Замена SSL-сертификата для веб-портала РЕД ВИРТ 8

Можно настроить сертификат стороннего центра сертификации вашей организации для идентификации на портале администратора пользователями, подключающимися по протоколу **HTTPS**.

Примечание:

Предварительные требования:

- **Сертификат стороннего центра сертификации (ЦС)**. Это сертификат ЦС, выдавшего сертификат, который вы хотите использовать. Он предоставляется в виде PEM-файла. Цепочка сертификатов должна быть полной до корневого сертификата. Данная процедура предполагает, что сертификат стороннего ЦС находится в /tmp/ca-cert-new.pem.
- **Закрытый ключ, который вы хотите использовать для Apache httpd**. Он не должен иметь пароля. Данная процедура предполагает, что он находится в /tmp/apache.key.
- **Сертификат, выданный центром сертификации**. Данная процедура предполагает, что он находится в /tmp/apache.cer.
- Выпускаемый сертификат должен иметь расширение **Subject Alternative Name (SAN)**, поэтому необходимо убедиться, что в нём присутствуют все доменные имена и IP-адреса, для которых будет использоваться сертификат.
- Все описанные действия выполняются от пользователя **root**.

Описание стенда:

Для замены сертификата будет использоваться:
И м я **HostedEngine** (имя хоста для конфигурации Standalone) — https://engine.mydomain.local.

Сертификат может быть выпущен самостоятельно или по инструкции по выпуску самоподписанного сертификата.

Процедура замены SSL-сертификата

1. Если РЕД ВИРТ развернута в режиме Hosted Engine, перейдите в консоль хоста, на котором происходит замена сертификата, и включите режим глобального обслуживания, выполнив команду:

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

2. Создайте резервную копию директории /etc/pki, скопировав ее в безопасное место (например в директорию /home):

```
cp -r /etc/pki /home
```

3. Добавьте свой сертификат центра сертификации (/tmp/ca-cert-new.pem) в общесистемное хранилище доверенных сертификатов (/etc/pki/ca-trust/source/anchors) и примените изменения:

```
cp /tmp/ca-cert-new.pem /etc/pki/ca-trust/source/anchors
update-ca-trust
```

4. Менеджер управления настроен на использование /etc/pki/ovirt-engine/apache-ca.pem, который символически связан с /etc/pki/ovirt-engine/ca.pem. Поэтому необходимо удалить символическую ссылку, выполнив команду:

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

5. Сохраните свой сертификат центра сертификации (ЦС) /tmp/ca-cert-new.pem как /etc/pki/ovirt-engine/apache-ca.pem:

```
cp /tmp/ca-cert-new.pem /etc/pki/ovirt-engine/apache-ca.pem
```

6. Создайте резервную копию существующего закрытого ключа /etc/pki/ovirt-engine/keys/apache.key.nopass и сертификата /etc/pki/ovirt-engine/certs/apache.cer:

```
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
```

7. Перезапишите закрытый ключ /etc/pki/ovirt-engine/keys/apache.key.nopass своим ключом /tmp/apache.key:

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

8. Назначьте владельцем закрытого ключа пользователя **root** и группу **root** и установите права доступа 0640:

```
chown root:root /etc/pki/ovirt-engine/keys/apache.key.nopass
chmod 0640 /etc/pki/ovirt-engine/keys/apache.key.nopass
```

9. Перезапишите имеющийся сертификат /etc/pki/ovirt-engine/certs/apache.cer на сертификат, выданный центром сертификации (ЦС) /tmp/apache.cer:

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

10. Перезапустите сервер **Apache**:

```
systemctl restart httpd.service
```

11. Создайте новый файл конфигурации хранилища доверенных сертификатов /etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf:

```
vi /etc/ovirt-engine/engine.conf.d/99-custom-truststore.conf
```

12. Добавьте в файл следующие параметры:

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

13. В файле /etc/ovirt-engine/engine.conf.d/12-setup-keycloak.conf закомментируйте строки с `EXTERNAL_OIDC_HTTPS_PKI_TRUST_STORE` и `EXTERNAL_OIDC_HTTPS_PKI_TRUST_STORE_PASSWORD` и добавьте следующие строки:

```
EXTERNAL_OIDC_HTTPS_PKI_TRUST_STORE="/etc/pki/java/cacerts"
EXTERNAL_OIDC_HTTPS_PKI_TRUST_STORE_PASSWORD=""
```

14. Скопируйте /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf файл и переименуйте его, присвоив ему порядковый номер больше 10 (например, 99-setup.conf):

```
cp /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/10-setup.conf /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/99-setup.conf
```

15. В скопированном файле /etc/ovirt-engine/ovirt-websocket-proxy.conf.d/99-setup.conf измените строки с `SSL_CERTIFICATE` и `SSL_KEY`, заменив значение после знака «**=**» на путь к сертификату /etc/pki/ovirt-engine/certs/apache.cer и ключу /etc/pki/ovirt-engine/keys/apache.key.nopass соответственно:

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

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

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

17. Если были внесены изменения в файл /etc/ovirt-provider-ovn/conf.d/10-setup-

ovirt-provider-ovn.conf вручную или используется конфигурационный файл из более старой установки, необходимо убедиться, что менеджер управления по-прежнему настроен на использование /etc/pki/ovirt-engine/apache-ca.pem в качестве источника сертификата. Для проверки необходимо открыть файл и проверить наличие в строке с ovirt-ca-file пути к файлу /etc/pki/ovirt-engine/apache-ca.pem:

```
vi /etc/ovirt-provider-ovn/conf.d/10-setup-ovirt-provider-ovn.conf
```

18. Перезапустите службу **ovirt-provider-ovn**:

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

19. Перезапустите службу **ovirt-imageio**:

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

20. Для возможности получения сертификата со страницы ***https://engine.mydomain.local/ovirt-engine*** через кнопку «**Корневой сертификат**» нужно изменить путь на странице приветствия /usr/share/ovirt-engine/brands/ovirt.brand/welcome_page.template. Для этого сперва необходимо сделать резервную копию страницы приветствия:

```
cp /usr/share/ovirt-engine/brands/ovirt.brand/welcome_page.template /usr/share/ovirt-engine/brands/ovirt.brand/welcome_page.template.bck
```

21. Скопируйте файл сертификата центра сертификации (ЦС) /tmp/ca-cert-new.pem в /var/www/html/ для дальнейшего использования относительно этой директории:

```
cp /tmp/ca-cert-new.pem /var/www/html/
```

22. Откройте файл /usr/share/ovirt-engine/brands/ovirt.brand/welcome_page.template:

```
vi /usr/share/ovirt-engine/brands/ovirt.brand/welcome_page.template
```

23. Замените в файле /usr/share/ovirt-engine/brands/ovirt.brand/welcome_page.template в строке с id="WelcomePage_certificate" параметр href="services/pki-resource?resource=ca-certificate&format=X509-PEM-CA" на параметр href="/ca-cert-new.pem"
24. Перезапустите службу **ovirt-engine**:

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

25. Если РЕД ВИРТ развернута в режиме Hosted Engine, отключите глобальный режим обслуживания, выполнив на хосте команду:

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

На машине, где будет производиться администрирование системы РЕД ВИРТ, можно скачать новый сертификат с главной страницы РЕД ВИРТ ***https://engine.mydomain.local/ovirt-engine*** по кнопке "**Корневой сертификат**" и установить его в качестве корневого.

Теперь возможно подключение к порталу администратора и порталу виртуальных машин, без предупреждения о подлинности сертификата, используемого для шифрования HTTPS-трафика.

Источник: https://redvirt.red-soft.ru/base/knowledge-base/replacement-SSL-certificate/