libvrt — TLS

Стандартный вариант создания ключей и сертификатов для работы libvrt по TLS

Нужно установить пакет:

```
apt install gnutls-bin
```

Типовые действия

- Создание нового центра сертификации
- Создание сертификата центра сертификации

Создание нового сервера

- Создание ключа сервера
- Создание сертификата сервера
- Настройка сервера
- Настройка libvirtd для TLS

Создание нового клиента

- Создание ключа клиента
- Создание сертификата клиента
- Настройка клиента

Создание нового центра сертификации

```
certtool --generate-privkey > cakey.pem
```

Создание сертификата центра сертификации

Файл с информацией

ca.info

```
cn = Organozation
ca
cert_signing_key
```

```
certtool --generate-self-signed --load-privkey cakey.pem \
  --template ca.info --outfile cacert.pem
```

Создание ключа сервера

```
certtool --generate-privkey > serverkey.pem
```

Создание сертификата сервера

Файл с информацией

server.info

```
organization = test_organization
cn = server
dns_name = server
dns_name = server.domain.ru
ip_address = 10.10.1.100
ip_address = 192.168.1.100
tls_www_server
encryption_key
signing_key
```

```
certtool --generate-certificate --load-privkey serverkey.pem \
  --load-ca-certificate cacert.pem --load-ca-privkey cakey.pem \
  --template server.info --outfile servercert.pem
```

Создание ключа клиента

```
certtool --generate-privkey > clientkey.pem
```

Создание сертификата клиента

Файл с информацией

client.info

```
country = RU
state =
locality =
organization = Organization
cn = user
tls_www_client
encryption_key
signing_key
```

```
certtool --generate-certificate --load-privkey clientkey.pem \
  --load-ca-certificate cacert.pem --load-ca-privkey cakey.pem \
  --template client.info --outfile clientcert.pem
```

Ссылки

libvirt: Remote support

http://sysadminmosaic.ru/libvirt/tls

2019-02-18 13:57