Назначение сертификатов РЕД Виртуализации

Окружение

- **Версия РЕД Виртуализации:** 7.3

В РЕД Виртуализации используется инфраструктура открытых ключей (PKI) для обеспечения безопасности взаимодействий между компонентами системы. Вся сетевая коммуникация внутри кластера шифруется с помощью протокола SSL/TLS. Корнем доверия выступает корневой сертификат ca.pem, который генерируется при развертывании ВМ **HostedEngine**.

Ниже указано назначение и расположение основных сертификатов, используемых на стороне ВМ **HostedEngine** и на стороне хоста РЕД Виртуализации.

Сертификаты Engine

Файлы сертификатов, расположенные в директории **/etc/pki/ovirt-engine/** обеспечивают работу центральных сервисов управления.

- **/etc/pki/ovirt-engine/ca.pem** — корневой сертификат удостоверяющего центра (CA). Главный сертификат всей системы безопасности. Этим сертификатом подписываются все сертификаты в системе РЕД Виртуализации. Когда Engine связывается с хостом, он проверяет, что сертификат хоста подписан этим CA. Хост делает тоже самое в ответ. Это гарантирует, что Engine доверяет хостам, а хосты доверяют Engine. У него самый длинный срок действия.
- **/etc/pki/ovirt-engine/qemu-ca.pem** — дополнительный корневой сертификат для защиты компонентов **QEMU**. Необходим для шифрования трафика при операциях с образами дисков. Например, для загрузки образа диска с помощью ovirt-imageio или живой миграции.
  Когда ВМ мигрирует с одного хоста на другой, то её оперативная память передается по сети. Этот CA подписывает сертификаты, которые используются для шифрования потока данных.
- **/etc/pki/ovirt-engine/certs/apache.cer** — сертификат веб-сервера **Apache**. Обеспечивает защищенное HTTPS-соединение для доступа к Порталу администратора, Порталу виртуальных машин и REST API. Он шифрует весь веб-трафик между браузером и сервером Apache на ВМ **HostedEngine**, защищая учётные данные и все действия, которые выполняются в веб-интерфейсе.
- **/etc/pki/ovirt-engine/certs/engine.cer** — сертификат службы **ovirt-engine**. Используется для SSH и SSL-аутентификации при взаимодействии с агентами vdsm на хостах, а также для шифрования полей базы данных.
- **/etc/pki/ovirt-engine/certs/websocket-proxy.cer** — сертификат прокси-службы **Websocket**, с которой браузер устанавливает соединение на ВМ **HostedEngine**. Обеспечивает шифрование при подключении к графической

консоли ВМ через браузер (noVNC).
- **/etc/pki/ovirt-engine/certs/jboss.cer** — внутренний сертификат сервера приложений **Java/WildFly** на котором работает бэкенд ВМ **HostedEngine**. Используется для защиты внутренних коммуникаций, безопасности локальных интерфейсов и межпроцессного взаимодействия среды **Java**.

Группа сертификатов OVN

OVN (Open Virtual Network) — программно-определяемые сети (**SDN**), построенные на базе **Open vSwitch**. Решение позволяет создавать и управлять виртуальными сетями, разделяя физическую топологию сети от логической.

- **/etc/pki/ovirt-engine/certs/ovirt-provider-ovn.cer** — сертификат OVN-провайдера. Идентифицирует провайдера OVN, позволяя ВМ **HostedEngine** управлять сетевыми настройками. Используется сервисом ovirt-provider-ovn для аутентификации и безопасного общения с базами данных OVN.

OVN состоит из двух баз данных: **Northbound** (логическая конфигурация сети) и **Southbound** (физическое состояние).

- **/etc/pki/ovirt-engine/certs/ovn-ndb.cer** — сертификат для аутентификации при подключении к «северной» базе данных OVN (Northbound Database).
- **/etc/pki/ovirt-engine/certs/ovn-sdb.cer** — сертификат для подключения к «южной» базе данных OVN (Southbound Database).

Группа сертификатов сервиса ovirt-vmconsole

Группа сертификатов, используемая сервисом **ovirt-vmconsole** для создания защищённого канала связи при доступе к консоли виртуальных машин (VNC или SPICE).

- **/etc/pki/ovirt-engine/certs/vmconsole-proxy-helper.cer** — служебный сертификат вспомогательных процессов прокси.
- **/etc/pki/ovirt-engine/certs/vmconsole-proxy-host.cer** — сертификат, который обеспечивает защищённый канал связи между прокси-сервером и хостами виртуализации.
- **/etc/pki/ovirt-engine/certs/vmconsole-proxy-user.cer** — сертификат, который применяется для аутентификации пользовательских сессий при подключении к консоли.

Сертификаты хостов

- **/etc/pki/vdsm/certs/vdsmcert.pem** — основной сертификат агента **VDSM**.

Используется для шифрования всего управляющего трафика между ВМ **HostedEngine** и сервисом **VDSM** на хосте. Все действия по управлению ВМ на Портале администратора проходят по этому защищенному каналу.

- **/etc/pki/vdsm/libvirt-spice/server-cert.pem** — сертификат для протокола **SPICE**. Обеспечивает TLS-шифрование при подключении клиента к графической консоли ВМ. Шифрует весь spice-трафик (передача видео, ввод с мыши/клавиатуры) между spice-клиентом (например, remote-viewer) и хостом, на котором запущена ВМ.
- **/etc/pki/vdsm/libvirt-vnc/server-cert.pem** — сертификат для протокола **VNC**. Обеспечивает TLS-шифрование при подключении клиента к графической консоли ВМ. Шифрует весь vnc-трафик (передача видео, ввод с мыши/клавиатуры) между vnc-клиентом (например, remote-viewer) и хостом, на котором запущена ВМ.
- **/etc/pki/vdsm/libvirt-migrate/server-cert.pem** — сертификат миграции. Используется для шифрования потока живой миграции ВМ между хостами, предотвращая перехват данных оперативной памяти в сети.
- **/etc/pki/libvirt/clientcert.pem** — сертификат **libvirt**. Этот сертификат используется агентом **VDSM** для аутентификации и обеспечения безопасной связи между сервисами **vdsmd** и **libvirtd** на самом хосте, чтобы авторизованно управлять демоном **libvirtd**.

Источник: https://redvirt.red-soft.ru/base/knowledge-base/assign-cert-rv/