Содержание

Actions in case of problems with TLS/SSL certificates on VEOS

In case you have a problem with installing packages on the server and you see an error like this:

```
  - 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]Error: Failed to download
metadata for repo «baseos»: Cannot download repomd.xml: Cannot download
repodata/repomd.xml: All mirrors were tried
```

1. You need to check the date and time on the server/in the bios. The date and time must be up to date.

   The output of `timedatectl` should state: `System clock synchronized: yes`.
   If not specified, edit `/etc/chrony.conf`, then execute `systemctl restart chronyd`.

   You can also swap out the VEOS pool for the Centos pool: `pool 2.veos.pool.ntp.org` → `pool 2.centos.pool.ntp.org`
2. Verify that the root TLS certificate is not being spoofed:

   ```
   openssl s_client -connect abcdef.com:443
   ```

3. Check firewall settings — port 443 should be open.
4. Disable `sslverify` in `/etc/dnf.conf` (the line `sslverify=0` should be added).

Disabling `sslverify` is an extreme and unrecommended measure that only disables certificate verification when installing packages, while other utilities (like `curl`) will not work.