

????????? ? ??????????????
?????????????

?????????

Состав, формат и обязательные атрибуты SSL-сертификатов для установки Printum. Набор файлов зависит от схемы установки:

Конфигурация	Что требуется
Сингл	Один комплект сертификатов (корневой + серверный + ключ) на весь сервер.
Кластер Active-Active	Отдельный сертификат и ключ на каждый сервер, корневой сертификат общий.
Филиальная сеть	Собственный сертификат на сервере каждого филиального ПринтМенеджера, корневой сертификат общий.

????????????? ??????????????
?????????????

Мониторинг и ПринтМенеджер могут генерировать самоподписанные сертификаты при установке, если не указано использование собственных. Использование автоматических сертификатов **допустимо только для конфигурации Сингл**.

При их использовании веб-браузеры будут показывать предупреждение о недоверии при входе в Личный кабинет и панели администратора. Для Кластера и Филиальной сети такие сертификаты не подходят — там требуется отдельный сертификат на каждый сервер (см. ниже).

?????? ??????????????
??????

Нужны три файла:

Файл	Описание
ca.crt	Корневой сертификат (CA)
server.crt	Сертификат сервера
server.key	Закрытый ключ сертификата сервера

Если используется промежуточный CA сертификат — он тоже должен быть передан отдельным файлом.

???????

Отдельный сертификат и ключ для каждого сервера (HAProxy, Мониторинг, каждый ПринтМенеджер, сервер БД + NFS). Все сертификаты должны быть выпущены одним корневым удостоверяющим центром (CA).

?????????? ? ??????????????? ??? ??????????

Пример комплекта сертификатов для развёртывания системы в конфигурации с балансировщиком, состоящей из 6 серверов:

Сервер	Роль
Сервер 1	Балансировщик
Сервер 2	Мониторинг
Сервер 3	ПринтМенеджер №1
Сервер 4	ПринтМенеджер №2
Сервер 5	ПринтМенеджер №3
Сервер 6	База данных и NFS-хранилище

Необходимые файлы:

- Корневой сертификат.
- Сертификат сервера и ключ — для каждого сервера отдельно (сертификат + ключ HAProxy, сертификат + ключ Сервера 1, сертификат + ключ Сервера 2 и т.д.).

?????????? ?????

Комплект и требования к сертификатам в филиальной сети идентичны сингл конфигурации, за исключением того, что для каждого филиального ПринтМенеджера требуются

собственные сертификаты с общим корневым сертификатом.

???????? ???? ?????

- Установка системы по IP: сертификат выпускается на IP-адрес сервера.
- Установка системы по FQDN (хостнейму): сертификат выпускается на FQDN (доменное имя).

Должно соблюдаться соответствие между адресом сервера и адресом в выпускаемом сертификате: если система установлена по FQDN, а сертификат выпущен на IP или наоборот — возникнет ошибка `Hostname mismatch`.

???????? ???? ?????

SSL-сертификат сервера должен соответствовать следующим требованиям:

- X509v3 Extended Key Usage — `TLS Web Server Authentication` и `TLS Web Client Authentication`.
- Алгоритм — RSA, длина ключа не менее 2048 бит.
- X509v3 Subject Alternative Name (SAN) — обязателен и должен содержать все доменные имена и/или IP-адреса, по которым будет доступен сервер.

Пример SAN для одного сервера:

```
DNS:server1.example.com
DNS:server1
IP:10.0.0.1
```

В кластере у каждого сервера — свой сертификат с собственным набором SAN (свои DNS-имена и IP); общий сертификат с одним SAN на весь кластер не используется.

Без SAN будет ошибка `unable to get local issuer certificate`.

Корневой сертификат (CA):

- X509v3 Key Usage: `Digital Signature`, `Certificate Sign`, `CRL Sign`
- X509v3 Basic Constraints: `critical`

??????

- Данные в сертификатах — в незашифрованном текстовом виде, кодировка UTF-8.
- Поддерживаемые расширения: `.cer`, `.crt`, `.pem` (для сертификатов), `.key` (для ключа).
- Корневой сертификат — отдельный файл. Нельзя включать его содержимое в `server.crt`.

???????? ???? ? ? ???? ?

Ошибка в логах	Причина
Hostname mismatch	Адрес сервера не совпадает с CN или SAN сертификата
ERR_CERT_COMMON_NAME_INVALID	Адрес сервера не совпадает с CN или SAN сертификата
self signed certificate in certificate chain	Содержимое CA включено в <code>server.crt</code>
unable to get local issuer certificate	Отсутствует поле SAN в сертификате

???????? ???? ?

- [Требования к сетевой доступности и портам](#)
 - [Требования к серверу и сайзинг](#)
-