Мессенджер и ВКС

Логи

Портал с документацией: https://biz.mail.ru/docs/on-premises/

Оглавление

Назначение документа

В данном документе описаны инструменты сбора серверных логов и описано расположение логов.

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 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.

Расположение логов

Логи звонков

Логи видеоконференций можно смотреть в k9s, под janus.

В службу технической поддержки можно передать как выжимку за конкретную дату, так и файл целиком в виде архива.

Логи отдельных служб

Сервисы Мессенджер и ВКС 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** (логи сервисов за последний час).

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**. Данный интерфейс отображает запущенные поды с их статусами.

Логи Docker

Статус сервисов, запущенных в Docker-контейнере: docker ps

Статус всех сервисов, развернутых в Docker-контейнере: docker ps -a

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.

Технический писатель: Белова Ирина

26 ноября 2025 г.