Сбор журналов событий Windows и Active Directory в Graylog

winitpro.ru/index.php/2024/05/14/sbor-zhurnalov-sobytij-windows-i-ad-graylog

В предыдущей статье мы рассмотрели, как развернуть собственный централизованный сервер сбора лога с различных типов сетевых устройства на базе стека Graylog (`Graylog` + `OpenSearch` + `MongoDB`). В этой статье мы покажем, как настроить отправку журналов событий с серверов Windows (включая события Active Directory) в Graylog.

Настройка сборщика данных и индексов Graylog для устройств Windows

Сначала нужно настроить в Graylog отдельные сборщики данных и потоки для логов, которые будут отправлять хосты Windows Server (чтобы не смешивались события от разных классов устройств). Перейдите в раздел **System** -> **Inputs** и добавьте новый сборщик *Windows Server Devices* типа **Beats**, который слушает на порту `TCP:5044` .

Затем создайте отдельный индекс для логов журналов событий Windows. На базе нового Input и индекса создайте новый поток для Windows в разделе Streams и запустите его.

Отправка событий Windows в Graylog с помощью Winlogbeat

Для отправки логов из журналов событий EventViewer с хостов Windows на сервер Graylog можно воспользоваться службой сборщика логов **Winlogbeat**. Winlogbeat это один из свободно распространяемых компонентов стека ELK. Службу Winlogbeat нужно установить на каждом хосте Windows, события с которого вы хотите видеть на сервере Graylog.

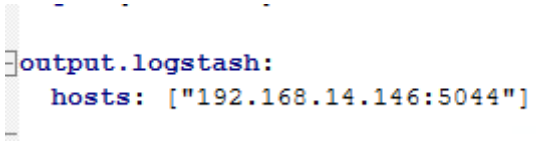
1. Скачайте архив Winlogbeat со страницы загрузки (https://www.elastic.co/downloads/beats/winlogbeat)
2. Распакуйте архив в папку `C:\Program Files\winlogbeat`
3. Отредактируйте конфигурационный файл **winlogbeat.yml**

В самом простом случае можно использовать следующую конфигурацию, когда все события из журналов Application, Security и System будут отправлены на указанный сервер Graylog.

Обратите внимание, что в конфигурационном файле winlogbeat используется синтаксис YAML, а это значит нужно быть внимательным с пробелами и отступами.

```
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h
  - name: Security
  - name: System
output.logstash:
  hosts: ["192.168.14.146:5044"]
```

Можно использовать более гибкие условия фильтрации, чтобы получить только нужны логи. Например, чтобы получить события с определенными уровнями критичности и номерам EventID, используется такой конфиг:

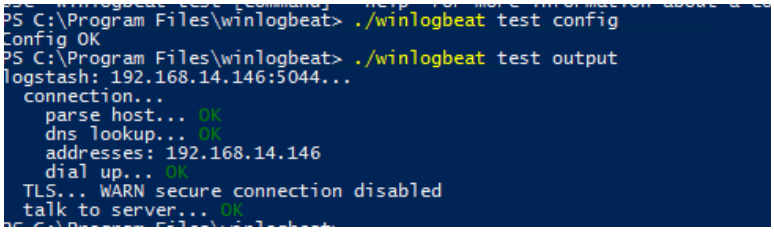



```
winlogbeat.event_logs:
  - name: Security
    event_id: 4627, 4703, 4780-4782
    ignore_older: 24h
    level: critical, error

  - name: Microsoft-Windows-TerminalServicesRDPClient/Operational
    event_id: 1102
```

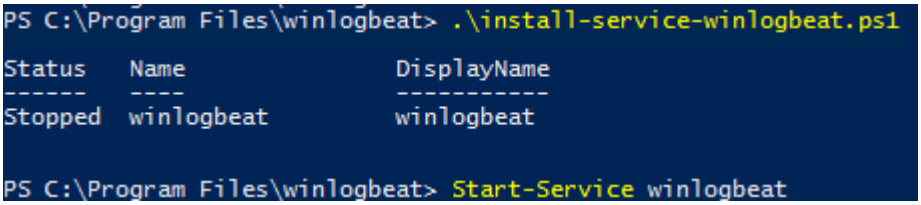
Примеры типовой универсальной конфигурации winlogbeat.yml для Windows Server можно посмотреть тут.
Сохраните файл winlogbeat.yml и проверьте корректность конфигурации Winlogbeat и доступность сервера сбора логов:

```
cd "C:\Program Files\winlogbeat"
./winlogbeat test config
./winlogbeat test output
```

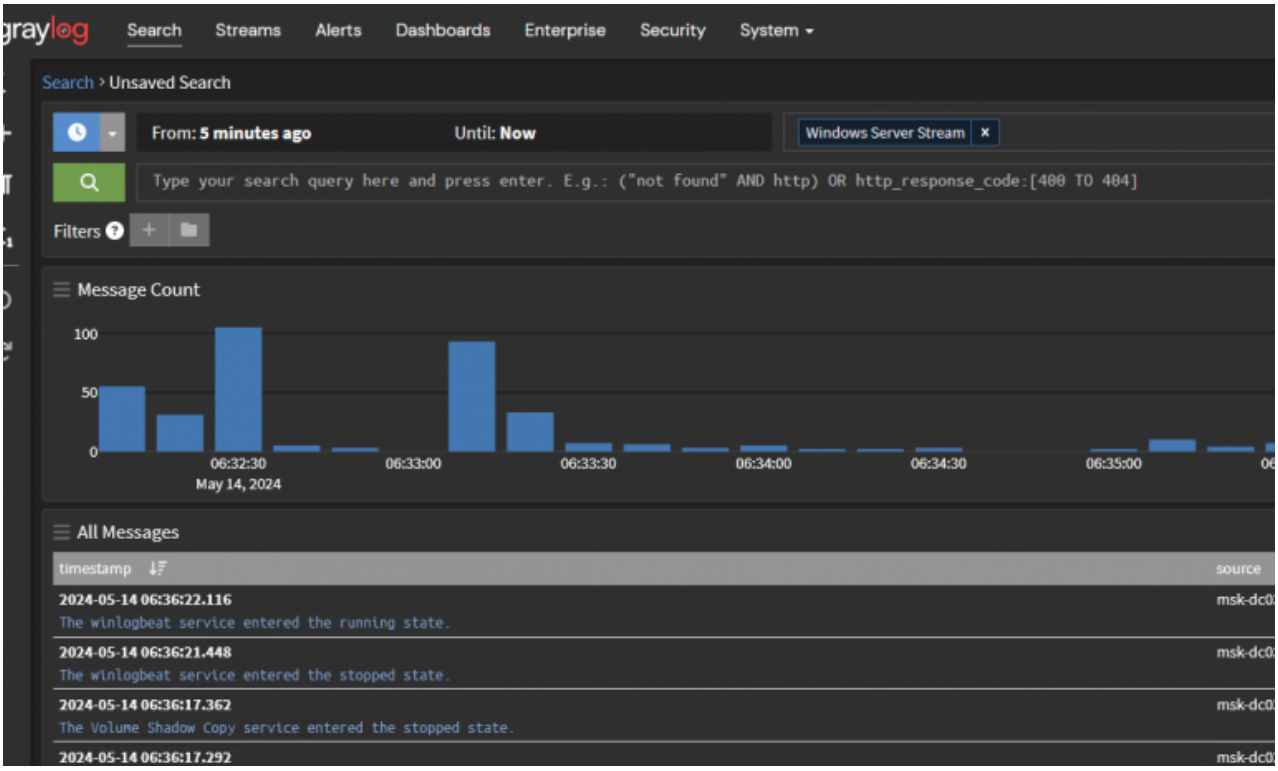


Если все ОК, установите и запустите службу winlogbeat:

```
.\install-service-winlogbeat.ps1
Start-Service winlogbeat
```



Перейдите в веб-интерфейсе GrayLog сервера и проверьте, что в соответствующем потоке стали появляться события с ваших серверов Windows.



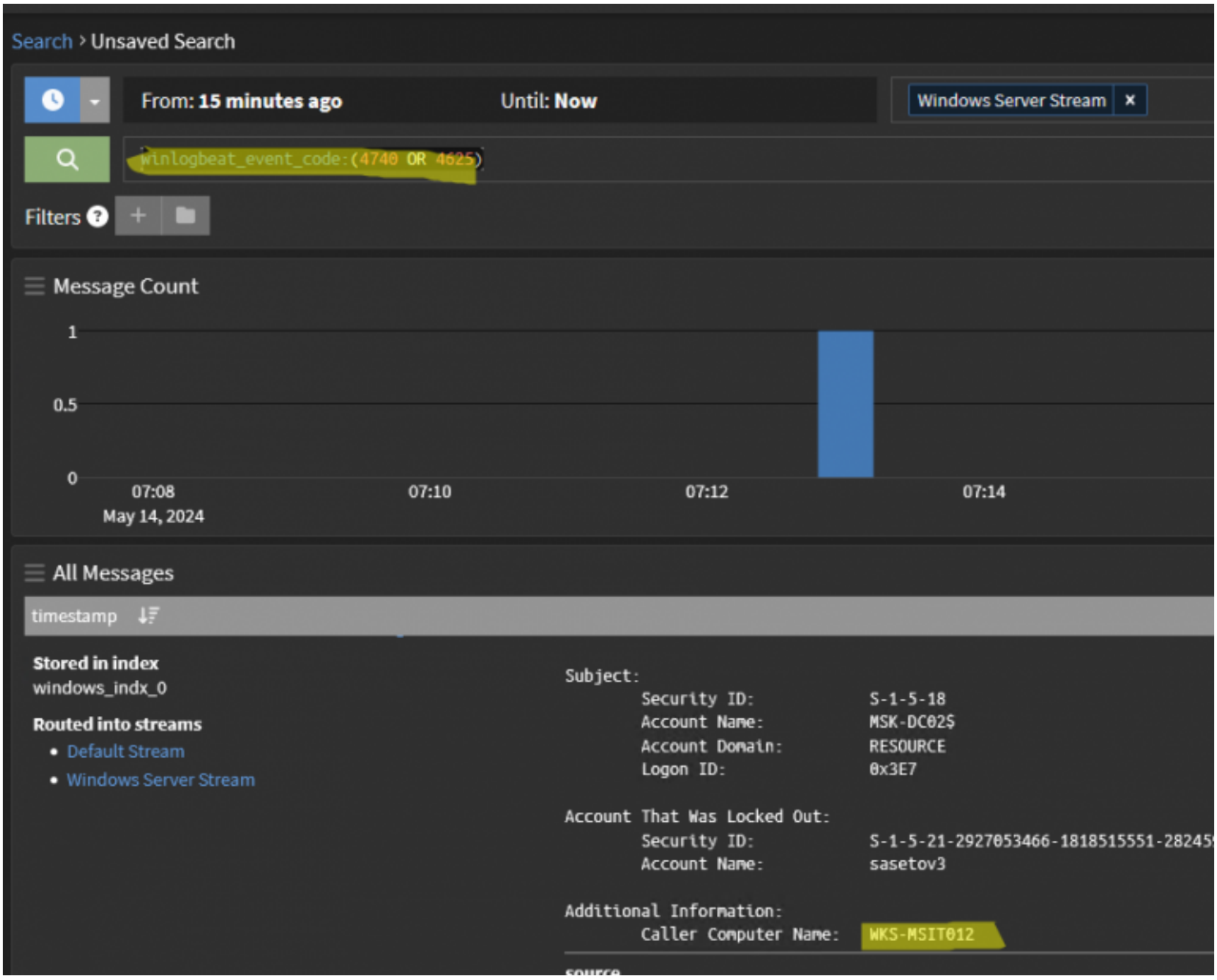
Сбор и анализ событий с контроллеров домена Active Directory с помощью Graylog

Рассмотрим, как использовать сервер Graylog для поиска и анализа событий Windows на примере контроллеров домена Active Directory.

При наличии множества контроллеров Active Directory администратору бывает сложно найти определенное событие, так как приходится просматривать журналы на каждом DC. Благодаря централизованному серверу Graylog, который хранит события со всех контроллеров домена, нужно событие нужно найти за секунды.

Например, вам нужно найти компьютер, с которого была заблокирована учетная запись пользователя из-за неверного ввода пароля. Для этого откройте строку фильтра Graylog, выберите нужный Stream, или укажите его в запросе (`streams:xxxxxxxxxxxxx`) и выполните следующий запрос:

```
winlogbeat_event_code:(4740 OR 4625) AND
winlogbeat_event_provider:Microsoft\-Windows\-Security\-Auditing
```



Сервер Graylog быстро нашел нужно событие и в его свойствах видно имя компьютера, с которого была заблокирована учетная записью.

Еще несколько примеров поиска различных событий в Active Directory:

- Event ID 4767 – позволяет определить кто разблокировал пользователя AD
- Event ID 4724 – кто и когда сбросил пароль пользователю домена
- Event ID 4720 – позволяет узнать, кто и когда создал нового пользователя в AD, 4722 – событие включения учетной записи, 4725 – отключение, 4726 – удаление.

- Отслеживание изменения в группах безопасности AD: 4727 (создана новая группа), 4728 (новый пользователь добавлен в группу), 4729 (пользователь удален из группы), 4730 (группа безопасности удалена)
- Event ID 5137 (создана новая групповая политика домена), 5136 (изменена GPO), 5141 (удалена GPO)
- Event ID 4624 — событие успешного входа пользователя в домен (позволяет быстро получить историю входа пользователя в AD)

Важно настроить отправку логов через Winlogbeat со всех контроллеров домена (список активных DC можно получить с помощью команды **Get-ADDomainController**. Сбор некоторых событий безопасности Active Directory нужно отдельно включить в настройках политик аудита в **Default Domain Controller Policy.**

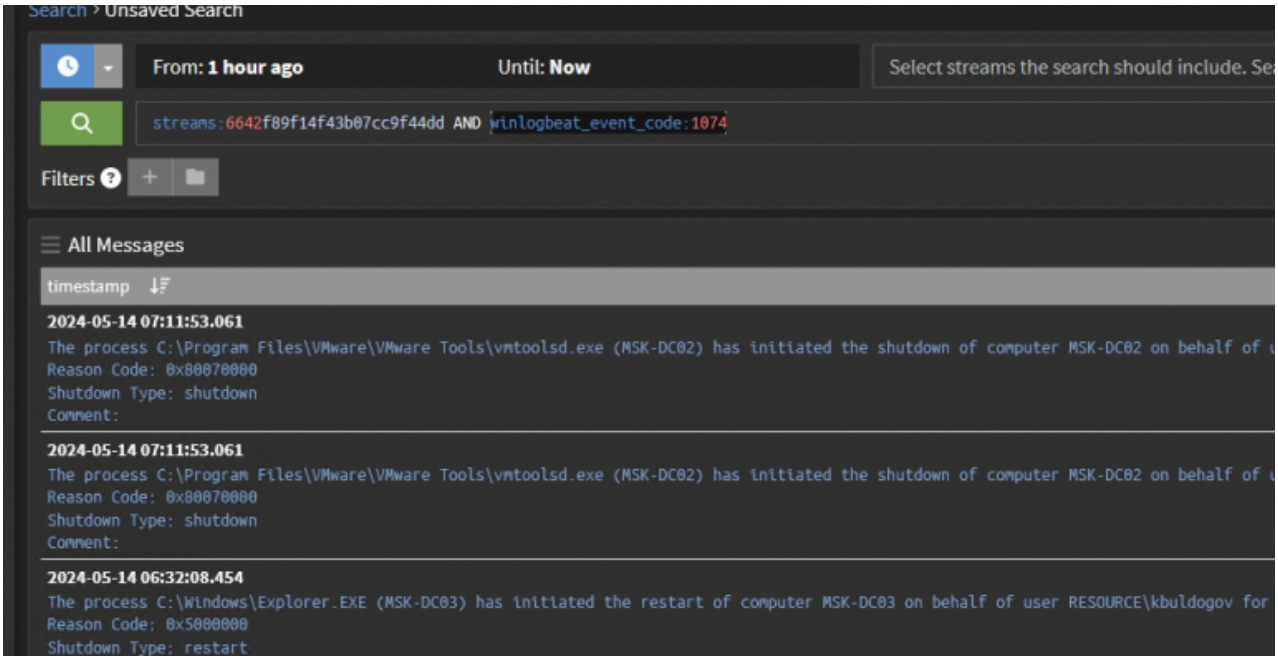
Вы можете создать в Graylog сохранённые запросы и dashboardы для быстрого поиска интересующих вас событий. С помощью оповещений можно настроить рассылку алертов о критических событиях в AD.

Централизованное хранилище логов для хостов Windows

Graylog столь же удобно позволяет хранить, искать и анализировать события от других служб Windows Server. Ниже приведены примеры различных сценариев, в которых администратору приходится выполнять поиск по журналам событий Windows.

- Аудит доступа к файлам и папкам на файловом сервере
- Аудит удаления файлов в сетевой папке
- Аудит изменений NTFS разрешений объектов
- Анализ логов RDP подключений
- Обнаружение перебора паролей к RDP серверу
- Определить кто и когда перезагрузил или выключил сервер Windows: `winlogbeat_event_code:1074`
- Реагирование на очистку журналов событий Windows (возможная компрометация сервера)
- Оповещение об обнаружении вируса на одном из серверов Windows встроенным антивирусом Windows Defender (Event ID 1006, 1116)

При использовании быстрого и простого сервера Graylog поиск и фильтрация событий в журналах Windows существенно упрощается. На сайте Graylog есть статья, в которой указывается список критических событий безопасности Windows, которые рекомендуется отслеживать.



Централизованное хранилище логов Windows и Active Directory удобно использовать для быстрого расследования и реагирования на инциденты информационной безопасности, анализа работы компонентов, выявления сбоев.

1. 

   Роман 14.05.2024

   А почему не NXlog?

   Ответить

   itpro 14.05.2024

   По опыту коллег, для windows машин winlogbeat в разы лучше чем nxlog. Меньше засирает базу и чистые логи без лишних дублирований сообщений.

   Ответить

2. 

Иван 15.05.2024
А можно пример конфига? Для windows на вскидку winlogbeat ?
Что то не выходит ни как. Там по дефолту еще и эластик указан.

Ответить

itpro 15.05.2024
В первом блоке YAML кода полностью рабочая конфигурация для winlobeat. Скопирована напрямую из файла.
Движок сайта немного пожевал структуру, но сейчас все поправлено — можно копировать в вашwinlogbeat.yml

Ответить

3. 

Иван 15.05.2024
То есть и все все остальное можно убирать то что в дефолте?

Ответить

itpro 15.05.2024
Да, это минимальный рабочий конфиг. Остальное в YML шаблоне можно удалить.

Ответить

4. 

Иван 15.05.2024
Для этого откройте строку фильтра Graylog, выберите нужный Stream, или укажите его в запросе (streams:xxxxxxxxxxxxx) и выполните следующий запрос:

winlogbeat_event_code:(4740 OR 4625) AND
winlogbeat_event_provider:Microsoft\-Windows\-Security\-Auditing

Откуда это берется? , streams:xxxxxxxxxxxxx что скрывается под xxxxxxxx. Как выбрать понял просто выпадающий список.
Например меня интересует Event ID 4724, как мне сделать запрос?

winlogbeat_event_code:(4724) ??? получаю восклицательный знак с текстом
Unknown field: Query contains unknown field: winlogbeat_event_code

Вроде данные летят но везде Routed into streams
Default Stream , а для чего тогда создавали Windows Stream?

Ответить

Иван 15.05.2024
Да все работает с запросами но в дефолтном стриме, странно почему не работает тот что я создал?
Этот стрим пустой

Ответить

5. 

Иван 16.05.2024
Все таки вопрос как отключить дефолтный стрим поток? Он вообще нужен, настроил но теперь они оба работают, и новый и дефолтный.

Ответить

Виталий 11.06.2024
Убрать тег default с дефолтного, чтобы он автоматом не цеплялся к windows машинам.

Ответить

6. 

Alexl 21.11.2024
А какую версию Graylog вы использовали?
У меня не получается запустить сбор логов на версии Graylog 5.2 Данные с windows-сервера идут, но в веб-интерфейсе graylog не отображаются. Input типа beats создал. В логах ошибки типа:
ERROR [AbstractTcpTransport] Error in Input [Beats/WinEvents/673ddcb932c2603ef465e2b6] (channel [id: 0x1bc4a5d7, L:/192.168.XXX.50:5044 ! R: /192.168.XXX.28:51228]) (cause io.netty.handler.codec.DecoderException: java.lang.IllegalStateException: Unknown beats protocol version: 69)
Пробовал менять настройки beat-input, но не помогло.

Ответить

Alexl 11.12.2024
Отвечу сам себе. Вся проблема оказалась в версии winlogbeat. Я использовал последнюю, версию 8. Оказывается она не вполне совместима с Graylog 5.2 Откатился на версию winlogbeat 7 и все заработало.

Ответить