VK WorkSpace

Корпоративный мессенджер VK Teams

Логи VK Teams

Оглавление

Назначение документа

В данном документе представлена информация об инструментах сбора логов клиентских приложений и серверных логов, описано расположение логов, а также приведены примеры логов клиентских приложений.

Документ предназначен для использования администраторами организации.

Дополнительная документация

Инструкция по настройке интеграции с SIEM-системой — в документе представлено описание логируемых событий и формат log-файлов, а также настройка отправки log-файлов в SIEM-систему.

Сбор серверных логов

Способ 1. Универсальный инструмент сбора логов report.sh

Для сбора логов, информации о системе и оборудовании, а также копий конфигурационных файлов — под пользователем root выполнить команду `/usr/local/bin/report.sh` с необходимым ключом:

- `-s` — информация о системе;
- `-k` — логи подов кубернетиса;
- `-l` — информация о системе и логи за последние 2 часа;
- `-h` — справка;
- `-F` — выгрузка полных логов;
- `-f` — выгрузка указанных логов сервиса за определенный период времени:
  Для выгрузки необходимо указать ключи:
  - `-f` — сервис;
  - `-B` — начальная дата поиска;
  - `-A` — конечная дата для поиска.
    Формат указания даты ГОД-МЕСЯЦ-ЧИСЛО.
    Можно указывать несколько сервисов через ключ `-f`, например: `-f beagle -f krtek`.
    Если ключ `A` не указан, то будут найдены log-файлы за период указанный в `-B` по текущий день.
    Если ключи `-A` и `-B` не указаны, будут найдены все доступные log-файлы за весь период.
    Пример работы скрипта report.sh с ключом `-f`:

    ```
    report.sh -f beagle -f krtek -B 2023-11-20 -A 2023-11-22
    ```

    Скрипт соберет логи за указанный период. Вывод команды будет следующим:

    ```
    [14:44:12] Все данные будут размещены в каталоге /mnt/log/report
    [14:44:12] Создаю директорию /mnt/log/report
    [14:44:12] Создаю директорию /mnt/log/report/find_log
    [14:44:13] Для отправки данных в MAIL.RU GROUP вам потребуется сетевой доступ к
    https://files.icq.com
    [14:44:13] Отправить собранные данные в MAIL.RU GROUP?
    1) Yes
    2) No
    ```

- `-d` — выбор директории для выгрузки логов;

  Пример работы ключа:

  ```
  /usr/local/bin/report.sh -F -d /tmp
  ```

  Команда сохранит полную выгрузку report.sh в папку /tmp/report. Вывод команды будет следующим:

```
[10:00:04] Все данные будут размещены в каталоге /tmp/report
[10:00:04] Создаю директории /tmp/report/archive /tmp/report/sysinfo
[10:00:04] Собираю информацию о systemd units.
[10:00:04] Собираю сетевые настройки.
[10:00:04] Собираю информацию о конфигурации оборудования.
```

Ключи можно комбинировать, а также указывать несколько сервисов для поиска, например:

```
report.sh -s -l -f beagle -f krtek
```

Скрипт report.sh умеет отправлять собранные данные в службу технической поддержки. Для отправки выберите пункт 1 (Yes) в ответ на вопрос «Отправить собранные данные в MAIL.RU GROUP?». Отправка осуществляется только в том случае, если есть сетевой доступ до сервера https://files.icq.com. Иначе необходимо передать все собранные данные другим способом, например, разместить их для скачивания на собственных серверах.

Пример работы скрипта report.sh с ключом `-f`:

```
[16:09:38] Все данные будут размещены в каталоге /mnt/log/report
[16:09:38] Создаю директории.
[16:09:38] Собираю данные из системных журналов.
[16:09:39] Собираю данные из сервисных журналов.
[16:09:40] Собираю конфигурацию сервисов.
[16:09:40] Собираю информацию о systemd units.
[16:09:40] Собираю сетевые настройки.
[16:09:40] Собираю информацию о конфигурации оборудования.
[16:09:41] Собираю информацию об использовании памяти.
[16:09:42] Собираю информацию об открытых файлах.
[16:10:42] Собираю информацию об использование дискового пространства.
[16:10:42] Собираю информацию о запущенных процессах.
[16:10:42] Собираю информацию о работе сервисов.
[16:10:54] Собираю информацию об установленном программном обеспечении.
[16:10:55] Сжимаю всю полученную информацию.
[16:10:57] Сжимаю конфигурационный файл инициализации.
tar: Removing leading `/' from member names
[16:10:57] Для отправки данных в MAIL.RU GROUP вам потребуется сетевой доступ к https://
files.icq.com
[16:10:57] Отправить собранные данные в MAIL.RU GROUP?
1) Yes
2) No
```

По умолчанию все собранные данные сохраняются в каталоге **/mnt/log/report**.

Если необходимо изменить каталог, выполните команду с указанием каталога, в котором будут сохраняться временные данные, например:

```
/usr/local/bin/report.sh /tmp
```

Способ 2. Логи Vector

Данный способ используется, если нет возможности загрузить **report.sh**, либо это избыточно (например, после выполнения команд по просьбе службы технической поддержки).

Под пользователем root выполнить команду:

```
tar -czf vector.tar.gz /var/log/vector/
```

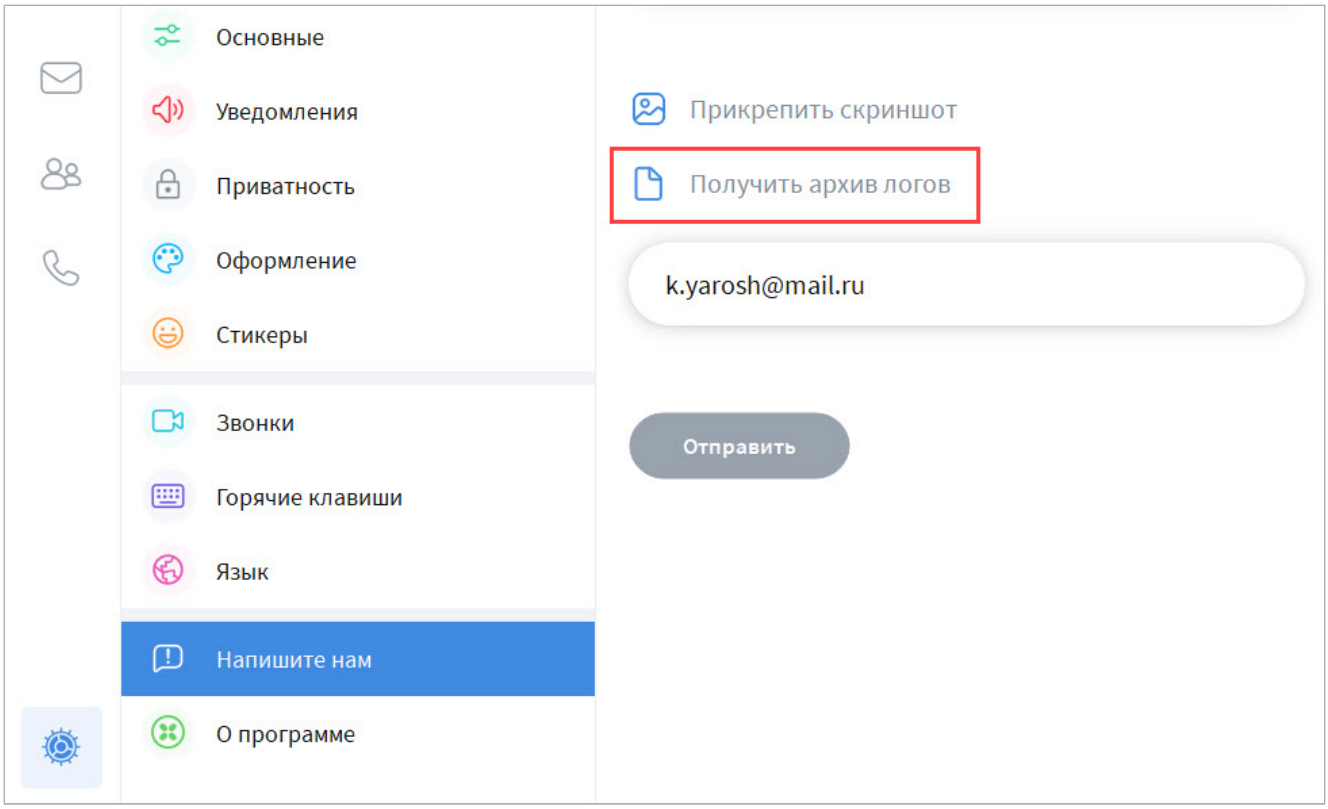
и прислать поддержке архив **vector.tar.gz**.

В Vector хранятся логи всех сервисов, которые пишут их в стандартное место (большинство сервисов). Логи размещаются в директорию **/var/log/vector/k8s** в виде текстовых файлов с группировкой по пространству имен.

Сбор логов клиентских приложений

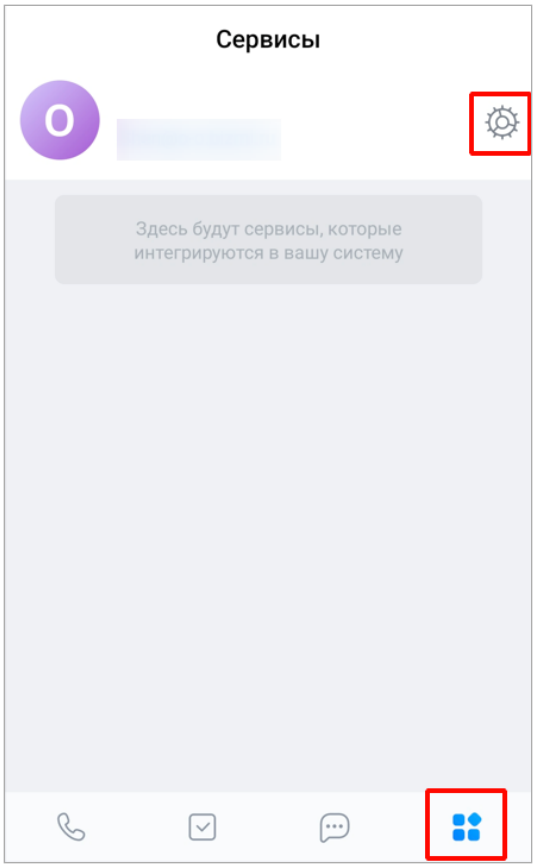
В десктопной версии приложения

1. Перейдите в настройки VK Teams, нажав на значок  в левом нижнем углу.
2. Выберите раздел **Напишите нам**, затем нажмите на кнопку **Получить архив логов**:



В мобильной версии приложения

1. Выберите пункт **Сервисы**, затем нажмите на значок  .



2. Выберите пункт **Общие**, затем нажмите на пункт **О программе** и удерживайте его нажатым в течение 15 секунд.

Расположение логов

Логи десктопных приложений

В зависимости от операционной системы логи десктопных приложений находятся:

Windows: AppData/Local/VKTeams/logs

Mac Site: ~/Library/Application Support/VKTeams/logs

Mac Store: ~/Library/Containers/com.icq.macicq/Data/Library/Application Support/VKTeams/logs

Linux: .config/VKTeams/logs

Логи звонков: логи десктопных приложений находятся в расширенных настройках или, если релизная версия, перейти **Настройки** > **Напишите нам** > **Получить архив логов**. Для получения логов мобильных приложений перейти **Настройки** > долгое нажатие на версию приложения внизу экрана > **Develop** > **Действия с логами** > **Получить архив**.

Серверные логи

Логи звонков

Хранятся в файле **/var/log/janus.log**. В службу технической поддержки можно передать как выжимку за конкретную дату, так и файл целиком в виде архива.

Логи отдельных служб

Сервисы VK Teams могут писать логи в нестандартное место, указанное в конфигурационном файле сервиса.

Большинство логов находится в **/var/log/service/** (пишутся только ошибки и выводы) и в **/mnt/log/oap/icq/logs**.

Php: /srv/store/logs/

Nginx до ротации: /oap/icq/domains/local_proxy.icq.com/logs

Nginx после ротации: /oap/icq/domains/local_proxy.icq.com/logs/old_logs

Сервис Go-files: /oap/icq/logs/go.files.icq.com/

БД MySQL: /db/logs/mysql

БД Tarantool: /data/tarantool/logs

Логи Kubernetes

В случае проблем с подами Kubernetes:

Ошибки: kubectl logs <pod>

Описание: kubectl describe <pod>

Либо под пользователем root можно использовать оснастку **k9s**.

Логи сервиса Keycloak

Логи находятся в **/var/log/vector/k8s/keycloak/keycloak/***

При наличии проблем с синхронизацией пользователей в первую очередь следует отслеживать записи уровня ERROR. Пример такой ошибки: дубликат пользователя — когда один и тот же пользователь заведен в нескольких ветках LDAP-каталога. Как правило, после каждой записи ERROR идет трассировка ошибки для более детального анализа.

Базовые действия и методы к логами клиентских приложений и серверными логами

Действие	Метод
Сессии	
Логин по паролю	clientLogin
Логин по номеру телефона	loginWithPhoneNumber
Запрос кода для логина	requestPhoneValidation
Проверка валидности номера	smsphoneinfo
Нормализация номера телефона	normalizePhoneNumber
Старт сессии (после логина, обновления или по директиве сервера)	startSession
Проверка, активна ли сессия	pingSession
Окончание сессии (пользователь разлогинился сам, либо это выполнил сервер)	endSession
История	
Отправка сообщения	sendIM
Удаление сообщения	delMsgBatch
Редактирование сообщения	sendIM
Запрос истории	getHistory
Список пользователей для упоминания	getRecentWriters

Действие	Метод
Недавние чаты	
Отправка статуса прочитанности чата	setDlgState
Получение нового сообщения (не из пуша)	histDlgState
Удаление контакта из листа контактов	removeBuddy
Скрыть чат из недавних	hideChat
Группы	
Получение информации о группе	getChatInfo
Получение списка участников чата	getChatMembers
Список тех, кто уже добавлен в группу	getChatContacts
Принять/отклонить пользователя в чат с включенной настройкой «Вступление по запросу»	chatResolvePending
Создание чата	createChat
Изменение настроек чата	modChat
Добавление в чат	addChat
Пользователь	
Получение информации о пользователе	getUserInfo
Получение информации по ссылке	getIdInfo
Галерея	
Запрос галереи чата	getEntryGallery
Настройки	

Действие	Метод
Запрос настроек приватности	getPrivacySettings
Изменение настроек приватности	updatePrivacySettings
Привязка номера телефона	attachPhoneNumber
Получить список сессий	session/list
Завершить сессию	session/reset
Получить список игнорируемых	getPermitDeny
Добавить пользователя в игнорируемые	setPermitDeny
Обновление своего профиля	memberDir/update
Установить никнейм	setNick
Проверить никнейм на уникальность	checkNick
Поиск	
Поиск сообщений по одному чату	searchOneDialog
Поиск сообщений по всем чатам	searchAllDialogs
Поиск (люди, глобальный поиск групп)	search
Опросы	
Информация об опросе	poll/get
Проголосовать	poll/set
Реакции	
Получить реакцию на сообщения	reaction/get
Отправить реакцию на сообщения	reaction/set

Действие	Метод
Получить список отправивших реакцию на сообщение	reaction/list
Файлы и сниппеты	
Превью внешней ссылки	getPreview
Оригинал внешней ссылки	getUrlContent
Заливка файла	files/init
Информация о файле	files/getinfo
Расшифровка Push-to-talk	speechToText
Звонки	
Создать звонок по ссылке / вебинар	conference/create
	type: equitable - ссылка на звонок со множеством участником webinar - вебинар
Инициация обычного звонка	webrtc/alloc
Дозвон обычного звонка	voip/webrtcMsg
Получение списка масок	masks/list
Стикеры, умные ответы, саджесты	
Саджесты стикеров	getSuggest
Витрина стикеров	/store/store/my
Умные ответы на цитату	getSmartReply

Примеры запросов и ответов для логов клиентских приложений

Логи клиентских приложений хранятся на рабочих станциях пользователей.

Ниже представлены примеры логов клиентских приложений — примеры запросов клиента к серверу и примеры ответа сервера VK Teams.

Пример 1. Запрос getPrivacySettings и успешный ответ (20000)

```
POST /api/v34/rapi/getPrivacySettings HTTP/2
Host: u.icq.net
User-Agent: ICQ Desktop 728059286 ic18eTwFBO7vAdt9 3.0.0(30191) MacOSX_11.0 PC
Accept: */*
Accept-Encoding: gzip
Connection: keep-alive
Content-Type: application/json;charset=utf-8
Content-Length: 71

{"aimsid":"030.4294792228*:728059286","reqId":"1-1606731232"}
We are completely uploaded and fine
HTTP/2 200
```

Ответ:

```
{"status": {"code": 20000}, "results": {"groups":
{"allowTo": "myContacts", "inviteBlacklistSize": 1}, "calls":
{"allowTo": "myContacts"}, "smsNotify": {"allowTo": "everybody"}}}
```

Пример 2. Запрос getChatMembers и ответ 50000 (Request timed out)

```
POST /api/v31/rapi/getChatInfo HTTP/2
Host: u.icq.net
User-Agent: ICQ Desktop a.yatskov@corp.mail.ru ic18eTwFBO7vAdt9 3.0.0(30096) MacOSX_10.15 PC
Accept: */*
Content-Encoding: zstd
IM-ZSTD-Request-Dict: im-zstd-dict-desktop-request-210720.zdict
Connection: keep-alive
Content-Type: application/json;charset=utf-8
Accept-Encoding: zstd, gzip
IM-ZSTD-Response-Dict: im-zstd-dict-desktop-response-210720.zdict
Content-Length: 79
```

```
{"aimsid":"153.3649523331.*:a.yatskov@corp.mail.ru","params":{"memberLimit":
5,"sn":"681826564@chat.agent"},"reqId":"21257-1606742661"}
```

Ответ:

```
{"ts": 1606742665, "status": {"code": 50000, "reason": "Request timed out"},
"method": "getChatInfo", "reqId": "21257-1606742661", "results": {}}
```

Пример 3. Запрос getChatMembers и ответ 40000 (Bad request)

```
POST /api/v31/rapi/getChatInfo HTTP/2
Host: u.icq.net
User-Agent: ICQ Desktop a.yatskov@corp.mail.ru ic18eTwFBO7vAdt9 3.0.0(30096) MacOSX_10.15 PC
Accept: */*
Content-Encoding: zstd
IM-ZSTD-Request-Dict: im-zstd-dict-desktop-request-210720.zdict
Connection: keep-alive
Content-Type: application/json;charset=utf-8
Accept-Encoding: zstd, gzip
IM-ZSTD-Response-Dict: im-zstd-dict-desktop-response-210720.zdict
Content-Length: 79

{"aimsid":"153.3649523331.*:a.yatskov@corp.mail.ru","params":{"memberLimit":
5,"sn":"681826564@chat.agent"},"reqId":"21257-1606742661"}
```

Ответ:

```
{"ts": 1606742665, "status": {"code": 40000, "reason": "Bad request"},
"method": "getChatInfo", "reqId": "21257-1606742661", "results": {}}
```

Пример 4. Проблемы с DNS

```
curl_easy_perform result is 6 (Couldn't resolve host name)
Could not resolve host: u.icq.net
```

Дата обновления документа: 18.04.2024 г.