

# HarborSafe - Secure Docker Rootless Stack

```
# Checklist - Installation d'un environnement Docker securis avec Portainer BE
#
  /\  /\_ _ _ _ | | _ _ _ _ _ / _\ _ _ _ / _ | _ _
 / /_ / _ ` | ' _ | ' _ \ / _ \ | ' _ \ \ / _ ` | | _ / _ \
 / _ _ / ( _ | | | | | _ ) | ( _ | | | _ \ \ ( _ | | _ | _ /
 \ / /_ / \ _ , _ | | | _ . _ / \ _ _ / | _ | \ _ / \ _ , _ | | | \ _ |
```

```
# =====
# HarborSafe - Secure Docker Rootless Stack
# TLS + Portainer BE + UFW + usersns-remap
# [OK] Checklist Markdown
# Script : install_projet_HarborSafe.sh
# Date : 2025-03-27
# Author : LLE
# =====
```

---

## ## Objectif

Dployer une stack Docker rootless, securise via TLS, et manage par Portainer Business Edition, avec un accs securis l'API Docker (TCP 2376).

---

## ## tapes de dploiment

### ### 1. Crer / diter le script principal

```
```bash
nano install_docker_tls_secure_with_client_cert.sh
```
```

### ### 2. Rendre le script excutable

```
```bash
chmod +x install_docker_tls_secure_with_client_cert.sh
```
```

### ### 3. Executer le script

```
```bash
sudo ./install_docker_tls_secure_with_client_cert.sh
```
```

---

## ## tapes ralises par le script

- Mise jour des paquets
- Installation de Docker CE

## HarborSafe - Secure Docker Rootless Stack

- Cration du dossier de certificats
- Gnration de la CA + certificat serveur
- Gnration du certificat client
- Dplacement des certificats serveur dans `/etc/docker/certs/`
- Configuration securise du `daemon.json`
- Configuration systemd pour activer l'coute TCP (`2376`)
- Redmarrage propre de Docker
- Configuration UFW : SSH, Portainer, Docker TLS
- Prparation des variables et chemins pour Portainer
- Cration des dossiers `/opt/portainer/certs` et `/opt/portainer/license`
- Suppression de l'ancien conteneur Portainer (s'il existe)
- Dploiement de Portainer BE avec SSL (port 9443)

---

## tapes post-script

### 4. Export automatique des certificats client

la fin du script, les certificats `cert.pem`, `key.pem`, et `ca.pem` sont automatiquement copis vers `/tmp/certs` avec les bons droits pour tre tlchargs via **\*\*WinSCP\*\***.

Tu peux maintenant rcuprer ces fichiers (`ca.pem`, `cert.pem`, `key.pem`) via **\*\*WinSCP\*\*** et les utiliser pour connecter l'instance Docker via TLS securis.

---

## [OK] Prochaines tapes recommandes

- Se connecter Portainer BE : `https://<IP>:9443`
- + Ajouter un environnement Docker via :
  - Type : **\*Docker Standalone\***
  - URL : `tcp://127.0.0.1:2376`
  - Mode : **\*TLS\***
  - Certificats : `ca.pem`, `cert.pem`, `key.pem`

---

**\*Penser supprimer le dossier `/tmp/certs` une fois les fichiers transfrs.\***