Настройка выгрузки событий ovirt-engine на удалённый rsyslog сервер

Окружение

- **Версия РЕД ВИРТ:** 7.3

При необходимости отправки определённых записей журнала **События** можно настроить отправку на удалённый сервер журналирования — **rsyslog**.
В данной статье будет рассмотрен один из способов реализации отправки некоторых типов сообщений и хранения этой информации из журналов **ovirt-engine**.
Процесс настройки сервера журналирования представлен в статье https://redos.red-soft.ru

Настройка ВМ HostedEngine

Для реализации будет использоваться модуль для работы с файлами **imfile** сервиса **rsyslog**. Для его работы необходимо предварительно обновить пакет **rsyslog** на виртуальной машине управления HostedEngine:

```
dnf update rsyslog --enablerepo=*
```

Для отправки событий из журнала `/var/log/ovirt-engine/engine.log` по заданным ключевым словам, содержащимся в сообщении журнала, необходимо создать конфигурационный файл. На виртуальной машине управления HostedEngine в директории `/etc/rsyslog.d/` создать файл с расширением `.conf`:

```
module(load="imfile")

input(
  type="imfile"
  File="/var/log/ovirt-engine/engine.log"
  Tag="My_Engine:"
  Facility="local0"
  Severity="info"
  PersistStateInterval="100"
)

if ($msg contains "PATTRN1" or $msg contains "PATTRN2" or $msg contains "Failed")
then {
```

```
  action(
    type="omfwd"
    target="remote.rsyslog.fqdn"
    port="514"
    protocol="tcp"
    template="RSYSLOG_SyslogProtocol23Format"
  )
  stop
}
```

Где:

- **/var/log/ovirt-engine/engine.log** — Путь до журнала на ВМ HostedEngine;
- **My_Engine:** — Тэг, добавляемый службой **rsyslog** при перенаправлении сообщений на удалённый сервер;
- **PATTRN1, PATTRN2, Failed** — Ключевое слово, которое должно содержаться в сообщении, для перенаправления сообщения на сервер;
- **remote.rsyslog.fqdn** — Доменное имя **rsyslog** сервера, на который будет производиться перенаправление сообщений;
- **514** — Порт **rsyslog** сервера, на который будет производиться перенаправление сообщений;
- **tcp** — Протокол, по которому будет производиться перенаправление сообщений на сервер **rsyslog**.

После внесения изменений в конфигурацию перезагрузите сервис **rsyslog**:

```
systemctl restart rsyslog
```

Пример сообщения с удалённого сервера **rsyslog** содержащего **PATTRN1** и **Failed**:

```
[root@localhost rsyslog]# cat /var/log/rsyslog/eng/engine.log
Dec 18 18:13:42 eng My_Engine 2025-12-18T18:13:42+03:00 TEST PATTRN1
Dec 18 18:15:38 eng My_Engine 2025-12-18T18:15:38+03:00 Failed to resume VM
117-RO-8
(Host: host.redvirt.test, User: ivan.ivanov@internal).
```

Источник: https://redvirt.red-soft.ru/base/knowledge-base/event-rsyslog-server/