

Настройки аудита в Windows, групповые политики, WEC. Способы сбора логов с ОС (агенты, подписки (коллекторы), WMI)

Настройка аудита Windows.

Настройка расширенной политики аудита Windows: Локальная настройка политик аудита производится через оснастки: `gpedit.msc`, `secpol.msc`, или с помощью утилиты `auditpol.exe`.

Настройка в домене производится через `gpmc.msc`.

Рекомендации по настройке аудита приводятся для следующих сущностей:

- Контроллеры домена
- Серверы
- Рабочие станции

Для настройки следует руководствоваться следующими ресурсами:

- Microsoft Audit Policy Recommendations;
- Malware Archaeology;
- CIS Microsoft Windows Server Benchmark;
- CIS Microsoft Windows Desktop Benchmark;
- blue-resources/Windows_MITRE_Data_Source_Mapping.xlsx

Настройка логирования командной строки:

Для настройки логирования командной строки включается следующий параметр: > > > > > .

При включении командной строки в события создания процесса, сведения командной строки для каждого процесса будут регистрироваться в виде обычного текста в событии 4688.

Настройка списков управления доступом к объектам SACL:

- При включении подкатегорий аудита: Аудит файловой системы и Аудит реестра необходимо настроить SACL для критичных ветвей реестра и системных директорий.
- Аудит лучше настраивать для всех пользователей (Everyone) и выбирать тип Успеха. Разрешения необходимо настроить в зависимости от сценариев мониторинга.

SACL

- Системный список управления доступом (SACL) позволяет администраторам регистрировать попытки доступа к защищенному объекту.
- Каждый ACE (элемент управления доступом) указывает типы попыток доступа со стороны указанного доверенного лица, которые приводят к созданию системой записи в журнале событий безопасности.
- ACE в SACL может создавать записи аудита при сбое попытки доступа, при успешном выполнении или и в том, и в другом случае.

Резюмируя:

- SACL – регистрационная запись попыток доступа (как успешных, так и неуспешных, в журнал безопасности);
- DACL – непосредственные права доступа (разрешения или запреты)

Подробнее про SACL можно прочитать на странице [Playbook UC-24.009 Modification Windows SACL \(Александр Ющенко\)](#)

Настройка powershell:

```
> > Windows > Windows PowerShell > . Для Имен модулей необходимо указать *. (event.id 4103)

> > Windows > Windows PowerShell > PowerShell. (event.id 4104)
```

Настройка Sysmon:

1. Скачайте Sysmon.
2. Создайте/скачайте/адаптируйте конфигурационный файл Sysmon.
3. Установить Sysmon: `sysmon -accepteula -i config.xml`
4. Обновить Sysmon с новым конфигом: `sysmon -c config.xml`

GPO

GPO (**Group Policy Object**) — это компонент системы управления групповой политикой в Windows, который позволяет администраторам централизованно управлять настройками пользователей и компьютеров в домене Active Directory (AD). GPO используется для создания и внедрения правил, обеспечивающих безопасность, контроль над доступом, а также настройку рабочих сред пользователей и устройств.

Основные возможности GPO включают:

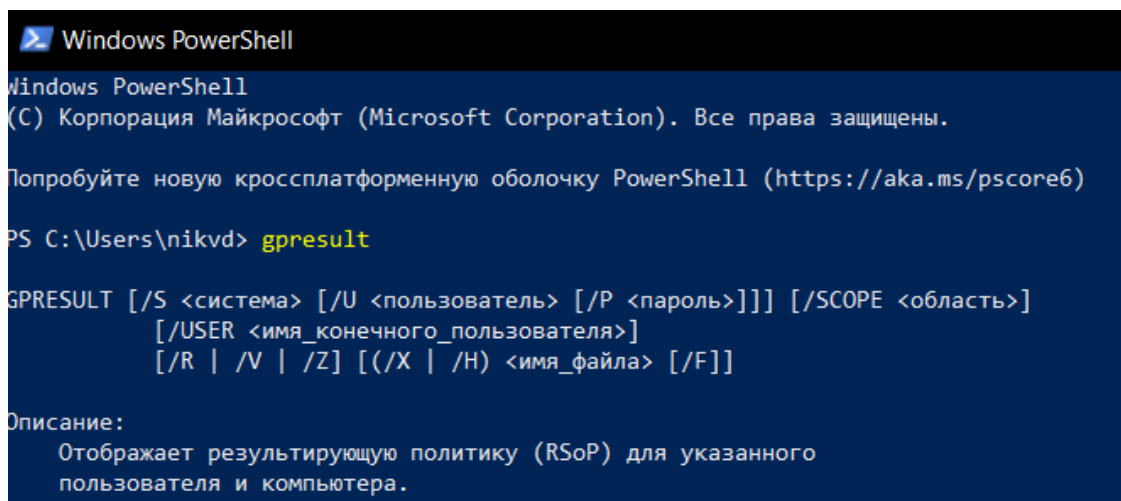
1. Настройка политик безопасности: Администраторы могут задавать правила для паролей, настройки брандмауэра, ограничение доступа к определенным функциям или файлам и т. д.
2. Управление учетными записями пользователей и компьютеров: Можно настроить, какие программы могут запускаться, доступ к сетевым ресурсам, а также задать разрешения для конкретных файлов и папок.
3. Автоматизация установки программ: С помощью GPO можно автоматически устанавливать, обновлять и удалять программное обеспечение на всех компьютерах в домене.
4. Настройка рабочей среды: Администраторы могут настраивать рабочий стол, меню «Пуск», конфигурацию сетевых подключений и другие аспекты пользовательской среды.
5. Управление обновлениями Windows: GPO позволяет централизованно управлять обновлениями ОС, задавая время, когда они будут установлены, и другие параметры.

Как работают GPO

GPO создаются и управляются с помощью инструмента Group Policy Management Console (GPMC). Их можно привязывать к различным уровням **Active Directory: сайтам, доменам и организационным единицам (OU)**. При этом GPO наследуются — например, политика, назначенная на уровне домена, будет применена ко всем организациям и подразделениям в этом домене, если наследование не отключено.

Применение и приоритет GPO

Область действия: GPO можно применять к пользователям, компьютерам, группам и организационным единицам в зависимости от иерархии в Active Directory !



```
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/pscore6)

PS C:\Users\nikvd> gresult

GPRESULT [/S <система> [/U <пользователь> [/P <пароль>]] [/SCOPE <область>]
        [/USER <имя_конечного_пользователя>]
        [/R | /V | /Z] [/X | /H] <имя_файла> [/F]

Описание:
    Отображает результирующую политику (RSoP) для указанного
    пользователя и компьютера.
```

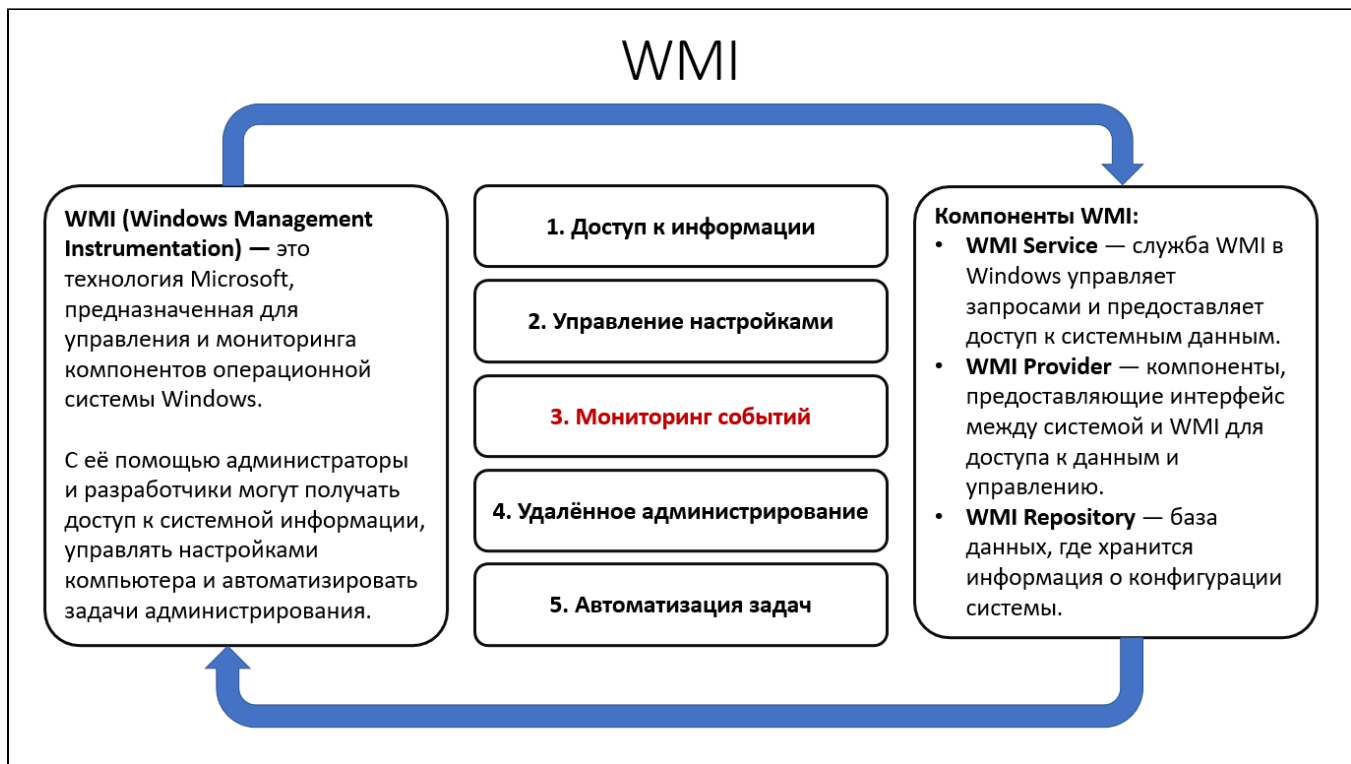
Получить список групповых политик можно с помощью утилиты командной строки `GPResult.exe`. Она позволяет вывести список доменных политик (GPO), которые применяются к компьютеру и пользователю.

Последовательность применения

В случае конфликтующих настроек, Windows применяет GPO в следующем порядке:

1. Локальные политики
2. Политики сайта
3. Политики домена
4. Политики организационных единиц (сверху вниз).

WMI (Windows Management Instrumentation)



WMI (Windows Management Instrumentation) — это технология Microsoft, предназначенная для управления и мониторинга компонентов операционной системы Windows. С её помощью администраторы и разработчики могут получать доступ к системной информации, управлять настройками компьютера и автоматизировать задачи администрирования.

Основные возможности WMI:

1. Доступ к информации — WMI предоставляет доступ к широкому спектру данных, таких как параметры операционной системы, информация о сети, процессах, оборудовании, установленных приложениях и многом другом.
2. Управление настройками — можно управлять параметрами системы, например, изменять настройки сети, управлять службами, процессами и пр.
3. Мониторинг событий — WMI может отслеживать события, такие как изменения состояния устройств, запуск процессов или изменение параметров системы. Это полезно для реагирования на определённые события или построения системы мониторинга.
4. Удалённое администрирование — через WMI можно управлять удалёнными компьютерами в сети. Это делает его удобным инструментом для системных администраторов.
5. Автоматизация задач — с помощью скриптов или приложений, использующих WMI, можно автоматизировать рутинные задачи, такие как настройка рабочих станций, получение отчётов о состоянии системы и т.д.

Программный доступ к WMI

WMI можно использовать через языки программирования, такие как PowerShell, C#, VBScript, Python (через соответствующие библиотеки). WMI предоставляет стандартный интерфейс для запросов — WQL (WMI Query Language), который схож с SQL.

Пример простого запроса через PowerShell для получения списка запущенных процессов:

```
Get-WmiObject -Query "SELECT * FROM Win32_Process"
```

Компоненты WMI:

- WMI Service — служба WMI в Windows управляет запросами и предоставляет доступ к системным данным.
- WMI Provider — компоненты, предоставляющие интерфейс между системой и WMI для доступа к данным и управлению.
- WMI Repository — база данных, где хранится информация о конфигурации системы.

Win32_NTLogEvent

Win32_NTLogEvent — это класс WMI, который используется для работы с событиями, записанными в журнале событий Windows. С его помощью можно получать данные из системных журналов, таких как System, Application, Security и других, что делает его удобным для анализа и мониторинга событий, происходящих в системе.

Основные возможности Win32_NTLogEvent

Win32_NTLogEvent *позволяет:*

- Получать информацию о событиях из журналов;
- Фильтровать события по разным критериям (например, ID события, тип журнала, время создания, уровень важности);
- Автоматизировать сбор данных о сбоях, ошибках безопасности или других событиях, которые важны для мониторинга и аудита.

Структура и свойства Win32_NTLogEvent

Win32_NTLogEvent предоставляет множество свойств для фильтрации и анализа событий. Вот некоторые из основных свойств:

Свойство	Описание
Category	категория события (например, логическое подразделение типа события)
EventCode	уникальный код события, указывающий на тип события (например, код 4625 для неудачной попытки входа)
EventIdentifier	идентификатор события
EventType	тип события: например, ошибка, предупреждение или информационное сообщение
InsertionStrings	массив строк, содержащий дополнительные данные о событии
Logfile	имя журнала, в котором хранится событие (например, System, Application, Security)
Message	текстовое сообщение, описывающее событие
RecordNumber	уникальный номер записи события в журнале
SourceName	источник события (например, имя приложения или службы)
TimeGenerated	время, когда событие было записано
User	имя пользователя, связанного с событием

Примеры использования Win32_NTLogEvent

Пример 1: Получение всех событий из журнала System

Этот пример показывает, как можно получить все события из журнала System. Команда PowerShell с запросом через WMI:

```
Get-WmiObject -Query "SELECT * FROM Win32_NTLogEvent WHERE Logfile = 'System'"
```

Этот запрос вернет все события, записанные в системный журнал.

```
PS C:\Users\nikvd>
PS C:\Users\nikvd> Get-WmiObject -Query "SELECT * FROM Win32_NTLogEvent WHERE Logfile = 'System'"

Category           : 1014
CategoryString      :
EventCode           : 1014
EventIdentifier      : 1014
TypeEvent           :
InsertionStrings     : {yandex.ru, 128}
LogFile             : System
Message             : Разрешение имен для имени yandex.ru истекло после отсутствия ответа от настроенных серверов DNS.
RecordNumber        : 47397
SourceName          : Microsoft-Windows-DNS-Client
TimeGenerated        : 20241014173338.274383-000
TimeWritten         : 20241014173338.274383-000
Type                : Предупреждение
UserName            :
```

Пример 2: Получение событий по коду события

Чтобы найти конкретные события, можно фильтровать результаты по EventCode. Например, получить события с кодом 4625 (неудачная попытка входа):

```
Get-WmiObject -Query "SELECT * FROM Win32_NTLogEvent WHERE EventCode = '4625'"
```

```
PS C:\Users\nikvd>
PS C:\Users\nikvd> Get-WmiObject -Query "SELECT * FROM Win32_NTLogEvent WHERE EventCode = '4625'"

Category           : 0
CategoryString     : 
EventCode          : 4625
EventIdentifier    : 1073746449
TypeEvent         : 
InsertionStrings   : {86400, SuppressDuplicateDuration, Software\Microsoft\EventSystem\EventLog}
LogFile           : Application
Message           : Подсистема EventSystem подавляет повторяющиеся элементы журнала событий в течение 86400 сек. Таймаут
                   : подавления управляется значением REG_DWORD с именем SuppressDuplicateDuration в следующем разделе
                   : реестра: HKLM\Software\Microsoft\EventSystem\EventLog.
RecordNumber      : 77917
SourceName         : Microsoft-Windows-EventSystem
TimeGenerated      : 20241014134213.132803-000
TimeWritten       : 20241014134213.132803-000
Type              : Сведения
UserName          :
```

Пример 3: Фильтрация событий по источнику и времени создания

Чтобы сузить результаты и получить события только от определенного источника и за определенный период времени, можно комбинировать несколько условий. Например, получить события с именем источника Security за последние сутки:

```
$lastDay = (Get-Date).AddDays(-1).ToString("yyyyMMddHHmmss.000000-000")
Get-WmiObject -Query "SELECT * FROM Win32_NTLogEvent WHERE Logfile = 'Security' AND SourceName = 'Microsoft-
Windows-Security-Auditing' AND TimeGenerated >= '$lastDay'"
```

Этот запрос полезен для анализа событий безопасности, чтобы отслеживать критические действия, такие как изменения учетных записей или настройки безопасности.

Автоматизация мониторинга с помощью Win32_NTLogEvent

Пример 4: Создание WMI-подписки

С помощью Win32_NTLogEvent и подписок на события можно настроить автоматическое оповещение о важных событиях. Например, используя PowerShell, можно создать подписку, которая будет автоматически записывать в лог определенные события, такие как системные ошибки, предупреждения или попытки взлома.

```
Register-WmiEvent -Query "SELECT * FROM Win32_NTLogEvent WHERE EventCode = '4625'" -SourceIdentifier
"FailedLoginAlert" -Action { Write-Output " !" }
```

Эта команда создаст подписку на события с кодом 4625, указывающим на неудачные попытки входа. Когда такое событие произойдет, оно выведет сообщение в консоль или может быть дополнительно настроено для отправки уведомления.

Сбор логов и событий с узлов

WEC (Windows Event Collector)

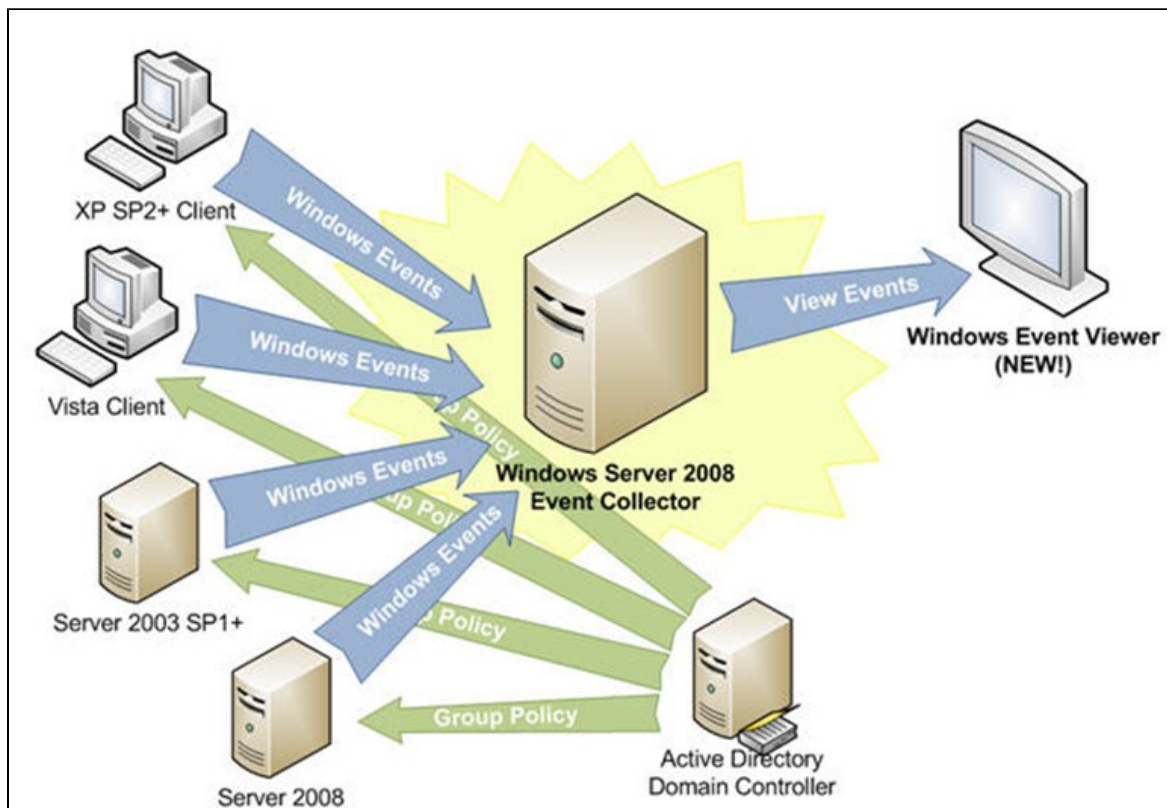
WEC (Windows Event Collector) — это служба в Windows, которая позволяет собирать события с других компьютеров в централизованное хранилище на одном сервере. Это полезно для мониторинга, аудита и анализа событий безопасности, предупреждения сбоев, а также для централизованного хранения логов.

Как работает WEC

WEC настраивается для сбора событий из журналов Windows Event Log (например, события безопасности, системы, приложений и т.д.). Для настройки WEC необходимы два компонента:

1. WEC-сервер — устройство, на котором будет храниться собранная информация.
2. Клиентские устройства — компьютеры, события с которых необходимо собирать (см. рисунок ниже)

WEC работает по протоколу WS-Management и использует Event Subscription, где клиентские устройства "подписываются" на отправку определённых событий на WEC-сервер.



Настройка WEC

Процесс настройки WEC состоит из нескольких этапов:

1. Подготовка WEC-сервера

На сервере, который будет собирать события, нужно установить роль WEC:

1. Откройте Server Manager.
2. Перейдите в Manage Add Roles and Features.
3. Выберите Features и найдите Windows Event Collector.
4. Установите её и дождитесь завершения установки.

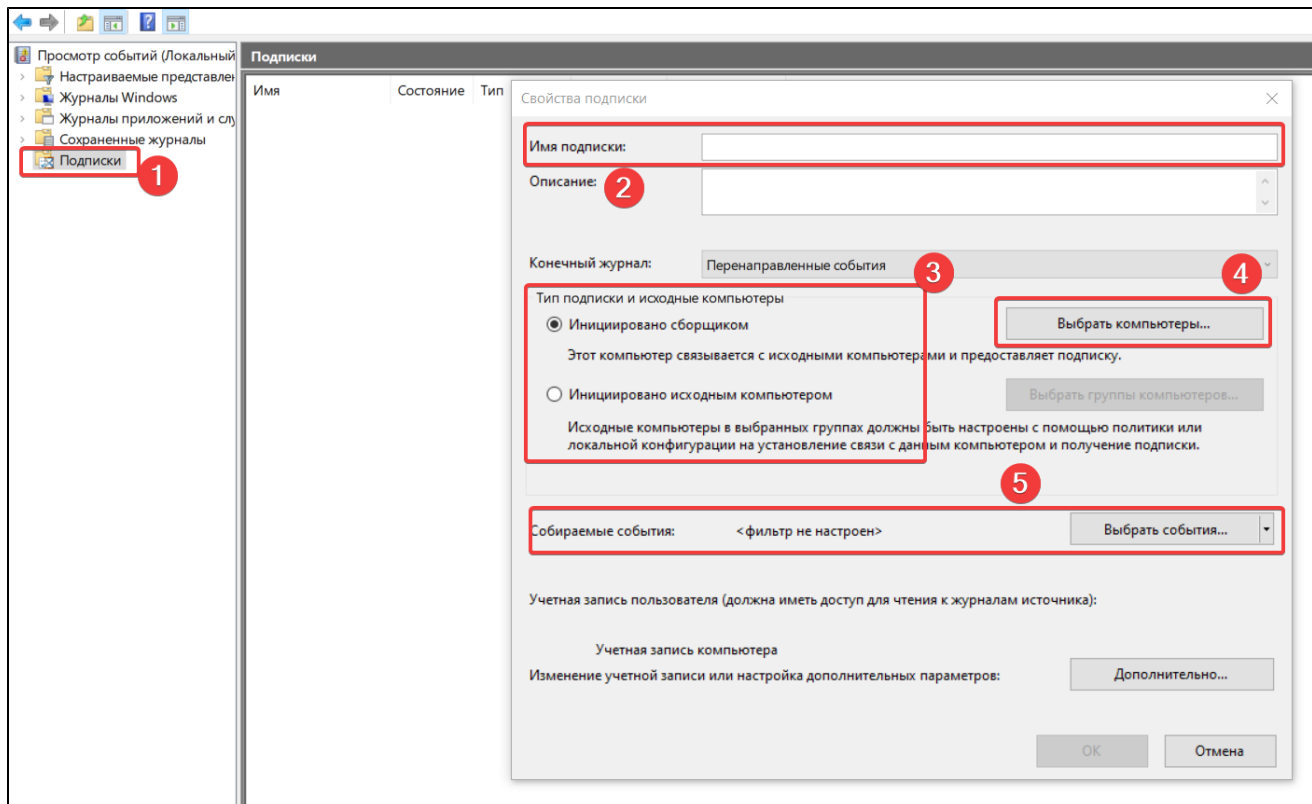
После установки запустите службу:

```
wecutil qc
```

Эта команда настроит и включит базовую конфигурацию Windows Event Collector.

2. Создание подписки на события

Создание подписки позволит вам указать, какие именно события и с каких устройств нужно собирать.



1. Откройте Event Viewer на WEC-сервере.
2. В меню слева выберите Subscriptions и нажмите Create Subscription.
3. Введите имя и описание для подписки.
4. Выберите тип подписки (например, Collector Initiated — иницируемый сервером, или Source Initiated — иницируемый клиентом).
5. Укажите устройства, с которых нужно собирать события (по IP-адресам или именам устройств).
6. Настройте фильтры событий, выбрав интересные журналы и уровень важности (например, Security с уровнем Error).
7. Нажмите OK для сохранения подписки.

3. Настройка клиентских устройств

На каждом клиентском устройстве, с которого нужно собирать события, необходимо выполнить следующие шаги:

Убедитесь, что включена служба Windows Remote Management (WinRM):

```
winrm quickconfig
```

Настройте доверие для сервера WEC. Для этого добавьте его в доверенные узлы WinRM:

```
winrm set winrm/config/client '@{TrustedHosts="__IP__WEC-"}'
```

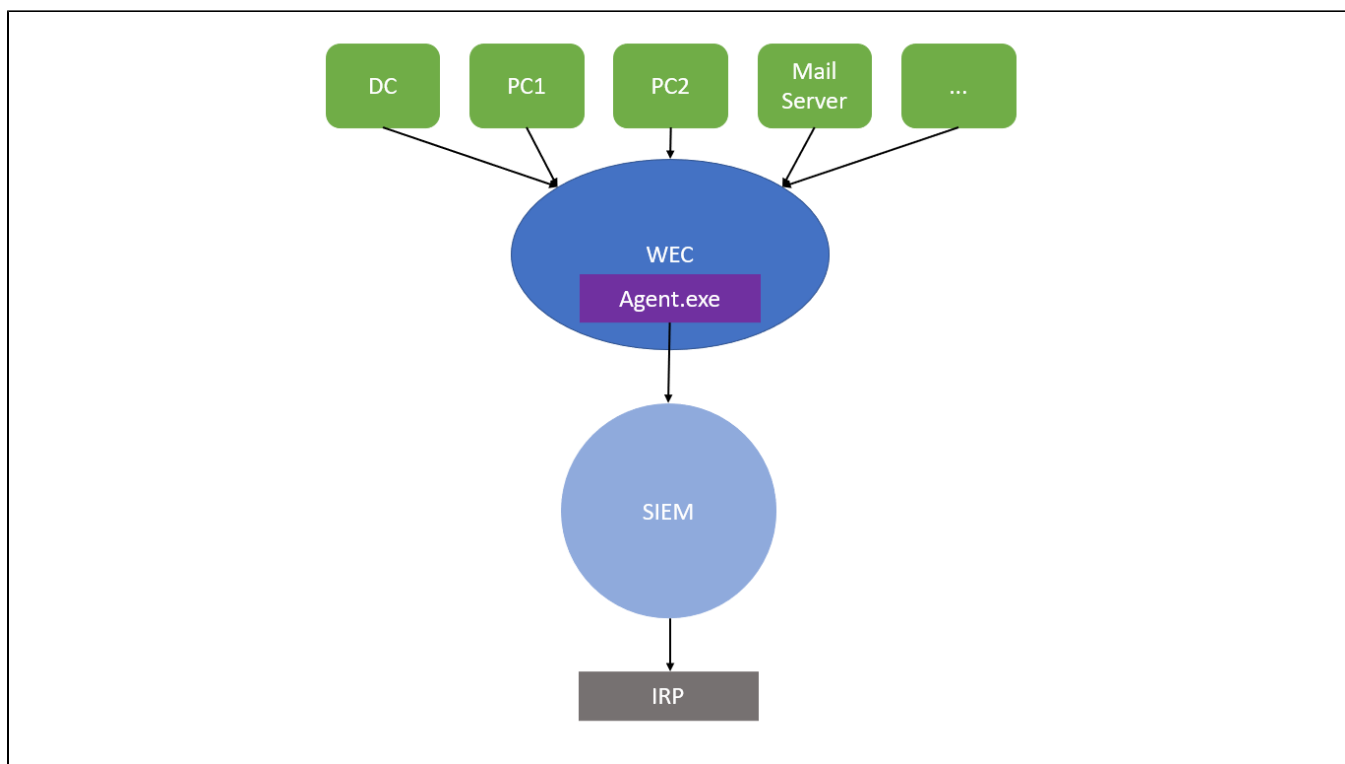
Убедитесь, что на клиентском устройстве настроены необходимые политики, разрешающие отправку событий на WEC-сервер. Откройте **Local Group Policy Editor (gpedit.msc)**, и в разделе **Computer Configuration Administrative Templates Windows Components Event Forwarding** настройте политики:

Configure target Subscription Manager — **укажите путь к WEC-серверу, например, Server=http://< IP >:5985/wsman /SubscriptionManager/WEC,Refresh=10**

4. Проверка работы

После настройки, убедитесь, что события корректно передаются. Для этого:

1. В Event Viewer на WEC-сервере зайдите в Forwarded Events и проверьте наличие событий.
2. Также можно использовать команду PowerShell для проверки статуса подписок: `wecutil es`



Полезный материал на тему WEC

[Лабораторная работа №5.2 Средства мониторинга Windows. PT-Start \(GitHub\)](#)
[OS Windows. Занятие 5. FS, мониторинг.pdf](#)

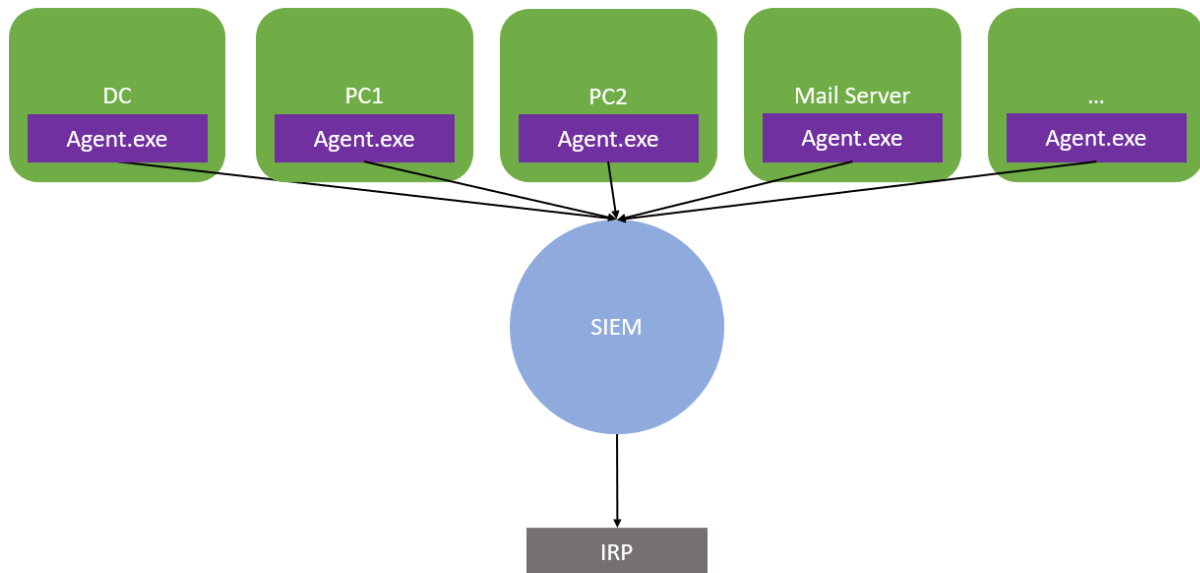
Агенты

Агент SIEM — это программное обеспечение, установленное на конечных устройствах или серверах, которое помогает собирать, фильтровать и передавать данные в основную SIEM-платформу.

Функции агента SIEM:

- Сбор данных: Агент собирает информацию о событиях (логах) с различных источников, таких как сетевые устройства, серверы, базы данных и приложения.
- Фильтрация и нормализация: Агент может фильтровать незначительные события и нормализовать логи, приводя их к единому формату для упрощения анализа.
- Передача данных в SIEM: После сбора и предварительной обработки данные отправляются в SIEM-систему для дальнейшего анализа и корреляции.
- Мониторинг и оповещение: Некоторые агенты могут выполнять предварительный анализ событий и отправлять уведомления, если обнаружена подозрительная активность.

Сбор логов. Агенты.



Агент vs. WEC

Параметр	Агент	WEC
Установка и администрирование	Гибкая настройка, но сложная установка	Удобство централизованного управления
Производительность	Может потреблять ресурсы клиента	Меньшее влияние на производительность
Надежность	Кэширование и устойчивость к сбоям	Завязан на сеть и сервер
Безопасность	Зависит от качества клиента	Встроенные механизмы безопасности Windows
Совместимость	Кроссплатформенность	Только Windows
Гибкость	Высокая, с расширенной настройкой	Ограниченная гибкость

Сбор логов у наших клиентов

Полезные ссылки

[Про GPO и Active Directory \(Хабр\)](#)

[Auditpol.exe \(Microsoft Learn\)](#)

[Документация Sysmon \(Microsoft Learn\)](#)

[OS Windows. Занятие 2. AD.pdf](#)