Docker images configuration

This section covers the configuration details that applies to both images.

If you want the default configuration you can go to verify the image authencity.

Environment variables

You can also modify the behaviour of Tuleap with environment variables.

GENERAL

- `TULEAP_FQDN` : the Tuleap server name (without protocol).

DATABASE

- `TULEAP_SYS_DBHOST` : database server name. See database installation for specific configuration.
- `DB_ADMIN_USER` : admin user (`root` or equivalent).
- `DB_ADMIN_PASSWORD` : admin user password.
- `TULEAP_SYS_DBPASSWD` : application user (typically `tuleapadm`) password.
- `TULEAP_SYS_DBPORT` : define this variable if your database runs on a port different of `3306` .
- `TULEAP_SYS_ENABLESSL` : can be either `0` to disable or `1` to enable encryption of traffic with database. Default is `0` .
- `TULEAP_SYS_DB_SSL_VERIFY_CERT` : can be either `0` to disable or `1` to enable verification of database's certificates. Default is `0` . **WARNING**: perl code (used for subversion core and some maintenance scripts) cannot enforce this, those parts will do encryption without certificate verification.
- `TULEAP_SYS_DB_SSL_CA` : path toward a custom CA file for certiface verification.

SITE ADMINISTRATION

- `SITE_ADMINISTRATOR_PASSWORD` : tuleap `admin` user password.
- `TULEAP_SYS_EMAIL_ADMIN` : email address where all the system emails will be redirected (**since 13.8**).

REDIS

- `TULEAP_FPM_SESSION_MODE` : you can set it to `redis` so php sessions will be stored in a Redis K/V store.
- `TULEAP_REDIS_SERVER` : needed if you set `redis` for `TULEAP_FPM_SESSION_MODE` .
- `TULEAP_REDIS_PORT` : needed if redis is listening on port that is not `6379` (the default).
- `TULEAP_REDIS_PASSWORD` : needed if redis requires a password.
- `TULEAP_REDIS_USE_TLS` : set to 1 if you want to encrypt the connection to Redis.

EMAIL

- `TULEAP_EMAIL_TRANSPORT` : email transport (sendmail by default). (**since 13.12**).
- `TULEAP_EMAIL_RELAYHOST` : email relay host (none by default).

> Warning
>
> Please note that not all plugins can be used with this configuration setting (email_relay) and you might need to customize the image to fit your needs.

Passwords

- We recommend at least 20 chars but only alphabetical & numbers,
- They are set at the first run only (not updated automatically).

TLS Certificates

Tuleap container generate a self signed certificate can only communicate in https. In order to have a valid certificate for your end users you either need to:

- Delegate the certificate management to your ingress controller (Kubernetes)
- Have a reverse proxy in front of the Tuleap container to deal with the certificate
- I you don't want to bother with a reverse proxy, you can modify the certificate generated by tuleap and set yours:
  - They key must be `/data/etc/pki/tls/private/localhost.key.pem`
  - The cert must be `/data/etc/pki/tls/certs/localhost.cert.pem`
  - If you need something more complex, use a reverse proxy.

Certification Authority

If you manage your own trust chain, you might need to let container be aware of your own CA. It's mainly useful when Tuleap should be able to communicate with a 3rd party systems (jenkins, jira, gitlab, webhooks servers, etc) exposed over TLS but with a certificate that is not part of the standard CA bundle.

The extra CA must be mounted at the container root `/extra_ca.pem`. Tuleap will ensure this CA is added to system's bundle automatically.

Backup/Restore

You probably want to take a look at the Backup/Restore guide to check data/folder structure for your docker volumes.

⬅ Previous   Next ➡

enalean
software engineering is now

Trademarks   Security   Legal