

Ubuntu Server - Docker/portainer/tra efik

Solution de gestion de containers.

- [Docker - Installation docker + swarm](#)
- [Portainer - Configuration SSO Oauth avec keycloak](#)

Docker - Installation docker + swarm



Difficulté : Confirmé

Notions : docker, container, portainer, docker swarm.

I. Introduction

[Introduction à la containerisation](#)

Cette procédure à pour but de décrire la mise en place d'une infrastructure docker + portainer en standalone et en swarm.

plus d'informations sur : <https://docs.docker.com/>

Prérequis :

- (ici) Ubuntu server 22.04
 - 4vcpu
 - 4Gb de RAM
 - 20Gb disque OS
 - disque supplémentaire pour docker (taille dépendante du contenu prévu, prévoir minimum 10Gb)
-

II. Installation de docker

Attention : Avant toute installation, il est conseillé de mettre à jour son système.

Information : Un assistant d'installation contenant les instructions sur mesures est disponible ici : [get-docker](#)

2.1 Installer les prérequis

Tout d'abord, il faut installer les prérequis.

```
sudo apt install ca-certificates curl gnupg lsb-release
```

```
root@template:/home/sc4d-# apt install ca-certificates curl gnupg lsb-release
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
lsb-release est déjà la version la plus récente (11.1.0ubuntu4).
lsb-release passé en « installé manuellement ».
ca-certificates est déjà la version la plus récente (20211016ubuntu0.22.04.1).
ca-certificates passé en « installé manuellement ».
curl est déjà la version la plus récente (7.81.0-1ubuntu1.7).
curl passé en « installé manuellement ».
gnupg est déjà la version la plus récente (2.2.27-3ubuntu2.1).
gnupg passé en « installé manuellement ».
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libflashrom1 libftdi1-2
Veuillez utiliser « apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 1 non mis à jour.
root@template:/home/sc4d-# _
```

2.2 Installer docker

Ajouter la clé des dépôts.

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o
/etc/apt/keyrings/docker.gpg
sudo chmod a+r /etc/apt/keyrings/docker.gpg
```

```
root@template:/home/sc4d-# curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dear
mor -o /usr/share/keyrings/docker.gpg
root@template:/home/sc4d-#
```

Vérifier la présence de la clé avec :

```
ls /etc/apt/keyrings/docker.gpg
```

```
root@template:/home/sc4d-# ls /etc/apt/keyrings/docker.gpg
/etc/apt/keyrings/docker.gpg
```

Ajouter le dépôt :

```
echo "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg]
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" | sudo tee
/etc/apt/sources.list.d/docker.list > /dev/null
```

Lancer ensuite une nouvelle fois :

```
apt update
```

```
root@template:/home/sc4d-# apt update
Atteint :1 http://fr.archive.ubuntu.com/ubuntu jammy InRelease
Atteint :2 http://fr.archive.ubuntu.com/ubuntu jammy-updates InRelease
Atteint :3 https://download.docker.com/linux/ubuntu jammy InRelease
Reception de :4 http://fr.archive.ubuntu.com/ubuntu jammy-backports InRelease [99,8 kB]
Atteint :5 http://fr.archive.ubuntu.com/ubuntu jammy-security InRelease
99,8 ko réceptionnés en 1s (174 ko/s)
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
1 paquet peut être mis à jour. Exécutez « apt list --upgradable » pour le voir.
root@template:/home/sc4d-# _
```

Installer docker et ses composants avec la commande :

```
sudo apt install docker-ce docker-ce-cli containerd.io docker-compose-plugin
```

```
Les NOUVEAUX paquets suivants seront installés :
  containerd.io docker-ce docker-ce-cli docker-ce-rootless-extras
  docker-compose-plugin docker-scan-plugin libltdl7 libslirp0 pigz slirp4netns
0 mis à jour, 10 nouvellement installés, 0 à enlever et 1 non mis à jour.
Il est nécessaire de prendre 113 Mo dans les archives.
Après cette opération, 431 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

Valider et attendre la fin de l'installation.

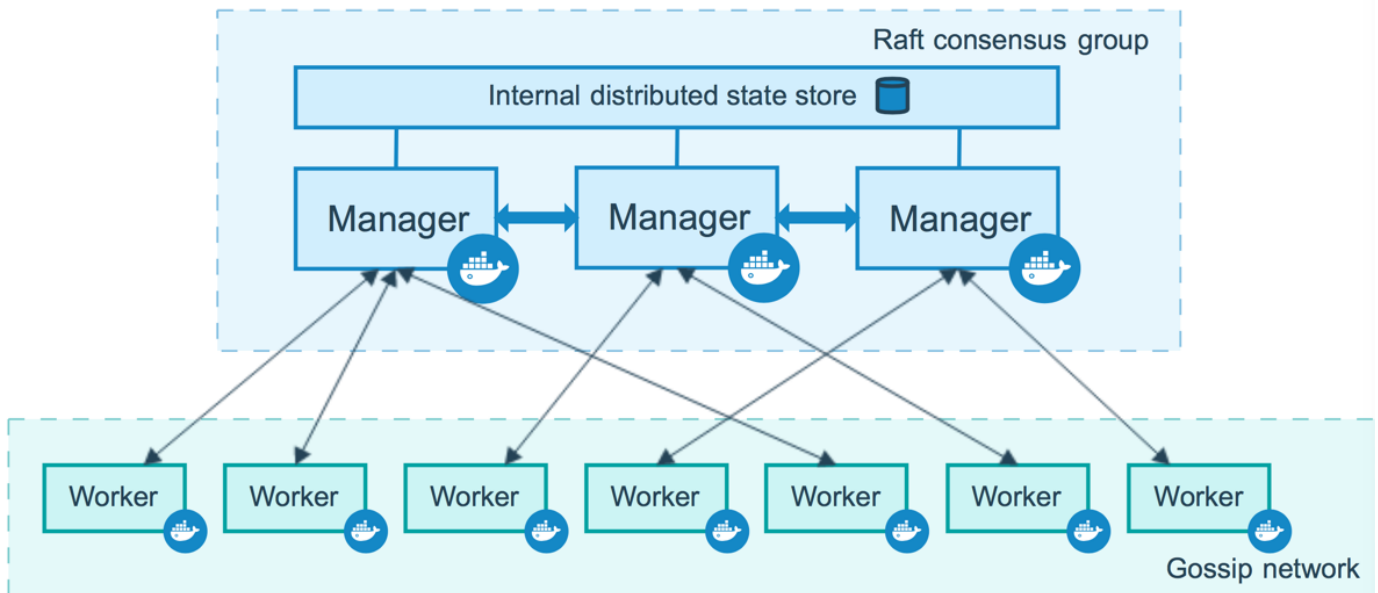
```
Réception de :4 http://fr.archive.ubuntu.com/ubuntu jammy/main amd64 libslirp0 a
md64 4.6.1-1build1 [61,5 kB]
Réception de :5 http://fr.archive.ubuntu.com/ubuntu jammy/universe amd64 slirp4n
etns amd64 1.0.1-2 [28,2 kB]
9% [2 containerd.io 884 kB/27,7 MB 3%]
```

Best practice : Il est conseillé d'utiliser un disque dédié pour docker et de réaliser un point de montage sur `"/var/lib/docker"`. Pour cela, suivre la procédure : [Ubuntu Server - Ajouter un disque/volume](#) ou [Ubuntu Server - Gérer les volumes avec LVM](#)

Information : Dans le cadre du déploiement d'un swarm, répéter les opérations ci-dessus sur l'ensemble des nœuds.

étape optionnelle - création du swarm

Cette étape est optionnelle et n'est nécessaire que dans le cadre de la mise en place d'un cluster. Ou dans le cas de docker d'un **SWARM**.



2.1.1 Initialisation du swarm

Sur le serveur docker qui sera le master du cluster, Exécuter la commande suivante pour initialiser le swarm.

```
docker swarm init --advertise-addr <adresse ip>
```

```
root@template:/home/sc4d-# docker swarm init --advertise-addr 192.168.1.28
Swarm initialized: current node (zrt0xxnkgd4s2hxxk96yo91grz) is now a manager.

To add a worker to this swarm, run the following command:

    docker swarm join --token SWMTKN-1-4onnwsb5ya2k13zwqw0c88qa83u0otnjotrjjtzeh72y27i0rt-cl16owen1
v4hara0f34ejce0 192.168.1.28:2377

To add a manager to this swarm, run 'docker swarm join-token manager' and follow the instructions.
root@template:/home/sc4d-# _
```

Plus de paramètres : [swarm init](#)

Bien noter lors de l'initialisation du swarm la commande qui permettra au workers de rejoindre le swarm ainsi que le token.

```
root@template:/home/sc4d-# docker swarm init --advertise-addr 192.168.1.28
Swarm initialized: current node (zrt0xxnkgd4s2hxxk96yo91grz) is now a manager.

To add a worker to this swarm, run the following command:

    docker swarm join --token SWMTKN-1-4onnw5b5ya2k13zww0c88qa83u0otnjotrjttzeh72y27i0rt-cl16owen1
    v4hara0f34ejce0 192.168.1.28:2377

To add a manager to this swarm, run 'docker swarm join-token manager' and follow the instructions.
root@template:/home/sc4d-# _
```

Astuce : Si cette commande avec le token n'est plus affiché. Il est possible de la récupérer en exécutant sur le manager la commande suivante.

```
docker swarm join-token worker
```

2.1.2 Jonction du/des workers

Pour rejoindre le swarm, entrer la commande suivante sur les workers.

```
docker swarm join --token <token> <ip du master>:<port>
```

```
root@template:/home/black# docker swarm join --token SWMTKN-1-1xghop5rs96clqdwpggik5iz4xkvc935xie1yyz5ihnvz594v-015wrmqax0cd9cgtqoovlm1un 192.168.1.11:2377
This node joined a swarm as a worker.
root@template:/home/black#
```

2.1.3 Autres opérations

Pour vérifier le status du cluster, utiliser la commande suivante sur un manager.

```
docker node ls
```

```
root@template:/home/black# docker node ls
ID                HOSTNAME        STATUS    AVAILABILITY    MANAGER STATUS    ENGINE VERSION
ng0030sbogsxnddf7k33yocbw    template    Ready     Active
yr7wdttc53mg1tt026swfjhtc *    template    Ready     Active           Leader             20.10.12
root@template:/home/black#
```

Pour quitter le swarm.

```
docker swarm leave
```

Puis sur le dernier nœud du cluster :

```
docker swarm leave --force
```

III. Pricipes de base

Information : La liste des commandes est disponible ici : [commandes docker](#)

L'utilisation de docker est assez intuitive une fois que l'on a saisi les bases. Les commandes docker sont assez simples et structurées.

Docker	<objet>	<action>	<nom ou ID>
	image	create	
	network	rm (remove)	
	service	ls (list)	
	stack	prune (delete all unused)	
	volume		

exemples :

```
docker image ls
```

```
root@dgc-prd-docker01:/home/dgc4d-# docker image ls
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
dgc/glpi             1.0                [REDACTED]         6 days ago        535MB
dgc/bookstack       1.0                [REDACTED]         6 days ago        424MB
traefik              <none>             [REDACTED]         12 days ago       135MB
wordpress            <none>             [REDACTED]         13 days ago       615MB
dgc/phpmyadmin       1.0                [REDACTED]         2 weeks ago       359MB
dgc/mysql            1.0                [REDACTED]         2 weeks ago       784MB
portainer/portainer-ee <none>            [REDACTED]         3 weeks ago       298MB
portainer/agent      <none>            [REDACTED]         3 weeks ago       183MB
mysql                <none>            [REDACTED]         3 weeks ago       455MB
ubuntu               latest             [REDACTED]         4 weeks ago       77.8MB
```

Pour les conteneurs, les commandes sont un peu différentes :

docker ps : liste les conteneurs

```
root@dgc-prd-docker01:/home/dgc4d-# docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED    STATUS    PORTS                               NAMES
[REDACTED]    wordpress:latest                    "docker-entrypoint.s..." 5 days ago Up 5 days 80/tcp                                tdo-lab-wptest1_wordpress.1.i9ja6i5u6kiv6v3bnozdz58qlm
[REDACTED]    mysql:5.7                          "docker-entrypoint.s..." 5 days ago Up 5 days 3306/tcp, 33060/tcp                 tdo-lab-wptest1_db.1.z5lg72kf6sqfxxqvebj9unjb3
[REDACTED]    dgc/glpi:1.0                       "apache2ctl -D FOREG..." 6 days ago Up 6 days                               dgc-prd-glpi_glpi.1.91lxtqpc4de4vafue37dl5u2
[REDACTED]    dgc/bookstack:1.0                  "apache2ctl -D FOREG..." 6 days ago Up 6 days                               dgc-prd-bookstack_bookstack.1.xf8g3uj5aoyeft302gfoqaxix
[REDACTED]    dgc/mysql:1.0                      "mysqld"                  7 days ago Up 7 days                               dgc-prd-mysql_mysql.1.njkgvt2qo55g4m6ejslmmuc3j
[REDACTED]    dgc/phpmyadmin:1.0                 "apache2ctl -D FOREG..." 7 days ago Up 7 days                               dgc-prd-mysql_phpmyadmin.1.91v7716u5j2y37zzmiel4nxwe
[REDACTED]    traefik:latest                      "/entrypoint.sh --ap..." 7 days ago Up 7 days 80/tcp                             dgc-prd-traefik_traefik.1.nolo9r8401aykjryfse4xf490
[REDACTED]    portainer/agent:latest              "/agent"                  7 days ago Up 7 days                               dgc-prd-portainer_agent.h9v376doa5k5kphb4ifiooj0a.epfpgrgsu
[REDACTED]    portainer/portainer-ee:latest       "/portainer -H tcp://..." 7 days ago Up 7 days 8000/tcp, 9000/tcp, 9443/tcp        dgc-prd-portainer_portainer.1.k0g5dwbk8agjmdl90iddm2vi
```

docker run <container> : lance le conteneur

docker stop <container> : stoppe le conteneur

3.1 Manipulation des images

information : Les images peuvent être téléchargées depuis dockerhub par exemple :
[docker HUB](#)

docker image pull <nom:tag> : Pour télécharger une image.

docker image push <nom:tag> : Pour pousser une image sur le repo.

docker image prune : efface les images non utilisées.

3.2 Manipulation des volumes

Les commandes vues plus haut permettent l'essentiel des manipulations.

Il est également bon de savoir les choses suivantes :

- un volume peut être monté sur un ou plusieurs conteneurs simultanément avec des autorisations différentes
- le contenu d'un volume peut être accédé depuis l'hôte docker au même titre qu'un dossier.

3.3 Manipulation des réseaux

Les commandes vues plus haut permettent de manipuler les réseaux.

Lors d'une création de réseau, il est possible d'en fixer les propriétés à l'aide des options suivantes :

```
Options:
  --attachable          Enable manual container attachment
  --aux-address map     Auxiliary IPv4 or IPv6 addresses used by Network driver (default map[])
  --config-from string  The network from which to copy the configuration
  --config-only         Create a configuration only network
  -d, --driver string   Driver to manage the Network (default "bridge")
  --gateway strings     IPv4 or IPv6 Gateway for the master subnet
  --ingress             Create swarm routing-mesh network
  --internal            Restrict external access to the network
  --ip-range strings    Allocate container ip from a sub-range
  --ipam-driver string  IP Address Management Driver (default "default")
  --ipam-opt map        Set IPAM driver specific options (default map[])
  --ipv6               Enable IPv6 networking
  --label list          Set metadata on a network
  -o, --opt map         Set driver specific options (default map[])
  --scope string        Control the network's scope
  --subnet strings      Subnet in CIDR format that represents a network segment
```

Astuce : chaque réseau reconnaît le nom des conteneurs qui y sont affecté comme nom DNS, il est ainsi possible d'adresser un conteneur par son nom.

exemple : le stack 'wordpress' contient deux conteneurs. 'wpweb' et 'wpmysql'.

Si les deux conteneurs partagent un réseau, le conteneur 'wpweb' pourra adresser le conteneur de base de donnée avec le nom 'wpmysql'.

IV. Créer un conteneur ou un service

4.1 sur un hôte standalone

4.1.1 créer via commande :

Dans l'exemple de conteneur suivant, il s'agira d'un service web apache sans base de données avec seulement un volume pour les données et une exposition des ports 80 et 443.

```
docker run -d -p 8001:80 -p 4431:443 --name webserver --restart=always -v
webserver_data:/var/www/html apache:latest
```

Docker run [options] <image>	lance le conteneur avec les options spécifiées basé sur l'image <image>
-d	lance le conteneur en arrière plan avec un ID.
-p 8001:80 -p 4431:443	mappe les ports de l'hôte et les redirige sur les 80 et 443 du conteneur
--name	nom du conteneur
--restart	donne les options de redémarrage du conteneur
-v webserver_data:/var/www/html	mappe le volume webserver_data sur le dossier /var/www/html
apache:latest	image à utiliser

4.1.2 créer une image avec un dockerfile :

pour compiler une image, utiliser la commande :

```
docker image build -f <nomdefichier> -t <nom image> .
```

4.2 sur un swarm

Sur un swarm, la logique change un peu du fait de pouvoir déclarer un service avec des propriétés de déploiement au lieu d'un simple conteneur.

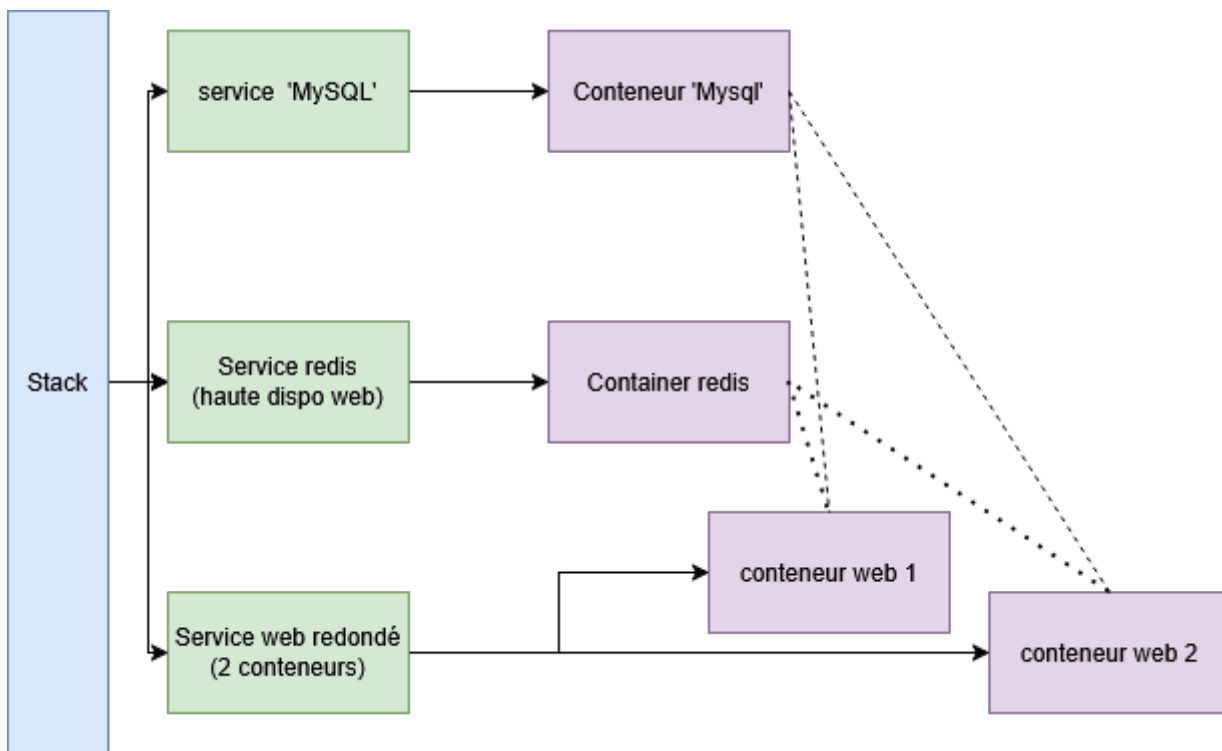
Dans la liste des options supplémentaires, certaines sont notables :

--constraint : ajoute des contraintes de déploiement (que sur un nœud manager, que sur les workers, etc...)

--deployment : ajoute des spécificités au déploiement (labels, nombre de copies, priorités, etc...)

4.2.1 Architecture du service :

La logique change donc par rapport à un déploiement classique, l'on ne parle plus de container directement.



Un Stack deviens un ensemble de services. Qui en fonction de leurs propriétés de déploiement contiennent un ou plusieurs containers.

La définition des propriétés se font donc au niveau du service et non plus au niveau du container.

4.2.2 Le réseau Overlay

Idem pour les réseaux, un nouveau type de réseau fait sont apparition, le type "**overlay**".

Il s'agit d'une encapsulation réseau par dessus la couche 3 pouvant utiliser divers mécanismes afin de créer une topologie virtuelle qui sera partagée entre tous les nœuds du cluster. Ainsi un réseau virtuel ou (VXLAN) sera perçu de la même façon depuis tous les hôtes du cluster et les container dans ce réseaux pourrons communiquer ensemble peut importe le nœud sur lequel ils sont situés.

4.2.2 Les secrets et configurations

Il devient également possible d'utiliser deux mécaniques supplémentaires jusque là absentes :

- les secrets

- les configs

Les secrets :

En effet, il peut être nécessaire de partager une information entre les différents conteneurs d'un même service, et ce indépendamment du nœud sur lequel il se situe. Cependant, cela veut également dire que cette information doit être propagée à l'ensemble des nœuds.

La plupart du temps, il peut s'agir de données sensibles (mot de passe, clé api, etc...).

Pour répondre à cela, il est possible de créer un "**secret**".

```
docker secret create [OPTIONS] SECRET [file|-]
```

Cette information sera alors chiffrée et ne sera accessible en clair qu'à l'intérieur des conteneurs qui la demande sous la forme d'un fichier présent dans **'/run/secrets/<secret_name>'**

Les configurations :

Sur le même principe que les secrets, il s'agit de fichiers déclarés sur le swarm qui sera distribué sur les nœuds.

Cependant celui-ci ne sera pas chiffré et restera modifiable.

```
docker config create [OPTIONS] CONFIG [file|-]
```

Il sera monté sur les conteneurs dans **'/run/configs/<nom_fichier_config>'**.

Cela permet de propager une configuration unique à l'ensemble des conteneurs du service. Par exemple des configurations de Vhost apache.

Portainer - Configuration SSO Oauth avec keycloak



Difficulté : Confirmé

Notions : Authentification, SSO

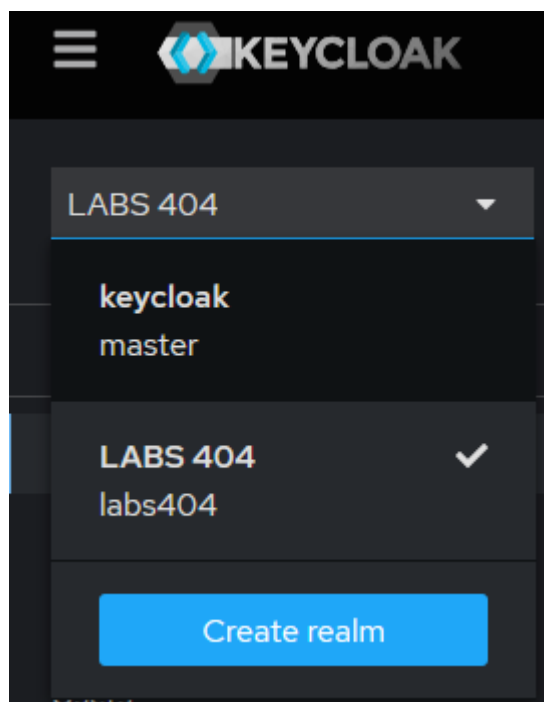
I. Introduction

Cette procédure à pour but d'expliquer le paramétrage de l'authentification SSO de portainer avec Keycloak.

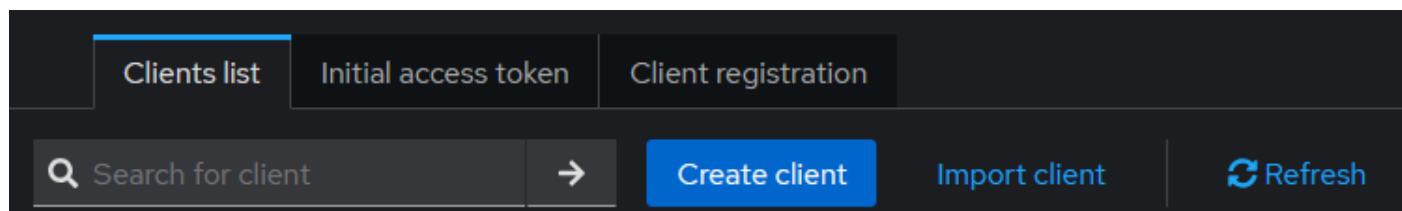
II. Côté Keycloak

2.1 Créer le client

Se connecter au keycloak et choisir le realm sur lequel ajouter le client portainer.



Cliquer sur '**Create client**'



Sélectionner le type '**OpenID Connect**'

Générer ou définir un '**clientId**'.

Il est possible d'utiliser un générateur afin de générer un e chaîne de 32 caractères. Par exemple : [ici](#).

Best Practice : 32 caractères avec minuscules, majuscules et chiffres.

Choisir un nom parlant.

Puis faire '**Next**'.

Create client

Clients are applications and services that can request authentication of a user.

1 General settings

2 Capability config

3 Login settings

Client type ⓘ

OpenID Connect ▼

Client ID ⓘ

UBMudbmPLGbMvn7BEjAeUcG7xro7vftU

Name ⓘ

sc-lab-portainer

Description ⓘ

Always display in UI ⓘ ☐ Off

Back

Next

Cancel

Sur la page suivante, activer '**Client authentication**' et '**Authorization**'.

Vérifier que les cases suivantes sont cochées.

Puis faire '**Next**'.

1

General settings

2

3

Login settings

Client authentication ?

On

Authorization ?

On

Authentication flow

☒ Standard flow ?

☐ Implicit flow ?

☒ OAuth 2.0 Device Authorization Grant ?

☐ OIDC CIBA Grant ?

☒ Direct access grants ?

☒ Service accounts roles ?

Back

Next

Cancel

Entrer les URL au format suivant (en modifiant les FQND).

Puis faire '**Save**'.

1

General settings

2

3

Login settings

Root URL ?

https://docker.labs404.fr/

Home URL ?

https://docker.labs404.fr/

Valid redirect URIs ?

https://docker.labs404.fr/*

+

Add valid redirect URIs

Valid post logout redirect URIs ?

https://docker.labs404.fr/#!/logout

+

Add valid post logout redirect URIs

Web origins ?

https://docker.labs404.fr/#|

+

Add web origins

Back

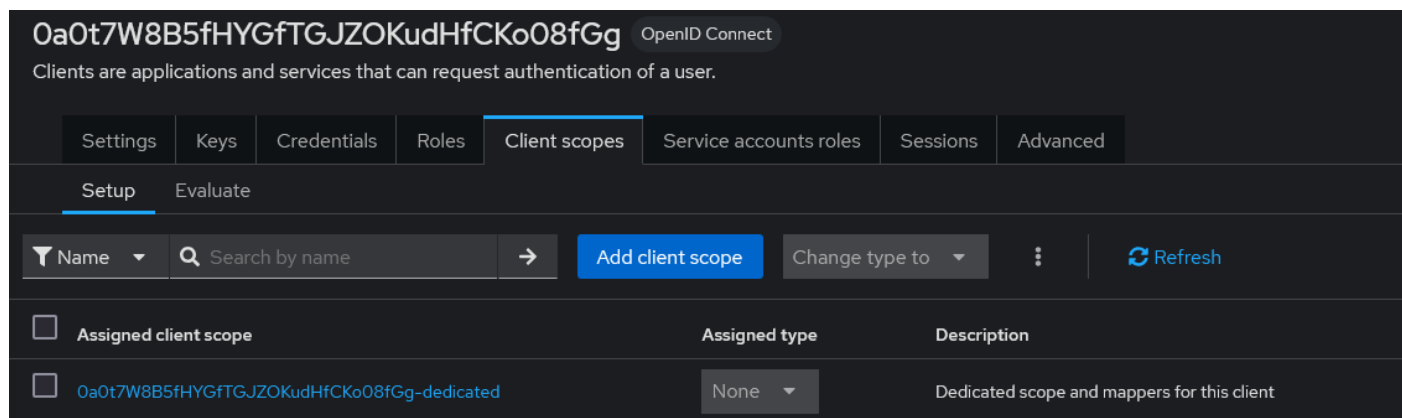
Save

Cancel

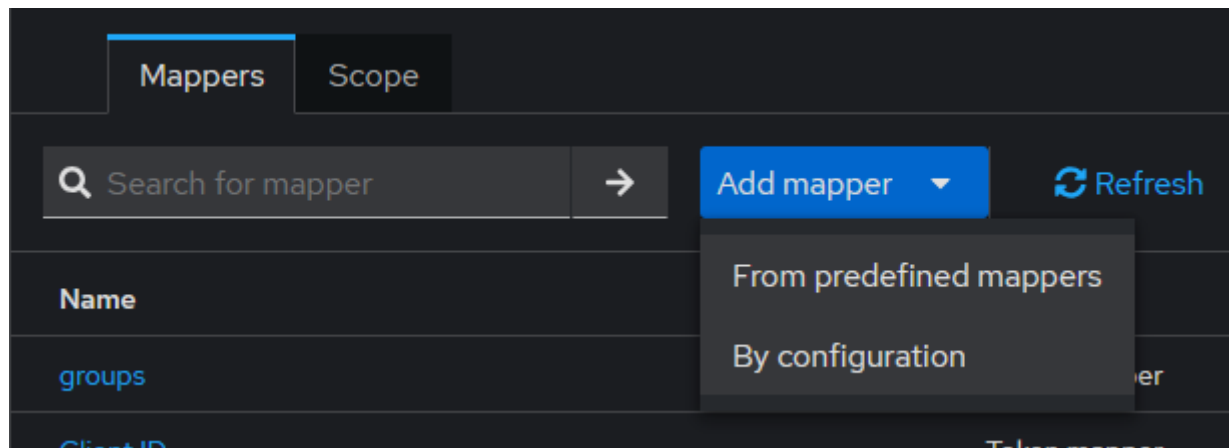
2.2 Préparer la synchro des groupes

Afin de pouvoir gérer les droits depuis le keycloak et synchroniser les groupes, aller dans l'onglet '**Client scope**'.

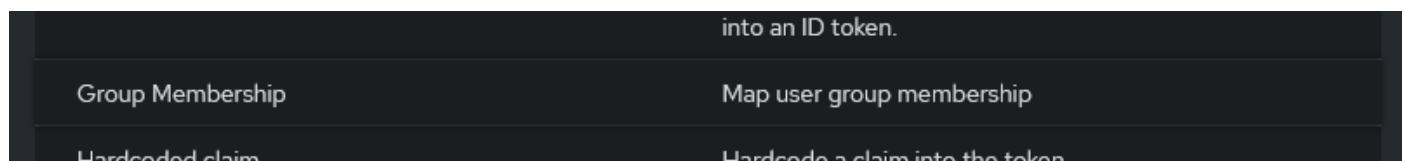
Choisir le client scope au nom du client suivi de '**-dedicated**'.



Faire '**Add Mapper**' puis '**By Configuration**'.



Choisir '**Group Membership**'.

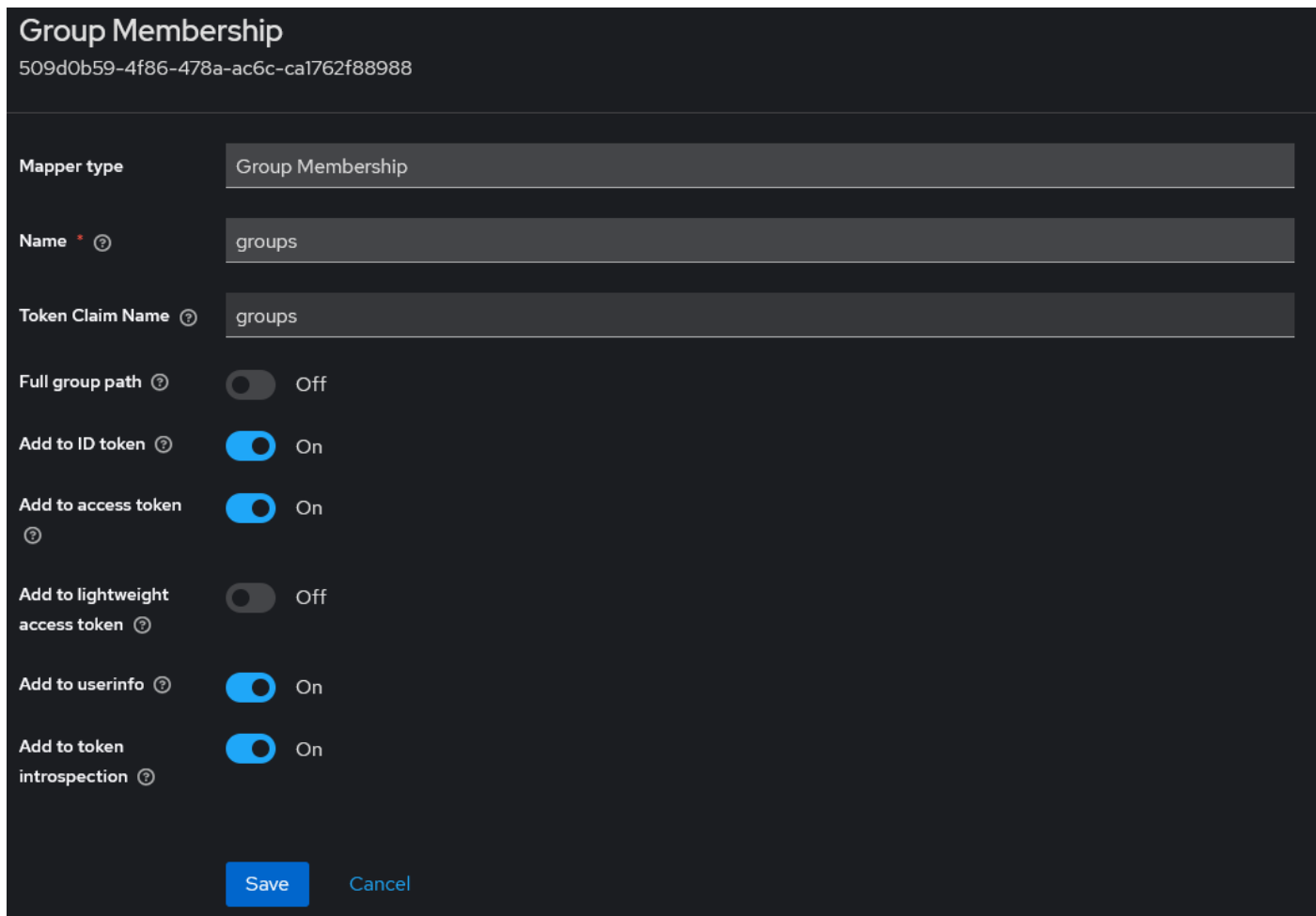


Définir le nom du **mapper** en '**groups**'.

Définir le Token **claim name** en '**groups**'.

Vérifier que les fonctions suivantes soit activées / désactivées.

Puis faire '**Save**'.

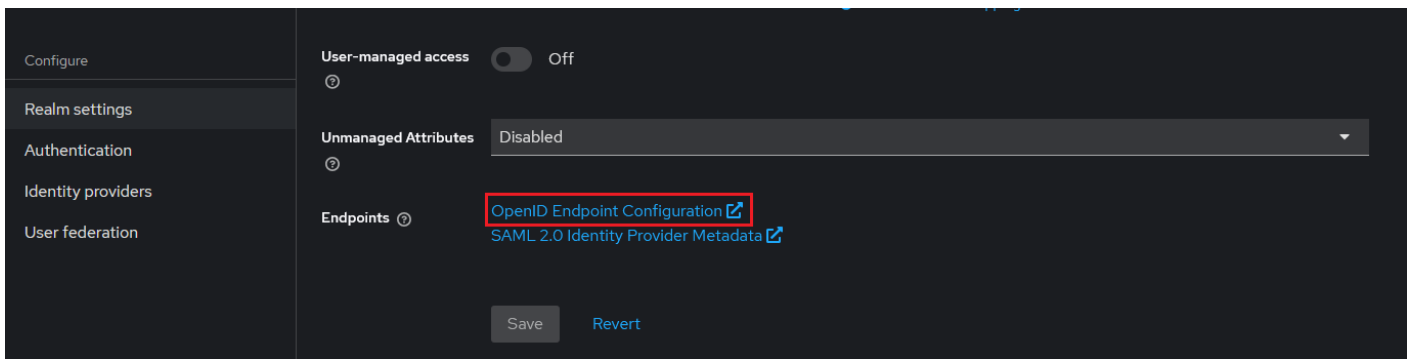


The screenshot shows a configuration window titled "Group Membership" with a unique ID "509d0b59-4f86-478a-ac6c-ca1762f88988". It contains several input fields and toggle switches. The "Mapper type" is set to "Group Membership". The "Name" and "Token Claim Name" fields both contain the text "groups". There are seven toggle switches: "Full group path" (Off), "Add to ID token" (On), "Add to access token" (On), "Add to lightweight access token" (Off), "Add to userinfo" (On), "Add to token introspection" (On), and a small question mark icon. At the bottom, there are "Save" and "Cancel" buttons.

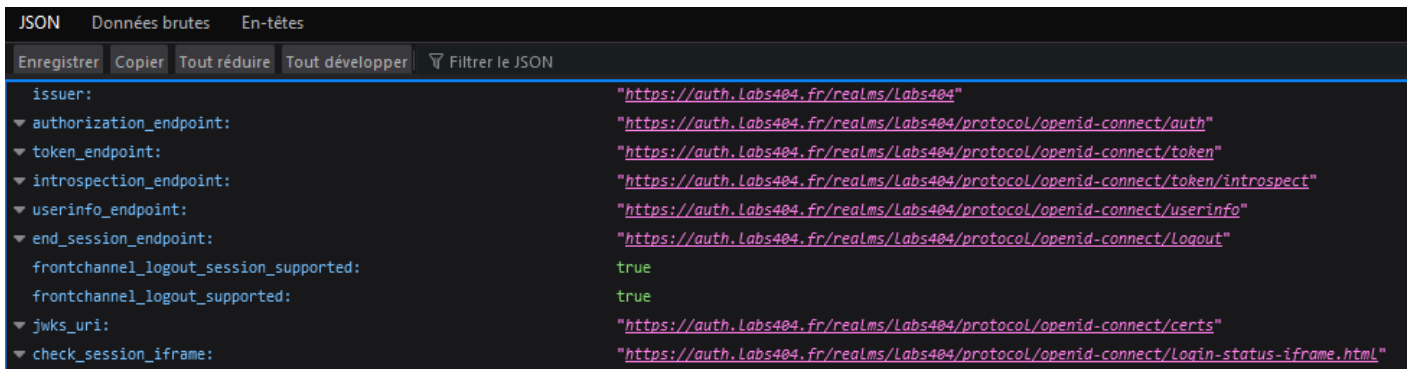
Configuration Item	Value / State
Mapper type	Group Membership
Name *	groups
Token Claim Name	groups
Full group path	Off
Add to ID token	On
Add to access token	On
Add to lightweight access token	Off
Add to userinfo	On
Add to token introspection	On

2.3 Récupérer les URL

Pour récupérer les URL, sélectionner le realm et faire '**Realm settings**' puis cliquer sur '**OpenID Endpoint Configuration**'.



Une page s'affiche et permet de récupérer les URL.



II. Côté Portainer

Se connecter au Portainer.

Aller dans '**Settings --> Authentication**'

Sélectionner '**Oauth**'

 **Authentication**

Configuration

Session lifetime ⓘ 8 hours ▼

⚠ Changing from default is only recommended if you have additional layers of authentication in front of Portainer.

Authentication method


Internal
Internal authentication mechanism


LDAP
LDAP authentication


Microsoft Active Directory
AD authentication


OAuth
OAuth authentication

Activer '**Use SSO**' et '**Automatic user provisioning**'.

Laisser la **Default Team** en '**No Team**'.

Note : Activer 'Hide internal authentication prompt' forcera la page de login SSO et désactivera l'authentification interne. Il sera toutefois possible d'y accéder en ajoutant **/#!/internal-auth** à la suite de l'url.

Single Sign-On

Use SSO ⓘ ☒

Hide internal authentication prompt ☐

Automatic user provisioning

With automatic user provisioning enabled, Portainer will create user(s) automatically with the standard user role. If disabled, users must be created beforehand in Portainer in order to login.

Automatic user provisioning ☒

The users created by the automatic provisioning feature can be added to a default team on creation.

By assigning newly created users to a team, they will be able to access the environments associated to that team. This setting is optional and if not set, newly created users won't be able to access any environments.

Default team ⓘ The default team option will be disabled when automatic team membership is enabled

No team ▼ ✕

Activer '**Use SSO**' et '**Automatic Team membership**'.

Définir les nom des groupes Keycloak à synchroniser et les associer aux groupes du portainer

Définir le groupe administrateur.

Team membership

Automatic team membership synchronizes the team membership based on a custom claim in the token from the OAuth provider.

Automatic team membership ☒

Claim name [?]

Statically assigned teams

claim value regex	GRP_SEC_GG_DOCKER-DGC	maps to	team	GRP_SEC_GG_DOCKER-DGC	delete
claim value regex	GRP_SEC_GG_DOCKER-GMG	maps to	team	GRP_SEC_GG_DOCKER-GMG	delete

The default team will be assigned when the user does not belong to any other team

Default team

Admin mapping

Assign admin rights to group(s) [?] ☒

claim value regex	GRP_SEC_GG_DOCKER-ADMIN	delete
-------------------	-------------------------	---------------------------------------

Définir les url de configuration comme suit en remplaçant, puis faire 'Save'.

OAuth Configuration

Client ID [?]

Client secret

Authorization URL [?]

Access token URL [?]

Resource URL [?]

Redirect URL [?]

Logout URL [?]

User identifier [?]

Scopes [?]

Auth Style [?]

Actions

Tout est prêt et la nouvelle page de connexion inclut désormais l'option d'authentification.



Log in to your account

Welcome back! Please enter your details

→] Login with OAuth

or

Use internal authentication