# Architecture

### Les prérequis matériels sont détaillés dans le document architecture.pdf

# **Prérequis avant installation**

### Serveur principale

partition applicative /app

partition backup /backup

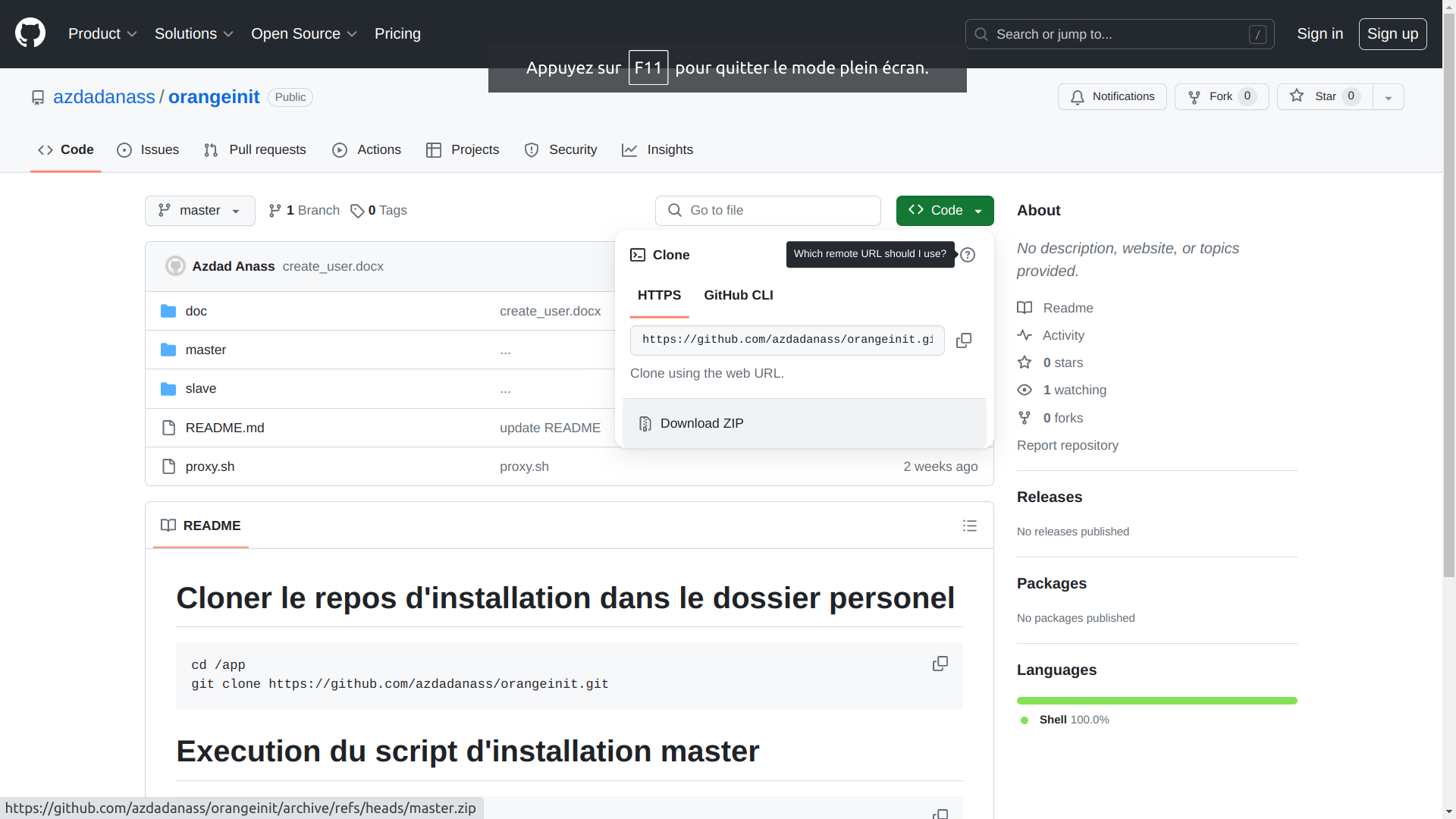
### **Serveur Backup**

1. partition applicative /app
2. partition backup /backup

# **Préparation Installation**

Depuis votre machine,téléchargez le repos suivant

https://github.com/azdadanass/orangeinit

****

à l’aide d’un outil de sftp (ex : mobaxterm <https://mobaxterm.mobatek.net/>), copiez le ficher téléchargé orangeinit-master.zip dans /app des2 serveurs

connectez vous par ssh dans les 2 serveurs, et lancez ces 2 commandes

cd /app

unzip orangeinit-master.zip

**Configuration du proxy Orange**

Pour configurer le proxy , lancez la commande suivante dans les deux serveurs

/app/orangeinit-master/proxy.sh

Puis Entrez l’adresse proxy (par défaut la valeur du proxy est [http://10.127.21.70:80](http://10.127.21.70:80/) ,vous pouvez appuyer sur Enter sans rien saisir si vous voulez utiliser cette adresse)

* + 1. **Installation**

Connectez vous par ssh dans les deux serveurs

dans le serveur principale,lancez la commande suivante

*app/*orangeinit-master/master/install.sh

dans le serveur backup, lancez la commande suivante

*app/*orangeinit-master/slave/install.sh

### Installation de portainer

portainer est l’outil qui va permettre la gestion et la visualisation des logs des applications

pour installer portainer, lancez le script suivant avec le compte de l’utilisateur personnel

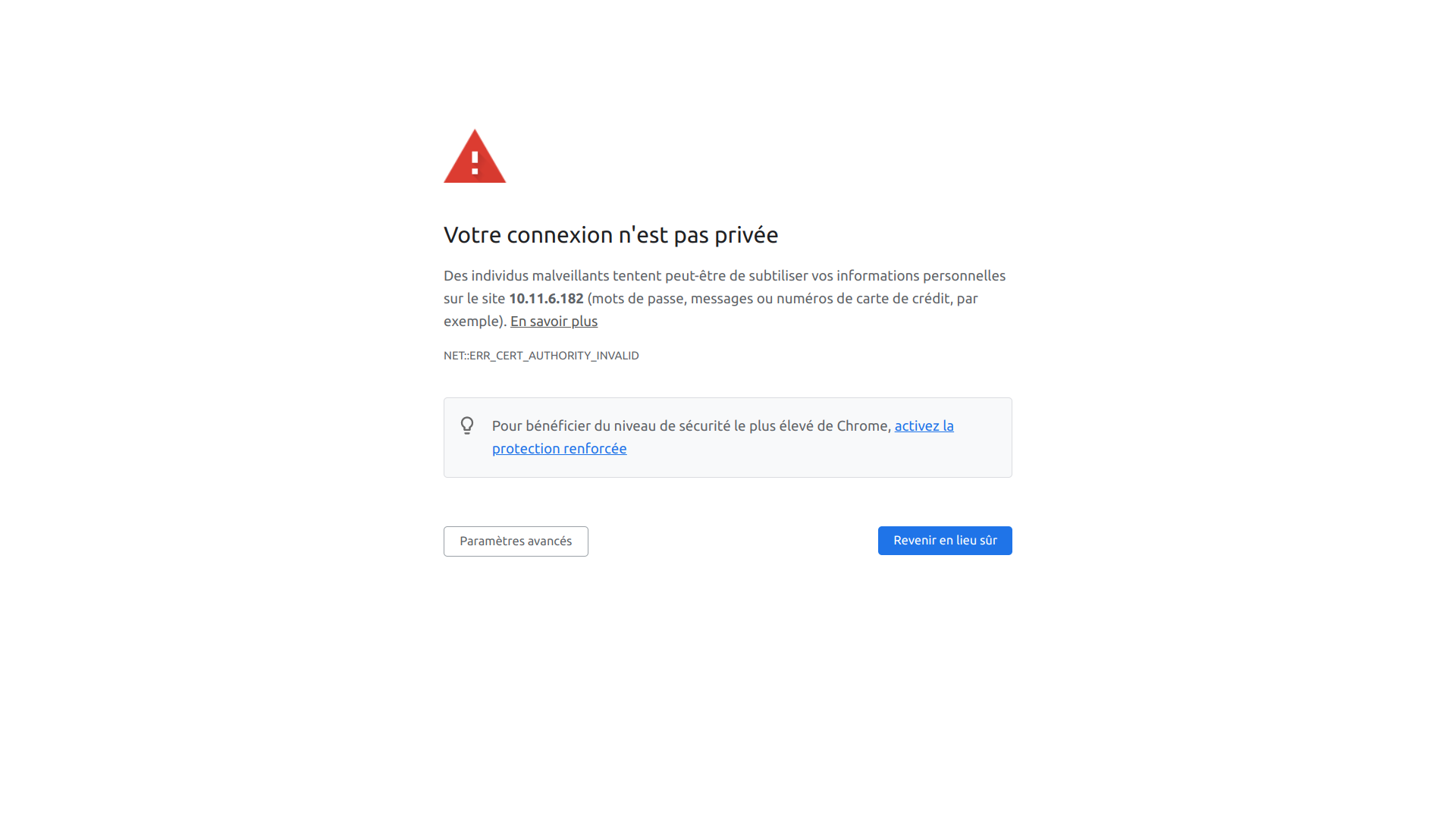
/app/scripts/deploy-portainer.sh

Après l exécution de la commande, vous pouvez accéder à l’interface depuis ce lien

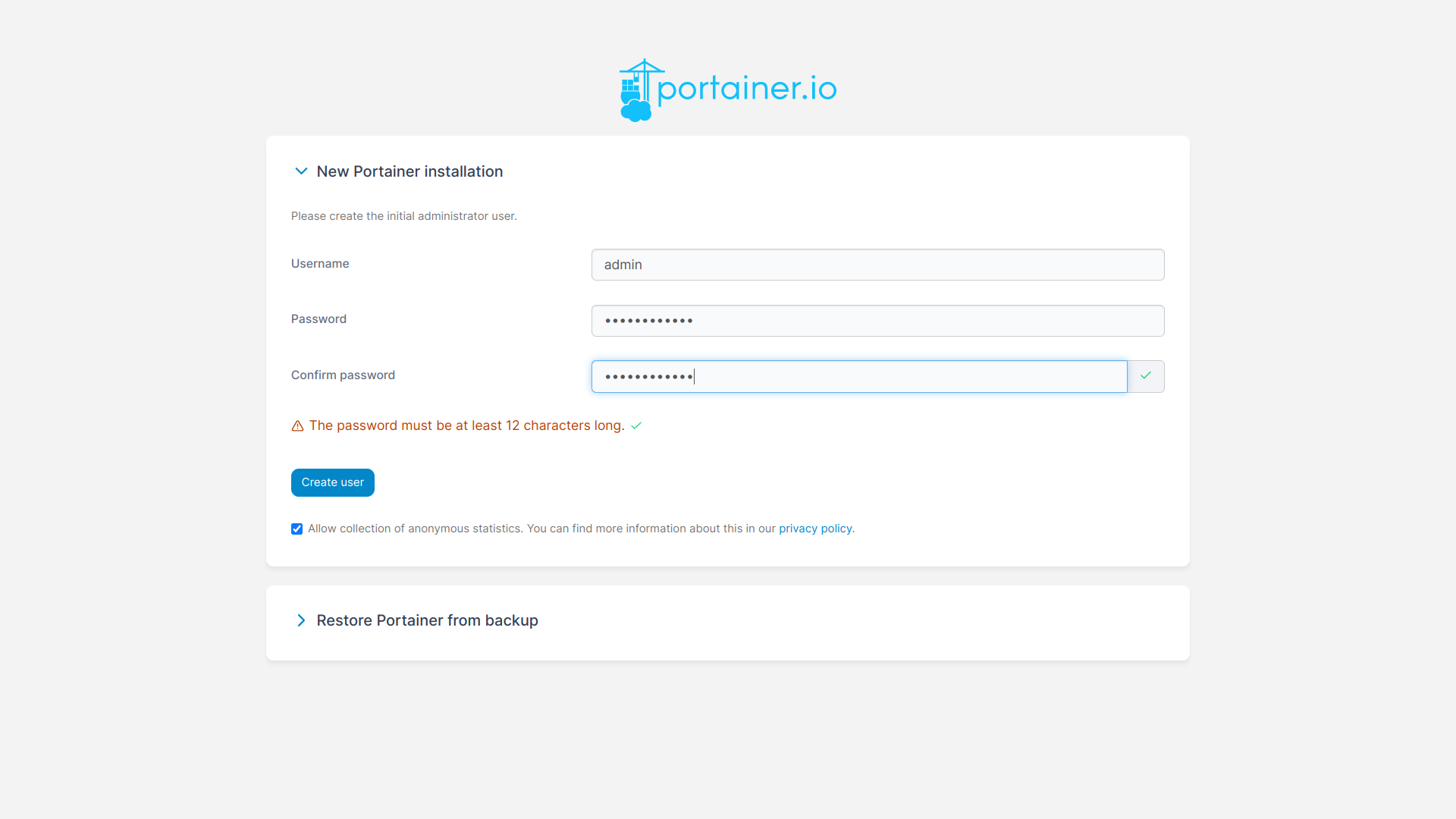
https://ip\_de\_la\_machine:9443

Cliquez sur Paramètres avancés, puis sur Continuer vers le site…

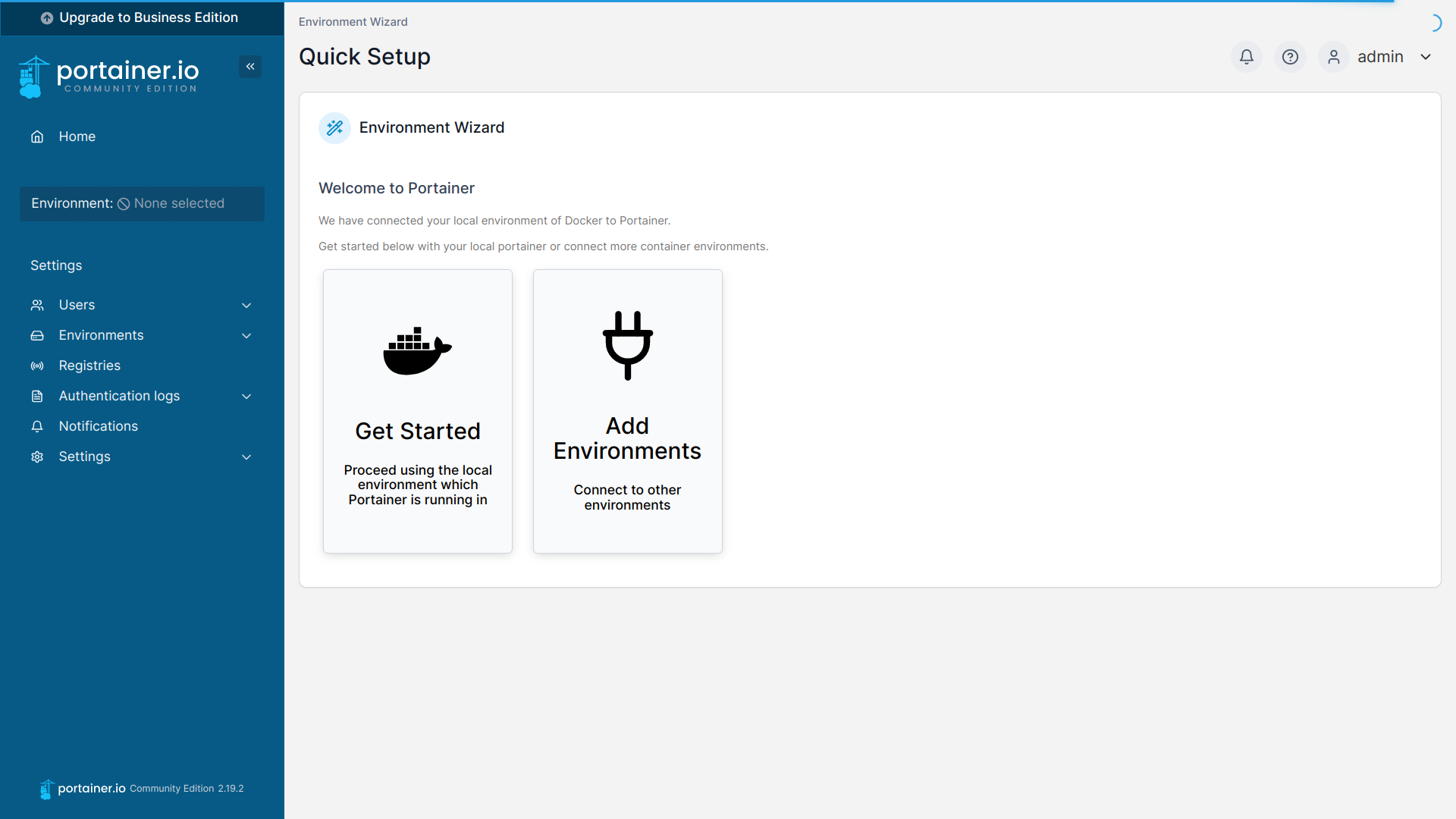
nous verrons après comment lancer portainer en https



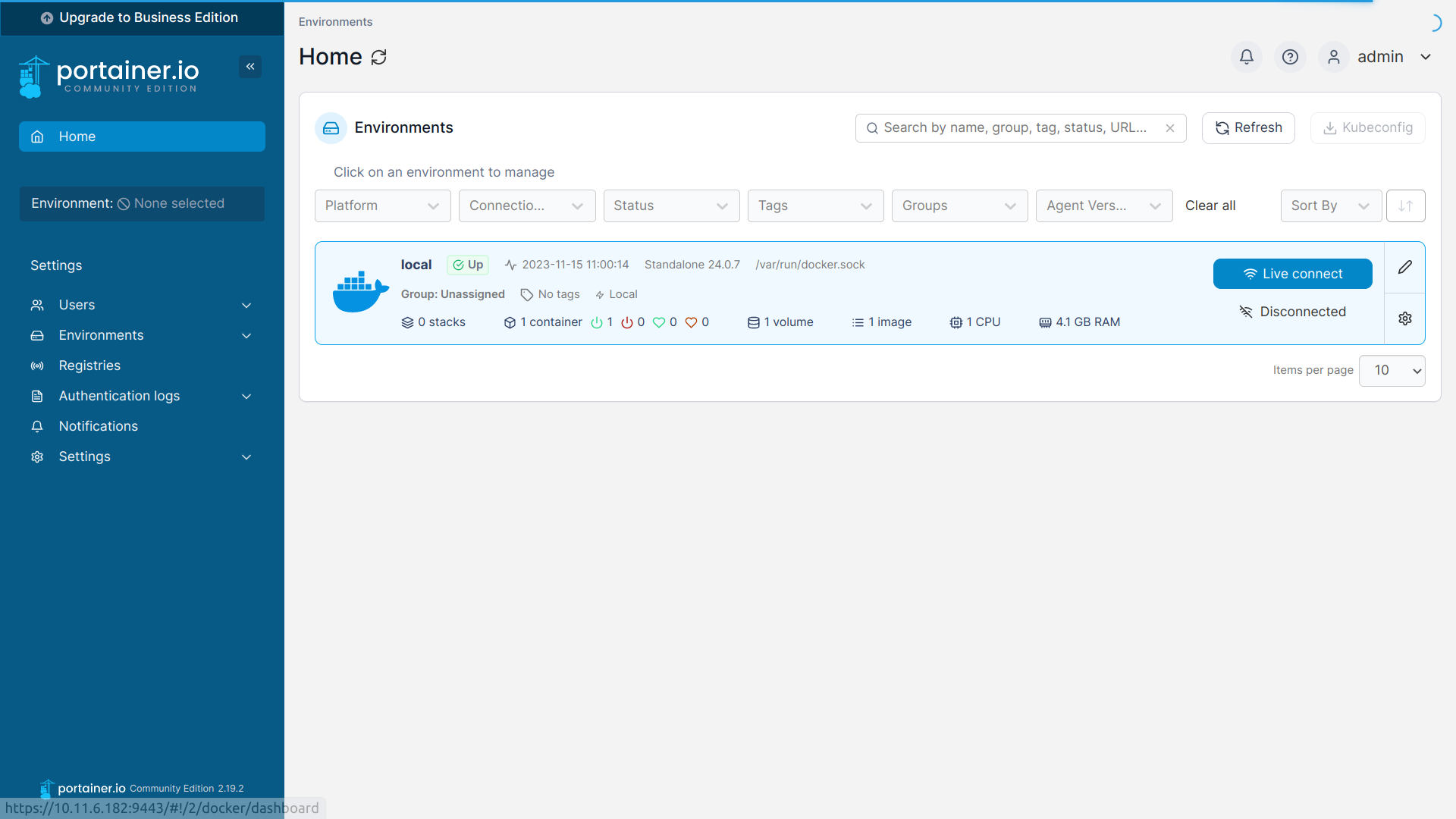
Le formulaire de création du compte admin vous sera proposé,créez le mot de passe admin puis cliquez sur create user



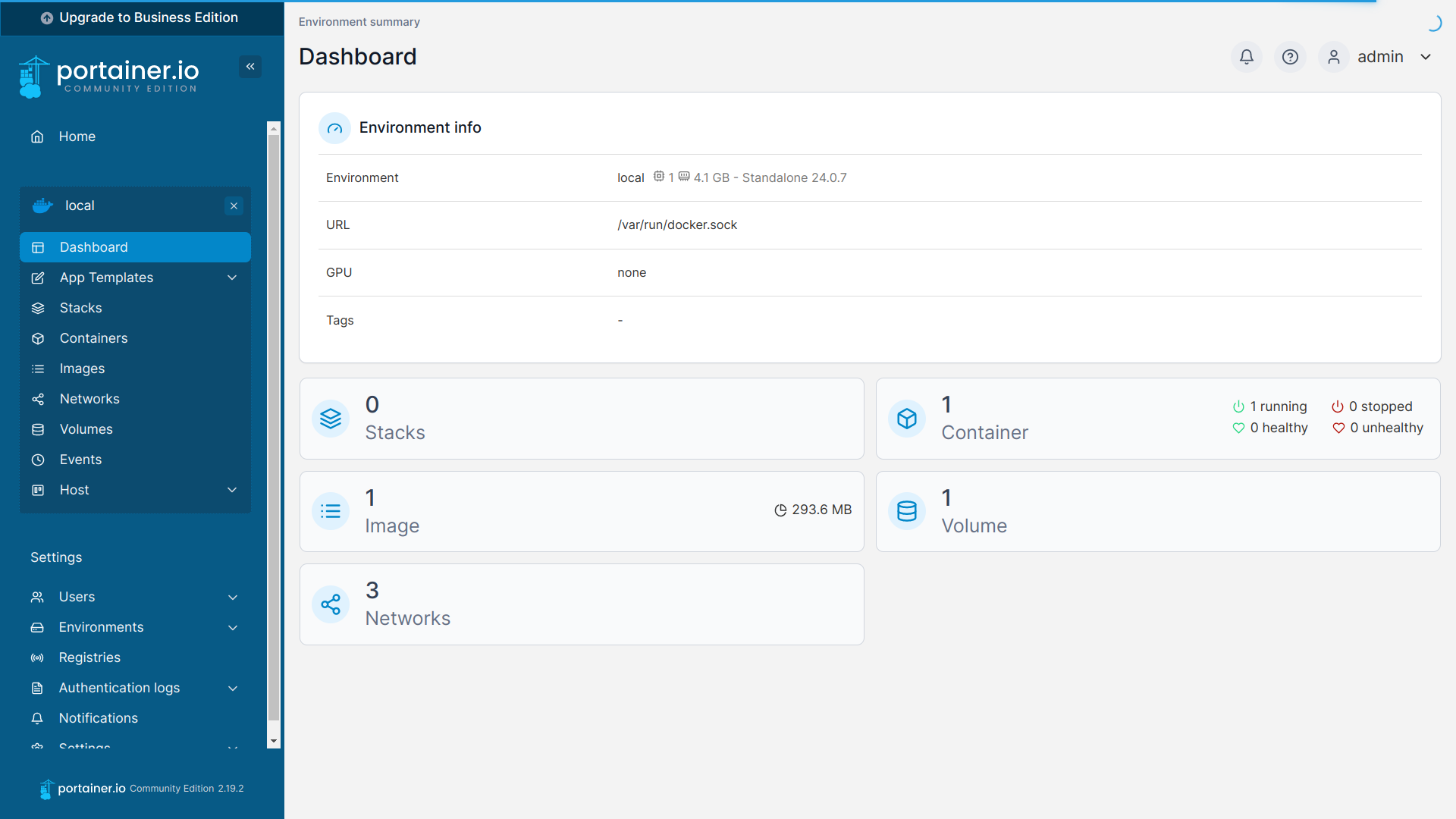
Dans le menu a gauche sélectionnez Home



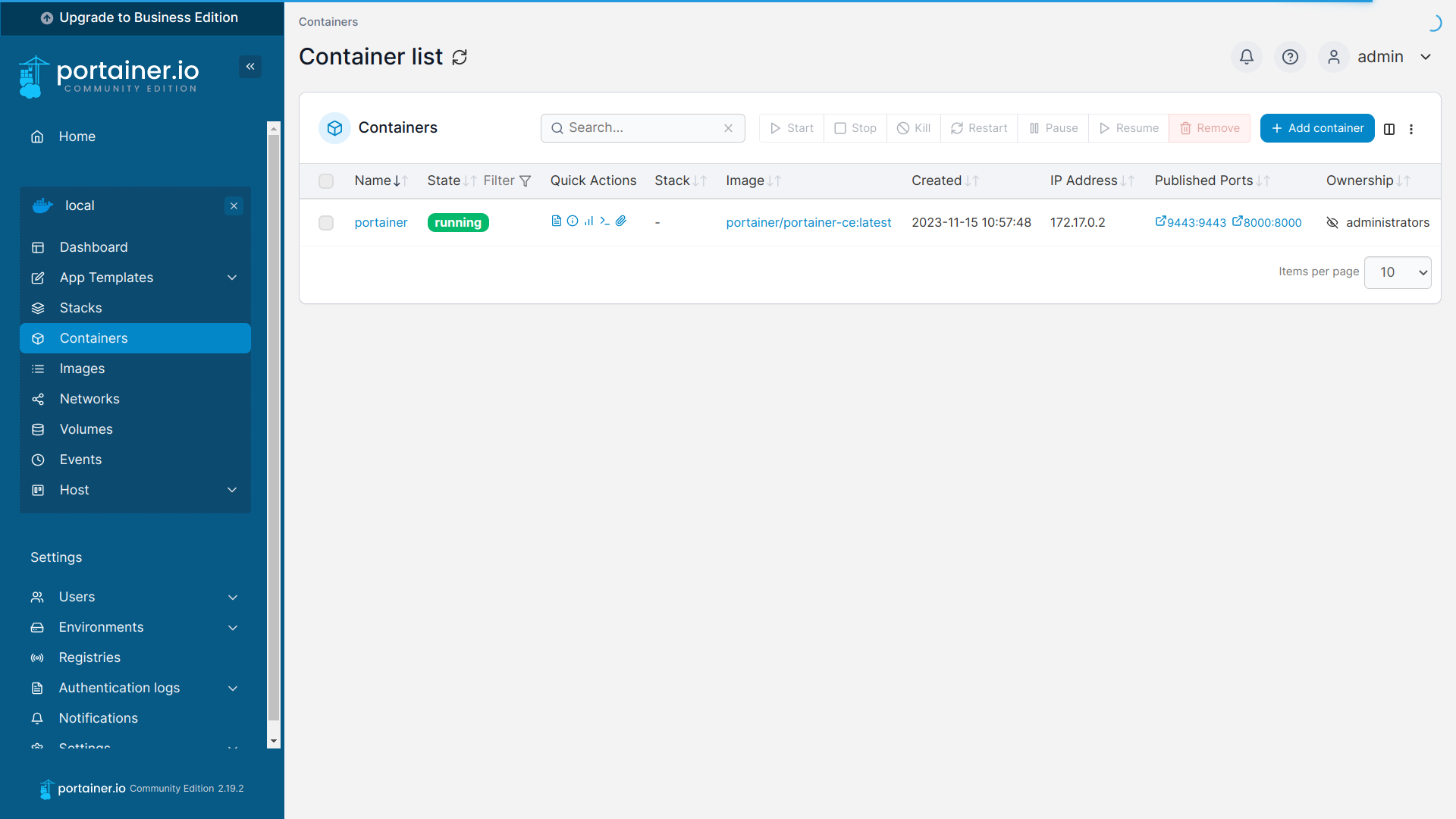
Cliquez sur l environnement local



Cliquer sur Container



Dans cette page, vous trouverez la liste des applications installées (pour l’instant seulement portainer est installé)



Mémorisez cette page, ça va nous permettre d’accéder aux logs des applications que nous allons installer par la suite

### Installation des applications (apps,iadmin ,sdm,ilogistics,public,qr,ibuy)

Pour installer ou faire la mise à jour des applications il suffit de lancer les commandes suivantes avec le compte de l’utilisateur personnel (chaque commande correspond a une application)

/app/scripts/deploy-apps.sh

/app/scripts/deploy-iadmin.sh

/app/scripts/deploy-sdm.sh

/app/scripts/deploy-ilogistics.sh

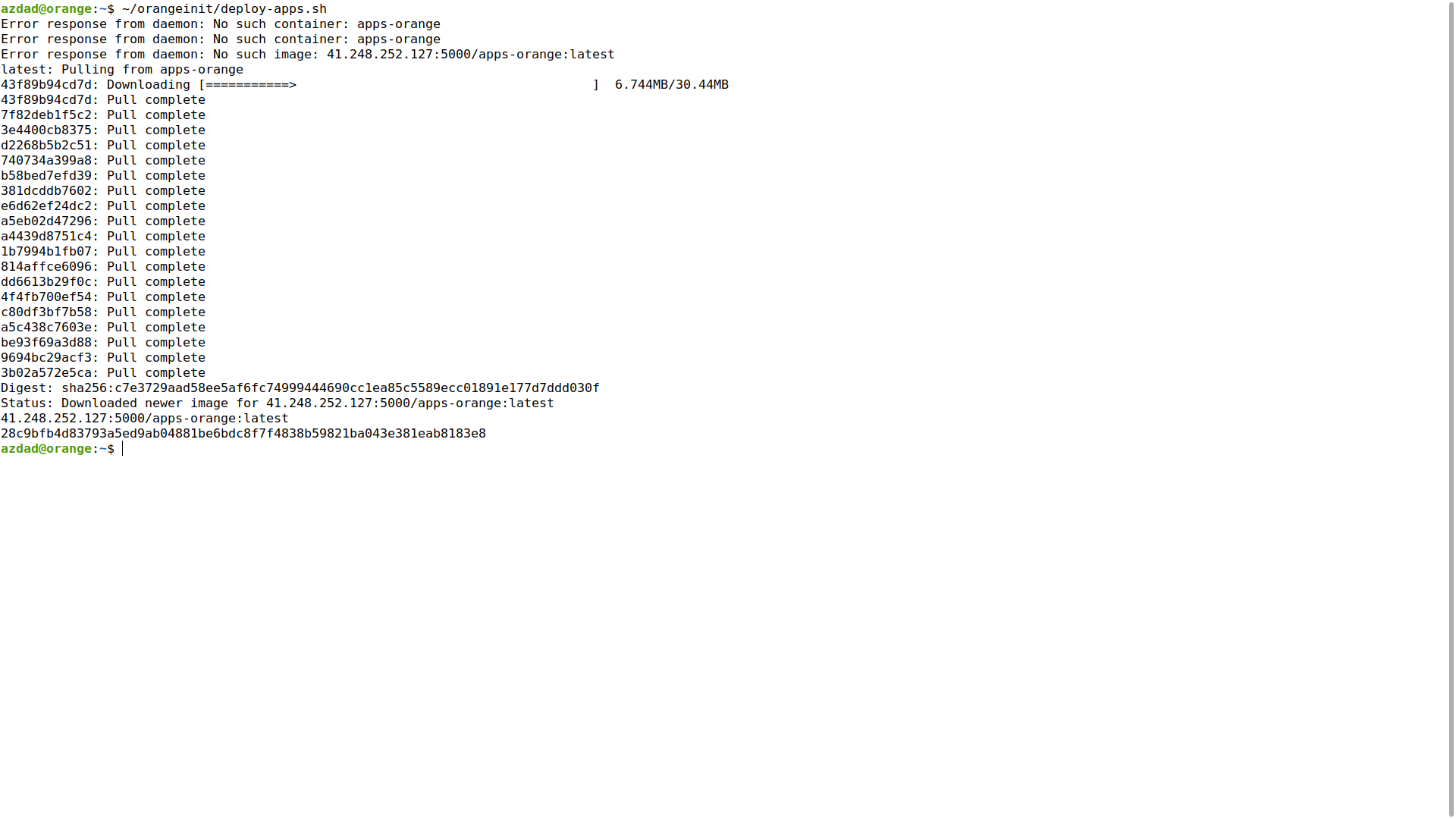
/app/scripts/deploy-public.sh

/app/scripts/deploy-qr.sh

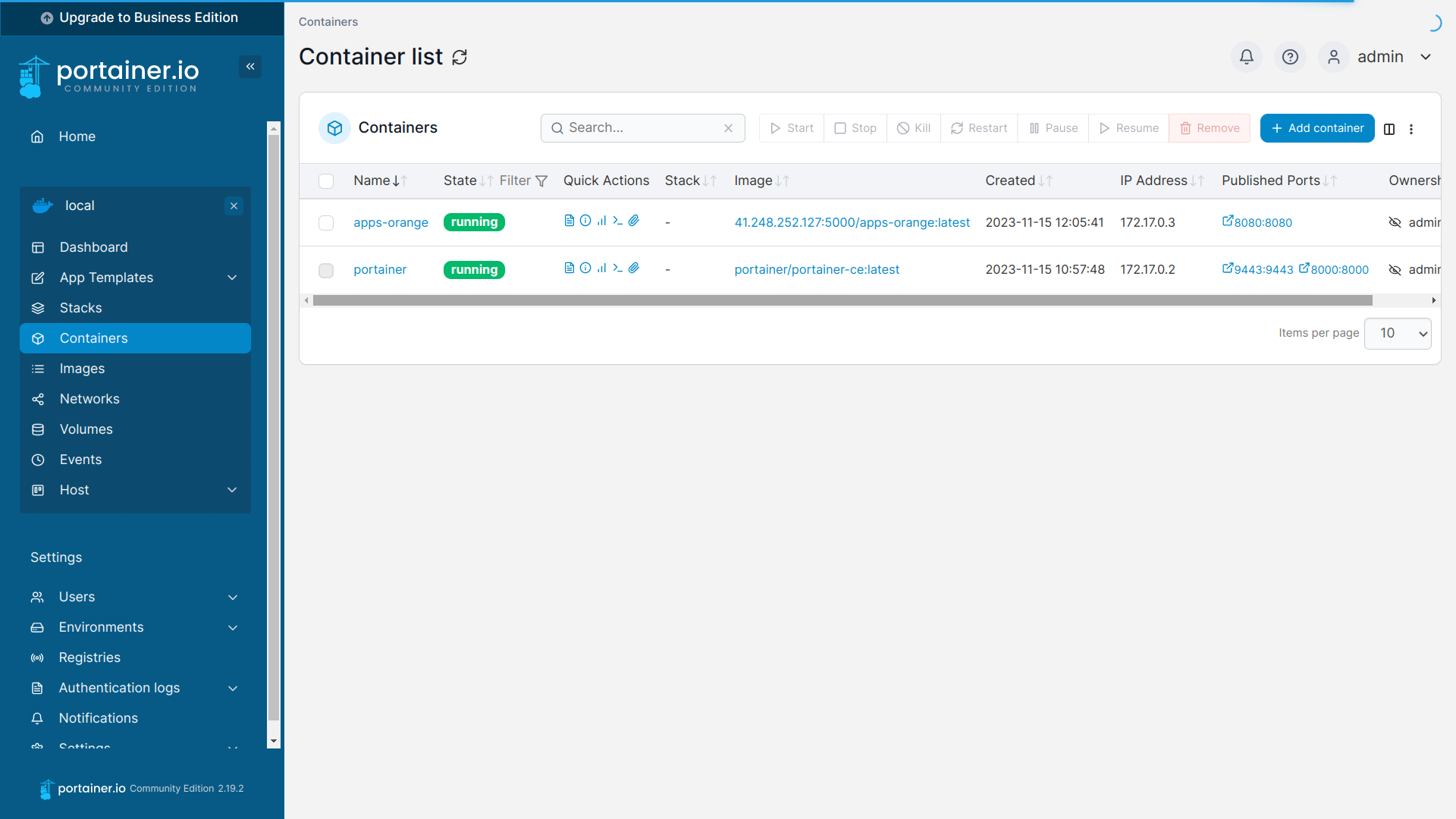
/app/scripts/deploy-ibuy.sh

NB : pour la mise à jour d’une application , il faut coordonner avec le prestataire avant de lancer la commande de maj

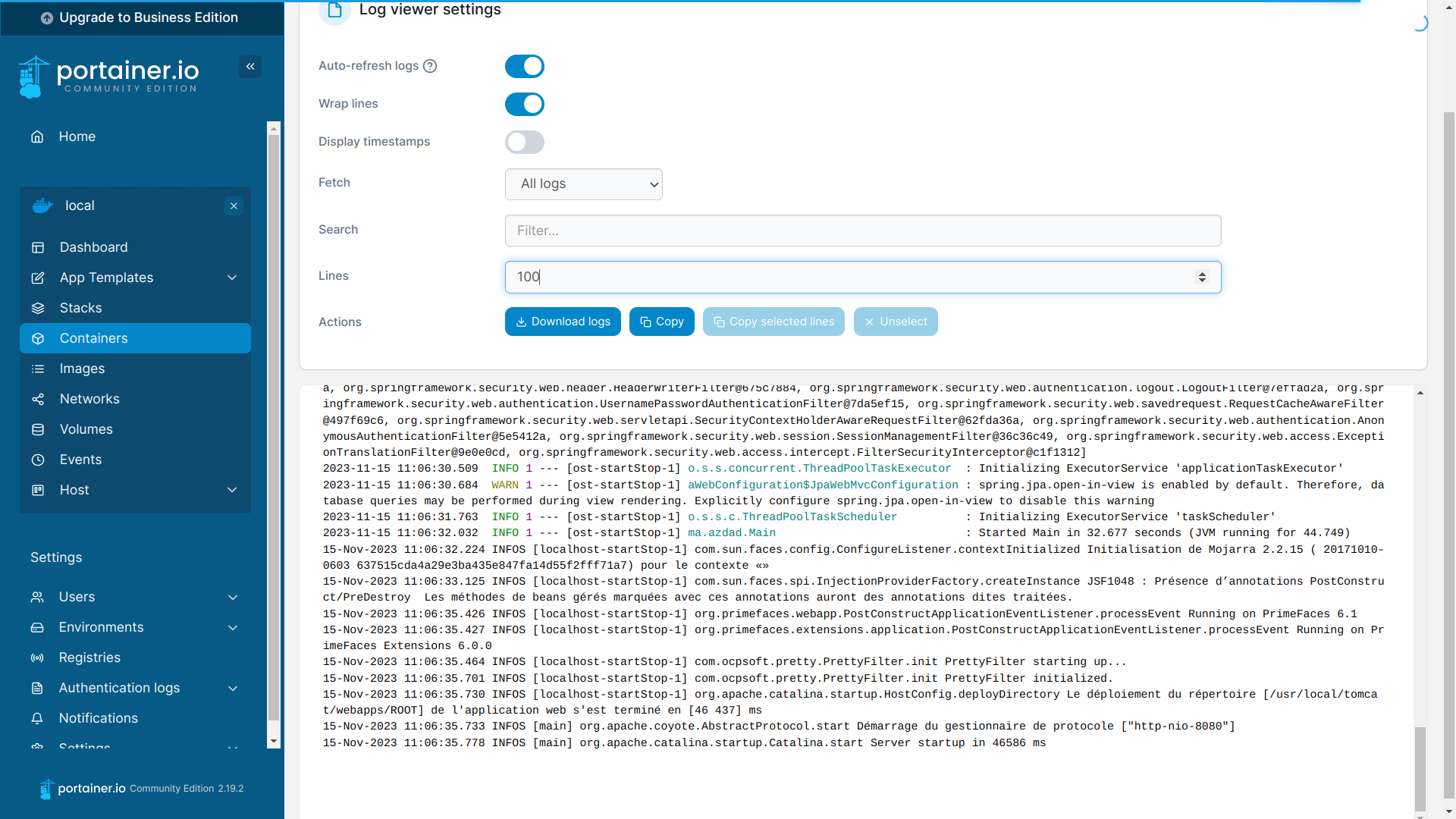
Exemple du lancement de apps



Après l’exécution de la commande /app/scripts/deploy-apps.sh,vous allez voir apparaître un nouveau container dans l’interface portainer

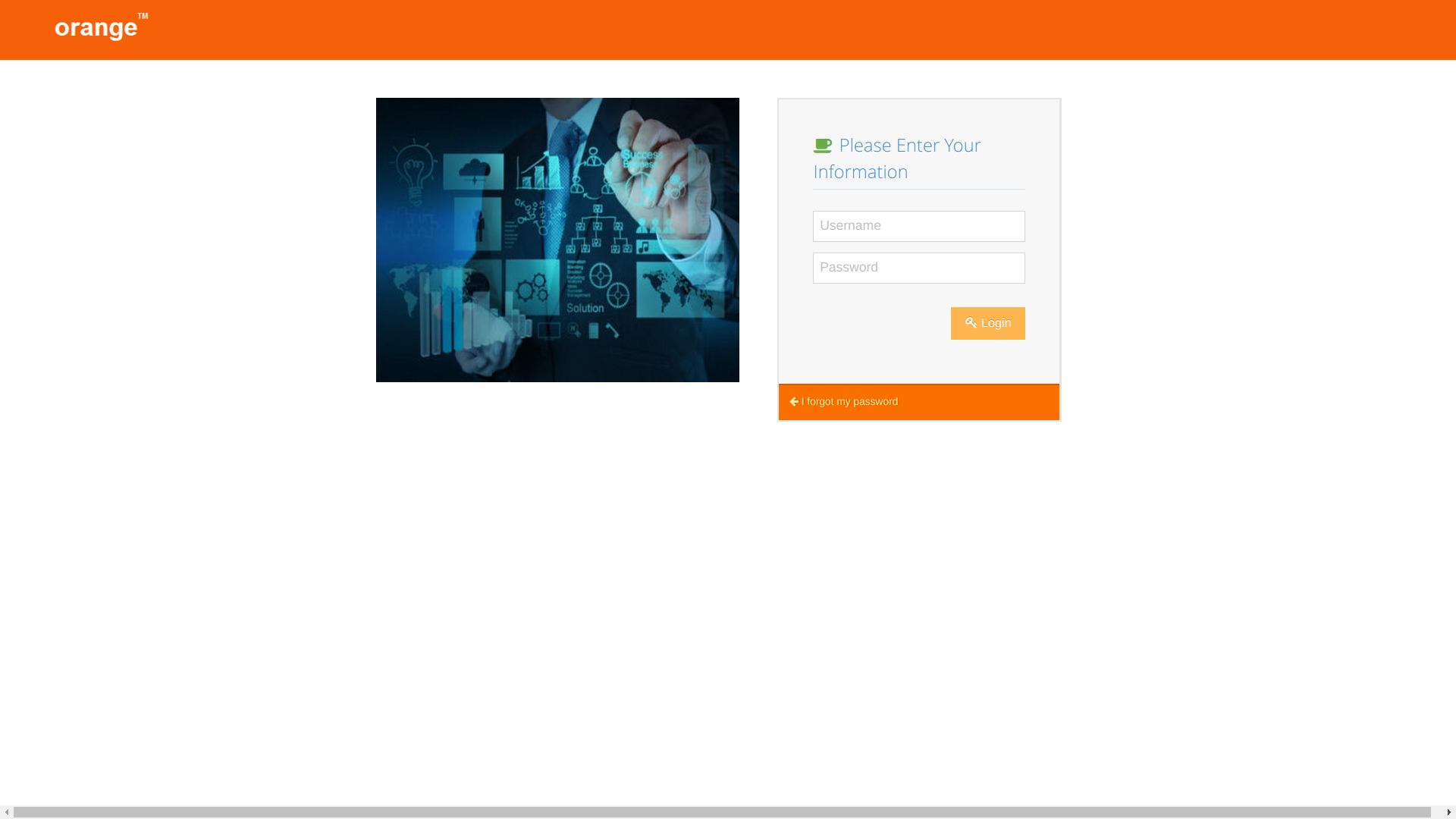


vous pouvez voir le log de apps-orange en cliquant sur l’icône de log dans Quick Actions, le log vous permettra de voir si le lancement de apps s’est bien déroulé



Si tout s’est bien déroulé,vous pouvez tester l’application apps-orange depuis ce lien :

http://ip\_de\_la\_machine:8080



pour les autres applications :

|  |  |
| --- | --- |
| Apps | [http://ip\_de\_la\_machine:8080](http://ip_de_la_machine:8080/) |
| iadmin | [http://ip\_de\_la\_machine:808](http://ip_de_la_machine:8080/)1 |
| sdm | [http://ip\_de\_la\_machine:808](http://ip_de_la_machine:8080/)2 |
| ilogistics | [http://ip\_de\_la\_machine:808](http://ip_de_la_machine:8080/)3 |
| public | [http://ip\_de\_la\_machine:808](http://ip_de_la_machine:8080/)4 |
| qr | [http://ip\_de\_la\_machine:808](http://ip_de_la_machine:8080/)5 |
| ibuy | [http://ip\_de\_la\_machine:808](http://ip_de_la_machine:8080/)6 |

NB : ces liens seront utilisés dans la configuration du reverse proxy nginx. Dans la partie qui viendra après, les ports [8080-8086] seront désactivés pour forcer seulement l’accès https (443) ou http (80)

# **Configuration du reverse proxy nginx**

#### Configuration pour accès HTTP

Pour configurer le serveur pour accès HTTP, lancez cette commande

/app/orangeinit-master/master/config/config-nginx.sh

Dans l’invite de commande , entrez les informations suivantes :

* l’ip locale du serveur principale (exemple : 192.168.1.100)
* le DNS qui sera utilisé pour les applications (exemple .orange.int) ce paramètre sera fourni par l’équipe responsable du DNS
* dans protocol, entrez http

Normalement les applications devront être accessible depuis les liens corrects (exemple si on suppose que le dns est orange.int)

* http://apps.orange.int
* http://iadmin.orange.int
* http://sdm.orange.int
* http://ilogistics.orange.int
* http://ibuy.orange.int
* http://qr.orange.int
* http://public.orange.int

#### **Configuration pour accès HTTPS**

1. Pour configurer le serveur pour accès HTTPS, il faut d’abord générer le certificat (fichier crt) pour chaque application
2. pour ce faire, lancez la commande suivante
3. /app/orangeinit-master/master/config/generate-csr.sh
4. les fichiers seront générés dans /app/certs/
5. Vous devez fournir les fichiers csr à l’équipe responsable de la génération des certificat https qui vont générer les certificat .crt
6. Il suffit maintenant de placer les fichiers crt reçu (apps.crt,iadmin.crt,sdm.crt,ilogistics.crt,qr.crt,public.crt,ibuy.crt,portainer.crt) dans /app/certs/ (la nomination du fichier est importante)

Maintenant que les fichiers crt sont bien placé il suffit de lancer cette commande

1. /app/orangeinit-master/master/config/config-nginx.sh
2. Dans l’invite de commande , entrez les informations suivantes :

* l’ip locale du serveur principale (exemple : **192.168.1.100**)
* le DNS qui sera utilisé pour les applications (exemple .**orange.int**) ce paramètre sera fourni par l’équipe responsable du DNS
* dans protocol, entrez **https**

les applications devront être accessible en HTTPS

* https://portainer-sdm.orange.int
* https://apps.orange.int
* https://iadmin.orange.int
* https://sdm..orange.int
* https://ilogistics.orange.int
* https://ibuy.orange.int
* https://qr.orange.int
* [https://public.orange.in](https://public.orange.int/)t

### **Activation et configuration du par-feu**

1. Pour configurer le par-feu, il suffit de lancer la commande suivante
2. /app/orangeinit-master/master/config/config-ufw.sh
   * 1. Après l’exécution de cette dernière commande,seuls ces ports seront accessibles
     + 80 (http)
     + 443 (https)
     + 9443 (portainer)
     + 5693 (ncpa :nagios agent)