Windows Management Instrumentation как способ мониторинга и аудита ИТ-инфраструктуры предприятия

Е.А. Верещагина, А.К. Рудниченко, Д.С. Колесникова

Дальневосточный федеральный университет, Владивосток

Аннотация: В данной работе приведено описание инструментария управления операционной системой Windows – Windows Management Instrumentation, а также проанализирована его применимость в целях мониторинга и аудита ИТ-инфраструктуры предприятия. Приведены основные классы WMI и их назначение. Описаны два метода по использованию WMI, их достоинства и недостатки.
Ключевые слова: операционная система, Windows, Windows Management Instrumentation, WMI, аудит, мониторинг, ИТ-инфраструктура, wbemtest.

С каждым годом на предприятиях различного уровня растёт количество компьютерной техники. Но, зачастую, данный рост не пропорционален росту штата сотрудников IT-отдела организации. В связи с этим остро встаёт вопрос об администрировании и мониторинге всего парка рабочих станций и серверов на предприятии с целью бесперебойной работы всей инфраструктуры [1]. Предполагается, что частично данную задачу мониторинга может решить использование Windows Management Instrumentation в операционных системах компании Microsoft.

Windows Management Instrumentation (WMI) – расширенная и адаптированная компанией Microsoft реализация стандарта WBEM [2] (WebBased Enterprise Management компании DMTF Inc. [3]). В основе WBEM 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 операционной системе Windows есть набор утилит, которые работают с WMI:

- wmimgmt.msc – оснастка консоли управления Windows, позволяющая в целом управлять самой системой WMI на выбранном компьютере.
- winmgmt.exe – консольная утилита, позволяющая управлять WMI. Аналогична утилите wmimgmt.msc.
- wbemtest.exe – утилита для интерактивной работы с WMI. В ней существует возможность формирования запросов и получения ответов на них. Может помочь при разработке приложения, которое использует WMI.

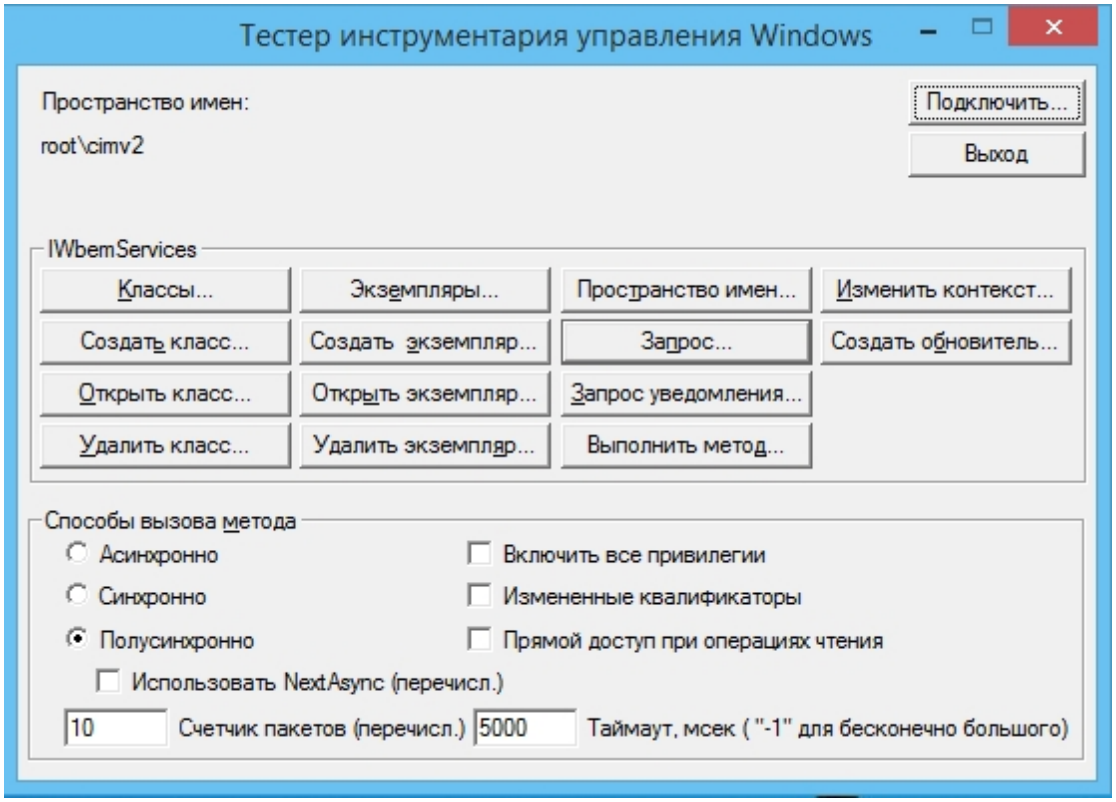

Рис. 1. – Внешний вид утилиты WBEMTEST

WMI имеет в себе корневое пространство «root», которое имеет в себе 4 пространства имён: CIMV2, Default, Security, WMI [4]. Вся необходимая информация о рабочей станции или сервере находится в классах, которые являются дочерними по отношению к CIMV2.

Таким способом, с помощью Windows Management Instrumentation можно получить информацию о системе, указанную в таблице 1 [5, 6].

Таблица №1

Перечень некоторых классов и их назначение

№ п/п	Имя класса WMI	Назначение
1	Win32_ComputerSystem	Хранение информации об имени компьютера, домене или рабочей группе, в которой он состоит, и активном пользователе (текущей сессии)
2	Win32_Processor	Хранение информации о процессоре (наименование, количество ядер)
3	Win32_PhysicalMemory	Хранение информации об оперативной памяти (изготовитель, серийный номер планки оперативной памяти, объём и частота)
4	Win32_VideoController	Хранение информации о видеокарте (наименование, видеопроцессор, объём видеопамяти)
5	Win32_Volume	Хранение информации о всех подключенных жёстких дисках (объём, свободное место, наименование, буква диска, серийный номер, файловая система)
6	Win32_OperatingSystem	Хранение информации об операционной системе (наименование, путь к папке Windows, версия, дата установки операционной системы, свободная оперативная память и пр.)
7	Win32_Service	Хранение информации о всех службах (наименование, путь до исполняемого файла

		и пр.)
8	Win32_Product	Хранение информации об установленном программном обеспечении в операционной системе (наименование программы, дата установки, путь установки, версия)
9	Win32_Process	Хранение информации о запущенных процессах (имя процесса, идентификатор, каталог запуска процесса)
10	Win32_UserAccount	Хранение информации о пользователях в операционной системе (имя пользователя, является ли пользователь локальным, SID пользователя и пр.)

Для того, чтобы было удобно работать с экземплярами объектов WMI, используется язык WMI Query Language (WQL), который является подмножеством ANSI SQL. Главное отличие WQL от ANSI SQL состоит в том, что WQL позволяет только считывать данные WMI (т.е. запросы типа SELECT), но не изменять их.

Так, чтобы получить информацию об операционной системе, необходимо выполнить запрос: SELECT * FROM Win32_OperatingSystem. Результат запроса изображён на рисунке 2.

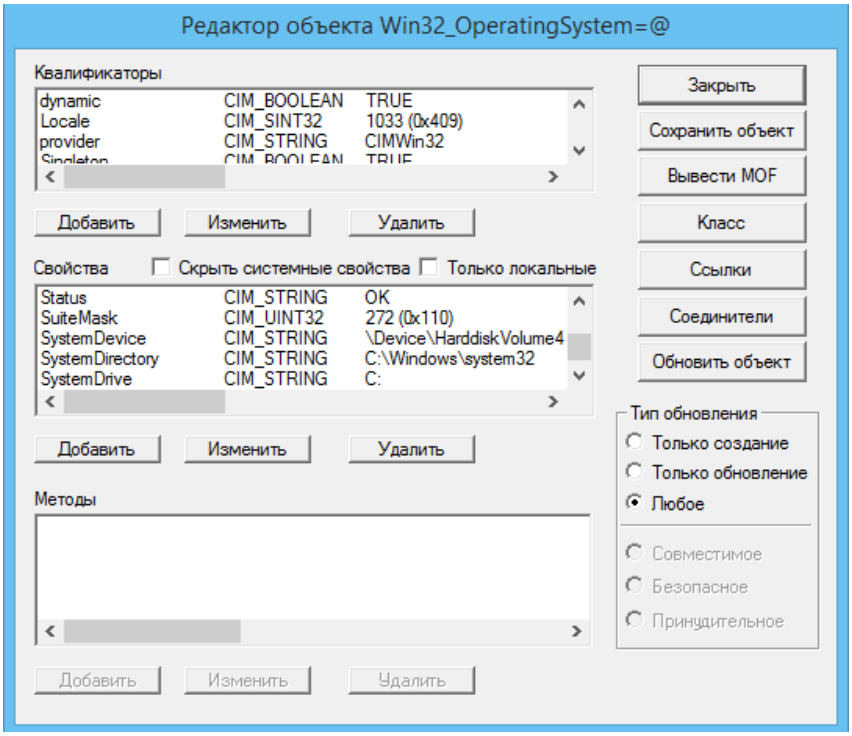

Рис. 2. – Пример запроса в WBEMTEST

Таким образом, для целей мониторинга или аудита инфраструктуры предприятия достаточно собрать необходимые данные из WMI и передать их на управляющий сервер [7]. Опытным путём установлено, что пакет с данными, приведёнными в таблице 1, в размере не превышает 300-350 Кбайт.

Windows Management Instrumentation возможно использовать в двух вариациях: локально и по сети.

Для локального использования WMI необходимо установить «программу-агент» на обследуемую рабочую станцию или сервер. С помощью неё возможно получить необходимые данные и после передать их на управляющий сервер по протоколу TCP. На рисунке 3 изображена диаграмма деятельности локального использования WMI.

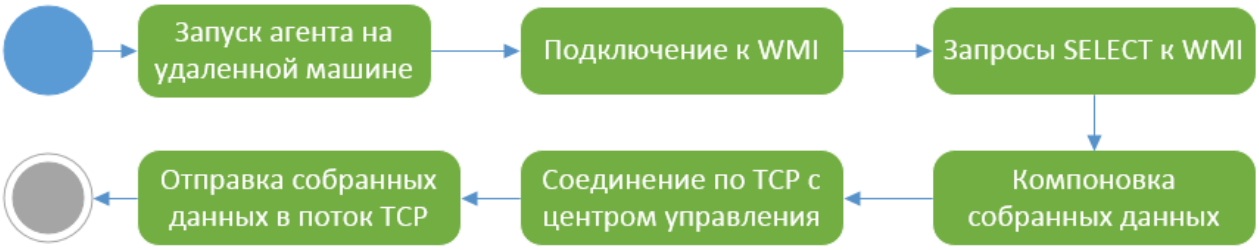

Рис. 3. – Локальное использование WMI

Данный тип взаимодействия оправдан, когда WMI является частью большого функционала системы. В случаях, когда программное обеспечение необходимо только для единовременного получения информации, подойдет сетевой тип взаимодействия с WMI.

Сетевой тип взаимодействия с WMI подойдёт, если все обследуемые рабочие станции и/или сервера находятся в одной локальной сети и домене Active Directory. Операционная система Windows позволяет подключаться к WMI другого устройства. На рисунке 4 изображена диаграмма деятельности использования WMI по сети.

Рис. 4. – Использование WMI по сети

Стоит отметить, что не всегда Windows Management Instrumentation может предоставить полную информацию о рабочей станции или сервере. В некоторых случаях WMI не может дать конкретного отклика, как, например, в случае с получением установленного программного обеспечения в операционной системе. В данном случае в список установленного программного обеспечения будут включены только те позиции, которые были установлены с помощью Windows Installer [8].

В связи с этим, аудит ИТ-инфраструктуры предприятия целесообразно проводить, комбинируя некоторый инструментарий между собой. В данном случае список установленного программного обеспечения возможно получить через реестр Windows. Учитывая данный факт, рекомендуется выбрать локальный тип использования с последующей передачей данных по каналам связи (например, используя протокол TCP [9]).

Кроме этого, с помощью WMI возможно проводить непрерывный мониторинг ресурсов операционной системы на рабочих станциях и серверах, что поможет вовремя предотвратить деградацию ИТ-инфраструктуры предприятия. WMI может помочь в определении свободного количества оперативной памяти, в загрузке центрального процессора, а также в определении свободного пространства на жёстких дисках.

Действия с WMI, как и другие действия в Windows, могут быть записаны (то есть логированы) штатными средствами операционной системы [10]. Это позволит отслеживать доступ к WMI в случаях отладки системы мониторинга или при других аналогичных задачах.

Таким образом, Windows Management Instrumentation является универсальным инструментом для разработки информационной системы, осуществляющей функции мониторинга и аудита ИТ-инфраструктуры предприятия, так как использует штатный функционал операционной системы Windows.

Литература

1. Пылаева Е.В. Разработка модели управления ИТ-инфраструктурой кредитной организации на основе архитектурной модели IT4IT // Инженерный вестник Дона, 2018, №2. URL: ivdon.ru/ru/magazine/archive/N2y2018/4927.

2. Использование Windows Management Instrumentation для диагностики. URL: docs.microsoft.com/ru-ru/dotnet/framework/wcf/diagnostics/wmi/ (дата обращения: 21.11.2019).

3. Distributed Management Task Force Inc. URL: dmtf.org (дата обращения: 21.11.2019).

4. Администрирование с помощью WMI. URL: sysengineering.ru/administration/administrationusingwmi/ (дата обращения: 22.11.2019).

5. WMI Samples. URL: activexperts.com/admin/scripts/wmi/ (дата обращения: 23.11.2019).

6. Попов Андрей, Шикин Евгений. Администрирование Windows с помощью WMI и WMIC. СПб.: БХВ-Петербург, 2004. 746 с.

7. Аудит системы при помощи «родных» приложений ОС Windows. URL: securitylab.ru/analytics/454684.php (дата обращения: 23.11.2019).

8. Win32_Product class // URL: docs.microsoft.com/en-us/previous-versions/windows/desktop/legacy/aa394378 (vpercentage3Dvs.85) (дата обращения: 25.11.2019).

9. Сироткин А.В., Брачун Т.А., Бархатов Н.И. Моделирование приоритетного управления информационными потоками с использованием сокетов // Инженерный вестник Дона, 2012, №4. URL: ivdon.ru/ru/magazine/archive/n4p1y2012/1192.

10. WMI auditing. URL: sevecek.com/EnglishPages/Lists/Posts/Post.aspx?ID=3 (дата обращения: 25.11.2019).

References

1. Ispol'zovanie Windows Management Instrumentation dlya diagnostiki [Using Windows Management Instrumentation for diagnostics]. URL:

docs.microsoft.com/ru-ru/dotnet/framework/wcf/diagnostics/wmi/ (accessed 11/21/2019).

2. Distributed Management Task Force Inc. URL: dmtf.org (accessed 11/21/2019).

3. Administrirovanie s pomoshch'yu WMI [Administration with WMI]. URL: sysengineering.ru/administration/administrationusingwmi/ (accessed 11/22/2019).

4. WMI Samples. URL: activexperts.com/admin/scripts/wmi/ (accessed 11/23/2019).

5. Andrey Popov, Evgeniy Shikin Administrirovanie Windows s pomoshch'yu WMI i WMIC [Windows Administration with WMI and WMIC]. SPb.: BKhV-Peterburg, 2004. 746 s.

6. Audit sistemy pri pomoshchi «rodnykh» prilozheniy OS Windows [System audit using native Windows applications]. URL: securitylab.ru/analytics/454684.php (accessed 11/23/2019).

7. Win32_Product class. URL: docs.microsoft.com/en-us/previous-versions/windows/desktop/legacy/aa394378 (vpercentage3Dvs.85) (accessed 11/25/2019).

8. WMI auditing. URL: sevecek.com/EnglishPages/Lists/Posts/Post.aspx?ID=3 (accessed 11/25/2019).

9. Pylaeva E.V. Inzenernyj vestnik Dona, 2018, №2. URL: ivdon.ru/ru/magazine/archive/N2y2018/4927.

10. Sirotkin A.V., Brachun T.A., Barkhatov N.I. Inzenernyj vestnik Dona, 2012, №4. URL: ivdon.ru/ru/magazine/archive/n4p1y2012/1192.