Обновление сертификатов в РЕД ВИРТ

Окружение

- **Версия РЕД ВИРТ:** 7.3

Сертификаты имеют ограниченный срок действия. Чтобы избежать сбоев в работе инфраструктуры, их необходимо своевременно обновлять.

Ниже приведена пошаговая инструкция по обновлению сертификатов как для виртуальной машины управления **HostedEngine**, так и для хостов виртуализации — независимо от того, просрочены сертификаты или нет.

ВАЖНО!

Инструкция актуальна для версий 7.3.2 и новее. После обновления сертификаты будут действительны 5 лет.

Если по техническим причинам обновление до актуальной версии недоступно, обратитесь в службу технической поддержки — специалисты помогут безопасно продлить срок действия ваших сертификатов.

Примечания:

Данная инструкция применима только при одновременном выполнении двух условий:

- до окончания срока действия сертификата осталось менее 60 дней или он уже просрочен;
- сертификат не является самоподписанным и не был выпущен сторонним центром сертификации.

Если ваш сертификат подпадает под исключение, свяжитесь с технической поддержкой для получения индивидуальных рекомендаций.

Обновление сертификатов на виртуальной машине HostedEngine

Перед началом убедитесь, что система обновлена до версии 7.3.2 или новее.

1. Перевод в режим глобального обслуживания

Для безопасного обновления сертификатов на виртуальной машине управления **HostedEngine** необходимо перевести всю систему в режим глобального обслуживания. Это можно сделать двумя способами:

Через веб-интерфейс:

1. Перейдите в раздел: **Виртуализация → Хосты**.
2. Нажмите кнопку **Дополнительные действия (⋮)** в правом верхнем углу.
3. Выберите: **Включить глобальный режим обслуживания высокой доступности**.

Через командную строку:

1. В веб-интерфейсе определите хост, на котором в данный момент запущена виртуальная машина **HostedEngine**.
2. Подключитесь к этому хосту по SSH и выполните команду:

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

3. Убедитесь, что система находится в режиме глобального обслуживания:

```
# hosted-engine --vm-status
```

В выводе должно присутствовать сообщение:

```
!! Cluster is in GLOBAL MAINTENANCE mode !!
```

2. Создание резервной копии сертификатов

Подключитесь к виртуальной машине **HostedEngine** и создайте резервную копию текущих сертификатов:

```
cp -a /etc/pki/ovirt-engine "$HOME/ovirt-engine-pki-backup-$(date '+%Y%m%d')"
```

3. Запуск обновления сертификатов

На виртуальной машине **HostedEngine** запустите скрипт настройки в автономном режиме:

```
engine-setup --offline
```

В процессе выполнения вам будет предложено указать параметры конфигурации. Можно отвечать вручную или использовать заранее подготовленный файл ответов.
Когда появится запрос:

```
Renew certificates? (Yes, No) [Yes]:
```

введите **Yes** и нажмите **Enter**.

4. Отключение режима глобального обслуживания

После успешного обновления сертификатов выведите хост из режима глобального обслуживания.

Через веб-интерфейс:

1. Перейдите в раздел: **Виртуализация → Хосты**.
2. Нажмите кнопку **Дополнительные действия (⋮)** в правом верхнем углу.
3. Выберите: **Выключить глобальный режим обслуживания высокой доступности**.

Через командную строку:

1. Подключитесь по SSH к хосту с запущенной ВМ HostedEngine.
2. Выполните команду:

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

3. Убедитесь, что система выведена из режима глобального обслуживания:

   ```
   # hosted-engine --vm-status
   ```

   В выводе не должно быть строки:

   ```
   !! Cluster is in GLOBAL MAINTENANCE mode !!
   ```

После выполнения этих действий сертификаты виртуальной машины управления **HostedEngine** успешно обновлены.
Теперь необходимо приступить к обновлению сертификатов на хостах виртуализации.

Обновление сертификатов на хостах виртуализации

Чтобы обновить сертификаты на хостах виртуализации, выполните следующие действия:

1. В веб-интерфейсе портала администрирования перейдите: **Виртуализация → Хосты**.

2. Выберите нужный хост и нажмите: **Управление → Обслуживание**, затем подтвердите действие кнопкой **OK**.

   Виртуальные машины автоматически мигрируют с хоста. Если какие-либо ВМ закреплены или по другим причинам не могут быть перемещены, их необходимо остановить вручную.

3. После того как хост перейдёт в режим обслуживания и на нём не останется запущенных виртуальных машин, нажмите: **Установка → Занесение сертификата**.
4. По завершении обновления сертификатов выведите хост из режима обслуживания: **Управление → Включить**.

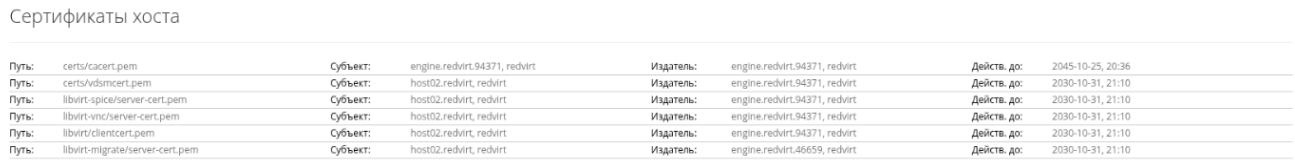
Сертификаты на выбранном хосте успешно обновлены. Повторите описанные шаги для каждого хоста в кластере.

Проверка обновления сертификатов

После выполнения всех шагов убедитесь, что сертификаты успешно обновлены.
Для проверки сертификатов хостов выполните следующие действия:

1. Перейдите в раздел **Виртуализация → Хосты**.
2. Выберите целевой хост, нажав по его имени.
3. Перейдите на вкладку **Система**

В таблице отображена информация о сертификатах и сроках их действия.



Сертификаты хоста

Для проверки сертификатов виртуальной машины HostedEngine выполните следующие действия:

1. Перейдите в раздел **Виртуализация → Виртуальные машины**.
2. Выберите виртуальную машину **HostedEngine**, нажав по её имени.
3. Перейдите на вкладку **Система**

В таблице отображена информация о сертификатах и сроках их действия.



Сертификаты Engine

ВАЖНО!

Если на любом этапе возникнут трудности — обратитесь в техническую поддержку.

Источник: https://redvirt.red-soft.ru/base/knowledge-base/updating-certificates/