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

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

Перед выпуском собственных сертификатов для установки или обновления Printum.

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

Для базовой (сингл) схемы нужны три файла:

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

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

Для схемы с балансировщиком — отдельный сертификат и ключ для каждого сервера (HAProxy, Мониторинг, каждый ПринтМенеджер, сервер БД+NFS).

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

- Установка по системы IP: сертификат выпускается на IP-адрес сервера.
- Установка по системы FQDN: сертификат выпускается на FQDN (доменному имени).

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:

- X509v3 Extended Key Usage: `TLS Web Server Authentication`, `TLS Web Client Authentication`
- X509v3 Subject Alternative Name (SAN) — обязателен. Должен содержать все адреса сервера:

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

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

Корневой сертификат (CA):

- X509v3 Key Usage: `Digital Signature`, `Certificate Sign`

??????

- 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
`self signed certificate in certificate chain`	Содержимое CA включено в `server.crt`
`unable to get local issuer certificate`	Отсутствует поле SAN в сертификате

Подробнее — в соответствующих troubleshooting-статьях (ссылки ниже).

????? ? ??????????????? HAProxy

Сертификат и ключ к нему должны быть предоставлены отдельно для каждого сервера. Корневой сертификат остаётся общим.

Пример комплекта сертификатов для развёртывания системы в конфигурации балансировщика:

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

Необходимые файлы:

- Корневой сертификат (`.cer` / `.crt` / `.pem`) — один общий для всех серверов.
- Сертификат сервера и ключ — для каждого из 6 серверов отдельно.

> **Примечание:** Для филиальных ПринтМенеджеров требуются собственные сертификаты с общим корневым сертификатом.

????????????: ??????????????? ???????????

Мониторинг и ПМ позволяют использовать самоподписанные сертификаты, автоматически генерируемые при установке без дополнительных параметров. Самоподписанные сертификаты подходят для работы системы в конфигурации сингл, где Мониторинг и ПМ устанавливаются на один сервер. При использовании самоподписанных сертификатов веб-браузеры будут показывать предупреждение о недоверии на входе в ЛК и панели администратора.

Revision #7
Created 2026-05-18 17:29:27 UTC by DD
Updated 2026-05-20 14:42:42 UTC by Артём Сидельников