Installer, configurer et gérer le sous-domaine "manager"

Notes : ce domaine hébergera l'outil Portainer permettant d'administrer les containers Docker.

Installer le domaine

- Créer un fichier de configuration : `vi /etc/nginx/sites-available/manager.conf`
  - Y placer le contenu suivant :

```
server {
    listen 80;
    listen [::]:80;

    server_name manager.<domaine-sinp>;

    location / {
        proxy_set_header Host $http_host;
        proxy_set_header X-Real-IP $realip_remote_addr;
        proxy_set_header X-Forwarded-Host $host:$server_port;
        proxy_set_header X-Forwarded-Server $host;
        proxy_set_header X-Forwarded-For
$proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;

        proxy_pass http://127.0.0.1:9000/;# ATTENTION : bien
mettre un slash final ! Sinon => erreur 404
    }
}
```

- Créer un lien depuis les sites actifs : `cd /etc/nginx/sites-enabled/ ; ln -s ../sites-available/manager.conf manager.conf`
  - Tester la config et relancer *Nginx* si OK : `nginx -t && nginx -s reload`
  - Tester l'URL http://manager.<domaine-sinp>/ qui doit afficher une erreur 502 car nous n'avons pas encore lancé le container Docker.
- Sur le serveur dans le dossier *docker* de l'utilisateur *admin* :
  - créer un nouveau réseau *Docker* spécifique à notre utilisation de type *bridge* nommé *nginx-proxy* (voir fichier *.env*) : `docker network create nginx-proxy`
  - se placer dans le dossier *manager.<domaine-sinp>* : `cd ~/docker/manager.<domaine-sinp>`
  - exécuter la commande : `docker-compose up`
  - vérifier que tout fonctionne à l'adresse : http://manager.<domaine-sinp>
    - indiquer le mot de passe pour l'utilisateur *admin* de *Portainer* afin de créer le compte d'administrateur
  - arrêter le container : CTRL+C
  - relancer le container en tant que service : `docker compose up -d`
    - si besoin de l'arrêter utiliser : `docker-compose down`

Activer le SSL et HTTP2 sur le domaine

- Installer un certificat SSL via *Certbot* (*Letsencrypt*) : `certbot --nginx -d manager.<domaine-sinp>`
    - Indiquer l'email de l'admin système : adminsys@<domaine-sinp>
    - Répondre : 2
    - Tester ensuite la redirection auto de HTTP vers HTTPS : http://manager.<domaine-sinp>/ → doit redirigé vers HTTPS automatiquement
- Tester la configuration SSL : https://www.ssllabs.com/ssltest/analyze.html?d=manager.<domaine-sinp>
- Tester l'URL https://manager.<domaine-sinp>/
- La config finale :

```
server {
    listen 443 ssl http2; # managed by Certbot
    listen [::]:443 ssl http2; # managed by Certbot

    server_name manager.<domaine-sinp>;

    location / {
        proxy_set_header Host $http_host;
        proxy_set_header X-Real-IP $realip_remote_addr;
        proxy_set_header X-Forwarded-Host $host:$server_port;
        proxy_set_header X-Forwarded-Server $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;

        proxy_pass http://127.0.0.1:9000/;# ATTENTION : bien mettre un slash final ! Sinon => erreur 404
    }

    ssl_certificate /etc/letsencrypt/live/manager.<domaine-sinp>/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/manager.<domaine-sinp>/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot
}

server {
    listen 80;
    listen [::]:80;

    server_name manager.<domaine-sinp>;

    if ($host = manager.<domaine-sinp>) {
        return 301 https://$host$request_uri;
    } # managed by Certbot
    return 404; # managed by Certbot
```

```
}
```

Configurer Portainer

- Se connecter à Portainer et se rendre dans le menu principal "*Endpoints*"

1. Pour l'instance *bkp-srv* :
    - Renommer simplement le endpoint local en *bkp-<region>-sinp*
2. Pour l'instance *db-srv* et *web-srv* :
    - Au préalable activer l'API Docker de l'instance db-srv ou web-srb
    - Cliquer sur le bouton *Add endpoint*
        - Sélectionner "Docker - Directly connect to the Docker API"
        - *Name* : db-<region>-sinp ou web-<region>-sinp
        - *Environment URL* : 10.0.1.20:2376 ou 10.0.1.10:2376
        - *Public IP* : 10.0.1.20 ou 10.0.1.10
        - *TLS* : true (voir doc)
            - Sélectionner : `TLS with server and client verification`
            - *TLS CA certificate* : sélectionner le fichier `ca.pem` récupéré précédemment sur votre machine locale.
            - *TLS certificate* : sélectionner le fichier `cert.pem` récupéré précédemment sur votre machine locale.
            - *TLS key* : sélectionner le fichier `key.pem` récupéré précédemment sur votre machine locale.
        - Valider le formulaire