Создание сертификатов для FreeIPA с помощью XCA

oot

Дополнительная информация по работе XCA содержится в статьях

- Управление ключами: XCA
- Создание ключей для OpenVPN с помощью графического инструмента XCA

Данная статья применима к:

- ОС ОН Орёл 2.12
- ОС СН Смоленск 1.6
- ОС СН Ленинград 8.1

Исходные данные

Имя домена IPADOMAIN.RU

Имя основного сервера SERVER.IPADOMAIN.RU

Имя сервера-реплики REPLICA.IPADOMAIN.RU

В качестве центра сертификации может использоваться любой компьютер, не обязательно находящийся в домене.

Описанная процедура позволяет получить сертификаты, максимально близкие к сертификатам, которые выпускаются при использовании центра сертификации DogTag.

Подготовка

Установить на компьютере, который будет выполнять роль центра сертификации, инструмент командной строки XCA:

apt install xca

Запустить инструмент с помощью графического меню

Пуск => "Утилиты" => "Цифровые сертификаты XCA"

при необходимости установить русский язык:

"File" => "Language" => "Russian"

и создать базу данных, в которой будут храниться сертификаты:

«Файл» => «Новая база данных» Выбрать место хранения базы=> Задать имя базы => «Сохранить» => При необходимости задать пароль для доступа к базе данных.

Создание корневого сертификата

В инструменте XCA

- Перейти на вкладку «Сертификаты»и выбрать «Новый сертификат»;
  - Убедиться, что выбран пункт "Создать самоподписанный сертификат...";
  - Выбрать "Шаблон для нового сертификата" "[Default] CA";
  - Нажать кнопку "Применить всё";
- Перейти на вкладку «Субъект» («Владелец»);
  - (рекомендуется) в поле "organizatioName" указать имя домена (IPADOMAIN.RU);
  - (рекомендуется) в поле "commonName" указать имя "Certification authority";
  - По необходимости заполнить остальные поля;
  - Выбрать «Создать новый ключ»:
    - В поле «Имя ключа» указать имя ключа, например CA
    - Нажать «Создать»

- Перейти на вкладку «Расширения»
  - Убедиться, что выбран «Тип» «Центр Сертификации»;
  - Отметить пункты "Critical", "Subject Key identifier", "Authority key Identifier"
  - Определить срок действия сертификата: «Временной диапазон» => 10 (года)
- Перейти на вкладку "Область применения ключа"
  - Отметить пункт "Critical", выбрать функции "Digital Signature", "Non repudation", "Certificate Sign", "CRL Sign";
- Сохранить созданный сертификат: «Применить» => «Да»

Создание сертификата для сервера

- Перейти на вкладку «Сертификаты»и нажать кнопку «Новый сертификат»;
  - Для использования для подписания ранее созданного сертификата установить отметку «Use this Certificate for signing» => «rootCA»;
  - Выбрать шаблон для нового сертификата "[Default] HTTPS_server"
  - Нажать кнопку "Применить всё"
- Перейти на вкладку «Субъект» («Владелец»);
  - (рекомендуется) в поле "organizatioName" указать имя домена (IPADOMAIN.RU);
  - В полях "commonName" и "Внутреннее имя" указать полное доменное имя сервера (строчными буквами) "server.ipadomain.ru", "replica.ipadomain.ru" и т.д.;

    Для того, чтобы сертификат был пригоден для работы с протоколом SSL имя, указанное в поле commonName, должно совпадать с DNS-именем сервера

  - Выбрать «Создать новый ключ»;
    - В поле «Имя ключа» указать имя ключа, например serverKey;
    - Нажать «Создать»;
  - По необходимости заполнить остальные поля;
- Перейти во вкладку «Расширения»;
  - Выбрать «Тип» «Конечный субъект» («Конечный пользователь»);
  - Отметить пункты "Critical", "Subject Key identifier", "Authority key Identifier"
  - Определить срок действия сертификата: «Временной диапазон» => 5;
  - В строке "X509v3 Subject Alternative Name" необходимо стереть значение по умолчанию (DNS:....) и оставить её пустой.
    Это значение будет задано далее с помощью текстового описания (вкладка "Дополнительно").
- Перейти на вкладку "Область применения ключа";
  - В левой части ("x509 v3 Key Usage") отметить пункты:
    - "Critical";
  - В левой части ("x509 v3 Key Usage") выбрать функции:
    - "Digital Signature";
    - "Non Repudiation";
    - "Key Encipherment";
    - "Data Encipherment";
    - "Key Agreement";
  - В правой части ("x509 v3 Extanded Key Usage") выбрать расширенные функции:
    - "TLS Web Server Authentication";
    - "KDC Authentication" (может также называться "Signing KDC response");
  - Дополнительно могут потребоваться следующие функции сертификата:
    - "OCSP Signing" - для службы протокола протокола OCSP;
    - "E-mail protection" - для ca-agent;
- Перейти во вкладку "Дополнительно" и нажать кнопку "Редактировать";
  - Удалить все записи в открывшемся окне;
  - Вставить в окно следующий текст, указав нужные имена домена и сервера (текст, который нужно заменить выделен красным):

Для повторяющегося создания типовых сертификатов можно создать собственный шаблон с типовыми настройками.

При наличии ранее созданных сертификатов можно импортировать их в XCA и воспользоваться функцией XCA "Преобразовать" - "Похожий сертификат" (доступ через контекстное меню по правой кнопке мыши) для создания копии, после чего исправить в копии нужные атрибуты, или использовать эту копию в качестве шаблона.

issuerAltName=issuer:copy
subjectAltName=otherName:1.3.6.1.5.2.2;SEQUENCE:kdc_princ_name,DNS:server.ipadomain.ru

[kdc_princ_name]
realm = EXP:0, GeneralString:IPADOMAIN.RU
principal_name = EXP:1, SEQUENCE:kdc_principal_seq

[kdc_principal_seq]
name_type = EXP:0, INTEGER:1
name_string = EXP:1, SEQUENCE:kdc_principals

[kdc_principals]
princ1 = GeneralString:krbtgt
princ2 = GeneralString:IPADOMAIN.RU@IPADOMAIN.RU

- Нажать кнопку "Проверить";
- Нажать кнопку "Да" для сохранения сертификата;
- Если при сохранении сертификата выдаётся сообщение "The certificate will be earlier valid than the signer. This is probably not what you want.", то нажать кнопку "Скорректировать дату и продолжить";

Импорт сертификата (для включения сервера реплики)

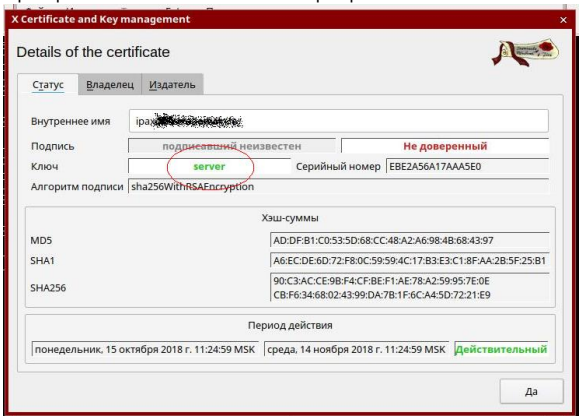
1. Запускаем инструмент XCA на основном сервере (для удобства работы - лучше от имени суперпользователя).
2. Создаём, при необходимости, новую базу данных XCA.
3. Импортируем в XCA корневой сертификат, автоматически созданный при установке основного сервера FreeIPA:

   /etc/ssl/freeipa/server.crt

4. Импортируем в XCA закрытый ключ корневого сертификата, автоматически созданный при установке основного сервера FreeIPA:

   /etc/ssl/freeipa/server.key

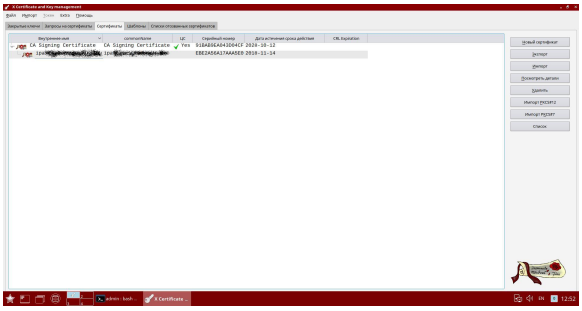
   Если всё сделано правильно, то закрытый ключ автоматически привяжется к сертификату. Проверить это можно в свойствах сертификата:



5. Импортировать в XCA сертификат и ключ сервера FreeIPA:

/etc/ssl/freeipa/ca.crt
/etc/ssl/freeipa/ca.key

В случае правильного выполнения операции импортированный сертификат автоматически привяжется к корневому сертификату:



Если импортировать существующий сертификат сервера то вместо "ручного" создания следующих сертификатов вручную можно просто копировать импортированный сертификат:
Открыть список сертификатов

- Правой кнопкой мыши выбрать копируемый сертификат;
- В открывшемся меню выбрать "Преобразовать" - "Похожий сертификат" ("Transform" - "Similar Certificate");
- Далее следовать по шагам описанным в разделе "Создание сертификата для сервера"

Экспорт сертификата

- Выбрать нужный сертификат сервера, далее «Экспорт» => «Формат экспорт» => PKCS12 chain => «Да»
- Задать пароль на экспортируемый контейнер => «Да»

На предполагаемом сервере установить пакет astra-freeipa-server:

apt install astra-freeipa-server

Для того что бы провести инициализацию сервера с указанием нужного контейнера сертификата, нужно запустить команду «astra-freeipa-server» с дополнительными ключами -l <путь_к_контейнеру> и -lp <пароль_контейнера>, например:

astra-freeipa-server -l /root/server.example.com.p12 -lp Password123

Посмотреть другие ключи команды astra-freeipa-server можно так:

astra-freeipa-server --help

Импорт корневого сертификата в WEB-браузер

Для того, чтобы WEB-браузер признавал подлинность сертификатов, выписанных с помощью XCA, нужно импортировать в WEB-браузер корневой сертификат удостоверяющего центра XCA. Для этого:

1. В XCA экспортировать корневой сертификат в формате "PEM (*.crt)";

При автоматическом создании сертификатов корневой сертификат находится в файле /etc/ssl/freeipa/ca.crt

2. Скопировать полученный файл на целевой сервер;
3. В WEB-браузере (на примере WEB-браузера FireFox):
    a. Открыть панель настроек;
    b. Перейти в раздел "Приватность и защита";
    c. Перейти в раздел "Сертификаты" - "Просмотр сертификатов";
    d. В закладке "Центры сертификации" нажать кнопку "Импортировать";
    e. Выбрать нужный файл с сертификатом;
    f. Нажать кнопку "Открыть";
    g. Выбрать функцию "Доверять при идентификации пользователей электронной почты";
    h. Нажать "ОК";
    i. Перезапустить WEB-браузер.