15.02.2024

Курс:

Практическая работа к уроку № Lesson_8

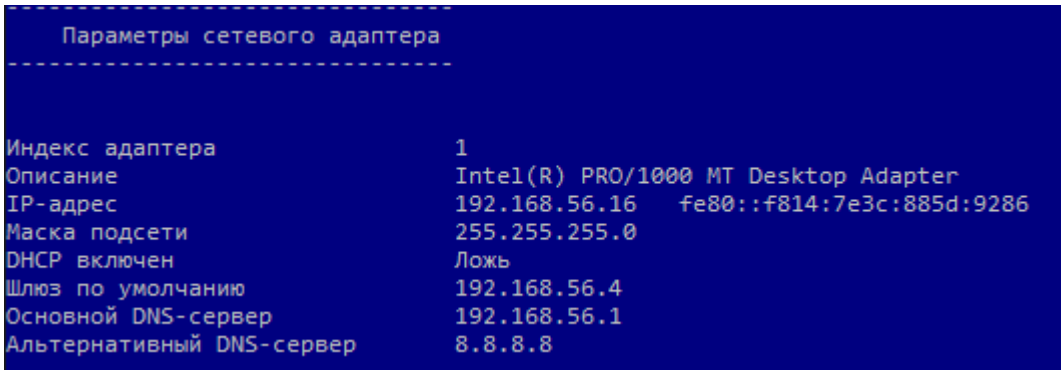
--

Windows Management Instrumentation (WMI)

Задание:

1. Посмотрите информацию о физических дисках
2. Посмотрите список всех логических разделов в Windows
3. Создайте раздел на диске объемом 1 Гб
4. Удалите ранее созданный раздел на диске
5. Включите мягкую квоту на диске C
6. Измените порог квоты для пользователя Администратор
7. Установите модуль Дедуплекации
8. Установите минимум для дедуплекации для файлов в 1GB
9. Настройте расписание таким образом, что бы процесс GarbageCollection запускался в пятницу в 22:00
10. Удалите созданное расписание
11. Используя wmi посмотрите запущенные процессы в системе
12. Запустите процесс cmd и с помощью wmi остановите его
13. Создайте GPO, WMI фильтр которой будет применяться к Windows 10

Serv1: win2019serv01 (gui)



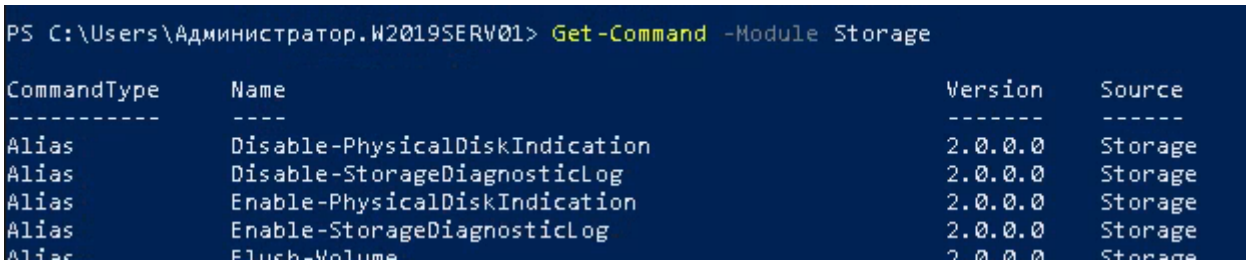
WMI – это Windows Management Instrumentation (инструментарий управления Windows). Из названия понятно, для чего создана и применяется эта технология. Стоит лишь добавить, что она давно перешагнула рамки управления только операционной системой Windows и позволяет контролировать множество других совместимых с ней приложений.

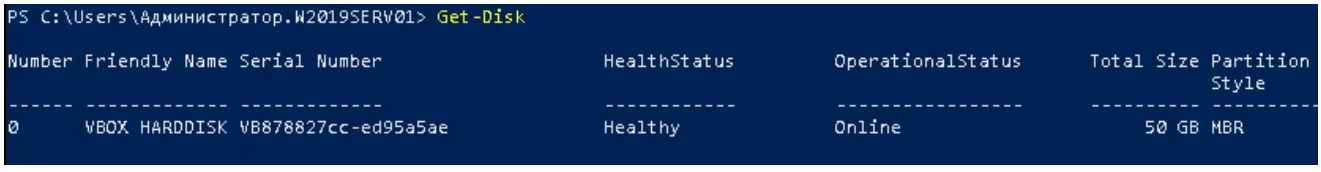
По своей сути WMI – это расширенная и адаптированная компанией Microsoft реализация стандарта WBEM (WebBased Enterprise Management компании DMTF Inc). В основе структуры представления данных в стандарте WBEM лежит CIM (Common Information Model – модель информации общего типа), реализующая объектно-ориентированный 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. Таким образом, любое приложение или драйвер в операционной системе, которая поддерживает стандарт WBEM, может добавить к системной модели CIM свой набор классов.
Таким образом, WMI – это открытая унифицированная библиотека (репозиторий) однотипных интерфейсов доступа к параметрам, настройки и свойствам различных систем и их компонентов
Многие производители программного и аппаратного обеспечения ведут разработку ПО в соответствии со стандартом WBEM. Как следствие, это ПО совместимо и с WMI, а значит, может управляться через единый и удобный интерфейс.

Задание_1:

Посмотрите информацию о физических дисках

```
Get-Command -Module Storage
# выводит сведения о дисках на логическом уровне
Get-Disk
Get-Disk | Where-Object IsSystem -eq $True | fl
Get-Disk | Where-Object IsOffline -Eq $True| ft -AutoSize
# Информацию о физических дисках
Get-PhysicalDisk
Get-Partition
Get-Volume
```





```
PS C:\Users\Администратор.W2019SERV01> Get-Disk | Where-Object IsSystem -eq $True | fl


UniqueId           :      ATAVBOX HARDDISK
Number             : 0
Path               : \\?\scsi#disk&ven_vbox&prod_harddisk#4&2617aeae&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
Manufacturer       :
Model              : VBOX HARDDISK
SerialNumber       : VB878827cc-ed95a5ae
Size               : 50 GB
AllocatedSize      : 53687091200
LogicalSectorSize  : 512
PhysicalSectorSize : 512
NumberOfPartitions : 2
PartitionStyle     : MBR
IsReadOnly         : False
IsSystem           : True
IsBoot             : True
```

```
PS C:\Users\Администратор.W2019SERV01> Get-PhysicalDisk

Number FriendlyName  SerialNumber        MediaType   CanPool OperationalStatus HealthStatus Usage        Size
------ ------------  ------------        ---------   ------- ----------------- ------------ -----        ----
0      VBOX HARDDISK VB878827cc-ed95a5ae Unspecified False   OK                Healthy      Auto-Select 50 GB


PS C:\Users\Администратор.W2019SERV01> Get-Partition


   DiskPath: \\?\scsi#disk&ven_vbox&prod_harddisk#4&2617aeae&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                            1048576                                    549 MB IFS
2                C           576716800                                49.46 GB IFS


PS C:\Users\Администратор.W2019SERV01> Get-Volume

DriveLetter FriendlyName             FileSystemType DriveType HealthStatus OperationalStatus SizeRemaining     Size
----------- ------------             -------------- --------- ------------ ----------------- -------------     ----
D                                    Unknown        CD-ROM    Healthy      Unknown                     0 B      0 B
            Зарезервировано системой NTFS           Fixed     Healthy      OK                  134.31 MB   549 MB
C                                    NTFS           Fixed     Healthy      OK                   27.73 GB 49.46 GB
```

Задание_2:

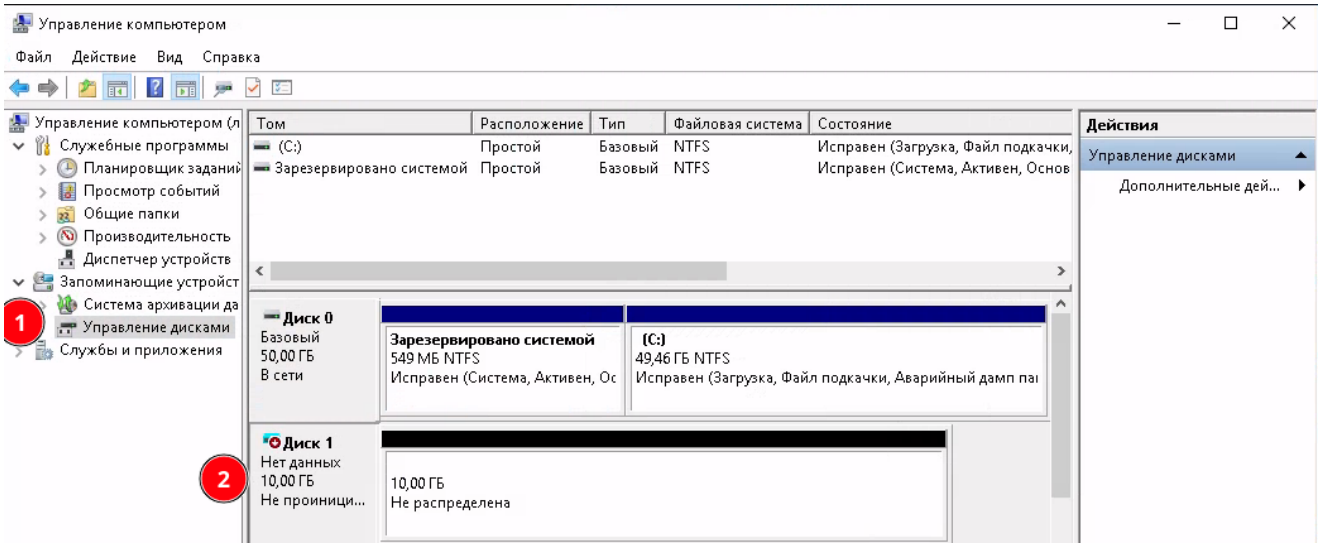
Посмотите список всех логических разделов в Windows

```
# выводит сведения о дисках на логическом уровне
Get-Disk
Get-Disk | Where-Object IsSystem -eq $True | fl
```

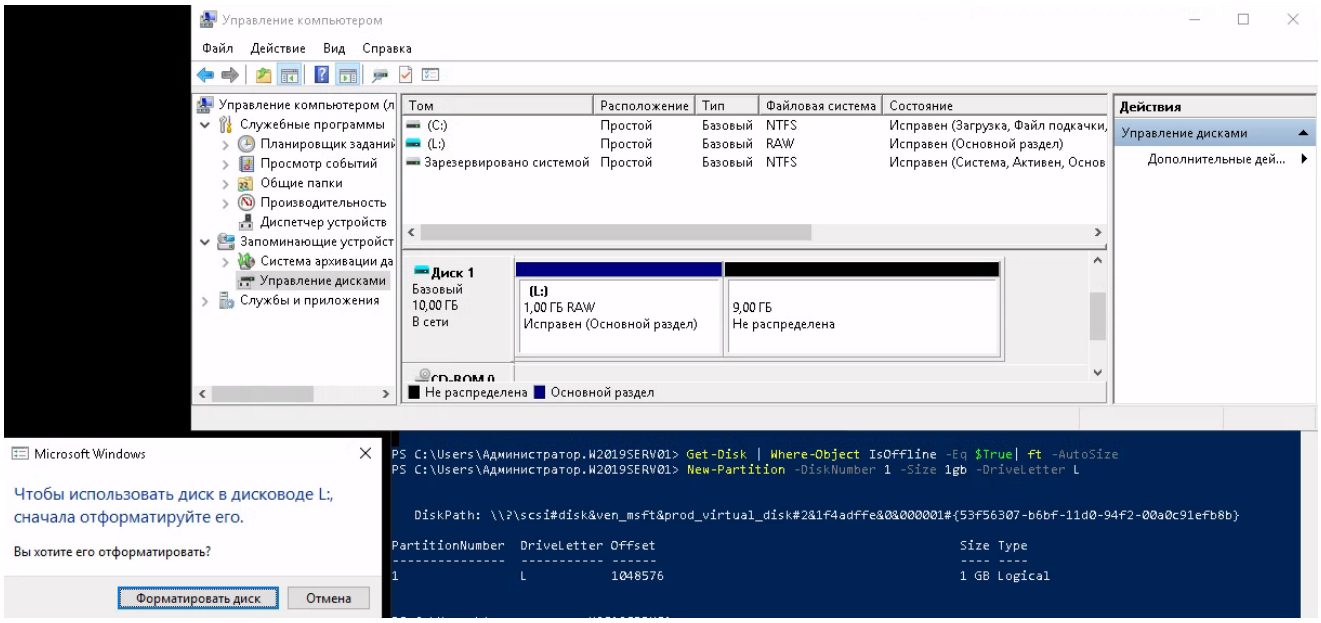
```
PS C:\Users\Администратор.W2019SERV01> Get-Disk

Number Friendly Name Serial Number                    HealthStatus         OperationalStatus      Total Size Partition
                                                                                                   Style
------ ------------ -------------                    ------------         -----------------      ---------- ----------
0      VBOX HARDDISK VB878827cc-ed95a5ae              Healthy              Online                      50 GB MBR


PS C:\Users\Администратор.W2019SERV01> Get-Disk | Where-Object IsSystem -eq $True | fl


UniqueId           :      ATAVBOX HARDDISK
Number             : 0
Path               : \\?\scsi#disk&ven_vbox&prod_harddisk#4&2617aeae&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
Manufacturer       :
Model              : VBOX HARDDISK
SerialNumber       : VB878827cc-ed95a5ae
```

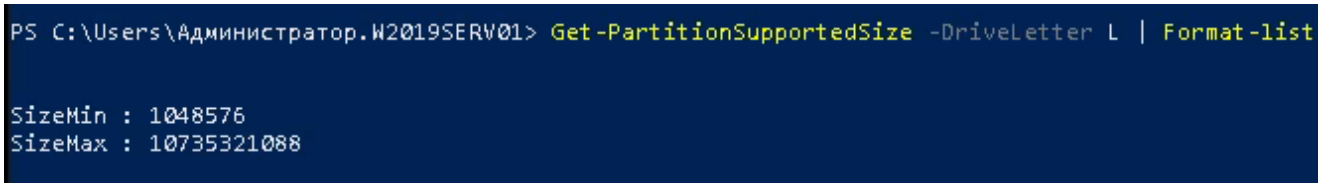
Задание_3:

Создайте раздел на диске объемом 1 Гб




```
# Инициализация
Get-Disk | Where-Object IsOffline -Eq $True| ft -AutoSize
New-Partition -DiskNumber 1 -Size 1gb -DriveLetter L
Initialize-Disk 1 -PartitionStyle MBR
Get-PartitionSupportedSize -DriveLetter L | Format-list
# Максимальный раздел
New-Partition -DiskNumber 1 -AssignDriveLetter -UseMaximumSize
$MaxSize = (Get-PartitionSupportedSize -DriveLeter L).SizeMax
Resize-Partition -DriverLetter -L -Size $MaxSize
Format-Volume -DriveLetter L -FileSystem NTFS -NewFileSystemLabel DBData -
Confirm:$false
# Format
Format-Volume -DriveLetter L -FileSystem NTFS -NewFileSystemLabel DBData -
Confirm:$false
```



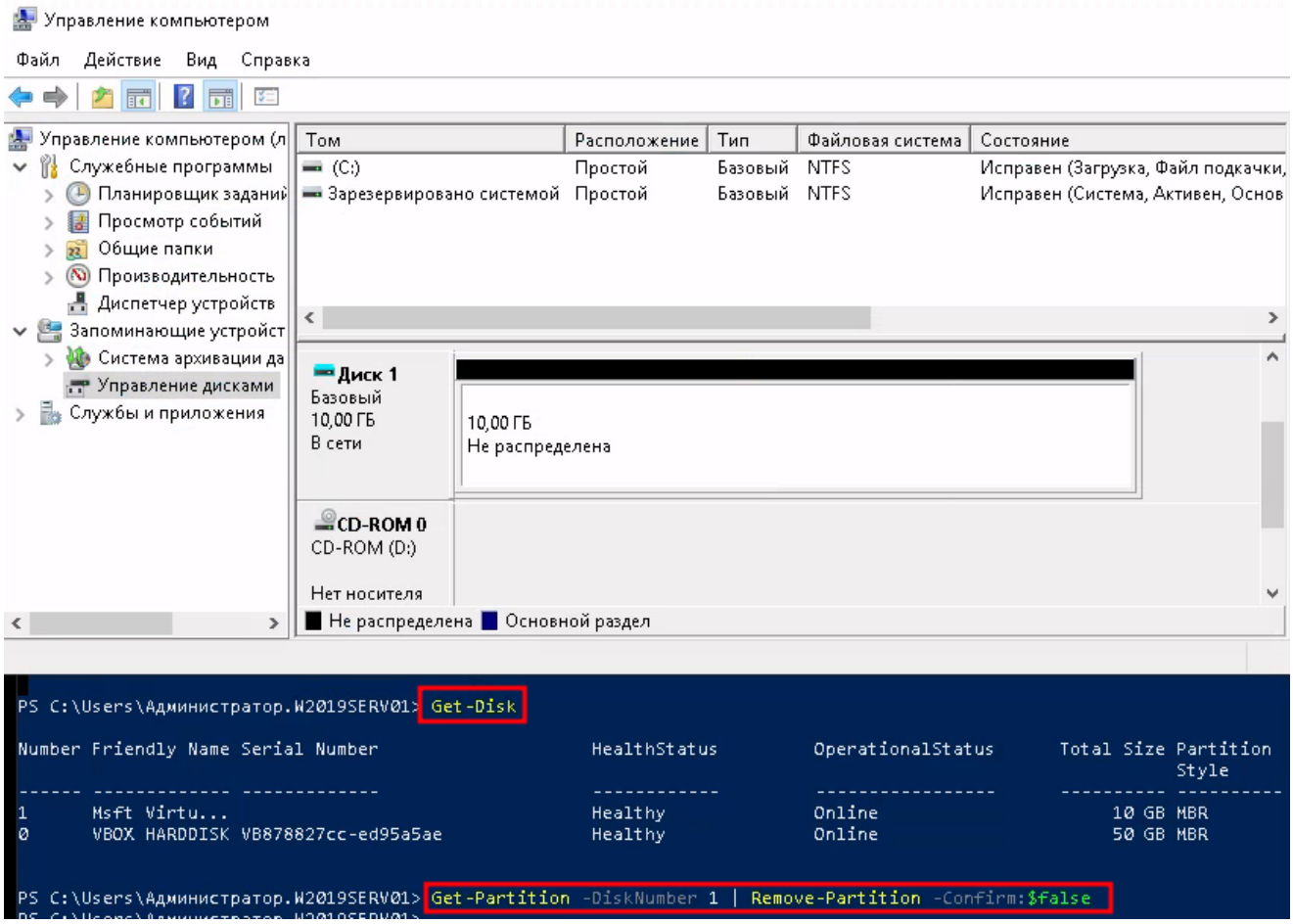


```
PS C:\Users\Администратор.W2019SERV01> New-Partition -DiskNumber 1 -AssignDriveLetter -UseMaximumSize


   DiskPath: \\?\scsi#disk&ven_msft&prod_virtual_disk#2&1f4adffe&0&000001#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
2                E           1074790400                                    9 GB Logical


PS C:\Users\Администратор.W2019SERV01> Format-Volume -DriveLetter L -FileSystem NTFS -NewFileSystemLabel DBData -Confirm
:$false

DriveLetter FriendlyName FileSystemType DriveType HealthStatus OperationalStatus SizeRemaining    Size
----------- ------------ -------------- --------- ------------ ----------------- -------------    ----
L           DBData       NTFS           Fixed     Healthy      OK                      1007.15 MB 1024 MB
```

Задание_4:

Удалите ранее созданный раздел на диске

```
Get-Partition -DiskNumber 1 | Remove-Partition -Confirm:$false
```



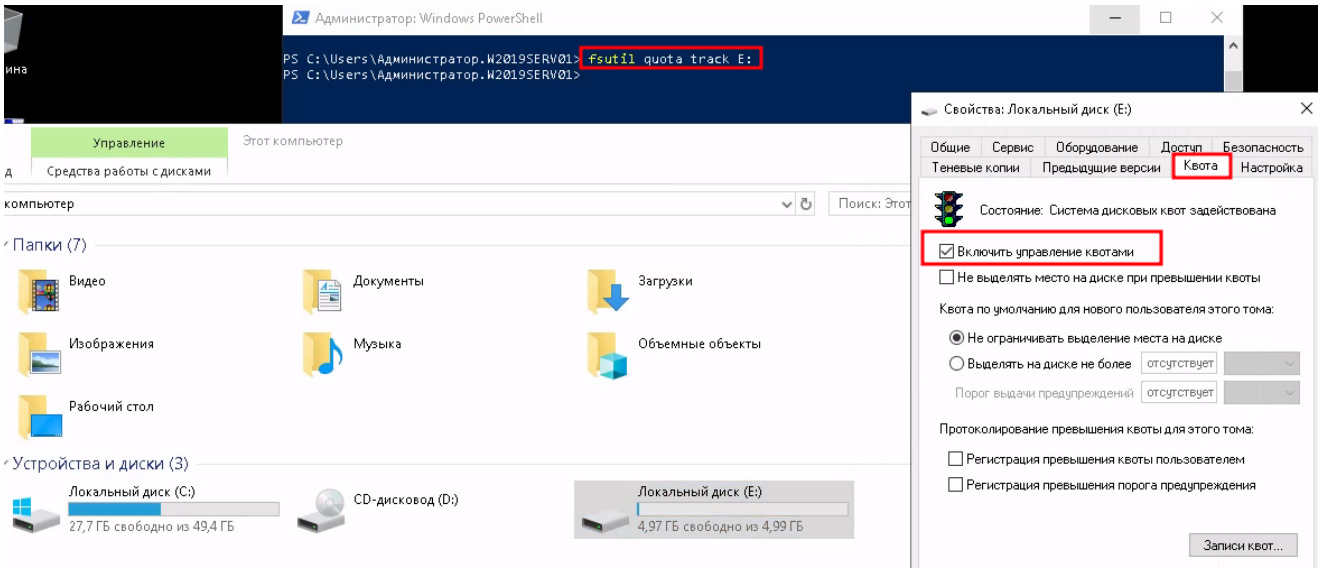
Задание_5:

- Включите мягкую квоту на диске C
- Измените порог квоты для пользователя Администратор

```
PS C:\Users\Администратор.W2019SERV01> Get-Disk

Number Friendly Name Serial Number                  HealthStatus         OperationalStatus      Total Size Partition
                                                                                                           Style
------ ------------- -------------                  ------------         -----------------      ---------- ----------
1      Msft Virtu...                                Healthy              Online                      10 GB MBR
0      VBOX HARDDISK VB878827cc-ed95a5ae            Healthy              Online                      50 GB MBR
```

```
Initialize-Disk Number 1
New-Partition -DiskNumber 1 -Size 5gb -DriveLetter E
Format-Volume -DriveLetter E -FileSystem NTFS -Confirm:$false

fsutil quota track E:
fsutil quota disable E:
fsutil quota track E:
fsutil quota query E:

fsutil quota violations
# 3gb и придупреждение при 2gb Администратор
fsutil quota modify E: 30000000000 20000000000 администратор
fsutil behavior query quotanotify
```

```
PS C:\Users\Администратор.W2019SERV01> New-Partition -DiskNumber 1 -Size 5gb -DriveLetter E


   DiskPath: \\?\scsi#disk&ven_msft&prod_virtual_disk#2&1f4adffe&0&000002#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                E           1048576                                       5 GB Logical
```




```
PS C:\Users\Администратор.W2019SERV01> fsutil quota query E:
FileSystemControlFlags = 0x00000001
    Квоты на данном томе протоколируются
    Регистрация событий квотирования не включена
    Значения квот обновлены

Пороговое значение квоты по умолчанию = 0xffffffffffffffff
Предел квоты по умолчанию             = 0xffffffffffffffff

Имя ИД безопасности = BUILTIN\Администраторы (Псевдоним)
Время изменения           = 15 февраля 2024 г.    13:08:43
Использованная квота      = 70656
Пороговое значение квоты = 18446744073709551615
Предел квоты              = 18446744073709551615

Имя ИД безопасности = NT AUTHORITY\NETWORK SERVICE (Известная группа)
Время изменения           = 15 февраля 2024 г.    13:14:25
Использованная квота      = 1024
Пороговое значение квоты = 18446744073709551615
Предел квоты              = 18446744073709551615

Имя ИД безопасности = NT AUTHORITY\СИСТЕМА (Известная группа)
Время изменения           = 15 февраля 2024 г.    13:14:25
Использованная квота      = 6294528
Пороговое значение квоты = 18446744073709551615
Предел квоты              = 18446744073709551615
```

```
PS C:\Users\Администратор.W2019SERV01> fsutil quota violations
Поиск в журнале событий "System"...
Поиск в журнале событий "Application"...
Нарушений квоты не обнаружено
```

```
PS C:\Users\Администратор.W2019SERV01> fsutil quota modify E: 30000000000 20000000000 администратор
```

```
PS C:\Users\Администратор.W2019SERV01> fsutil behavior query quotanotify
QuotaNotify = 3600  (Секунды)
```

Задание_6:

Установите модуль Дедуплекации

Установите минимум для дедуплекации для файлов в 1GB

```
Install-WindowsFeature -Name "FS-Data-Deduplication" -IncludeAllSubFeature
-IncludeManagementTools
Get-Command -Module Deduplication
Enable-DedupVolume -Volume 'E:\' -UsageType 'Default'
```

```powershell
Get-DedupVolume

# Ограничения. Минимум для дедуплекации для файлов в 1GB
New-Item -Path "E:\Folder1", "E:\Folder2" -ItemType Directory

Set-DedupVolume `
-Volume 'E:' `
-MinimumFileSize 1GB `
-ExcludeFolder 'E:\Folder1', 'E:\Folder2' `
-ExcludeFileType "txt", "rar" `
-MinimumFileAge 15
Get-DedupVolume | Select *

# Далее
Disable-DedupVolume -Volume 'E:'
Enable-DedupVolume -Volume 'E:' -UsageType 'Default'
```

```
PS C:\Users\Администратор.W2019SERV01> Install-WindowsFeature -Name "FS-Data-Deduplication" -IncludeAllSubFeature -Inclu
deManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Дедупликация данных}
```

```
PS C:\Users\Администратор.W2019SERV01> Get-Command -Module Deduplication

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Disable-DedupVolume                                2.0.0.0    Deduplication
Function        Enable-DedupVolume                                 2.0.0.0    Deduplication
Function        Expand-DedupFile                                   2.0.0.0    Deduplication
Function        Get-DedupJob                                       2.0.0.0    Deduplication
Function        Get-DedupMetadata                                  2.0.0.0    Deduplication
Function        Get-DedupSchedule                                  2.0.0.0    Deduplication
Function        Get-DedupStatus                                    2.0.0.0    Deduplication
Function        Get-DedupVolume                                    2.0.0.0    Deduplication
Function        Measure-DedupFileMetadata                          2.0.0.0    Deduplication
Function        New-DedupSchedule                                  2.0.0.0    Deduplication
Function        Remove-DedupSchedule                               2.0.0.0    Deduplication
Function        Set-DedupSchedule                                  2.0.0.0    Deduplication
Function        Set-DedupVolume                                    2.0.0.0    Deduplication
Function        Start-DedupJob                                     2.0.0.0    Deduplication
Function        Stop-DedupJob                                      2.0.0.0    Deduplication
Function        Update-DedupStatus                                 2.0.0.0    Deduplication
```

```
PS C:\Users\Администратор.W2019SERV01> Enable-DedupVolume -Volume 'E:\' -UsageType 'Default'

Enabled           UsageType         SavedSpace        SavingsRate       Volume
-------           ---------         ----------        -----------       ------
True              Default           0 B               0 %               E:
```

```
PS C:\Users\Администратор.W2019SERV01> Get-DedupVolume

Enabled           UsageType         SavedSpace        SavingsRate       Volume
-------           ---------         ----------        -----------       ------
True              Default           0 B               0 %               E:
```

```
PS C:\Users\Администратор.W2019SERV01> New-Item -Path "E:\Folder1", "E:\Folder2" -ItemType Directory


    Каталог: E:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       15.02.2024     16:39                Folder1
d-----       15.02.2024     16:39                Folder2
```

```
PS C:\Users\Администратор.W2019SERV01> Set-DedupVolume `
>> -Volume 'E:' `
>> -MinimumFileSize 1GB `
>> -ExcludeFolder 'E:\Folder1', 'E:\Folder2' `
>> -ExcludeFileType "txt", "rar" `
>> -MinimumFileAge 15
PS C:\Users\Администратор.W2019SERV01> Get-DedupVolume | Select *


ObjectId                : \\?\Volume{2bfc75fa-0000-0000-0000-100000000000}\
UsageType               : Default
AutoStart               : False
Capacity                : 5368705024
ChunkIndexCacheVolume   :
ChunkRedundancyThreshold : 100
DataAccessEnabled       : True
Enabled                 : True
ExcludeFileType         : {txt, rar}
ExcludeFileTypeDefault  : {edb, jrs}
ExcludeFolder           : {\Folder1, \Folder2}
FreeSpace               : 5339492352
IdleTimeoutDefault      : 60
InputOutputScale        : 0
MinimumFileAgeDays      : 15
MinimumFileSize         : 1073741824
NearInlineMode          : False
NoCompress              : False
NoCompressionFileType   : {asf, mov, wma, wmv...}
OptimizeInUseFiles      : False
OptimizePartialFiles    : False
SavedSpace              : 0
SavingsRate             : 0
UnoptimizedSize         : 29212672
UsedSpace               : 29212672
Verify                  : False
Volume                  : E:
VolumeId                : \\?\Volume{2bfc75fa-0000-0000-0000-100000000000}\
PSComputerName          :
CimClass                : ROOT/Microsoft/Windows/Deduplication:MSFT_DedupVolume
CimInstanceProperties   : {AutoStart, Capacity, ChunkIndexCacheVolume, ChunkRedundancyThreshold...}
CimSystemProperties     : Microsoft.Management.Infrastructure.CimSystemProperties
```

Задание_7:

- Настройте расписание таким образом, что бы процесс GarbageCollection запускался в пятницу в 22:00
- Удалите созданное расписание

```
Get-DedupSchedule

Set-DedupSchedule `
-Name 'WeeklyGarbageCollection' `
-Type 'GarbageCollection' `
-Enabled $True `
-StopWhenSystemBusy $True `
-Days 'Friday' `
-Start 22:00 `
```

```
Get-DedupSchedule

New-DedupSchedule `
-Name 'Оптимизация по будням' `
-Cores 80 `
-Days Monday,Tuesday,Wednesday,Thursday,Friday `
-DurationHours 8 `
-InputOutputThrottleLevel Medium `
-Priority Normal `
-Memory 80 `
-Start 21:00 `
-Type 'Optimization' `
-StopWhenSystemBusy `

New-DedupSchedule `
- Name 'Оптимизация по будням' `
- Cores 80 `
- Days Monday, Tuesday, Wednesday, Thursday, Friday `
- DurationHours 8 `
- InputOutputThrottleLevel Medium `
- Priority Normal `
- Memory 80 `
- Start 22:00 `
- Type 'Optimization' `
- StopWhenSystemBusy `

Get-DedupSchedule

Remove-DedupSchedule -Name '*опт*'

New-DedupSchedule -Type Unoptimization
```

```
PS C:\Users\Администратор.W2019SERV01> Get-DedupSchedule

Enabled    Type               StartTime             Days              Name
-------    ----               ---------             ----              ----
True       Optimization                                               BackgroundOptimization
True       GarbageCollection  2:45                  Saturday          WeeklyGarbageCollection
True       Scrubbing          3:45                  Saturday          WeeklyScrubbing
```

```
PS C:\Users\Администратор.W2019SERV01> Set-DedupSchedule `
>> -Name 'WeeklyGarbageCollection' `
>> -Type 'GarbageCollection' `
>> -Enabled $True `
>> -StopWhenSystemBusy $True `
>> -Days 'Friday' `
>> -Start 22:00 `
>>
PS C:\Users\Администратор.W2019SERV01> Get-DedupSchedule

Enabled    Type               StartTime             Days              Name
-------    ----               ---------             ----              ----
True       Optimization                                               BackgroundOptimization
True       GarbageCollection  22:00                 Friday            WeeklyGarbageCollection
True       Scrubbing          3:45                  Saturday          WeeklyScrubbing
```

```
PS C:\Users\Администратор.W2019SERV01> New-DedupSchedule `
>> -Name 'Оптимизация по будням' `
>> -Cores 80 `
>> -Days Monday,Tuesday,Wednesday,Thursday,Friday `
>> -DurationHours 8 `
>> -InputOutputThrottleLevel Medium `
>> -Priority Normal `
>> -Memory 80 `
>> -Start 21:00 `
>> -Type 'Optimization' `
>> -StopWhenSystemBusy `
>>

Enabled    Type              StartTime            Days              Name
-------    ----              ---------            ----              ----
True       Optimization      21:00                {Monday, Tuesda... Оптимизация по будням


PS C:\Users\Администратор.W2019SERV01> Get-DedupSchedule

Enabled    Type              StartTime            Days              Name
-------    ----              ---------            ----              ----
True       Optimization                                             BackgroundOptimization
True       GarbageCollection 22:00                Friday            WeeklyGarbageCollection
True       Scrubbing         3:45                 Saturday          WeeklyScrubbing
True       Optimization      21:00                {Monday, Tuesda... Оптимизация по будням
```

```
PS C:\Users\Администратор.W2019SERV01> Remove-DedupSchedule -Name '*опт*'
PS C:\Users\Администратор.W2019SERV01> Get-DedupSchedule

Enabled    Type              StartTime            Days              Name
-------    ----              ---------            ----              ----
True       Optimization                                             BackgroundOptimization
True       GarbageCollection 22:00                Friday            WeeklyGarbageCollection
True       Scrubbing         3:45                 Saturday          WeeklyScrubbing
```

```
PS C:\Users\Администратор.W2019SERV01> New-DedupSchedule -Type Unoptimization

Командлет New-DedupSchedule в конвейере команд в позиции 1
Укажите значения для следующих параметров:
Name: 1

Enabled    Type              StartTime            Days              Name
-------    ----              ---------            ----              ----
True       Unoptimization    1:45                 {Sunday, Monday... 1
```

Задание_8:

- Используя wmi посмотрите запущенные процессы в системе
- Запустите процесс cmd и с помощью wmi остановите его
- Создайте GPO, WMI фильтр которой будет применяться к Windows 10

Обзор средств работы с WMI для администратора

Разделим набор утилит на поставляемые с операционной системой по умолчанию и набор утилит, которые потребуется скачивать с сайта компании Microsoft. К первой категории относятся следующие утилиты:

• wmimgmt.msc – оснастка консоли MMC, позволяющая в целом управлять самой системой WMI на выбранном компьютере.

• Winmgmt.exe – консольная утилита управления WMI. Выполняет аналогичные действия, что и консоль MMC wmimgmt.msc.

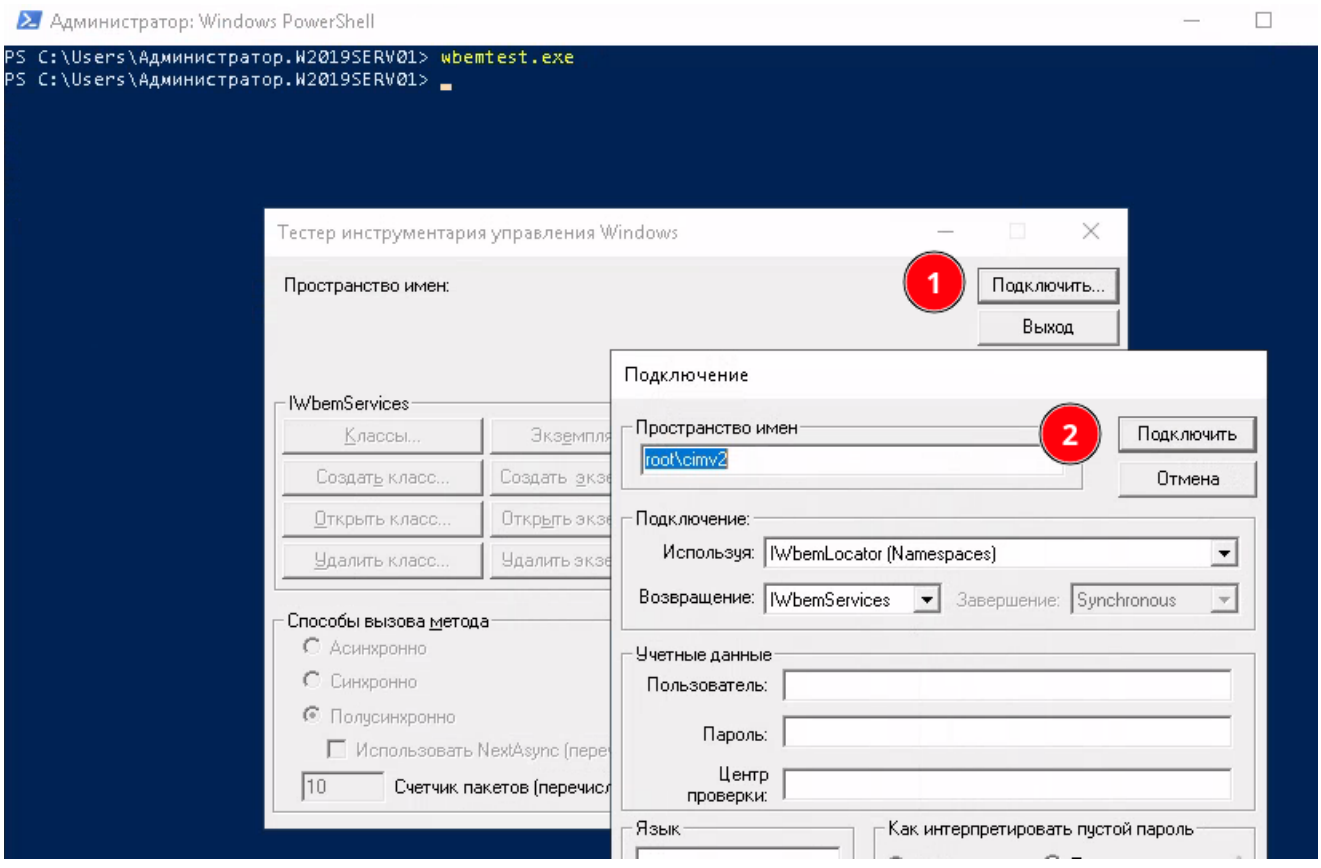
• Wbemtest.exe – графическая утилита для интерактивной работы с WMI. Удобна для тестирования классов и методов, просмотра свойств и т. п.

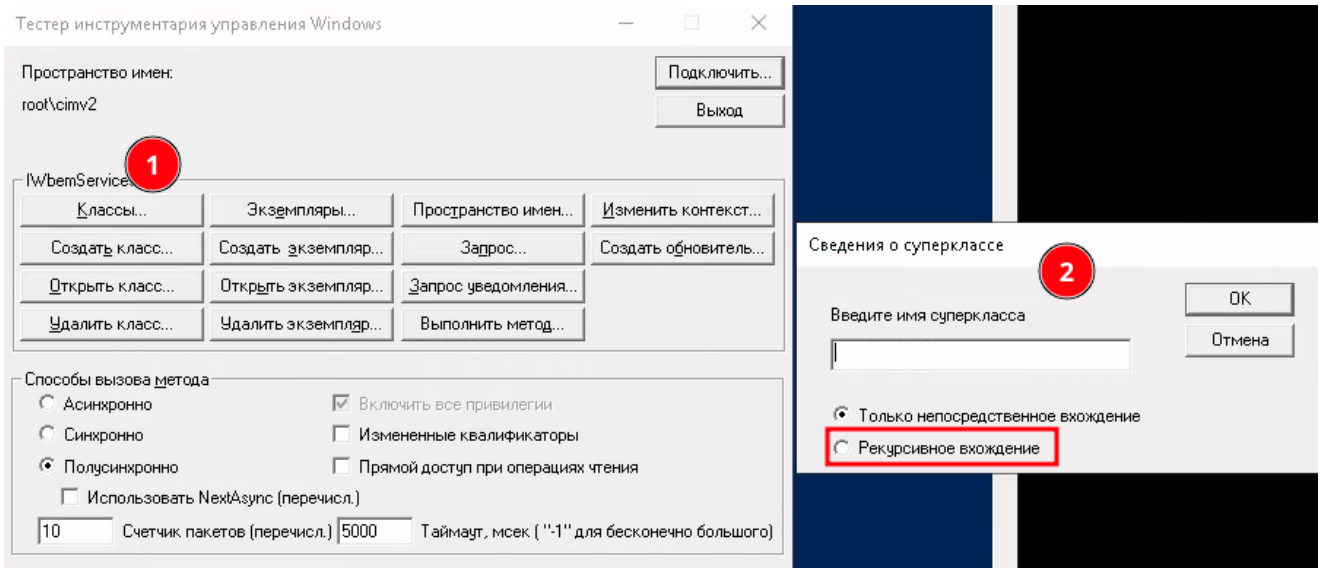
• Wmic.exe – консольная утилита для вызова объектов и методов WMI (WMI Console).
• mofcomp.exe – компилятор MOF-файлов. Служит для расширения репозитория WMI и тонких операций с библиотекой классов WMI, а также для «ремонта» нарушенного репозитория.
• WMI Code Creator 1.0 – очень удобная и полезная утилита для создания готовых сценариев WMI. Поддерживает языки Visual Basic Script, C# и Visual Basic .NET .

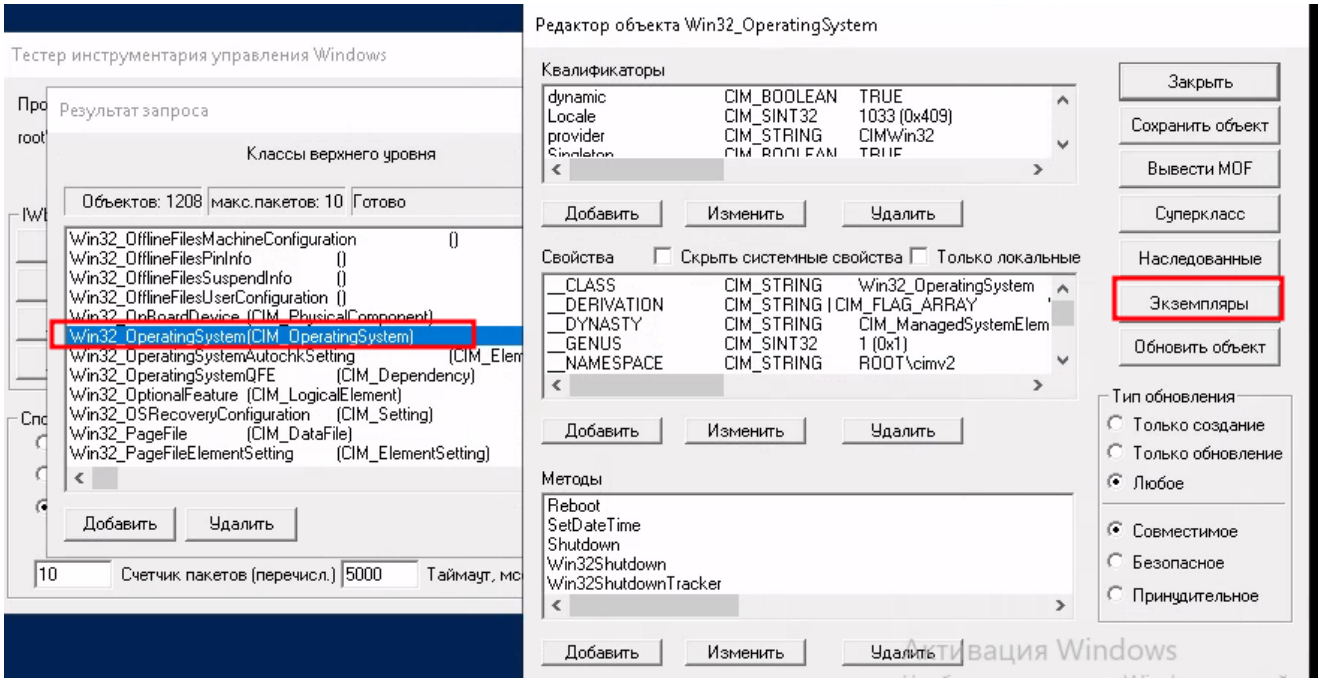
Ко второй категории средств для работы с WMI, которые требуется дополнительно устанавливать, относится:
• WMI Administrative Tools – комплект средств в составе: WMI CIM Studio, WMI Event Registration, WMI Event Viewer и WMI Object Browser). Удобная среда разработки и тестирования WMI-классов и методов .
• Scriptomatic 2.0 – мастер в формате Hyper Text Application (HTA). Удобна для создания готовых сценариев и на различных скриптовых языках. Поддерживает Visual Basic Script, Perl, Java Script и Python .
• Tweakomatic Utility – утилита в формате Hyper Text Application (HTA). Содержит множество настроек системы, обычно доступных через утилиты-твикеры, для которых позволяет сгенерировать WMI-скрипты для их автоматической настройки. Весьма полезна при разработке сценариев автоматизированной установки и настройки

Запускаем:

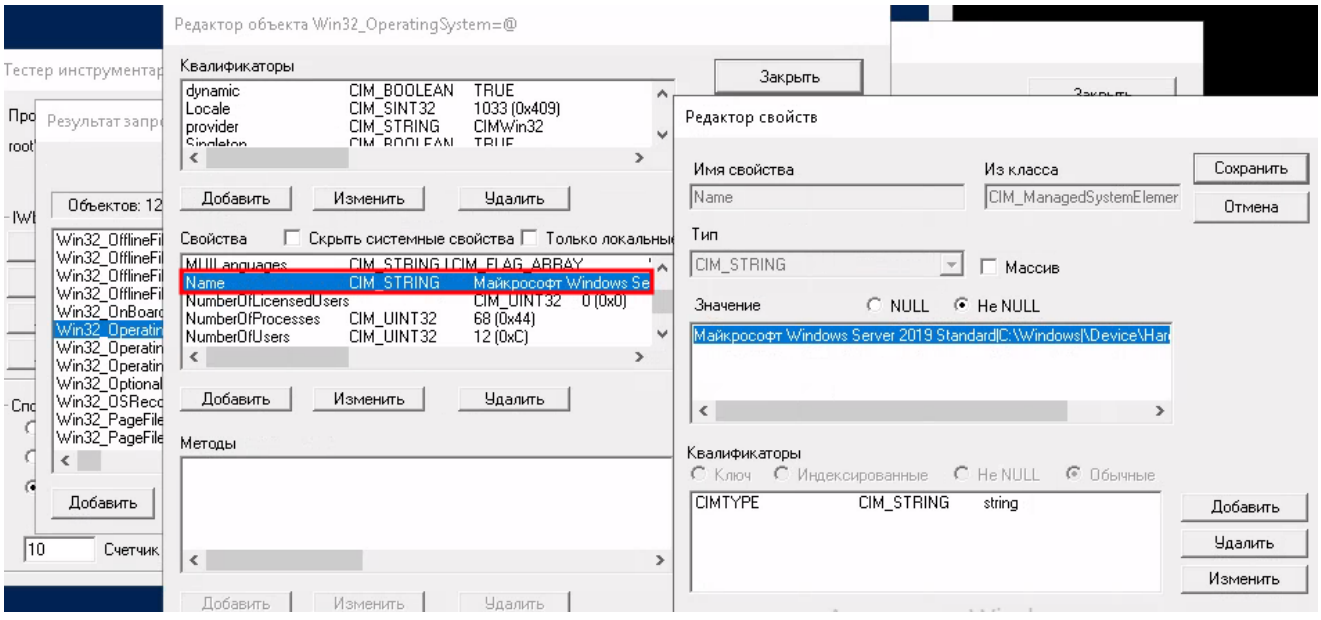
```
wbemtest.exe
```



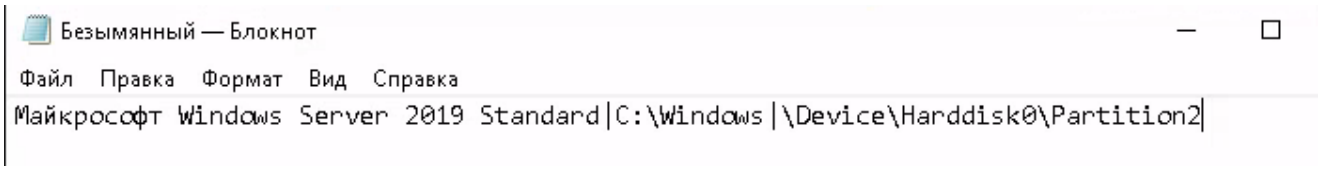




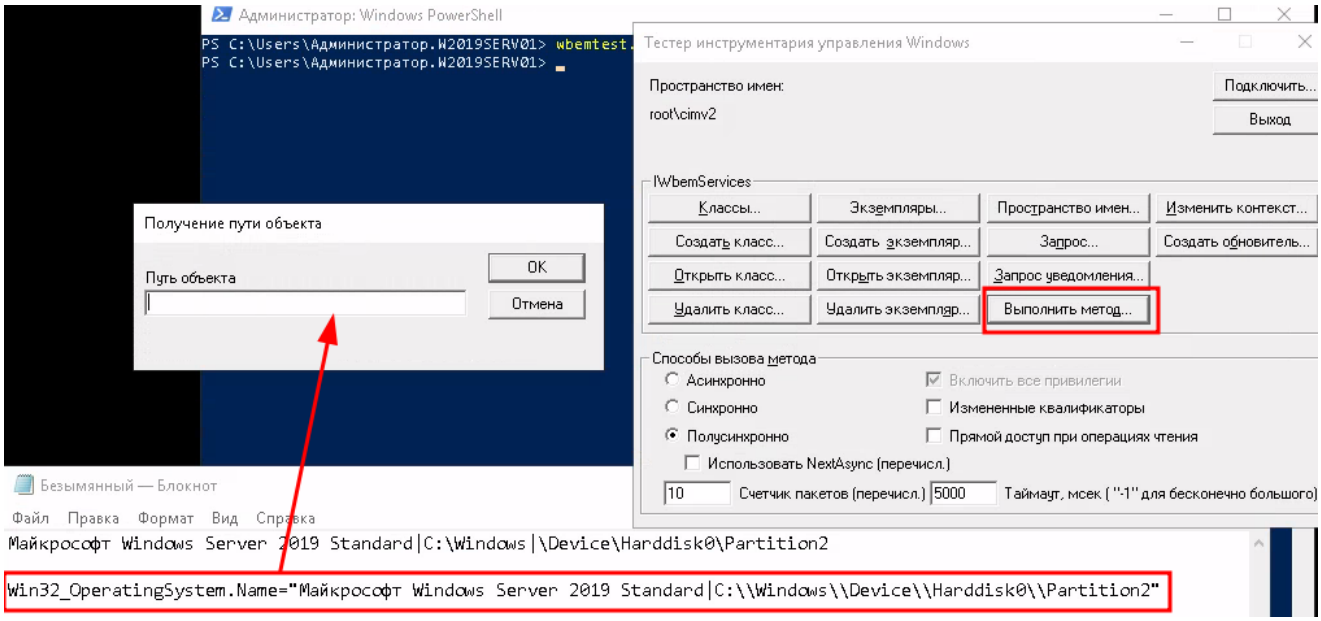
Экземпляры: 2 раза кликнуть

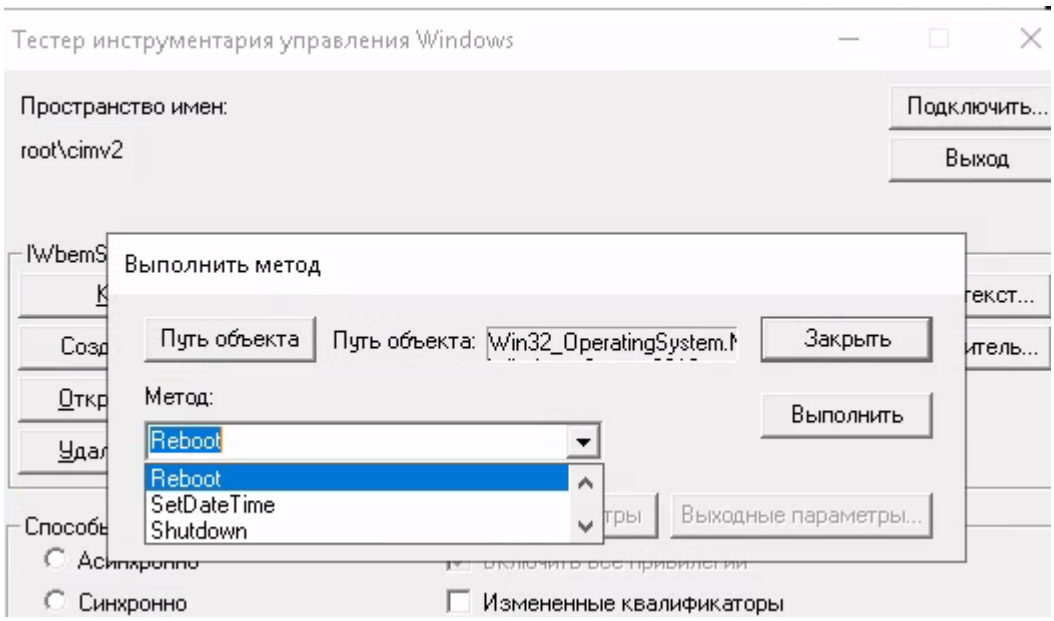


Сохранить в *Блокноте*

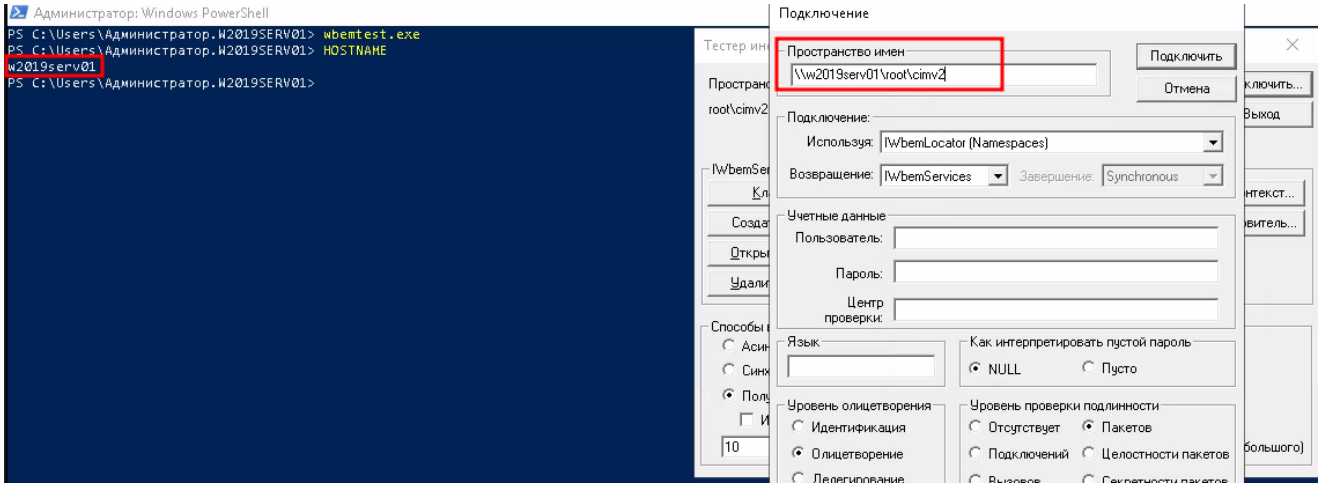



```
Майкрософт Windows Server 2019
Standard|C:\Windows|\Device\Harddisk0\Partition2

Win32_OperatingSystem.Name="Майкрософт Windows Server 2019
Standard|C:\\Windows\\Device\\Harddisk0\\Partition2"
```



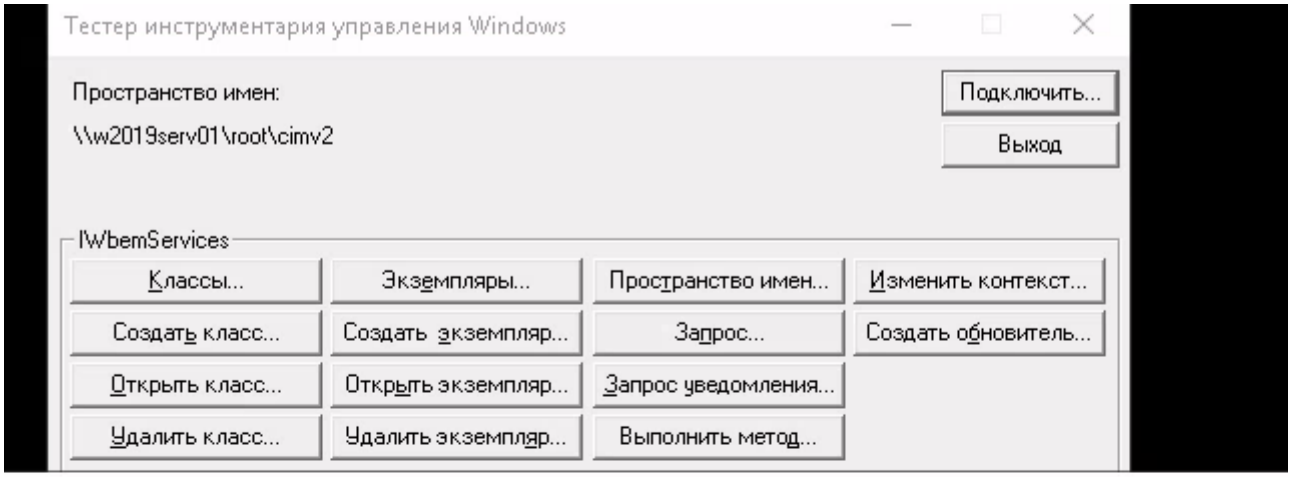


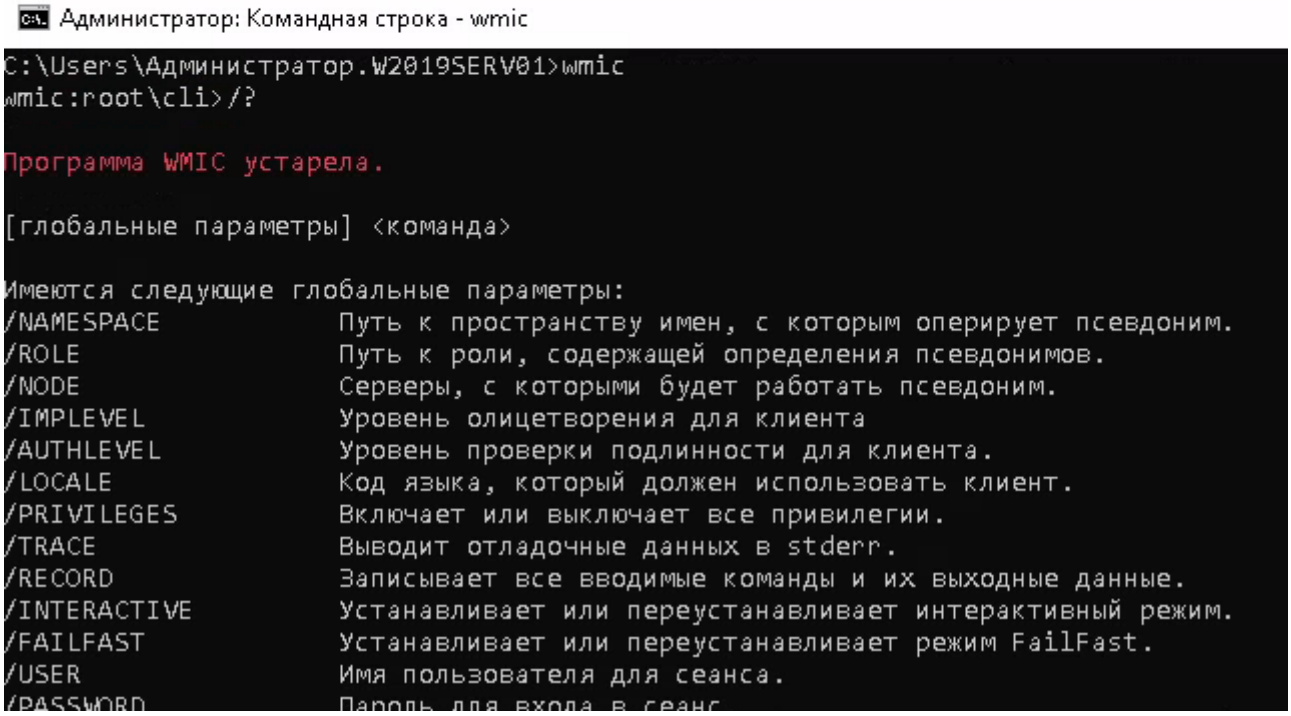
Подключимся удалено (на примере, сами к себе):



CMD - WMIC

```
C:\Users\Администратор.W2019SERV01>wmic
wmic:root\cli>/?
wmic:root\cli>process list /?
```





Классы, объекты, свойства и методы

Поскольку WMI построена по объектно-ориентированному принципу, то все данные об операционной системе, ее свойствах, управляемых приложениях и обнаруженном оборудовании представлены в виде объектов. Каждый тип объекта описан классом, в состав которого входят свойства и методы. Определения классов описаны в MOF-файлах, а объекты этих классов с заполненными свойствами и доступными методами при их вызове возвращаются WMI-провайдерами. Управляет созданием и удалением объектов, а также вызовом их методов служба CIM Object Manager.

Получается, что если мы хотим управлять настройками сетевого адаптера, то мы должны запросить у CIM Object Manager экземпляр объекта нужного нам сетевого адаптера (этот объект принадлежит классу Win32_NetworkAdapterConfiguration) и вызвать нужные нам методы. В частности, для того чтобы обновить аренду адреса на DHCP сервере, достаточно вызвать метод RenewDHCPLease экземпляра объекта Win32_NetworkAdapterConfiguration.

Список псевдонимов утилиты WMIC и соответствие их классам WMI

Псевдоним	Описание
BASEBOARD	Управление материнской платой, она также называется motherboard, или системная плата.
BIOS	Управления базовыми сервисами ввода/вывода (Basic input/output services, BIOS).
BOOTCONFIG	Управление конфигурацией загрузки (Boot configuration management).
CDROM	Управление приводом CD-ROM.
COMPUTERSYSTEM	Управление системой компьютера.
CPU	Управление процессовром.
CSPRODUCT	Получение от SMBIOS информации о компьютере как системном продукте.
DATAFILE	Управление данными файлов (DataFile Management).
DCOMAPP	Управление приложениями (DCOM Application management).
DESKTOP	Управление рабочим столом пользователя (User's Desktop management).
DESKTOPMONITOR	Desktop Monitor management
DEVICEMEMORYADDRESS	Управление адресами памяти устройств (Device memory addresses management).
DISKDRIVE	Управление диском на физическом уровне (Physical disk drive management).
DISKQUOTA	Управление квотами NTFS пространства диска (Disk space usage for NTFS volumes).
DMACHANNEL	Управление каналами прямого доступа к памяти (Direct memory access, DMA channel management).
ENVIRONMENT	Управление настройками системного окружения (System environment settings management)

FSDIR	Управление директориями файловой системы (Filesystem directory entry management).	Win32_Directory
GROUP	Управление группами учетных записей (Group account management).	Win32_Group
IDECONTROLLER	Управление контролером диска IDE (IDE Controller management).	Win32_IDEController
IRQ	Управление сигналами прерываний (Interrupt request line, IRQ management).	Win32_IRQResource
JOB	Предоставляет доступ к назначенным заданиям (jobs scheduled) с использованием службы назначенных заданий (schedule service).	Win32_ScheduledJob
LOADORDER	Управление службами системы, которые задают зависимости запуска (execution dependencies).	Win32_LoadOrderGroup

Рассмотрим различные примеры WMI фильтров GPO, который чаще всего используются. С помощью WMI фильтра вы можете выбрать тип ОС:
ProductType=1 – любая клиенская ОС
ProductType=2 – контроллер домена AD
ProductType=3 – серверная ОС (Windows Server)

Версии Windows:
Windows Server 2016, 2019 и Windows 10 — 10.%

Посмотрите запущенные процессы в системе

```
wmic:root\cli>exit
C:\Users\Администратор.W2019SERV01>

wmic process call /?
wmic process list brief
wmic process list brief | find "cmd.exe"
wmic process where description="cmd.exe" list brief
wmic process call /?
```

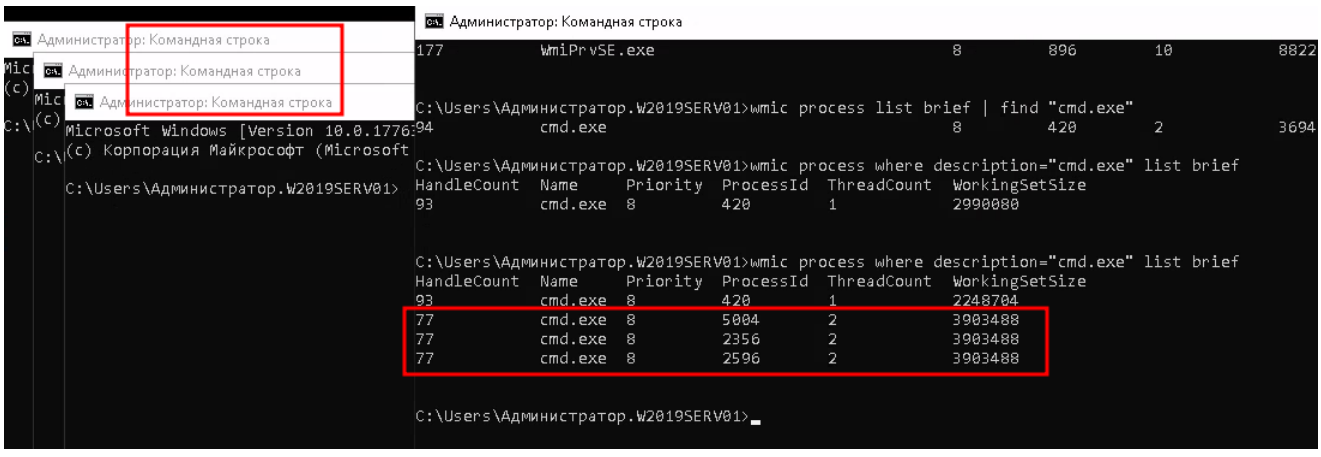
```
C:\Users\Администратор.W2019SERV01>wmic process call /?

Вызов методов.
Использование:

CALL <имя_метода> [<список_фактических_параметров>]
ПРИМЕЧАНИЕ. <список_фактических_параметров> ::= <фактический_параметр> | <фактический_параметр>,  <список_фактических_параметров>

Для псевдонима доступны следующие команды и методы:

Вызов                  [ вх/исх ]Парам_и_&тип                Состояние
=====                  ======================                =========
AttachDebugger                                               (null)


Create                 [IN ]CommandLine(STRING)              (null)

                       [IN ]CurrentDirectory(STRING)

                       [IN ]ProcessStartupInformation(OBJECT)

                       [OUT]ProcessId(UINT32)

GetOwner               [OUT]Domain(STRING)                   (null)

                       [OUT]User(STRING)

GetOwnerSid            [OUT]Sid(STRING)                      (null)

SetPriority            [IN ]Priority(SINT32)                 (null)

Terminate              [IN ]Reason(UINT32)                   (null)
```

```
Администратор: Командная строка
wmic:root\cli>exit

C:\Users\Администратор.W2019SERV01>wmic process list brief
HandleCount  Name                                Priority  ProcessId  ThreadCount  WorkingSetSize
0            System Idle Process                 0         0          1            8192
2124         System                              8         4          99           135168
0            Registry                            8         68         4            75149312
56           smss.exe                            11        260        2            1163264
331          csrss.exe                           13        352        9            5369856
172          wininit.exe                         13        428        1            7143424
```

```
C:\Users\Администратор.W2019SERV01>wmic process list brief | find "cmd.exe"
94           cmd.exe                             8         420        2            3694592

C:\Users\Администратор.W2019SERV01>wmic process where description="cmd.exe" list brief
HandleCount  Name     Priority  ProcessId  ThreadCount  WorkingSetSize
93           cmd.exe  8         420        1            2990080
```

Запустите процесс cmd и с помощью wmi остановите его

```
wmic process where description="cmd.exe" list brief
wmic process where processid='2356' call terminate(0)
wmic process where processid='2356' call terminate(0)
```

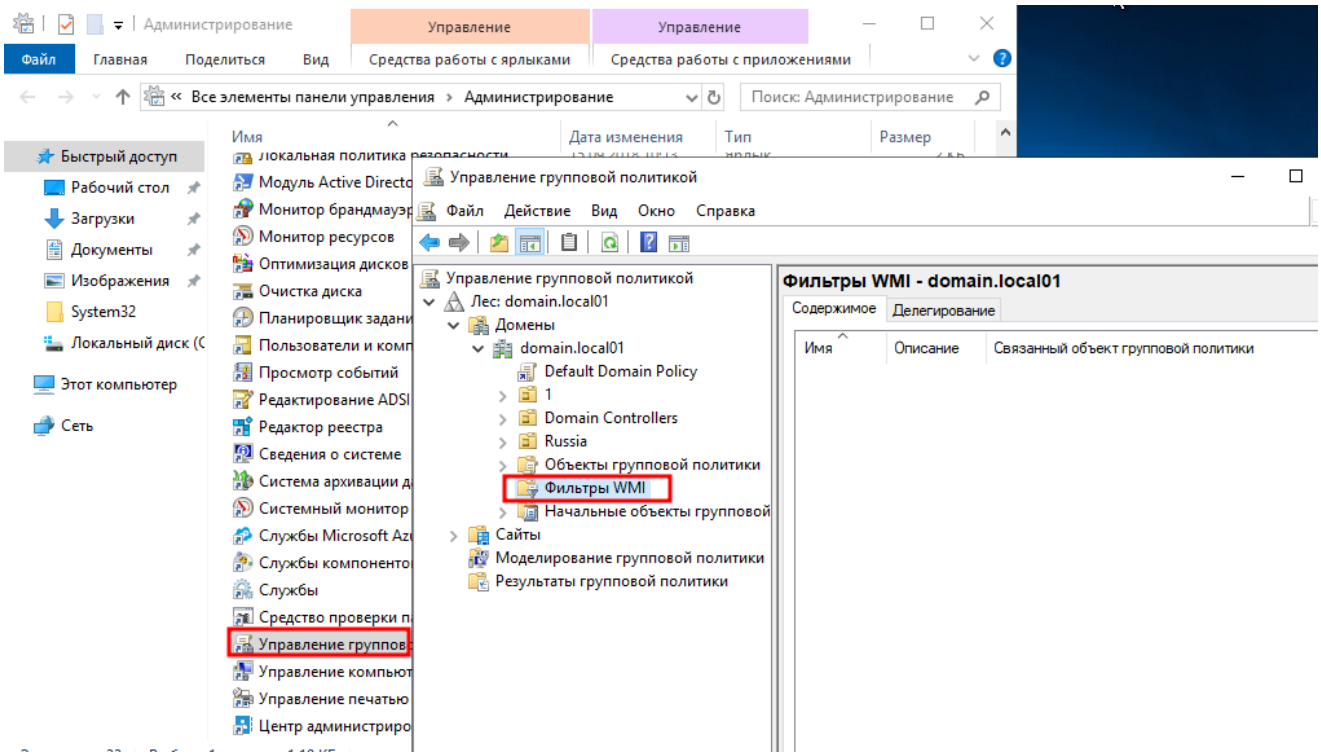


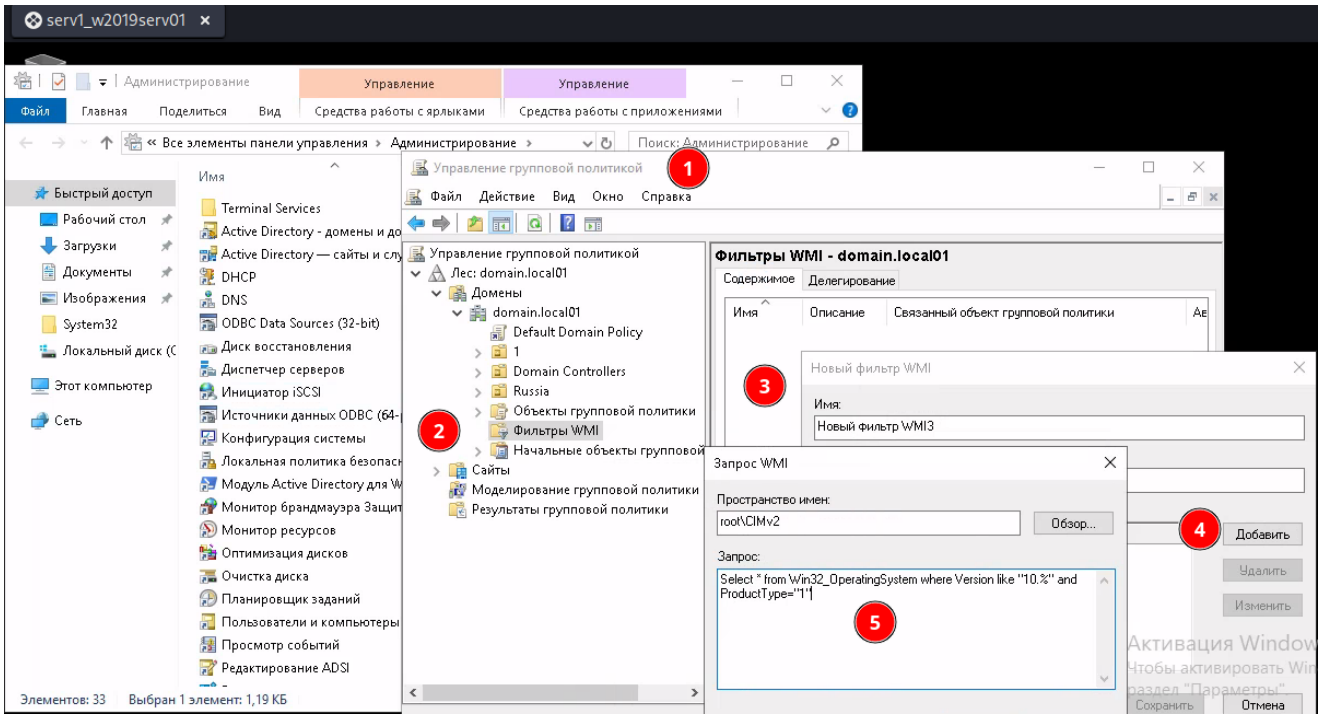
```
C:\Users\Администратор.W2019SERV01>wmic process where description="cmd.exe" list brief
HandleCount  Name     Priority  ProcessId  ThreadCount  WorkingSetSize
93           cmd.exe  8         420        1            2248704
77           cmd.exe  8         5004       2            3903488
77           cmd.exe  8         2356       2            3903488
77           cmd.exe  8         2596       2            3903488


C:\Users\Администратор.W2019SERV01>wmic process where processid='2356' call terminate(0)
Идет выполнение (\\W2019SERV01\ROOT\CIMV2:Win32_Process.Handle="2356")->terminate()
Метод успешно вызван.
Параметры вывода:
instance of __PARAMETERS
{
        ReturnValue = 0;
};


C:\Users\Администратор.W2019SERV01>wmic process list brief | find "cmd.exe"
94           cmd.exe                                       8         420        1            2228224
77           cmd.exe                                       8         5004       1            2355200
77           cmd.exe                                       8         2596       1            2433024
```

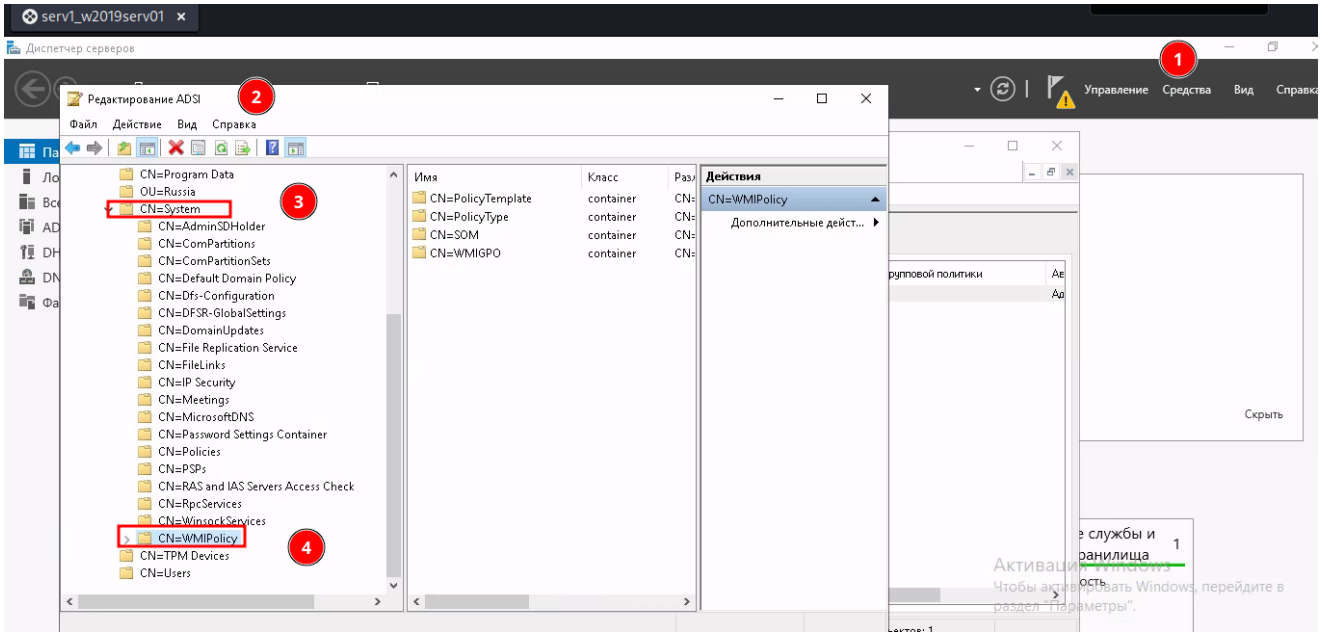
Задание_9:

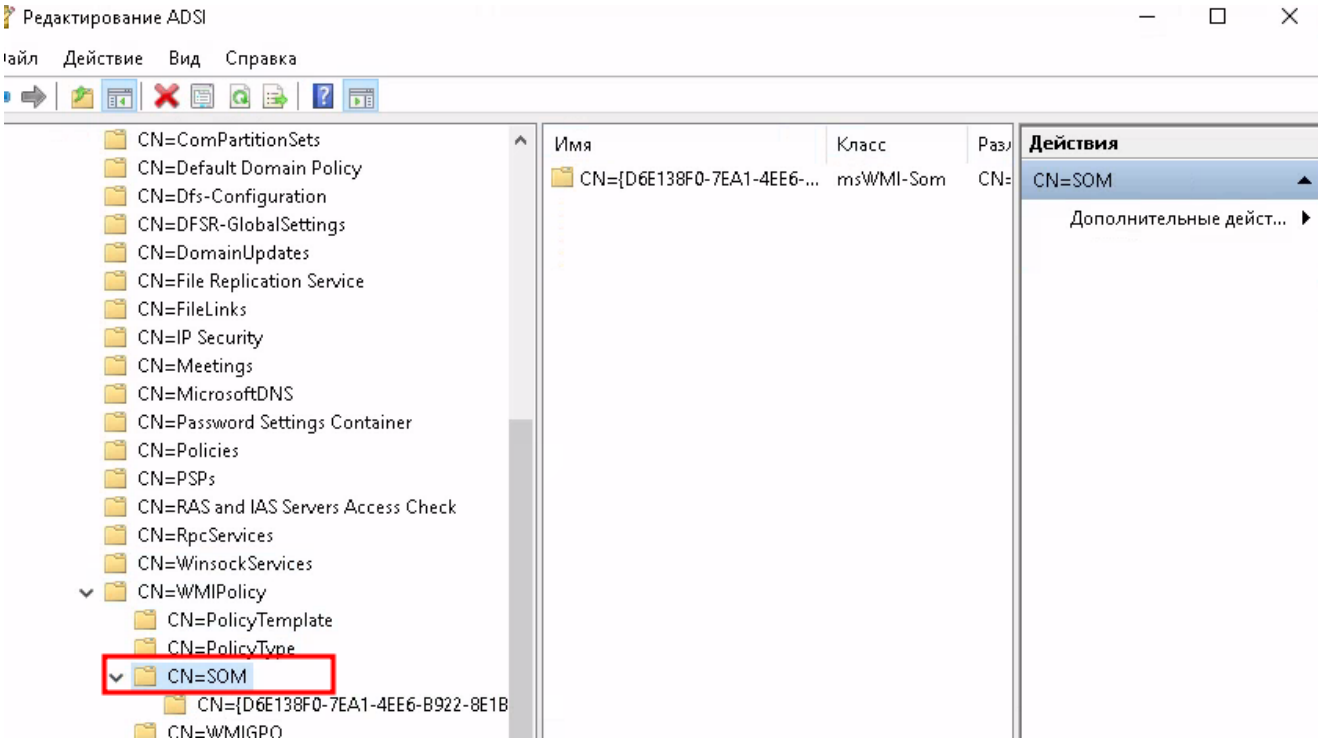
Создайте GPO, WMI фильтр которой будет применяться к Windows 10

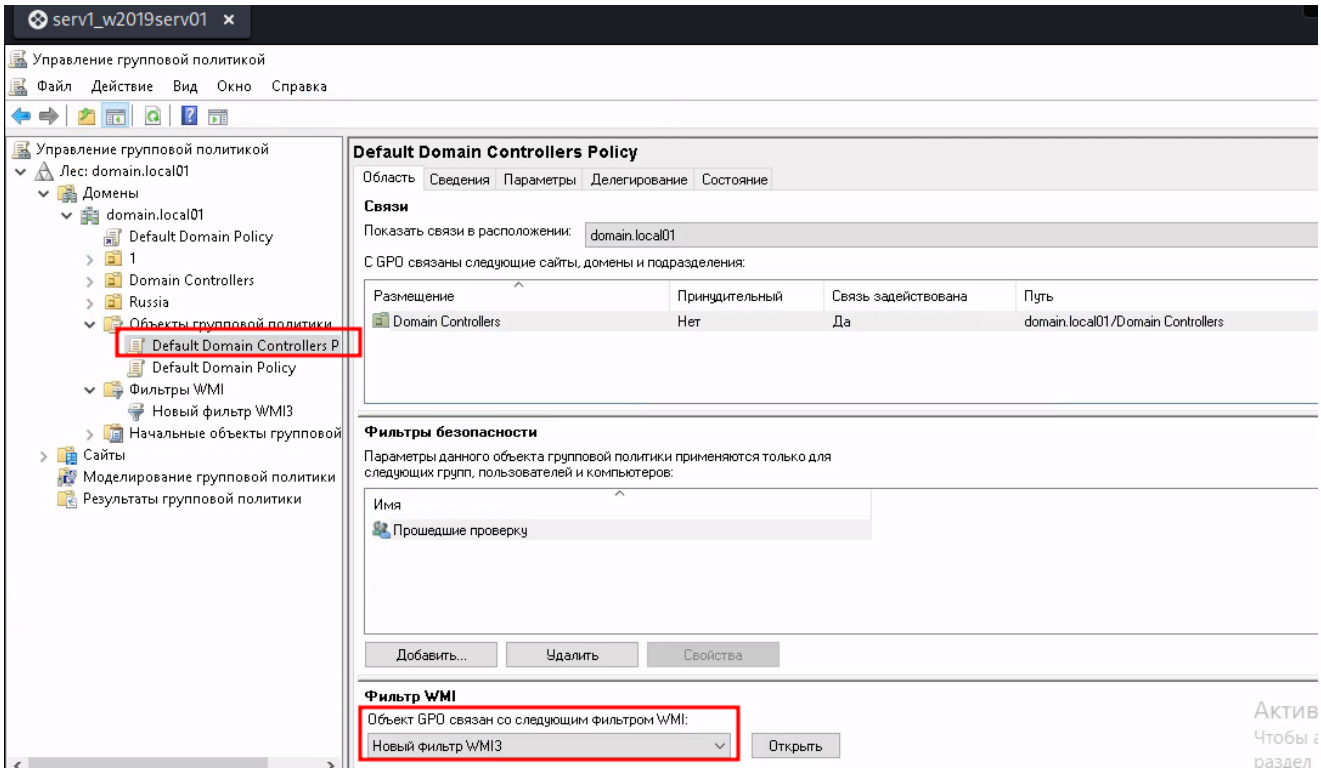
```
wmic path Win32_LogicalDisk WHERE FilesSystem='NTFS' get /value

#GPO
Select * from Win32_OperatingSystem where Version like "10.%" and
ProductType="1"

gpupdate /force
gpresult /r
```

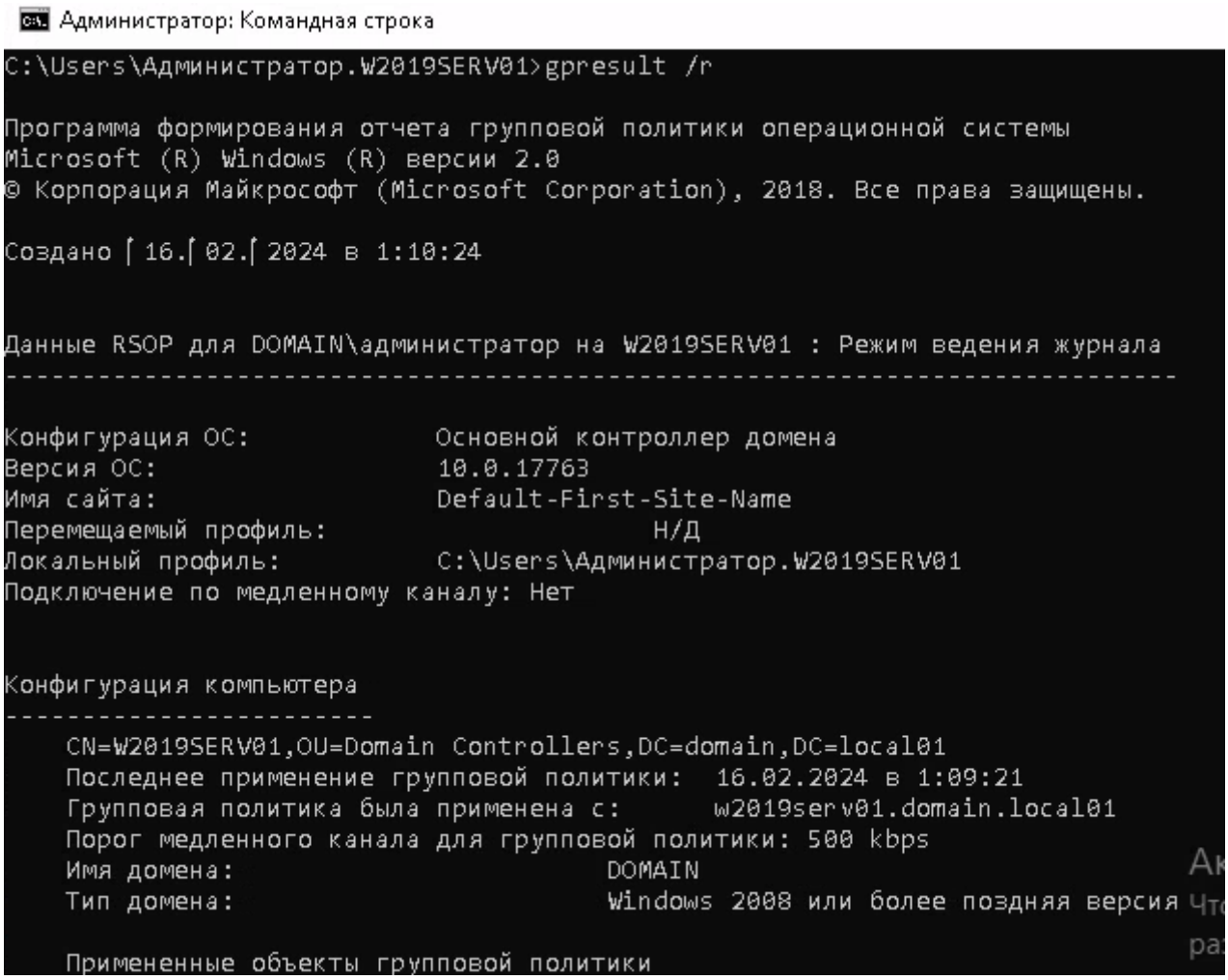


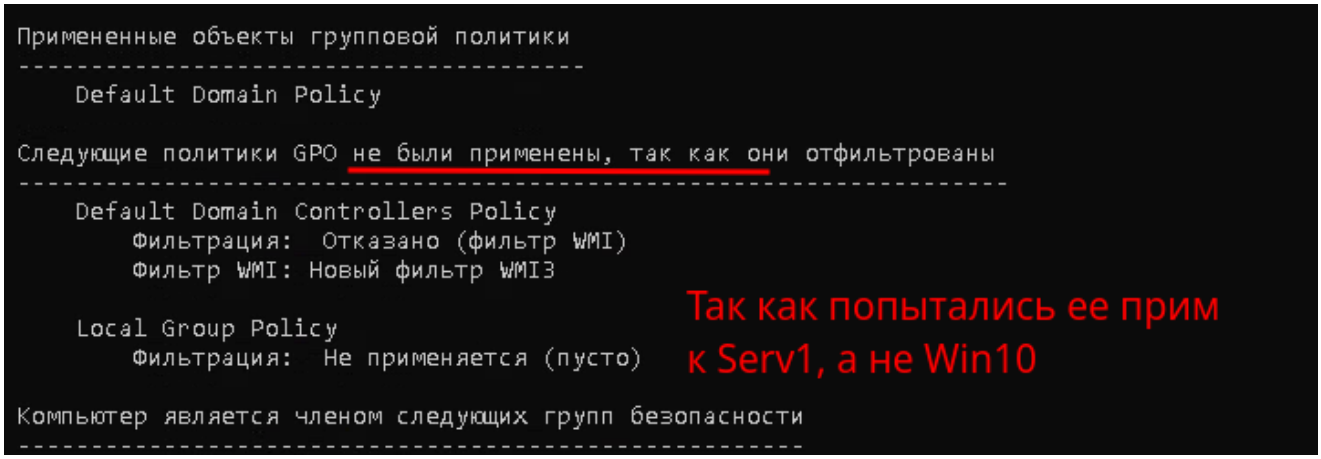

serv1_w2019serv01
Управление групповой политикой
Файл Действие Вид Окно Справка
Фильтры WMI - domain.local01
Содержимое Делегирование
Новый фильтр WMI
Имя: Новый фильтр WMI3
Запрос WMI
Пространство имен:
root\CIMv2
Обзор...
Запрос:
Select * from Win32_OperatingSystem where Version like "10.%" and ProductType="1"
Добавить
Удалить
Изменить
Сохранить
Отмена
1
2
3
4
5


serv1_w2019serv01
Диспетчер серверов
Редактирование ADSI
Файл Действие Вид Справка
CN=Program Data
OU=Russia
CN=System
CN=AdminSDHolder
CN=ComPartitions
CN=ComPartitionSets
CN=Default Domain Policy
CN=Dfs-Configuration
CN=DFSR-GlobalSettings
CN=DomainUpdates
CN=File Replication Service
CN=FileLinks
CN=IP Security
CN=Meetings
CN=MicrosoftDNS
CN=Password Settings Container
CN=Policies
CN=PSPs
CN=RAS and IAS Servers Access Check
CN=RpcServices
CN=WinsockServices
CN=WMIPolicy
CN=TPM Devices
CN=Users
Имя
Класс
CN=PolicyTemplate container
CN=PolicyType container
CN=SOM container
CN=WMIGPO container
Действия
CN=WMIPolicy
Дополнительные дейст...
Управление
Средства
Вид
Справка
Скрыть
1
2
3
4


Редактирование ADSI
Файл Действие Вид Справка
CN=ComPartitionSets
CN=Default Domain Policy
CN=Dfs-Configuration
CN=DFSR-GlobalSettings
CN=DomainUpdates
CN=File Replication Service
CN=FileLinks
CN=IP Security
CN=Meetings
CN=MicrosoftDNS
CN=Password Settings Container
CN=Policies
CN=PSPs
CN=RAS and IAS Servers Access Check
CN=RpcServices
CN=WinsockServices
CN=WMIPolicy
CN=PolicyTemplate
CN=PolicyType
CN=SOM
CN={D6E138F0-7EA1-4EE6-B922-8E1B
CN=WMIGPO
Имя
Класс
CN={D6E138F0-7EA1-4EE6-...
msWMI-Som
Действия
CN=SOM
Дополнительные дейст...

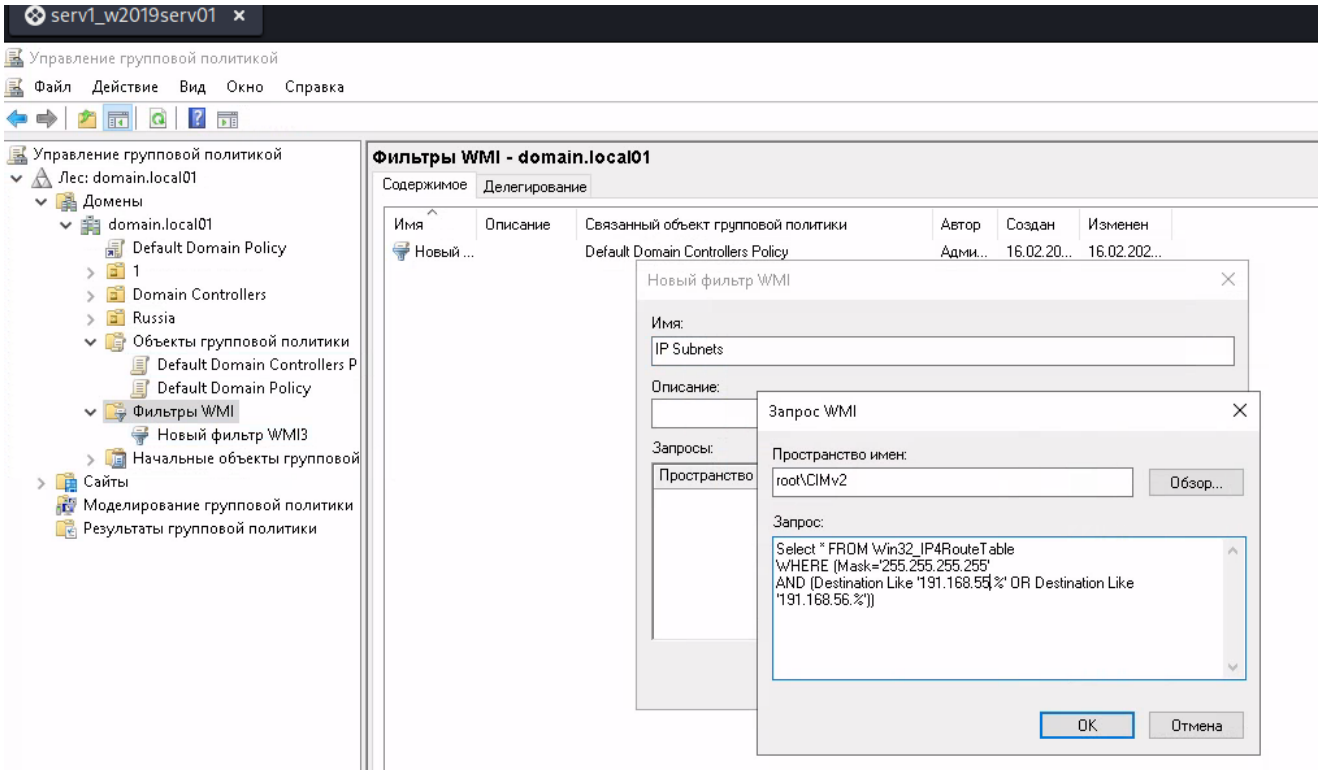

serv1_w2019serv01
Управление групповой политикой
Файл Действие Вид Окно Справка
Управление групповой политикой
Лес: domain.local01
Домены
domain.local01
Default Domain Policy
1
Domain Controllers
Russia
Объекты групповой политики
Default Domain Controllers P
Default Domain Policy
Фильтры WMI
Новый фильтр WMI3
Начальные объекты групповой
Сайты
Моделирование групповой политики
Результаты групповой политики
Default Domain Controllers Policy
Область Сведения Параметры Делегирование Состояние
Связи
Показать связи в расположении: domain.local01
С GPO связаны следующие сайты, домены и подразделения:
Размещение Принудительный Связь задействована Путь
Domain Controllers Нет Да domain.local01/Domain Controllers
Фильтры безопасности
Параметры данного объекта групповой политики применяются только для следующих групп, пользователей и компьютеров:
Имя
Прошедшие проверку
Добавить... Удалить Свойства
Фильтр WMI
Объект GPO связан со следующим фильтром WMI:
Новый фильтр WMI3
Открыть

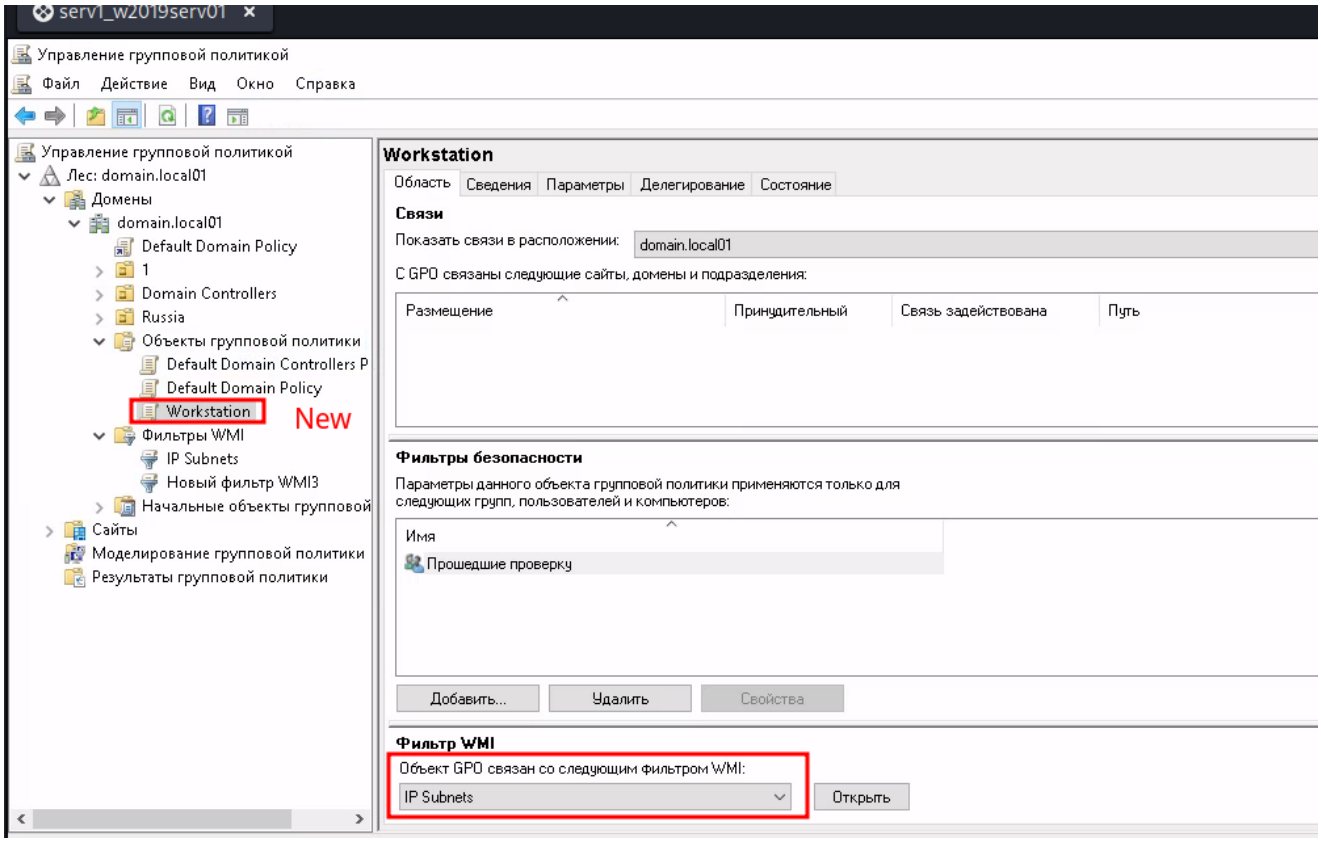




Дополнительно:

```
# GPO IP subnets
Select * FROM Win32_IP4RouteTable
WHERE (Mask='255.255.255.255'
AND (Destination Like '191.168.55.%' OR Destination Like '191.168.56.%'))
```






```
Get-WmiObject Win32_operatingsystem
Get-WmiObject Win32_operatingsystem | Select *

Get-WmiObject -query 'SELECT * FROM CIM_DataFile WHERE path="\\Program
Files\\Internet Explorer\\" AND filename="iexplore" AND extension="exe"
AND version>"11.%"'
```

```
PS C:\Users\Администратор.W2019SERV01> Get-WmiObject Win32_operatingsystem


SystemDirectory : C:\Windows\system32
Organization    :
BuildNumber     : 17763
RegisteredUser  : Пользователь Windows
SerialNumber    : 00429-00000-00001-AA323
Version         : 10.0.17763



PS C:\Users\Администратор.W2019SERV01> Get-WmiObject Win32_operatingsystem | Select *


PSComputerName                  : W2019SERV01
Status                          : OK
Name                            : Майкрософт Windows Server 2019 Standard|C:\Windows|\Device\Harddisk0\Partit
                                  ion2
FreePhysicalMemory              : 602780
FreeSpaceInPagingFiles          : 917568
FreeVirtualMemory               : 1489556
__GENUS                         : 2
__CLASS                         : Win32_OperatingSystem
__SUPERCLASS                    : CIM_OperatingSystem
__DYNASTY                       : CIM_ManagedSystemElement
__RELPATH                       : Win32_OperatingSystem=@
__PROPERTY_COUNT                : 64
__DERIVATION                    : {CIM_OperatingSystem, CIM_LogicalElement, CIM_ManagedSystemElement}
```

```
PS C:\Users\Администратор.W2019SERV01> Get-WmiObject -query 'SELECT * FROM CIM_DataFile WHERE path="\\Program Files\\Int
ernet Explorer\\" AND filename="iexplore" AND extension="exe" AND version>"11.%"'


Compressed : False
Encrypted  : False
Size       :
Hidden     : False
Name       : C:\Program Files\Internet Explorer\iexplore.exe
Readable   : True
System     : False
Version    : 11.0.17763.2989
Writeable  : True
```

Команды:

```
Get-Command -Module Storage
Get-Disk | ft -AutoSize
Get-Disk | Where-Object IsSystem -eq $True | fl
Get-Disk | Where-Object IsOffline -Eq $True| ft -AutoSize
Get-Partition
Get-Volume
#Выведем диски со статусом Offline:
Get-Disk | Where-Object IsOffline -Eq $True| ft -AutoSize
#Прежде всего нужно перевести такой диск в онлайн:
Get-Disk | Where-Object IsOffline -Eq $True | Set-Disk -IsOffline $False
#Теперь можно инициализировать этот диск (индекс 1):
Initialize-Disk -Number 1
#По умолчанию на диске создается таблица разделов GPT (GUID),
Initialize-Disk 1 -PartitionStyle MBR
#Если на диске уже имеются данные, вы можете изменить таблицу разделов с
MBR в GPT без удаления данных с помощью утилиты mbr2gpt.exe
Get-Disk | Where-Object PartitionStyle -Eq 'RAW' | Initialize-Disk
New-Partition -DiskNumber 1 -Size 10gb -DriveLetter L
New-Partition -DiskNumber 1 -AssignDriveLetter -UseMaximumSize
Set-Partition -DriveLetter L -NewDriveLetter U
Get-PartitionSupportedSize -DriveLetter L | Format-List
$MaxSize = (Get-PartitionSupportedSize -DriveLetter L).SizeMax
```

```
Resize-Partition -DriveLetter L -Size $MaxSize
Set-Partition -DriveLetter T -IsActive $true
Format-Volume -DriveLetter L -FileSystem NTFS -NewFileSystemLabel DBData -
Confirm:$false
Get-Partition -DiskNumber 1 | Remove-Partition -Confirm:$false
Clear-Disk -Number 1 -RemoveData -Confirm:$false
Clear-Disk -Number 1 -RemoveData -RemoveOEM
Get-Disk |Where-Object PartitionStyle -eq 'RAW' |Initialize-Disk -
PartitionStyle MBR -PassThru |New-Partition -AssignDriveLetter -
UseMaximumSize |Format-Volume -FileSystem NTFS -Confirm:$false
New-Partition -DiskNumber 1 -Size 20gb -DriveLetter E
Format-Volume -DriveLetter E -FileSystem NTFS -Confirm:$false
fsutil quota track E:
fsutil quota enforce E:
fsutil quota disable E:
fsutil quota query e:
fsutil quota violations
fsutil quota modify E: 3000000000 200000000 администратор
fsutil behavior query quotanotify
# дедупликации с помощью Powershell
Install-WindowsFeature -Name "FS-Data-Deduplication" -ComputerName "Имя
компьютера" -IncludeAllSubFeature -IncludeManagementTools
Get-Command -Module Deduplication
Enable-DedupVolume -Volume 'E:\' -UsageType 'Default'
Enable-DedupVolume -Volume 'E:\','D:\' -UsageType 'Default'
Get-DedupVolume
# Создадим на диске E папки folder1 и folder2:
New-Item -Path 'e:\Folder1' , 'e:\Folder2' -ItemType Directory
Set-DedupVolume `
-Volume 'E:' `
-ExcludeFolder 'E:\folder1', 'E:\folder2' `
-ExcludeFileType 'txt','rar' `
-MinimumFileAgeDays 15
Get-DedupVolume | Select *
# По умолчанию дедуплкиция работает только с файлами больше чем 32Kb. В
отличие от GUI это меняется в Powershell, но не в меньшую сторону. На
примере ниже я установлю этот минимум для файлов в 1GB:
Set-DedupVolume `
-Volume 'E:' `
-MinimumFileSize 1GB
Get-DedupVolume | Select *
Disable-DedupVolume -Volume 'E:\'

Get-DedupSchedule
Set-DedupSchedule `
-Name 'WeeklyGarbageCollection' `
-Type 'GarbageCollection' `
-Enabled $True `
-StopWhenSystemBusy $True `
```

```
-Days 'Friday' `
-Start 22:00 `

# Новая задача по оптимизации. Она будет проходить в будни, после 21:00, с
нагрузкой в 70% от максимальной на протяжении 8 часов:
New-DedupSchedule `
-Name 'Оптимизация по будням' `
-Cores 80 `
-Days Monday,Tuesday,Wednesday,Thursday,Friday `
-DurationHours 8 `
-InputOutputThrottleLevel Medium `
-Priority Normal `
-Memory 80 `
-Start 21:00 `
-Type 'Optimization' `
-StopWhenSystemBusy `
# Так же можно и удалять задачи:
Get-DedupSchedule -Name '*Полная*' | Remove-DedupSchedule
Remove-DedupSchedule -Name '*Полная*'
# Убрать дедупликацию на томе и обратить файлы в исходное состояние :
New-DedupSchedule -Type Unoptimization
```

Язык запросов WQL

```
SELECT * FROM Win32_LogicalDisk WHERE FileSystem IS NULL
SELECT * FROM Win32_LogicalDisk WHERE FileSystem IS NOT NULL
SELECT * FROM Win32_LogicalDisk WHERE FileSystem = "NTFS"
SELECT * FROM Win32_DiskDrive WHERE Partitions < 2 OR SectorsPerTrack >
100
SELECT * FROM Win32_LogicalDisk WHERE (Name = "C:" OR Name = "D:")
AND FreeSpace > 2000000 AND FileSystem = "NTFS"
SELECT * FROM Win32_NTLogEvent WHERE Logfile = 'Application'
SELECT * FROM Meta_Class WHERE __Class LIKE %Win32%
SELECT * FROM __InstanceCreationEvent WHERE TargetInstance ISA
"Win32_NTLogEvent"
GROUP WITHIN 600 BY TargetInstance.SourceName HAVING NumberOfEvents > 25
Select * from Win32_OperatingSystem where Version like "10.%" and
ProductType="1"
select * from Win32_OperatingSystem WHERE Version LIKE "10.%" AND (
ProductType = "2" or ProductType = "3" )
# статуса батареи (она есть только у ноутбуков):
SELECT * FROM Win32_Battery WHERE (BatteryStatus <> 0)
# типа оперативной памяти (SODIMM для ноутбуков):
Select * from Win32_PhysicalMemory WHERE (FormFactor = 12)
#свойства PCSystemType:
SELECT * FROM Win32_ComputerSystem WHERE PCSystemType = 2
Select * FROM Win32_IP4RouteTable
WHERE (Mask='255.255.255.255'
AND (Destination Like '191.168.55.%' OR Destination Like '191.168.56.%'))
```

```
Select * from WIN32_ComputerSystem where TotalPhysicalMemory >= 1073741824
SELECT path,filename,extension,version FROM CIM_DataFile WHERE
path="\\Program Files\\Internet Explorer\\" AND filename="iexplore" AND
extension="exe" AND version>"11.0"
```

Статус батареи (она есть только у ноутбуков):

```
SELECT * FROM Win32_Battery WHERE (BatteryStatus <> 0)
типа оперативной памяти (SODIMM для ноутбуков): Select * from
Win32_PhysicalMemory WHERE (FormFactor = 12)
свойства PCSystemType: SELECT * FROM Win32_ComputerSystem WHERE
PCSystemType = 2
```

Итоговый WMI запрос будет таким

```
select * from Win32_SystemEnclosure where ChassisTypes = "8" or
ChassisTypes = "9" or ChassisTypes = "10" or ChassisTypes = "11" or
ChassisTypes = "12" or ChassisTypes = "14" or ChassisTypes = "18" or
ChassisTypes = "21"
```

```
Get-WMIObject Win32_OperatingSystem
Get-WMIObject Win32_OperatingSystem| Select *
get-wmiobject -query 'SELECT * FROM CIM_DataFile WHERE path="\\Program
Files\\Internet Explorer\\" AND filename="iexplore" AND extension="exe"
AND version LIKE "11.%"'
```

Дополнительно:

Глоссарий

Дополнительные материалы

Используемые источники

*Выполнил: ==AndreiM