Руководство по использованию Terraform-провайдера zVirt

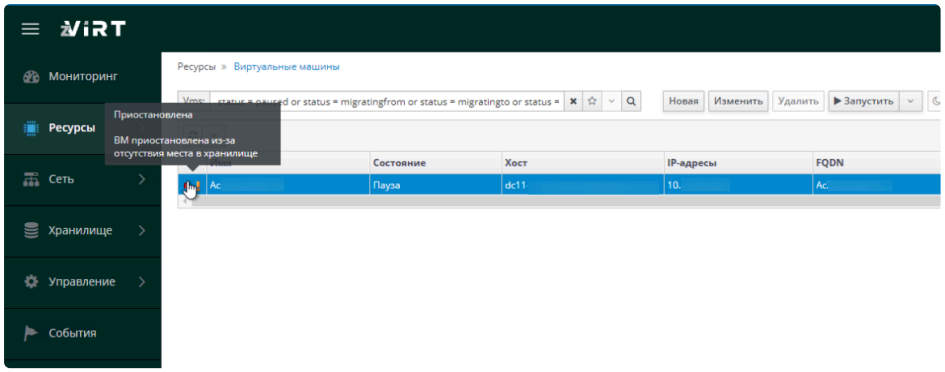
- Начало работы
- Источники данных Terraform
- Ресурсы TF
- Примеры использования

Ошибка ВМ приостановлена из-за отсутствия места в хранилище при восстановлении СРК Acronis

1. Вопрос

При восстановлении ВМ с использованием СРК Acronis возникает ошибка: **ВМ приостановлена из-за отсутствия места в хранилище**.

Данная проблема возникает при использовании **thin-provisioned** дисков.



2. Ответ

- Необходимо произвести настройку SPM по инструкции.
- Необходимо произвести настройку VDSM по инструкции.

Ошибка "Must be owner of extension uuid-ossp" при восстановлении из резервной копии

1. Описание проблемы

При восстановлении Менеджера управления из резервной копии с помощью команды **engine-backup** в режиме **restore**, возникает ошибка:

```
FATAL: Errors while restoring database engine
```

В логах числится ошибка:

```
pg_restore: error: could not execute query: ERROR:  must be owner of extension uuid-ossp
```

2. Решение

Пошаговое решение:

1. Подключитесь к Менеджеру управления
2. Выполните повторную очистку для удаления части восстановившихся данных

   ```
   engine-cleanup
   ```

3. Смените пользователя на **postgres**

   ```
   su - postgres
   ```

4. Подключитесь к базе данных **engine**:

   ```
   psql engine
   ```

5. Очистите лишние записи, занимающие uid:

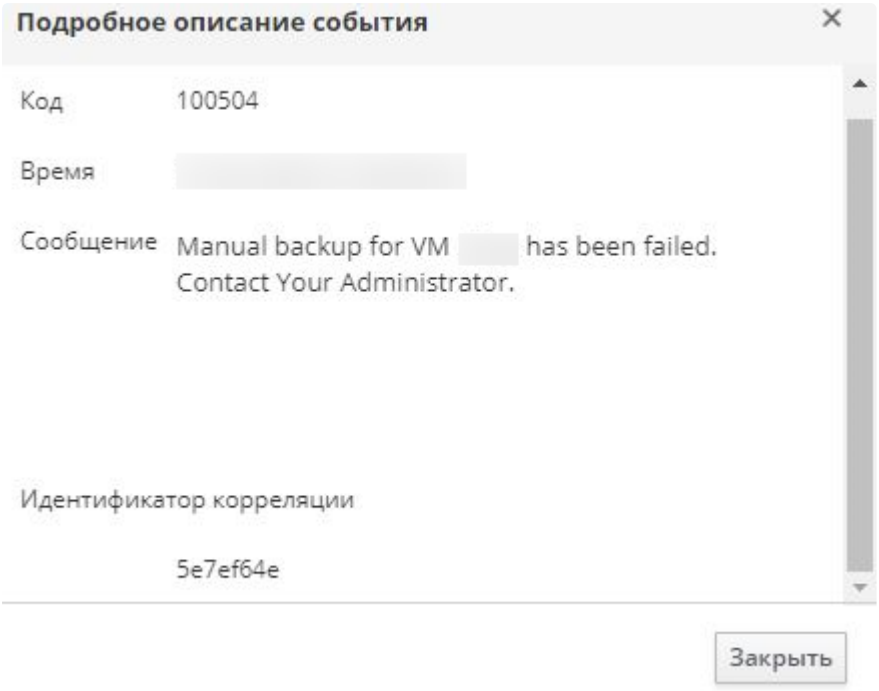
   ```
   SELECT lo_unlink(l.oid) FROM pg_largeobject_metadata l;
   ```

6. Вернитесь к пользователю **root** и повторите попытку восстановления Менеджера управления

Ошибка "Manual backup for VM NAME has failed"

1. Описание проблемы

Во время резервного копирования в zVirt 3.0 возникает ошибка: **Manual backup for VM NAME has failed. The is not enough free storage on the storage domain 'NAME' available to backup the VM**



В логах можно найти сообщение:

```
ERROR [org.ovirt.engine.core.common.utils.backup.] Backup script execution
failed.The storage domain DomainName is in state active.
!!! Got unexpected exception: !!! The is not enough free storage on the storage
domain 'StorageName' available to backup the VM 'VM_name'.

Executing backup script: [./backup.py -c ./config.cfg --vm-names ["VM_name"] --
vm-middle _21e0_MB --snapshot-description ubuntu_backup_temp_snapshot
--server https://ovirt-engine-name/ovirt-engine/api --username
BACKUP_USERNAME_2022-10-26 09:20:06@internal --password 1
--export-domain export --timeout 10 --cluster-name Default --vm-name-max-length
100 --storage-domain local --storage-space-threshold 5.0 --datacenter-name
Default]
```

Параметр **--storage-space-threshold** принимает значение **5.0**. При проверке свободного места в домене хранения и домене для резервного копирования - места достаточно.

2. Решение

1. Подключиться к менеджеру управления по SSH и скопировать RPM-пакет с исправлениями
2. Остановить **ovirt-engine.service** командой:

```
systemctl stop ovirt-engine.service
```

3. Перейти в директорию, куда был скопирован RPM-пакет с исправлениями и выполнить его переустановку командой:

```
dnf reinstall ovirt-engine-backend-4.4.9.5-1.el8.noarch.rpm
```

4. Запустить **ovirt-engine.service** командой:

```
systemctl start ovirt-engine.service
```

5. Повторно выполнить резервное копирование.

ВМ выключается при выполнении резервного копирования с помощью Acronis

1. Вопрос

При выполнении задачи резервного копирования с помощью **Acronis Защита Данных**, **ВМ Acronis** переходит в режим **Выключена**

2. Решение

Установите гостевые дополнения в гостевые ОС ВМ:

- ссылка на гостевые дополнения;
- ссылка на гостевые дополнения, включающие драйверы для устаревших версий ОС Windows;
- Пункт 2.1.2 по установке пакетов из репозитория.

Замена SSL-сертификата для веб-портала (zVirt 3.2 и ниже)

Данная инструкция актуальна только для zVirt версии 3.2 и ниже.

Сертификат стороннего ЦС (Certificate Authority) предоставляется в виде PEM-файла. Цепочка сертификатов должна быть полной вплоть до корневого сертификата. Порядок цепочки сертификатов является критически важным, цепочка должна строится от последнего промежуточного ЦС до корневого ЦС. В противном случае при проверка подлинности сервера может произойти сбой.

Закрытый ключ предоставляется в виде KEY-файла.

1. Соглашения

- **/root** - расположение файлов полученных от ЦС или в процессе выполнения процедуры замены.
- **/root/apache.p12** - сертификат полученный от ЦС в формате PKCS#12.
- **/root/ca.pem** - сертификат ЦС.
- **/root/apache.key** - новый закрытый ключ веб-сервера.
- **/root/apache.cer** - новый сертификат веб-сервера.

- Файл с расширением **pfx** должен содержать внутри себя закрытый ключ для дальнейшей успешной конвертации.
- Файл с расширением **pfx** , содержащий внутри себя закрытый ключ, может быть переименован в файл с расширением **p12** без дополнительной конвертации.
- Файл с расширением **pem** должен быть в кодировке **BASE-64** . Проверить корректной кодировки **BASE-64** можно открыв данный сертификат блокнотом. Если кодировка корректна, то сертификат будет расположен между строками **-----BEGIN CERTIFICATE----- и -----END CERTIFICATE-----** . Если в файле с расширением **pem** используется кодировка **DER**, то произвести конвертацию в **BASE-64** можно командной:

```
openssl x509 -in input.cer -inform DER -out output.pem
```

2. Описание процедуры замены SSL-сертификата

Внутренний ЦС хранит ключ и сертификат в формате **.p12** в каталоге **/etc/pki/ovirt-engine/keys**. Сохраните новый файл в том же месте.

1. Создайте резервную копию текущего файла **apache.p12**, например:

```
cp -p /etc/pki/ovirt-engine/keys/apache.p12 /etc/pki/ovirt-
engine/keys/apache.p12.bck
```

2. Замените текущий файл новым, например:

```
cp /root/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

3. Извлеките закрытый ключ и сертификат.

   Если файл защищен паролем, необходимо добавить `-passin pass:<your_password>`, заменив `<your_password>` на действительный пароль.

```
openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nocerts -nodes >
/root/apache.key
openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nokeys >
/root/apache.cer
```

4. Если zVirt развернут в режиме Hosted Engine, необходимо перейти в консоль хоста и включить режим глобального обслуживания:

```
hosted-engine --set-maintenance --mode=global
```

5. Добавьте сертификат ЦС в список доверенных сертификатов, например:

```
cp /root/ca.pem /etc/pki/ca-trust/source/anchors
update-ca-trust
```

6. Менеджер управления использует файл **/etc/pki/ovirt-engine/apache-ca.pem**, который является символической ссылкой на файл **/etc/pki/ovirt-engine/ca.pem**. Удалите символическую ссылку:

```
rm /etc/pki/ovirt-engine/apache-ca.pem
```

7. Сохраните сертификат ЦС, как файл **/etc/pki/ovirt-engine/apache-ca.pem**:

```
cp /root/ca.pem /etc/pki/ovirt-engine/apache-ca.pem
```

8. Создайте резервную копию существующего закрытого ключа и сертификата:

```
cp /etc/pki/ovirt-engine/keys/apache.key.nopass /etc/pki/ovirt-
engine/keys/apache.key.nopass.bck
```

```
cp /etc/pki/ovirt-engine/certs/apache.cer /etc/pki/ovirt-
engine/certs/apache.cer.bck
```

9. Скопируйте закрытый ключ:

```
cp /root/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
```

10. Установите владельцем закрытого ключа пользователя *root* и задайте права доступа **0640**:

```
chown root:ovirt /etc/pki/ovirt-engine/keys/apache.key.nopass
chmod 640 /etc/pki/ovirt-engine/keys/apache.key.nopass
```

11. Скопируйте сертификат:

```
cp /root/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

12. Установите владельцем сертификата пользователя *root* и задайте права доступа **0644**:

```
chown root:ovirt /etc/pki/ovirt-engine/certs/apache.cer
chmod 644 /etc/pki/ovirt-engine/certs/apache.cer
```

13. Перезапустите веб-сервер:

```
systemctl restart httpd.service
```

14. Создайте новый конфигурационный файл доверенных сертификатов **/etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf** со следующими параметрами:

```
ENGINE_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

Если каталог **engine.conf.d** отсутствует, создайте его с помощью команды:

```
mkdir -p /etc/ovirt-engine/engine.conf.d/
```

15. Скопируйте файл **/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf** и измените индекс в файле на значение, которое больше 10 (например, **99-setup.conf**). Добавьте следующие параметры в новый файл:

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/certs/apache.cer
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```

16. Перезапустите службу **websocket-proxy**:

```
systemctl restart ovirt-websocket-proxy.service
```

17. Если вручную производились изменения файла **/etc/ovirt-provider-ovn/conf.d/10-setup-ovirt-provider-ovn.conf** или используется файл конфигурации более ранней версии zVirt, необходимо убедиться, что менеджер управления по-прежнему настроен на использование **/etc/pki/ovirt-engine/apache-ca.pem** в качестве сертификата.
18. Настройте **engine-backup** на обновление системы при восстановлении. Создайте новый файл **/etc/ovirt-engine-backup/engine-backup-config.d/update-system-wide-pki.sh** со следующим содержимым:

```
BACKUP_PATHS="${BACKUP_PATHS}
/etc/ovirt-engine-backup"
cp -f /etc/pki/ovirt-engine/apache-ca.pem \
/etc/pki/ca-trust/source/anchors/ca.pem
update-ca-trust
```

Если каталог **engine-backup-config.d** отсутствует, создайте его с помощью команды:

```
mkdir -p /etc/ovirt-engine-backup/engine-backup-config.d/
```

19. Перезапустите сервис **ovirt-provider-ovn**:

```
systemctl restart ovirt-provider-ovn.service
```

20. Перезапустите сервис **ovirt-imageio**:

```
systemctl restart ovirt-imageio.service
```

21. Перезапустите сервис **ovirt-engine**:

```
systemctl restart ovirt-engine.service
```

22. Если zVirt развернут в режиме Hosted Engine, необходимо перейти в консоль хоста и выключить режим глобального обслуживания:

```
hosted-engine --set-maintenance --mode=none
```

Замена SSL-сертификата для веб-портала (zVirt 3.3 и выше)

Данная инструкция актуальна только для zVirt версии 3.3 и выше.

Сертификат стороннего ЦС (Certificate Authority) предоставляется в виде PEM-файла. Цепочка сертификатов должна быть полной вплоть до корневого сертификата. Порядок цепочки сертификатов является критически важным, цепочка должна строится от последнего промежуточного ЦС до корневого ЦС. В противном случае при проверке подлинности сервера может произойти сбой.

Закрытый ключ предоставляется в виде KEY-файла.

1. Соглашения

- **/root** - расположение файлов полученных от ЦС или в процессе выполнения процедуры замены.
- **/root/apache.p12** - сертификат полученный от ЦС в формате PKCS#12.

  Для версии zVirt 4.1 файл должен быть защищен паролем `mypass`.
- **/root/ca.pem** - сертификат ЦС.
- **/root/apache.key** - новый закрытый ключ веб-сервера.
- **/root/apache.cer** - новый сертификат веб-сервера.

- Файл с расширением **pfx** должен содержать внутри себя закрытый ключ для дальнейшей успешной конвертации.
- Файл с расширением **pfx** , содержащий внутри себя закрытый ключ, может быть переименован в файл с расширением **p12** без дополнительной конвертации.
- Файл с расширением **pem** должен быть в кодировке **BASE-64** . Проверить корректность кодировки **BASE-64** можно открыв данный сертификат блокнотом. Если кодировка корректна, то сертификат будет расположен между строками **-----BEGIN CERTIFICATE----- и -----END CERTIFICATE-----** . Если в файле с расширением **pem** используется кодировка **DER**, то произвести конвертацию в **BASE-64** можно командной:

  ```bash
  openssl x509 -in input.cer -inform DER -out output.pem
  ```

2. Описание процедуры замены SSL-сертификата

Внутренний ЦС хранит ключ и сертификат в формате **.p12** в каталоге **/etc/pki/ovirt-engine/keys/**. Сохраните новый файл в том же месте.

1. Создайте резервную копию текущего файла **apache.p12**, например:

```
BASH
cp -p /etc/pki/ovirt-engine/keys/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12.bck
```

2. Замените текущий файл новым, например:

```
BASH
cp /root/apache.p12 /etc/pki/ovirt-engine/keys/apache.p12
```

3. Извлеките закрытый ключ и сертификат.

   Если файл защищен паролем, необходимо добавить `-passin pass:<your_password>`, заменив `<your_password>` на действительный пароль.

```
BASH
openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nocerts -nodes > /root/apache.key
openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nokeys > /root/apache.cer
```

   Если **apache.p12** содержит также промежуточные сертификаты, используйте следующую команду:

```
BASH
openssl pkcs12 -in /etc/pki/ovirt-engine/keys/apache.p12 -nokeys -clcerts > /root/apache.cer
```

4. Если zVirt развернут в режиме Hosted Engine, необходимо перейти в консоль хоста и включить режим глобального обслуживания:

```
BASH
hosted-engine --set-maintenance --mode=global
```

5. Если сертификат **apache.p12** подписан промежуточным сертификатом предприятия, то нужно подготовить файл для добавления в хранилище сертификатов: нужно скомпоновать единый файл **ca.pem**, где сначала указывается промежуточный сертификат, а после него корневой сертификат.

```
TEXT
-----BEGIN CERTIFICATE-----
Промежуточный сертификат
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

```
Корневой сертификат
-----END CERTIFICATE-----
```

6. Добавьте сертификат ЦС в список доверенных сертификатов (**пароль mypass**), например:

```
keytool -import -file /root/ca.pem  -alias companyca -keystore
/etc/pki/ovirt-engine/.truststore
cp /root/ca.pem /etc/pki/ca-trust/source/anchors
update-ca-trust
```

7. Менеджер управления использует файл **/etc/pki/ovirt-engine/apache-ca.pem**, который является символической ссылкой на файл **/etc/pki/ovirt-engine/ca.pem**. Удалите символическую ссылку:

```
rm /etc/pki/ovirt-engine/apache-ca.pem
```

8. Сохраните сертификат ЦС, как файл **/etc/pki/ovirt-engine/apache-ca.pem**:

```
cp /root/ca.pem /etc/pki/ovirt-engine/apache-ca.pem
```

9. Создайте резервную копию существующего закрытого ключа и сертификата:

```
cp /etc/pki/ovirt-engine/keys/apache.key.nopass /etc/pki/ovirt-
engine/keys/apache.key.nopass.bck
cp /etc/pki/ovirt-engine/certs/apache.cer /etc/pki/ovirt-
engine/certs/apache.cer.bck
```

10. Скопируйте закрытый ключ:

```
cp /root/apache.key /etc/pki/ovirt-engine/keys/apache.key.nopass
```

11. Установите владельцем закрытого ключа пользователя *root* и задайте права доступа **0640**:

```
chown root:ovirt /etc/pki/ovirt-engine/keys/apache.key.nopass
chmod 640 /etc/pki/ovirt-engine/keys/apache.key.nopass
```

12. Скопируйте сертификат:

```
cp /root/apache.cer /etc/pki/ovirt-engine/certs/apache.cer
```

13. Установите владельцем сертификата пользователя *root* и задайте права доступа **0644**:

```
chown root:ovirt /etc/pki/ovirt-engine/certs/apache.cer
chmod 644 /etc/pki/ovirt-engine/certs/apache.cer
```

14. Перезапустите веб-сервер:

```
BASH
systemctl restart httpd.service
```

15. В конфигурационном файле **/etc/ovirt-engine/backend/backend.conf** сервиса измените параметр `SERVER_SSL_KEY_STORE_PASSWORD` (если строка отсутствует - добавьте), для которого укажите пароль от вашего сертификата **/root/apache.p12**. Если пароль не используется, то оставьте поле пустым (без кавычек: `SERVER_SSL_KEY_STORE_PASSWORD=`)

Пример 1. Пример содержимого файла /etc/ovirt-engine/backend/backend.conf

```
BASH
ENGINE_DEBUG_ADDRESS=*:8686
JBACKEND_HOME=/usr/share/java/zvirt/
SERVER_SSL_KEY_STORE_PASSWORD=apachep12pass
```

В zVirt 4.1 используйте пароль `mypass`, т.е. `SERVER_SSL_KEY_STORE_PASSWORD=mypass`.

Для версии **zVirt 3.3** предварительно скачайте файлы zvirt-engine-backend.conf и zvirt-engine-backend.py.

Скопируйте их в каталог **/usr/share/zvirt-engine/services/zvirt-engine-backend/** с заменой (в примере нужные файлы скачаны в каталог **/root**):

```
BASH
cp /root/zvirt-engine-backend.py /usr/share/zvirt-engine/services/zvirt-engine-backend/zvirt-engine-backend.py
cp /root/zvirt-engine-backend.conf /usr/share/zvirt-engine/services/zvirt-engine-backend/zvirt-engine-backend.conf
```

Также в **zVirt 3.3** вместо параметра `SERVER_SSL_KEY_STORE_PASSWORD` используется `SSL_PASSWORD`. Например:

```
BASH
ENGINE_DEBUG_ADDRESS=*:8686
JBACKEND_HOME=/usr/share/java/zvirt/
SSL_PASSWORD=apachep12pass
```

16. Перезапустите сервис **backend**.

```
BASH
systemctl restart zvirt-engine-backend.service
```

17. Скопируйте файл **/etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf** и измените индекс в файле на значение, которое больше 10 (например, **99-setup.conf**). Добавьте следующие параметры в новый файл (если строки уже присутствуют их необходимо заменить):

```
SSL_CERTIFICATE=/etc/pki/ovirt-engine/certs/apache.cer
SSL_KEY=/etc/pki/ovirt-engine/keys/apache.key.nopass
```
BASH

18. Перезапустите службу **websocket-proxy**:

```
systemctl restart ovirt-websocket-proxy.service
```
BASH

19. Если вручную производились изменения файла **/etc/ovirt-provider-ovn/conf.d/10-setup-ovirt-provider-ovn.conf** или используется файл конфигурации более ранней версии zVirt, необходимо убедиться, что менеджер управления по-прежнему настроен на использование **/etc/pki/ovirt-engine/apache-ca.pem** в качестве сертификата.
20. Перезапустите сервис **ovirt-provider-ovn**:

```
systemctl restart ovirt-provider-ovn.service
```
BASH

21. Перезапустите сервис **ovirt-imageio**:

```
systemctl restart ovirt-imageio.service
```
BASH

22. Перезапустите сервис **ovirt-engine**:

```
systemctl restart ovirt-engine.service
```
BASH

23. Если zVirt развернут в режиме Hosted Engine, необходимо перейти в консоль хоста и выключить режим глобального обслуживания:

```
hosted-engine --set-maintenance --mode=none
```
BASH