Содержание

Действия в случае возникновения проблем с TLS/SSL сертификатами на VEOS 3

Действия в случае возникновения проблем с TLS/SSL сертификатами на VEOS

В случае, если у вас возникает проблема с установкой пакетов на сервере и вы видите ошибку вида:

- Curl error (60): Peer certificate cannot be authenticated with given CA certificates for

https://repo.vasexperts.com/veos/8/BaseOS/x86_64/os/repodata/repomd.xml [SSL certificate problem: certificate has expired]Ошибка: Не удалось загрузить метаданные для репозитория «baseos»: Cannot download repomd.xml: Cannot download repodata/repomd.xml: All mirrors were tried

1. Необходимо проверить дату и время на сервере/в биосе. Дата и время должны быть актуальными.

В выводе timedatectl должно быть указано: System clock synchronized: yes. Если не указано, то необходимо отредактировать /etc/chrony.conf, далее выполнить systemctl restart chronyd.

Также можно выполнить замену пула VEOS на пул Centos: pool 2.veos.pool.ntp.org → pool 2.centos.pool.ntp.org.

2. Проверить, не происходит ли подмена корневого TLS сертификата:

```
openssl s_client -connect repo.vasexperts.com:443
```

- 3. Проверить настройки фаервола должен быть открыт 443 порт.
- 4. Отключить sslverify в /etc/dnf.conf (необходимо добавить строку sslverify=0).



Отключение sslverify — крайняя и нерекомендуемая мера, которая отключает проверку сертификатов только при установке пакетов, в то время как остальные утилиты (например, curl) работать не будут.