XCA — OpenVPN

Управление ключами и сертификатами OpenVPN в XCA

За основу взята статья 2011 года Using XCA to configure the OpenVPN PKI part as an alternative to OpenVPN's easy-rsa (carbonwind_xca-openvpn.odt)

Для удобства работы создана БД OpenVPN.xdb с шаблонами:

- OpenVPN_ЦС
- OpenVPN_Сервер
- OpenVPN_Клиент

Ограничения

1. Нельзя сохранить в БД параметры Диффи — Хеллмана, их можно только создать: Генерация параметров Диффи — Хеллмана. Открыта тема #96.
2. Нельзя создать и сохранить в БД `ta.key`, используемый для `tls-auth`. Открыта тема #89.

Типовые действия

- **Создание нового клиента**
- **Отзыв сертификата**
- **Создание нового сервера**
- **Создание нового центра сертификации**

Создание нового сервера

1. Экспорт сертификата центра сертификации
2. Создание сертификата сервера
3. Экспорт сертификата
4. Экспорт закрытого ключа
5. Генерация параметров Диффи — Хеллмана

Создание нового клиента

1. Экспорт сертификата центра сертификации
2. Создание сертификата клиента
3. Экспорт сертификата
4. Экспорт закрытого ключа

Создание нового центра сертификации

Перейти на вкладку Сертификаты и нажать кнопку Новый сертификат

На вкладке Первоисточник

- в разделе Подписание выбрать Создать самозаверенный сертификат
- в поле Алгоритм подписи выбрать SHA1
- в разделе Шаблон для нового сертификата выбрать OpenVPN_ЦС

Нажать кнопку Применить всё

На вкладке Субъект нужно заполнить поля:

- Internal Name
- countryName
- stateOfProvinceName
- localityName
- organizationName
- organizationUnitName
- commonName
- emailAddress

Нажать кнопку Сгенерировать новый ключ

В окне появившемся окне Certificate and Key management

- в поле Тип ключа выбрать RSA
- в поле Длина ключа выбрать 2048 bit

нажать кнопку Создать.

Из шаблона подставляются значения для вкладок:

- Расширения
- Область применения ключа
- Netscape

На вкладке Расширения нужно задать период действия сертификата.

После заполнения полей нужно нажать кнопку OK

При необходимости можно выполнить процесс «с нуля»:

Перейти на вкладку Сертификаты и нажать кнопку Новый сертификат

На вкладке Первоисточник

- в разделе Подписание выбрать Создать самозаверенный сертификат
- выбрать Алгоритм подписи выбрать SHA1
- в разделе Шаблон для нового сертификата выбрать [default] CA

Нажать кнопку Применить всё

На вкладке Субъект нужно заполнить поля:

- Internal Name
- countryName
- stateOfProvinceName
- localityName
- organizationName
- organizationUnitName
- commonName
- emailAddress

Нажать кнопку Сгенерировать новый ключ

В окне появившемся окне Certificate and Key management

- в поле Тип ключа выбрать RSA
- в поле Длина ключа выбрать 2048 bit

нажать кнопку Создать.

На вкладке Расширения в поле Тип нужно выбрать Центр сертификации, для остальных полей можно оставить значения по умолчанию.

На вкладке Область применения ключа в поле X509v3 Key usage нужно выбрать

- Certificate Sign
- CLR Sign

На вкладке Netscape в поле Netscape Cert Type нужно выбрать:

- SSL CA
- S/MIME CA
- Object Signing CA

Также нужно удалить значение поля Netscape Comment

На вкладке Дополнительно будет показана результирующая информация:

```
X509v3 Basic Constraints critical:
CA:TRUE
X509v3 Subject Key Identifier:
E1:88:9E:34:60:7B:00:4D:98:9B:03:62:D7:B3:BD:DC:D2:24:68:31
X509v3 Key Usage:
Certificate Sign, CRL Sign
Netscape Cert Type:
SSL CA, S/MIME CA, Object Signing CA
Netscape Comment:
xca certificate
```

Проверив её можно нажать кнопку OK

Создание сертификата сервера

Перейти на вкладку Сертификаты и нажать кнопку Новый сертификат

На вкладке Первоисточник, в разделе Подписание

- в поле Использовать этот сертификат для подписи нужно выбрать (созданный ранее) OpenVPN CA
- в поле Алгоритм подписи выбрать SHA 1
- в поле Шаблон для нового сертификата выбрать OpenVPN_Сервер

Нажать кнопку Применить всё

На вкладке Субъект нужно заполнить поля:

- Internal Name
- countryName
- stateOfProvinceName
- localityName
- organizationName
- organizationUnitName
- commonName
- emailAddress

Нажать кнопку Сгенерировать новый ключ

В окне появившемся окне Certificate and Key management

- в поле Тип ключа выбрать RSA
- в поле Длина ключа выбрать 2048 bit

Нажать кнопку Создать

Теперь в поле Закрытый ключ нужно выбрать только что созданный ключ OpenVPN Server (RSA:2048 bit)

Из шаблона подставляются значения для вкладок:

- Расширения
- Область применения ключа
- Netscape

На вкладке Расширения нужно задать период действия сертификата.

После заполнения полей нужно нажать кнопку OK

При необходимости можно выполнить процесс «с нуля»:

Перейти на вкладку Сертификаты и нажать кнопку Новый сертификат

На вкладке Первоисточник, в разделе Подписание

- в поле Использовать этот сертификат для подписи нужно выбрать (созданный ранее) OpenVPN CA
- в поле Алгоритм подписи выбрать SHA 1
- в поле Шаблон для нового сертификата выбрать [default] HTTPS_server

Нажать кнопку Применить всё

На вкладке Субъект нужно заполнить поля:

- Internal Name
- countryName
- stateOfProvinceName
- localityName
- organizationName
- organizationUnitName
- commonName
- emailAddress

Нажать кнопку Сгенерировать новый ключ

В окне появившемся окне Certificate and Key management

- в поле Тип ключа выбрать RSA
- в поле Длина ключа выбрать 2048 bit

Нажать кнопку Создать

Теперь в поле Закрытый ключ нужно выбрать только что созданный ключ OpenVPN Server (RSA:2048 bit)

На вкладке Расширения в разделе X509v3 Base constraints в поле Тип выбрать Конечный субъект

В разделе Key identifier нужно выбрать:

- ✔ Critical
- ✔ Subject Key Identifier

Также нужно задать период действия ключа.

На вкладке Область применения ключа в поле X509v3 Key Usage выбрать:

- Digital Signature

- `Key Encipherment`

в поле `X509v3 Extended Key Usage` выбрать:

- `TLS Web Server Authentication`

На вкладке `Netscape` нужно выбрать

- `SSL Server`

и удалить значение поля `Netscape Comment`

На вкладке `Дополнительно` будет показана результирующая информация:

```
X509v3 Basic Constraints critical:
CA:FALSE
X509v3 Subject Key Identifier:
C1:32:F2:14:7F:3B:CB:44:B4:25:C8:C2:41:4C:B1:D4:80:9B:D4:A3
X509v3 Key Usage:
Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Server Authentication
Netscape Cert Type:
SSL Server
```

Проверив её можно нажать кнопку `OK`

Создание сертификата клиента

Перейти на вкладку `Сертификаты` и нажать кнопку `Новый сертификат`

На вкладке `Первоисточник`, в разделе `Подписание`

- в поле `Использовать этот сертификат для подписи` нужно выбрать (созданный ранее) `OpenVPN CA`
- в поле `Алгоритм подписи` выбрать `SHA 1`
- в поле `Шаблон для нового сертификата` выбрать `OpenVPN_Клиент`

Нажать кнопку `Применить всё`

На вкладке `Субъект` нужно заполнить поля:

- `Internal Name`
- `countryName`
- `stateOfProvinceName`
- `localityName`
- `organizationName`
- `organizationUnitName`
- **`commonName`**
- `emailAddress`

Важно заполнить поле **`commonName`**

Нажать кнопку `Сгенерировать новый ключ`

В окне появившемся окне `Certificate and Key management`

- в поле `Тип ключа` выбрать `RSA`
- в поле `Длина ключа` выбрать `2048 bit`

Нажать кнопку `Создать`

Из шаблона подставляются значения для вкладок:

- Расширения
- Область применения ключа
- Netscape

На вкладке Расширения нужно задать период действия сертификата.

После заполнения полей нужно нажать кнопку OK

При необходимости можно выполнить процесс «с нуля»:

Перейти на вкладку Сертификаты и нажать кнопку Новый сертификат

На вкладке Первоисточник, в разделе Подписание

- в поле Использовать этот сертификат для подписи нужно выбрать (созданный ранее) OpenVPN CA
- в поле Алгоритм подписи выбрать SHA 1
- в поле Шаблон для нового сертификата выбрать [default] HTTPS_client

Нажать кнопку Применить всё

На вкладке Субъект нужно заполнить поля:

- Internal Name
- countryName
- stateOfProvinceName
- localityName
- organizationName
- **organizationUnitName**
- commonName
- emailAddress

Нажать кнопку Сгенерировать новый ключ

В окне появившемся окне Certificate and Key management

- в поле Тип ключа выбрать RSA
- в поле Длина ключа выбрать 2048 bit

Нажать кнопку Создать

На вкладке Расширения в разделе X509v3 Base constraints в поле Тип выбрать Конечный субъект

В разделе Key identifier нужно выбрать:

- ✔ Critical
- ✔ Subject Key Identifier

Также нужно задать период действия ключа.

На вкладке Область применения ключа в поле X509v3 Key Usage выбрать:

- Digital Signature
- Key Agreement

в поле X509v3 Extended Key Usage выбрать:

- TLS Web Client Authentication

На вкладке Netscape нужно выбрать

- SSL Client

- S/MIME

и удалить значение поля Netscape Comment

На вкладке Дополнительно будет показана результирующая информация:

```
X509v3 Basic Constraints critical:
CA:FALSE
X509v3 Subject Key Identifier:
1D:B8:66:BD:49:11:B3:83:10:E5:F3:7F:92:53:6D:AE:97:64:FB:83
X509v3 Key Usage:
Digital Signature, Key Agreement
X509v3 Extended Key Usage:
TLS Web Client Authentication
Netscape Cert Type:
SSL Client, S/MIME
```

Проверив её можно нажать кнопку OK

Ссылки

Using XCA to configure the OpenVPN PKI part as an alternative to OpenVPN's easy-rsa

Setting up OpenVPN with Certificates - Cult of Tech.net

Создание ключей для OpenVPN с помощью графического инструмента XCA. - Справочный центр - Справочный центр Astra Linux

https://sysadminmosaic.ru/xca/openvpn

2022-04-22 09:14