Activer l'API Docker sur l'instance "db-srv"

Rendre persistante l'activation

- Afin d'éviter que les modifications effectuées dans le fichier */lib/systemd/system/docker.service* soient écrasées à chaque mise à jour de Docker, vous devez ajouter un fichier qui écrasera les valeurs par défaut.
  - **Source** : Using systemd to control the Docker daemon
- Pour créer automatiquement l'arborescence de dossier et le fichier nécessaire, utiliser la commande suivante : `systemctl edit docker`
  - La commande précédente ouvre l'éditeur par défaut du système, vous pouvez ajouter le contenu suivant et sortir de l'édition du fichier en sauvegardant :

```
[Service]
ExecStart=
ExecStart=/usr/bin/dockerd -H fd:// --
containerd=/run/containerd/containerd.sock -H tcp://10.0.1.20:2376
```

    - **Note** : la première ligne *ExecStart=* vide permet de réinitialiser la commande de lancement de Docker
  - Les modifications devraient être présente dans le fichier suivant : `vi /etc/systemd/system/docker.service.d/override.conf`
- Lancer la prise en compte des modifications qui vérifiera une éventuelle erreur : `systemctl daemon-reload`
- Relancer le service Docker : `systemctl restart docker`
- Vérifier la présence des nouveaux paramètres dans *CGroup* : `systemctl status docker`

Tester temporairement l'activation

- Au préalable, sur le serveur *db-srv*, activer l'API *Docker* sur l'IP de l'hôte du VPN : `vi /lib/systemd/system/docker.service`
  - Modifier la ligne `ExectStart=` en ajoutant l'option `-H tcp://10.0.1.20:2376` juste aprés `-H fd://`
    - À voir si on active TLS et ajoute l'option `--tlsverify`
  - Prendre en compte les changements : `systemctl daemon-reload`
  - Redémarrer Docker : `systemctl restart docker`
- Puis accéder à https://manager.silene.eu pour configurer cet instance (voir la doc dédiée).

Utiliser TLS (HTTPS) pour sécuriser l'API (daemon Docker)

- Télécharger un script simplifiant la création des certificats :
  - Créer un dossier bin/ pour root : `mkdir /root/bin/`
  - Se placer dans le dossier en tant que root : `cd ~/bin/`
  - Télécharger le script : `wget https://raw.githubusercontent.com/kekru/linux-utils/master/cert-generate/create-certs.sh`

    - Donner les droits d'éxecution au script : `chmod +x create-certs.sh`
    - Éditer les variables suivantes du script :

```
EXPIRATIONDAYS=1825
CASUBJSTRING="/C=FR/ST=Hautes-Alpes/L=Gap/O=CBNA/OU=SI/CN=web-srv.silene.eu/emailAddress=adminsys@silene.eu"
```

- Créer un dossier qui contiendra les certificats : `mkdir -pv /etc/docker/ssl/`
    - Sécuriser le dossier : `chmod 600 /etc/docker/ssl/`
- Générer les différents certificats en suivant la documentation du script :
    - Créer un certificat valable 5 ans : `./create-certs.sh -m ca -pw <mot-de-passe-du-ca> -t /etc/docker/ssl/ -e 1825`
    - Créer le certificat du dameon Docker et sa clé avec le même mot de passe que l'étape précédente, avec le domaine du serveur web-srv.silene.eu et 1825 jours avant son expiration : `./create-certs.sh -m server -h web-srv.silene.eu -pw <mot-de-passe-du-ca> -t /etc/docker/ssl/ -e 1825`
    - Créer le certificat du client et sa clé avec le même mot de passe que l'étape précédente, avec le nom de client manager-portainer et 1825 jours avant son expiration : `./create-certs.sh -m client -h manager-portainer -pw silene-web-srv -t /etc/docker/ssl/ -e 1825`
    - Nettoyer votre historique des commandes précédente : `history` puis `history -d <n°-ligne-départ>-<n°-ligne-fin>`
- Surcoucher le service Systemd : `systemctl edit docker.service`
    - Remplacer le contenu par :

```
[Service]
ExecStart=
ExecStart=/usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock -H tcp://10.0.1.10:2376 --tls --tlsverify --tlscacert "/etc/docker/ssl/ca.pem" --tlscert "/etc/docker/ssl/server-cert.pem" --tlskey "/etc/docker/ssl/server-key.pem"
```

    - Recharger les service : `systemctl daemon-reload`
    - Arrêter le service Docker : `systemctl stop docker.service`
    - Démarrer le service Docker : `systemctl start docker.service`
- Tester la sécurisation : `docker -H 10.0.1.20:2376 --tls --tlscert=/etc/docker/ssl/client-manager-portainer-cert.pem --tlskey=/etc/docker/ssl/client-manager-portainer-key.pem --tlscacert=/etc/docker/ssl/ca.pem ps -a`