libvirt

libvirt — свободная реализация API, демон и набор инструментов для управления виртуализацией. Позволяет управлять гипервизорами Xen, KVM, а также VirtualBox, OpenVZ, LXC, VMware ESX/GSX/Workstation/Player, QEMU и другими средствами виртуализации, предоставляет возможность контролировать виртуальные машины по сети, расположенные на других компьютерах. Эти API широко используются в слоях гипервизоров при разработке облачных решений.

https://libvirt.org/

Fix Me!

TLSSetup - Libvirt Wiki

libvirt: Remote support

Подключаемся к Libvirt, SPICE и VNC через TLS/SSL | umVirt.Ru

TLS

Fix Me!

XCA — libvrt

Стандартный вариант создания ключей и сертификатов для работы по TLS libvrt — TLS

Файлы

- `cakey.pem`

Сервер

- `cacert.pem`
- `serverkey.pem`
- `servercert.pem`

Клиент

- `cacert.pem`
- `clientkey.pem`
- `clientcert.pem`

cakey.pem

Ключ центра сертификации, он должен храниться в надёжном месте.

Его нельзя хранить на серверах и клиентах!

cacert.pem

Сертификат центра сертификации

serverkey.pem

Ключ сервера

servercert.pem

Сертификат сервера

clientkey.pem

Ключ клиента

clientcert.pem

Сертификат клиента

Настройка клиента

Копирование файлов клиента

pki-libvirt_client.sh

```
#!/bin/bash

mkdir -p /etc/pki/libvirt/private/
mkdir -p /etc/pki/CA/

cp libvrt-ca.crt /etc/pki/CA/cacert.pem
cp libvrt-user.crt /etc/pki/libvirt/clientcert.pem
cp libvrt-user.pem /etc/pki/libvirt/private/clientkey.pem

chgrp libvirt /etc/pki/CA/cacert.pem
chgrp libvirt /etc/pki/libvirt/clientcert.pem
chgrp libvirt /etc/pki/libvirt/private/clientkey.pem
```

Настройка сервера

Копирование файлов на сервере

pki-libvirt_server.sh

```
#!/bin/bash
mkdir -p /etc/pki/libvirt/private/
mkdir -p /etc/pki/CA/

cp libvrt-ca.crt /etc/pki/CA/cacert.pem
cp libvrt-server.crt /etc/pki/libvirt/servercert.pem
```

```
cp libvrt-server.pem /etc/pki/libvirt/private/serverkey.pem
cp libvrt-crl.pem /etc/pki/CA/crl.pem
```

libvirtd для TLS

Здесь описан процесс настройки демона `libvirtd` для работы по TLS

1. Нужно исправить файл запуска демона:

   /etc/default/libvirtd

   ```
   libvirtd_opts="-l"
   ```

2. Внести изменения в файл настройки, минимальные изменения:

   /etc/libvirt/libvirtd.conf

   ```
   listen_tls = 1
   listen_tcp = 1
   ```

   или изменения включающие настройку сертификатов, ключей и списка отзыва сертификатов:

   /etc/libvirt/libvirtd.conf

   ```
   listen_tls = 1
   listen_tcp = 1
   key_file = "/etc/pki/libvirt/private/serverkey.pem"
   cert_file = "/etc/pki/libvirt/servercert.pem"
   ca_file = "/etc/pki/CA/cacert.pem"
   crl_file = "/etc/pki/CA/crl.pem"
   ```

3. Выполнить перезапуск демона:

   ```
   service libvirtd restart
   ```

   При перезапуске демона `libvirtd` гостевые домены (виртуальные машины) **будут работать**! (FAQ - Libvirt Wiki — 1.2.5 Will restarting the libvirt daemon stop my virtual machines?)

4. Проверка:

   ```
   netstat -lntp | grep libvirtd
   ```

   Пример вывода:

   ```
   tcp        0      0 0.0.0.0:16509           0.0.0.0:*               LISTEN      5594/libvirtd
   tcp        0      0 0.0.0.0:16514           0.0.0.0:*               LISTEN      5594/libvirtd
   tcp6       0      0 :::16509                :::*                    LISTEN      5594/libvirtd
   tcp6       0      0 :::16514                :::*                    LISTEN      5594/libvirtd
   ```

Ссылки

Логотип

https://ru.wikipedia.org/wiki/Libvirt

http://sysadminmosaic.ru/libvirt/libvirt

2020-08-28 12:33