OpenSSL v3

SRE-France

Mathieu Tortuyaux (@tormath1)

27 Janvier 2022

OpenSSL ?

```
$ ldd $(which curl) | grep ssl
    libssl.so.1.1 => /usr/lib64/libssl.so.1.1 (0x00007f1c07871000)
$ ldd $(which wget) | grep ssl
    libssl.so.1.1 => /usr/lib64/libssl.so.1.1 (0x00007f77190d3000)
$ ldd $(which ssh) | grep crypto
    libcrypto.so.1.1 => /usr/lib64/libcrypto.so.1.1 (0x00007ff139991000)
$ equery belongs \
    /usr/lib64/libcrypto.so.1.1 \
    /usr/lib64/libssl.so.1.1
 * Searching for /usr/lib64/libcrypto.so.1.1,/usr/lib64/libssl.so.1.1 ...
dev-libs/openssl-1.1.1k-r1 (/usr/lib64/libcrypto.so.1.1)
dev-libs/openssl-1.1.1k-r1 (/usr/lib64/libssl.so.1.1)
```

OpenSSL 3

- Backward compatibility
- Providers
- FIPS

FIPS on Flatcar

```
storage:
  files:
    - filesystem: "root"
      path: /etc/ssl/openssl.cnf.fips
      mode: 0644
      contents:
        inline: |
          config_diagnostics = 1
          openssl_conf = openssl_init

          # it includes the fipsmodule configuration generated
          # by the `enable-fips.service`
          .include /etc/ssl/fipsmodule.cnf

          [openssl_init]
          providers = provider_sect

          [provider_sect]
          fips = fips_sect
          base = base_sect

          [base_sect]
          activate = 1
```

```
systemd:
  units:
    - name: enable-fips.service
      enabled: true
      contents: |
        [Unit]
        Description=Enable OpenSSL FIPS provider
        ConditionPathExists=!/etc/ssl/fipsmodule.cnf
        After=system-config.target

        [Service]
        Type=oneshot
        RemainAfterExit=yes
        ExecStart=/usr/bin/openssl fipsinstall \
          -out /etc/ssl/fipsmodule.cnf \
          -module /usr/lib64/ossl-modules/fips.so
        ExecStart=/usr/bin/mv /etc/ssl/openssl.cnf.fips /etc/ssl/openssl.cnf

        [Install]
        WantedBy=multi-user.target
```

Discussions and resources

- Gentoo has masked OpenSSL-3: https://bugs.gentoo.org/797325
- LibreSSL ? https://gitlab.alpinelinux.org/alpine/tsc/-/issues/28
- OpenSSL-3.0.0 on Flatcar: what to expect? | Flatcar Container Linux
- OpenSSL 3.0 FIPS Module Has Been Submitted for Validation - OpenSSL Blog