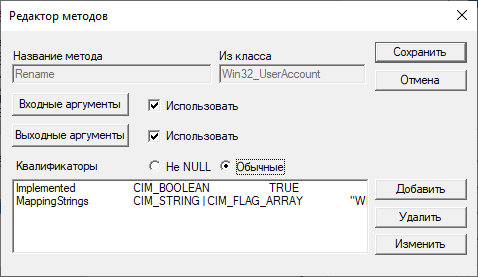


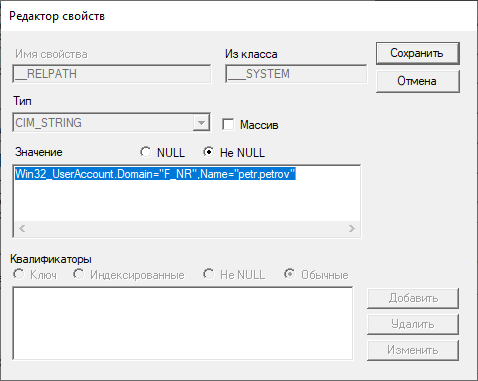
В объекте Win32\_UserAccount обнаружил метод Rename.



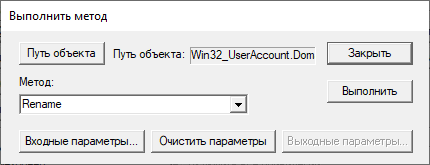
Перейдя в свойства метода и далее в режим редактирования входных аргументов нашел объект пользователя petr.petrov.

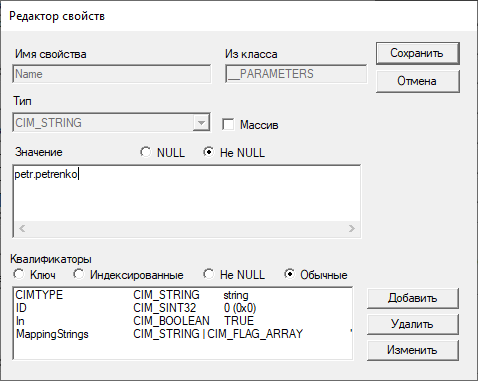
Скопировал в буфер обмена свойство объекта \_RELPATH.



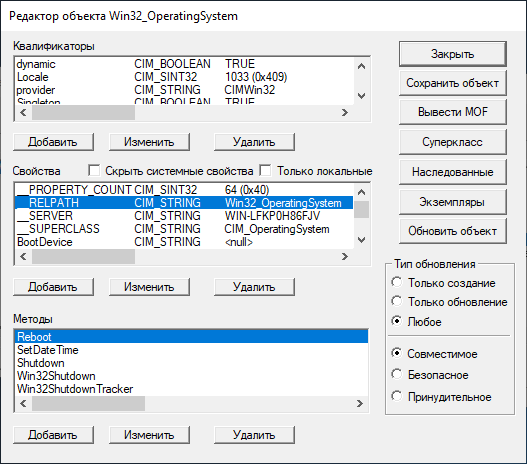


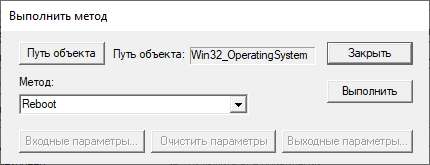
В главном окне воспользовался кнопкой «Выполнить метод», вставил из буфера обмена путь к объекту. В качестве входного параметра задал новое имя.



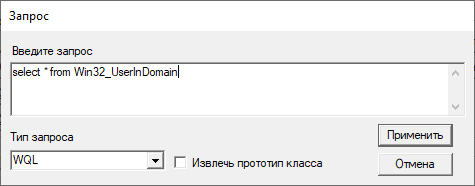


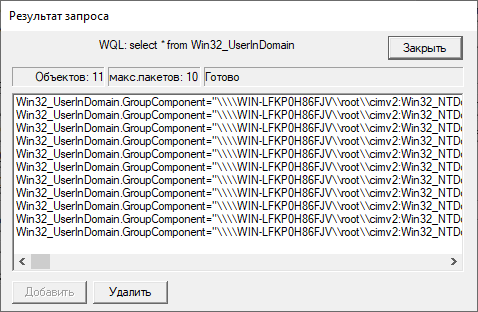
Аналогично воспользовался методом Reboot у объекта Win32\_OperatingSystem для перезагрузки системы.



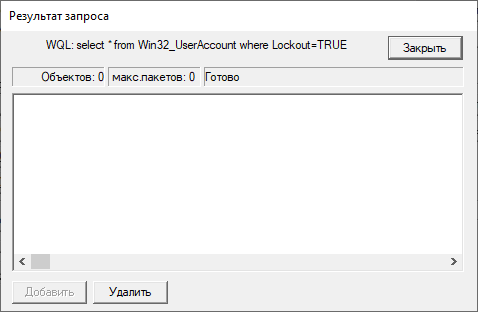


Воспользовался кнопкой «Запрос» в главном меню. Записал и выполнил запрос на получение списка пользователей в домене. Запрос прошел успешно.

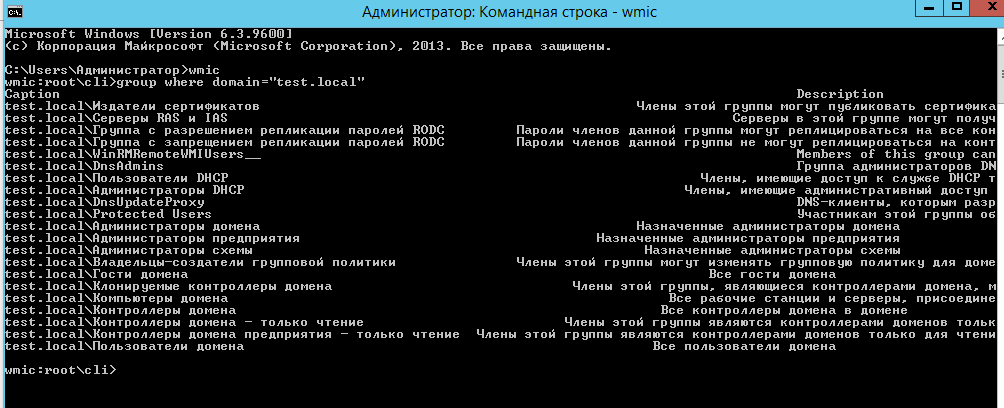




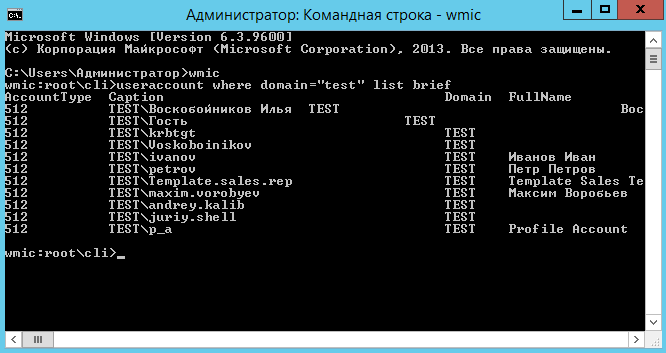
Создал и выполнил запрос на получение всех пользователей с заблокированным аккаунтом.



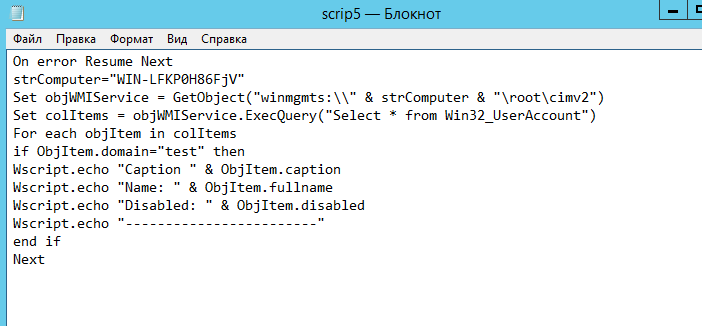
С помощью инструмента WMIC получил список групп в домене.

****

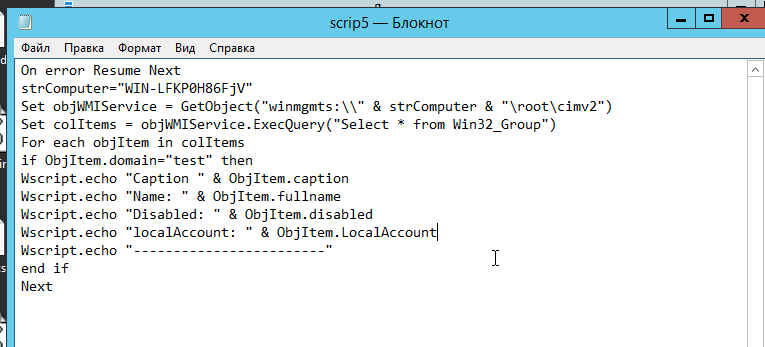
Также с помощью WMIC получил список пользователей в домене.

****

Используя возможности cscript, записал скрипт на VBS для вывода на экран объектов пользователей.

****

Следуя образцу, создал скрипт, выводящий на экран список групп.

****

**Вывод:** Познакомился с технологией WMI и структурой объектов в ней, способами доступа к ним. Научился работать с WMI с помощью утилит WBEMTEST и WMIC. На данный момент технология считается устаревшей и не рекомендуется к использованию.