VK WorkSpace

Корпоративный мессенджер VK Teams

Инструкция по настройке интеграции с SIEM-системой

Оглавление

Назначение документа 3

Дополнительная документация 3

Отправка логов в SIEM-систему 4

Логируемые события и формат логов 4

- Отправка текстового сообщения 6
- Отправка файла 6
- Аудио или видеовызов 6
- Вход в систему 7

Настройка отправки log-файлов в SIEM-систему 8

Назначение документа

В данном документе представлено описание логируемых событий и формат log-файлов, а также настройка отправки log-файлов в SIEM-систему.

Документ предназначен для использования системными администраторами.

Дополнительная документация

Логи клиентских приложений VK Teams — в документе представлена информация об инструментах сбора логов, расположении логов и приведены примеры запросов и ответов.

Отправка логов в SIEM-систему

Для интеграции с SIEM-системой используется мультиплатформенный инструмент сбора и централизации журналов NXLog.

По умолчанию отправка log-файлов в SIEM-систему осуществляется через syslog, однако используемый продукт поддерживает множество различных транспортов. Подробнее — в документации на продукт https://nxlog.co/products/nxlog-community-edition.

Логируемые события и формат логов

В SIEM-систему отправляются логи следующих событий мессенджера:

- Отправка текстового сообщения (IM).
- Отправка файла (FILE).
- Аудио или видеовызов (CALL).
- Логин (LOGIN).
- Удаление сообщения (DEL_MSG).
- Удаление истории (DEL_HISTORY).

Все записи в логе соответствуют следующему формату:

```
Дата время|IP пользователя A|ID пользователя A|ID пользователя Б|User-Agent пользователя A|Тип события|Специфические для события данные|Аутентификационый токен
```

Описание полей представлено в таблице ниже:

Поле	Описание	Формат
Дата	Дата события	YYYY-MM-DD
Время	Время события	hh:mm:ss
IP пользователя A	IP адрес пользователя, совершившего событие	XXX.XXX.XXX.XXX
ID пользователя A	Идентификатор пользователя, совершившего событие	email
ID пользователя Б		email или ID группы или «-», если не

Поле	Описание	Формат
	Идентификатор пользователя получателя события	применимо к событию
User-Agent пользователя A	User-Agent пользователя A, по заголовку User-Agent в HTTP-запросах	Описание формата представлено ниже
Тип события	Тип события: звонок, отправка сообщения и т.д.	CALL, IM, FILE, LOGIN, DEL_MSG, DEL_HISTORY
Специфические для события данные	Флаги и опции, специфичные для события	Зависит от события
Аутентификационый токен	Хэш от сессионного токена пользователя. Может отсутствовать. Например, при логине, так как сессия пользователя еще не создана. Хэш от токена можно использовать, чтобы отличить различные сессии одного пользователя. Получить аутентификационный токен из хэша нельзя.	d9ce1e74d5

Формат User-Agent:

- Для Android, iOS и Desktop:

```
VKTeams {Android, iOS, Desktop} <user email> <Application ID> <build version A.B.C(D)> <OS Version> <Device>
```

- Для WEB клиента User-Agent зависит от браузера и может выглядеть так:

```
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.185 YaBrowser/20.11.3.0 (beta) Yowser/2.5 Safari/537.36
```

Пути к log-файлам

/oap/icq/logs/*.on-premise.log — для данной группы файлов все строки логов являются источником информации для SIEM-системы.

/data/tarantool/logs/nomail-*.log — для данной группы файлов источником для SIEM-системы являются строки логов, попадающие под регулярное выражение **^.*?fss:.***

Отправка текстового сообщения

Пример: Пользователь i.ivanov@domain.ru отправил тестовое сообщение пользователю v.petrov@domain.ru. IP адрес и User-Agent пользователя i.ivanov@domain.ru - 109.195.135.94 и Myteam Desktop 155576093 ic1nmMjqg7Yu-0hL 10.0.0(42540) Windows_10 PC соответственно.

Запись в логе:

```
2020-11-30 10:06:38|109.195.135.94|i.ivanov@domain.ru|v.petrov@domain.ru|Myteam Desktop
i.ivanov@domain.ru ic1nmMjqg7Yu-0hL 10.0.0(42540) Windows_10 PC|IM|-|d9ce1e74d5
```

Отправка файла

Параметр	Описание
file_id	Хэш от идентификатора файла. Можно использовать для сопоставления с другими записями в этом же логе. Нельзя использовать для получение контента файла.

Пример: Пользователь d.sidorov@domain.ru отправил файл в группу 683673651@chat.agent.

Запись в логе:

```
2020-11-30 10:25:05|95.57.100.171|d.sidorov@domain.ru|683673651@chat.agent|Myteam Android
d.sidorov@domain.ru ao1mAegmj4_7xQOy 9.16.1(824729) Android_7.1.1_25 SM-J510FN|FILE|
file_id=5191ceb402|ac6208d080
```

Аудио или видеовызов

Пример: Пользователь a.smirnov@domain.ru вызвал пользователя d.kulikov@domain.ru. 2020-11-30 09:36:36 - дата и время начала звонка.

Запись в логе:

```
2020-11-30 09:36:36|176.59.142.53|a.smirnov@domain.ru|d.kulikov@domain.ru|Myteam Android
a.smirnov@domain.ru ao1mAegmj4_7xQOy 7.7.2(823881) Android_5.1.1_22 SM-J320F|CALL|-|5daaefde7f
```

Вход в систему

Параметр	Описание
type	Тип логина. Сейчас доступен только OTP.
result	- sent — OTP отправлен на почту пользователю; - invalid — введен неверный OTP, или срок его жизни истёк; - success — успешный логин.

Запрос OTP:

```
2020-11-30 01:21:21|172.11.11.67|d.sidorov@domain.ru|-|Myteam Android d.sidorov@domain.ru
ao1mAegmj4_7xQOy 7.7.2(823881) Android_5.1.1_22 SM-J320F|LOGIN|type=otp,result=sent|-
```

Неуспешная попытка логина пользователя d.kulikov@domain.ru по OTP:

```
2020-11-30 01:21:21|172.11.11.67|d.kulikov@domain.ru|-|Myteam Android d.kulikov@domain.ru
ao1mAegmj4_7xQOy 7.7.2(823881) Android_5.1.1_22 SM-J320F|LOGIN|type=otp,result=invalid|-
```

Успешная попытка логина пользователя d.kulikov@domain.ru по OTP:

```
2020-11-30 01:21:21|172.11.11.67|d.kulikov@domain.ru|-|Myteam Android d.kulikov@domain.ru
ao1mAegmj4_7xQOy 7.7.2(823881) Android_5.1.1_22 SM-J320F|LOGIN|type=otp,result=success|-
```

Удаление сообщения

```
21-12-10 17:02:59|100.100.31.151|dev001@nsoldatov.v2.im-sandbox.devmail.ru|
dev002@nsoldatov.v2.im-sandbox.devmail.ru|<-|Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36|DEL_MSG|-|
silent=0,msgid=7040073549926629644,
```

Удаление истории

```
21-12-10 17:14:34|100.100.31.151|dev001@nsoldatov.v2.im-sandbox.devmail.ru|
dev002@nsoldatov.v2.im-sandbox.devmail.ru|<-|Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36|DEL_HISTORY|-|
upTo=7040073549926629644,
```

Настройка отправки log-файлов в SIEM-систему

1. В конфигурационном файле **/usr/local/etc/k8s/helmwave/projects/nxlog/values/nxlog.yml** в блоке **<Output siem_system>**

   указать IP-адрес и порт приемника SIEM:

   ```
   <Output siem_system>
       Module  om_udp
       Host    <указать IP-адрес>
       Port    <указать порт>
       <Exec>
             $Severity = 'INFO';
             $SyslogFacility = 'AUDIT';
             $SourceName = 'logs';
             $Hostname = '${NODE_NAME}';
              to_syslog_bsd();
       </Exec>
   </Output>
   ```

   В данном блоке в качестве приемника используется Syslog-сервер. Если будет использоваться не Syslog-сервер, опишите настройки для другой системы (см. официальную документацию https://docs.nxlog.co/integrate/index.html).

2. В конфигурационном файле **/usr/local/etc/k8s/helmwave/projects.yml** удалить nxlog.

3. Для запуска nxlog выполните команды в зависимости от типа инсталляции.

   Для инсталляций на одну виртуальную машину:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwbuild -t nxlog
   HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t nxlog
   ```

   Для кластерной инсталляции:

   ```
   HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwbuild -t nxlog
   HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t nxlog
   ```

4. Посмотреть логи самого сервиса можно при помощи команды:

   ```
   kubectl -n vkteams -l app=nxlog --tail -1
   ```

Дата обновления документа: 09.10.2024 г.