

Установка SSL-сертификата на сервер с битрикс

Настройка бесплатного сертификата Let's encrypt

Важно! Прежде, чем выпускать сертификат Let's Encrypt, убедитесь, что у вас [создан сайт](#) на тот хост (и он доступен из интернета), на который выпускается сертификат, а также указаны правильные DNS-настройки у регистратора или хостера DNS для этого домена. Иначе он не будет выпущен. Плюс к этому есть лимит – 5 ошибок в час выпуска сертификата на аккаунт для одного домена.

Для создания SSL-сертификата Let's Encrypt нужно:

- Перейти в меню 8. Manage pool web servers > 3. Configure certificates:



- Выбрать пункт меню 1. Configure "Let's encrypt" certificate и ввести:
 - **site name** – имя сайта или несколько имен сайтов, для которых нужно выпустить сертификат(ы) Let's encrypt (в данном примере: **test2.b24test.site**)
 - **dns name(s)** – все домены данного сайта, для которых должен быть выпущен сертификат, включая домен с www и без, вводить несколько доменов через запятую
 - **email for LE notifications** – почтовый адрес для уведомлений сервиса Lets Encrypt

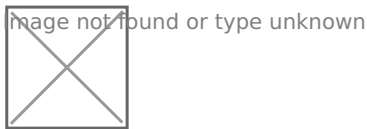
и подтвердить ввод:



- Мастер самостоятельно запросит и установит его в течение нескольких минут. Пути SSL-сертификатов будут указаны в этом же разделе:



- Проверить выпущенный сертификат можно легко – перейти на ваш сайт по протоколу https, у валидного сертификата будет замочек:



Срок действия – 90 дней. Перевыпуск происходит автоматически за 20 дней до окончания срока действия.

Ручное обновление

С версии *BitrixVM 7.4.0* проверка сертификатов автоматически производится еженедельно в субботу в 2 часа ночи по cron-y.

Если вам нужно вручную обновить сертификат, запустите его получение для существующего домена. Система проверит и при необходимости обновит сертификаты.

Также вы можете вручную командой:

```
/home/bitrix/dehydrated/dehydrated -c
```

Система проверит сроки действия и при необходимости запустит обновление.

Лог обновления можно посмотреть по пути: **`/home/bitrix/dehydrated_update.log`**.

Важно! У сервиса Lets Encrypt есть свои ограничения на выпуск сертификатов. Основные из них:

- Выпуск 50 штук в неделю на домены (на зарегистрированные домены у регистратора, поддомены не входят в этот счет).
- Если у вас много поддоменов, то можно все поддомены указать в одном сертификате, но здесь есть лимит в 100 поддоменов на одну штуку.
- 5 ошибок в час выпуска сертификата на аккаунт для одного домена (не доступен хост, не прописаны записи в DNS домена и т.д).
- Проверка HTTP-01 выполняется только с использованием порта 80. Если этот порт закрыт (провайдером, например), то [сертификат не перевыпустится](#).

Подробнее о лимитах Let's Encrypt читайте в статье [Rate Limits](#).

Установка собственного SSL сертификата

Если у вас есть свой сертификат, выпущенный любым [авторизованным центром](#), то можно также его подключить к сайту в *BitrixVM*.

Важно! Прежде, чем подключать его, убедитесь, что у вас [создан сайт](#) на тот хост (и он доступен из интернета), на который у вас выпущен сертификат, а также указаны правильные DNS-настройки у регистратора или хостера DNS для этого домена.

У вас должны быть следующие файлы: **приватный ключ (private key)**, **цепочка сертификатов (certificate chain)** и **сам сертификат (certificate)**.

Требования к импортируемым сертификатам:

- Все перечисленные файлы должны быть в **PEM-кодировке**.
- Приватный ключ не должен быть зашифрован.
- Обязательны файлы сертификата и приватного ключа, файл с цепочкой можно не указывать.
- Если вы используете свои пути для загрузки, то нужно указывать при импорте полные пути. Если хотите использовать относительные пути, то файлы сертификатов должны быть загружены в директорию **/etc/nginx/certs**.

Подключение

Для подключения своего SSL-сертификата нужно:

- Скопировать файлы сертификата в любую директорию на сервере с помощью любого клиента SFTP. В нашем примере мы создали директорию **/home/bitrix/ssl/** и скопировали файлы в неё.

Пути получились такие:

1. **приватный ключ** - `/home/bitrix/ssl/test2.b24test.site_privkey.pem`
2. **сам сертификат** - `/home/bitrix/ssl/test2.b24test.site_cert.pem`
3. **цепочка сертификатов** - `/home/bitrix/ssl/test2.b24test.site_chain.pem`

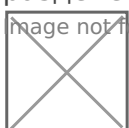
- Далее перейти в меню 8. Manage pool web servers > 3. Configure certificates:



- Выбрать пункт меню 2. Configure own certificate и ввести **имя домена** (Sitename) или несколько доменов, для которых нужно импортировать сертификат(ы) (в данном примере: **test2.b24test.site**), **путь для приватного ключа (Private Key path)**, **путь для сертификата (Certificate path)**, **путь для цепочки сертификатов (Certificate Chain path)** и подтвердить установку для этого домена:



- Мастер самостоятельно установит сертификат. Пути будут указаны в этом же разделе:



- Проверку результата можно выполнить легко – перейти на ваш сайт по протоколу https, у валидного сертификата будет зеленый замочек:



Поддерживается ввод нескольких сайтов, через запятую. Следить за сроком действия своего сертификата вы должны сами. Перевыпуск осуществляется также владельцем сайта. После перевыпуска нового сертификата нужно будет заново его импортировать.

Примечание: Если вы использовали свою директорию сервера для копирования исходных файлов, то после импорта сертификата в целях безопасности эти файлы желательно удалить (в примере - `/home/bitrix/ssl/`). Если вы копировали файлы в `/etc/nginx/certs`, то удалять их не нужно.

Версия #1

Кирилл создал 16 октября 2023 11:19:18

Кирилл обновил 16 октября 2023 11:43:25