Service Openstack Cloud de la DSI INRAE

Version 0.0.1

Quickstart

⚠ Pour vous assurer de consulter la dernière version de la documentation et ainsi disposer des informations les plus récentes ainsi que pour un rendu optimal, privilégiez la version en ligne : https://documentation.cloud.inrae.fr/

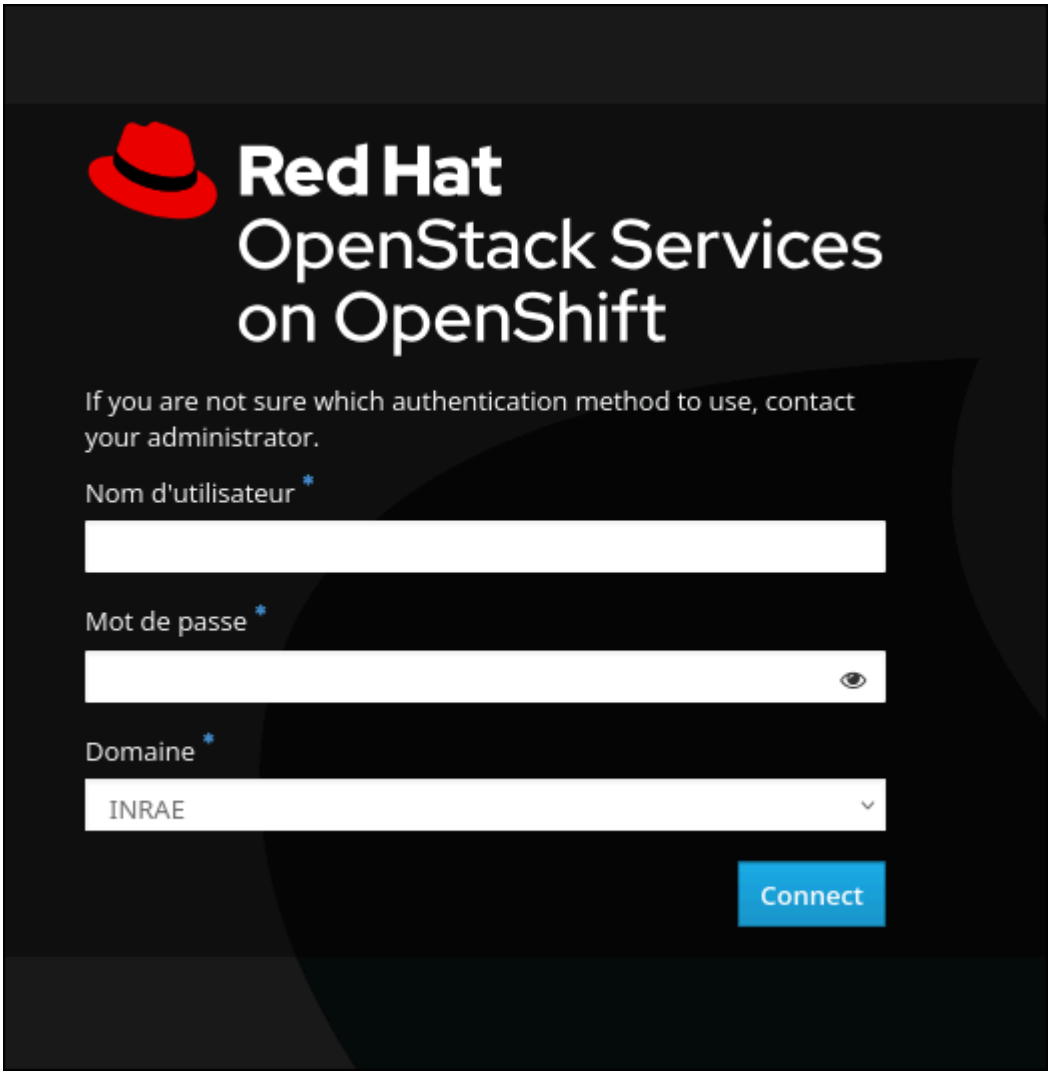
Quickstart

Cette documentation à pour objectif de vous aider a déployer votre premiere instance sur le cloud Openstack de la DSI INRAE.

Accès à l'interface Horizon

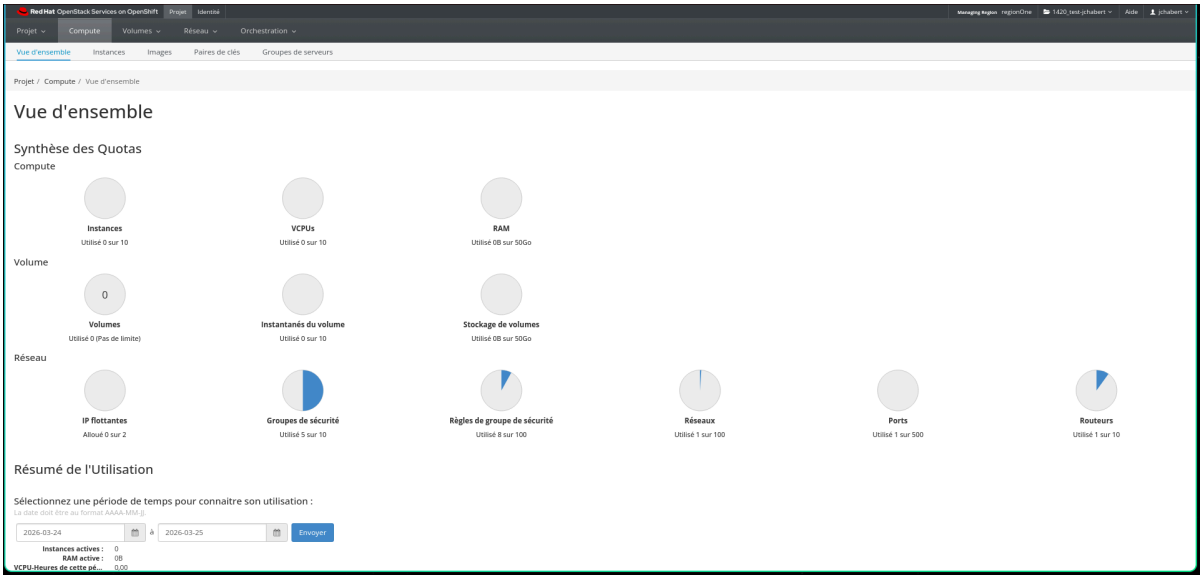
Une fois votre demande de création d'un project Openstack traitée, vous pourrez vous identifier sur la plateforme.

Pour cela, il vous suffira de suivre le lien suivant pour acceder à l'interface web d'Openstack (Horizon) : https://cloud.inrae.fr



> **A noter**
>
> Il vous faudra utiliser vos identifiants LDAP et choisir le domaine "INRAE" dans le menu déroulant

Une fois authentifié vous serez automatiquement redirigé vers la page "Vue d'ensemble" de votre projet. Cette page fait état du projet, de ses quotas, des ressources consommées et disponibles...



> **A noter**
>
> Par default, un projet vous sera livré avec :
>
> - un réseau interne
> - un routeur
> - des groupes de sécurités
>
> Ces éléments vous seront nécessaires pour pouvoir déployer votre instance et vous y connecter

Création / Import d'une clef SSH

Pour pouvoir accéder en SSH aux instances qui seront déployées, il est nécessaire de créer/d'importer une paire de clef sur l'Openstack.

> **Attention**
>
> Les paires de clefs sont entièrement personnelles. Chaque utilisateur pourra voir et utiliser uniquement les paires de clefs qu'il aura lui même crée ou importé sur la plateforme

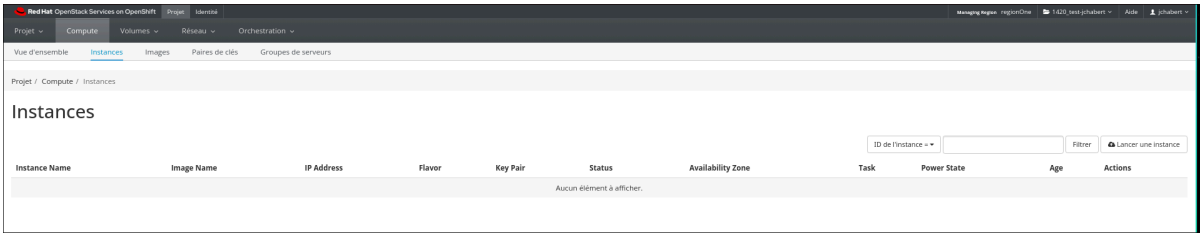
Méthode 1 : Créer une nouvelle clef

Placez vous dans la section **Projet** en haut a gauche, puis dans l'onglet **Compute** et enfin, cliquer sur **Paires de clés**. Sur cette page, vous pourrez ensuite aller sur **Créer une paire de clés**

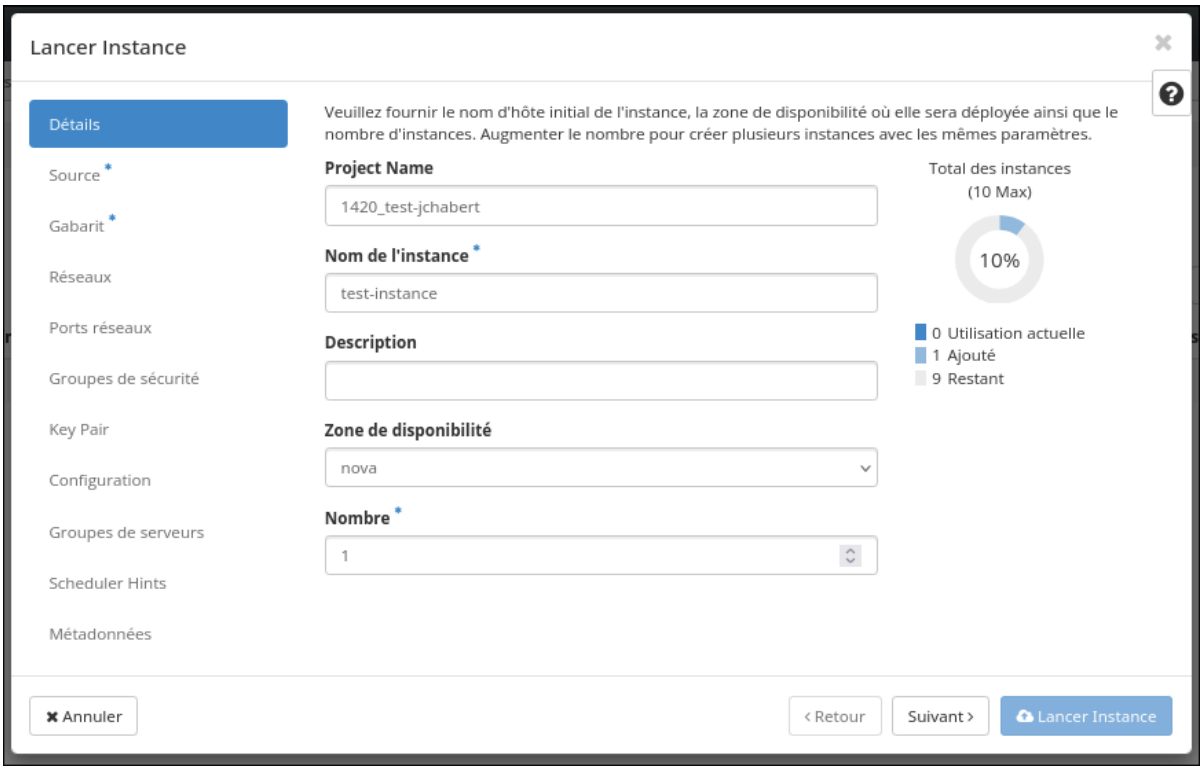
> **Rappel**
>
> Cette clef sera indispensable pour pouvoir accéder à vos instances déployées sur le cloud Openstack, car les connexions via mot de passe ne seront pas possible.

Création d'une instance

Placez vous dans la section **Projet** en haut à gauche, puis dans l'onglet **Compute** et enfin, cliquer sur **Instances**. Sur cette page, vous pourrez ensuite aller sur **Lancer une instance**



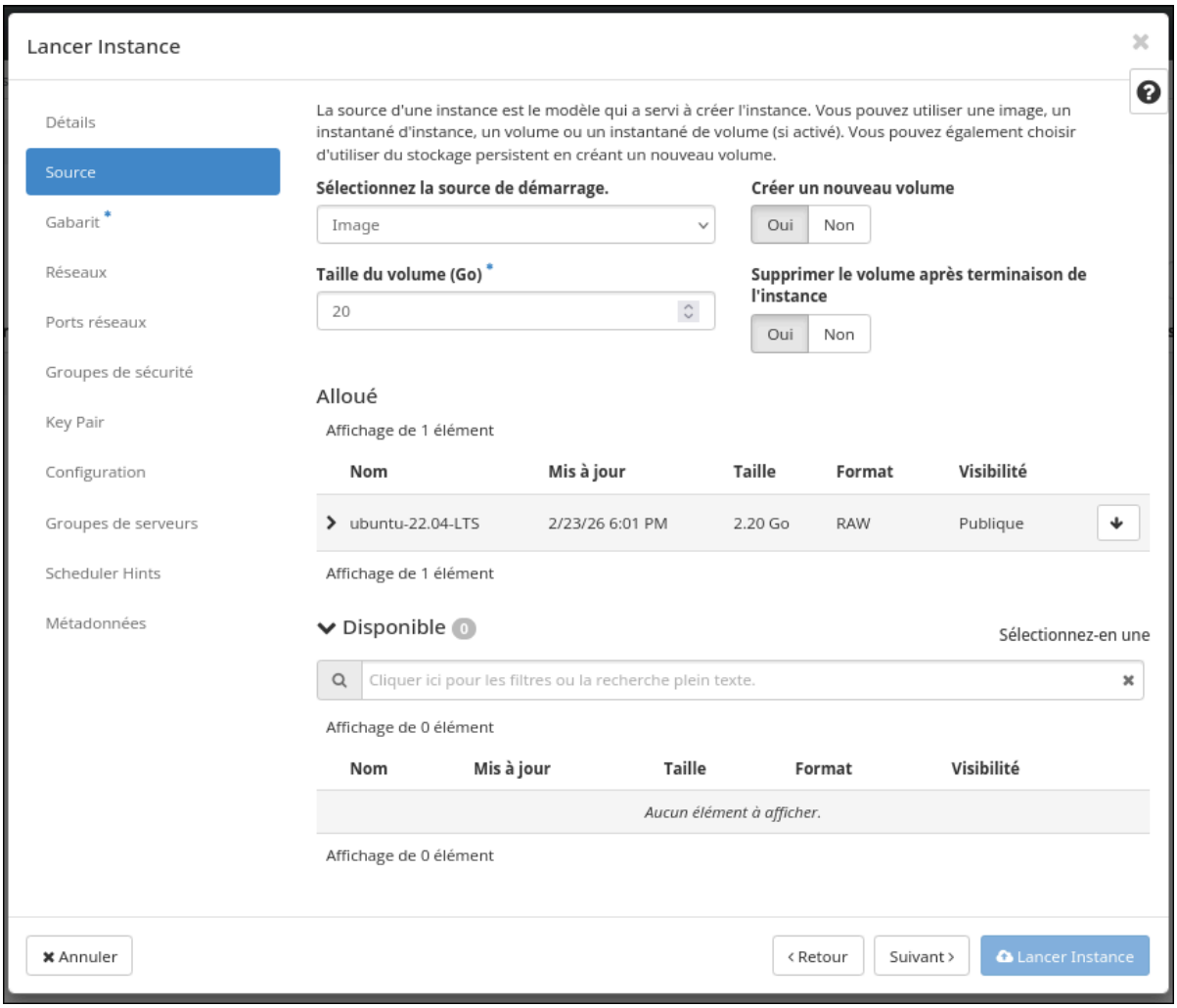
- Dans la vue **Détails**, saisir un nom d'instance.
- Indiquez le service porté dans le champ **Description**.
- Laissez le champ **Zone de disponibilité** à sa valeur par défaut : *Nova*.
- On peut créer une ou plusieurs instances en même temps : indiquez le nombre d'instances souhaitées dans le champ **Nombre**.



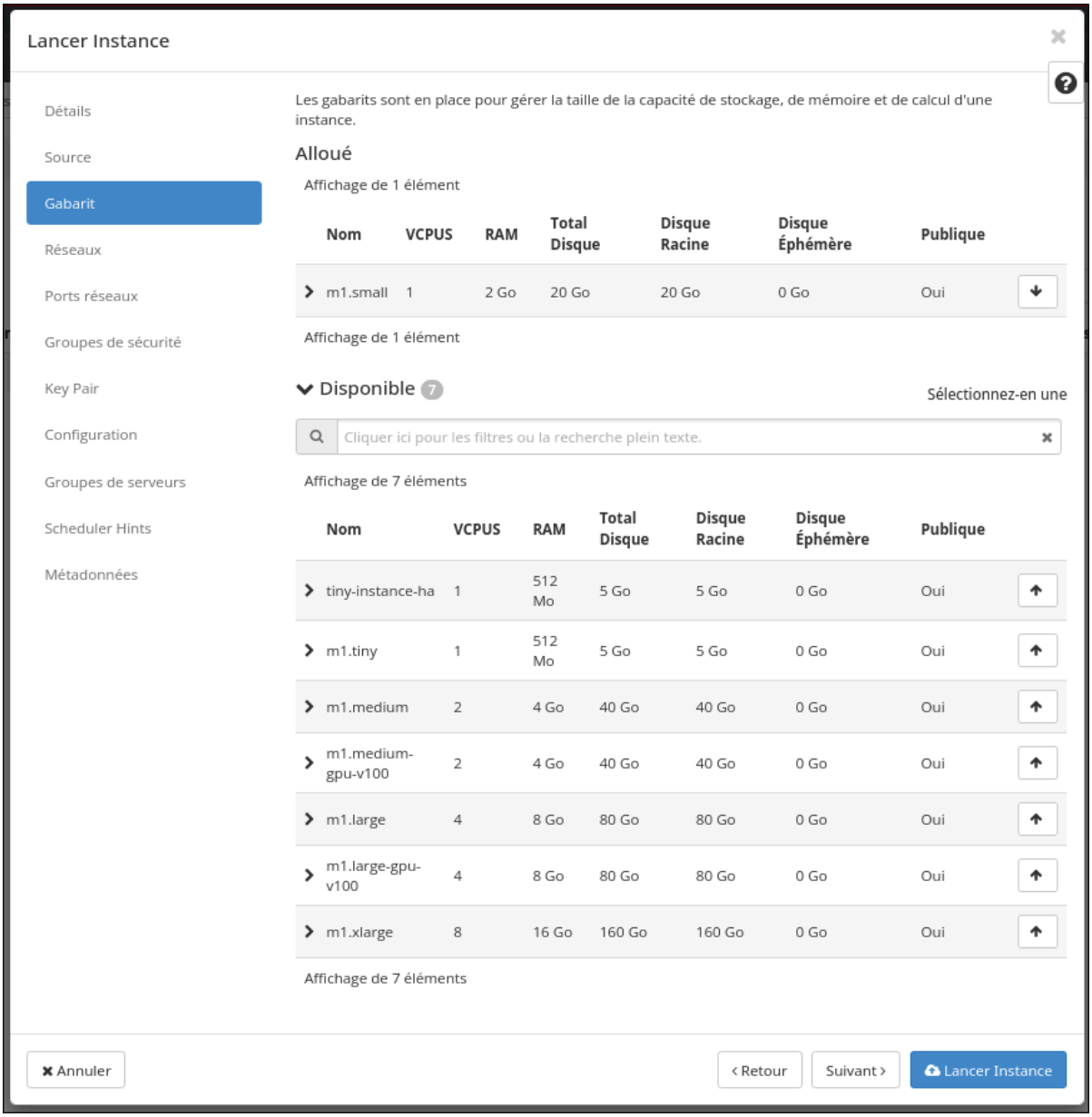
- Dans la vue **Source**, laisser les paramètres par défaut, **Create New Volume** à *Yes* et **Delete Volume on Instance Delete** à *No*

> **Attention**
>
> A la suppression de l'instance, son volume ne sera pas supprimé automatiquement, il faudra le supprimer manuellement

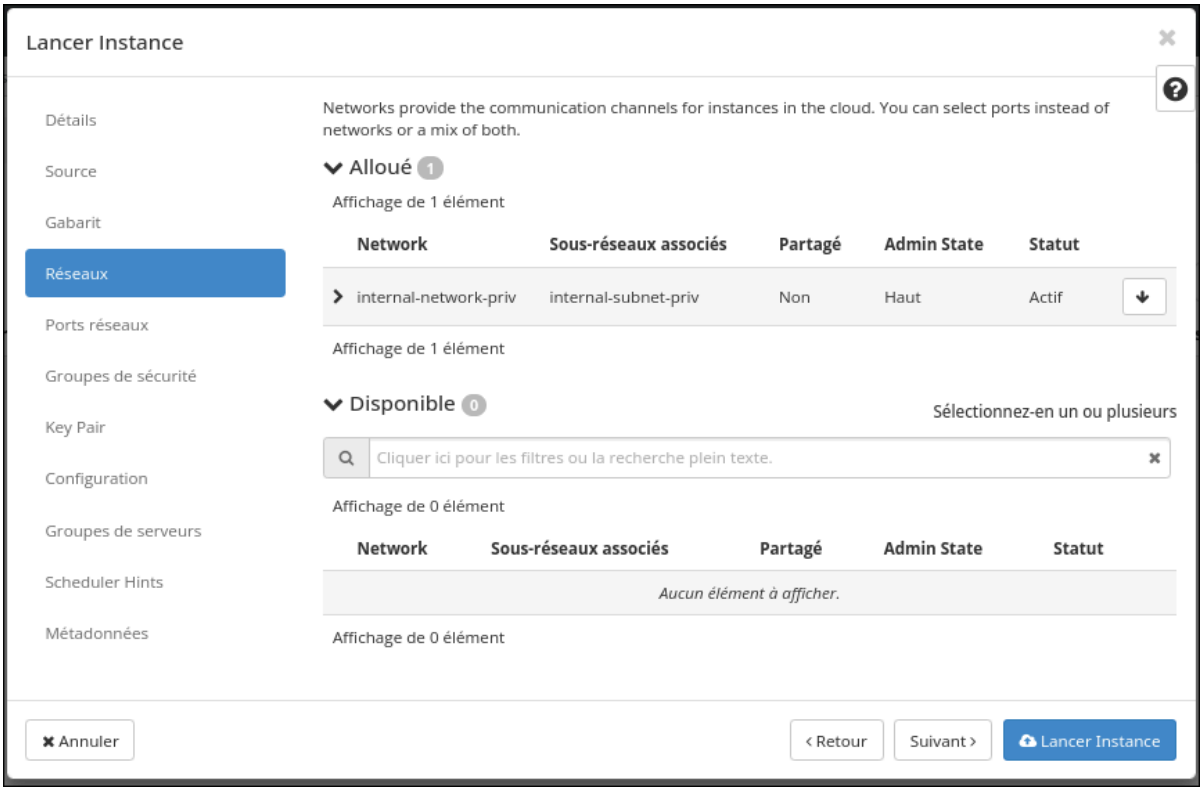
- Choisir de booter depuis une image (champ **Select Boot Source**), puis sélectionner l'image système à instancier en cliquant sur la flèche de la ligne correspondante (à droite), pour le faire monter dans la section **Allocated**. Cela positionne aussi une taille pour le volume (cette valeur peut être modifiée).



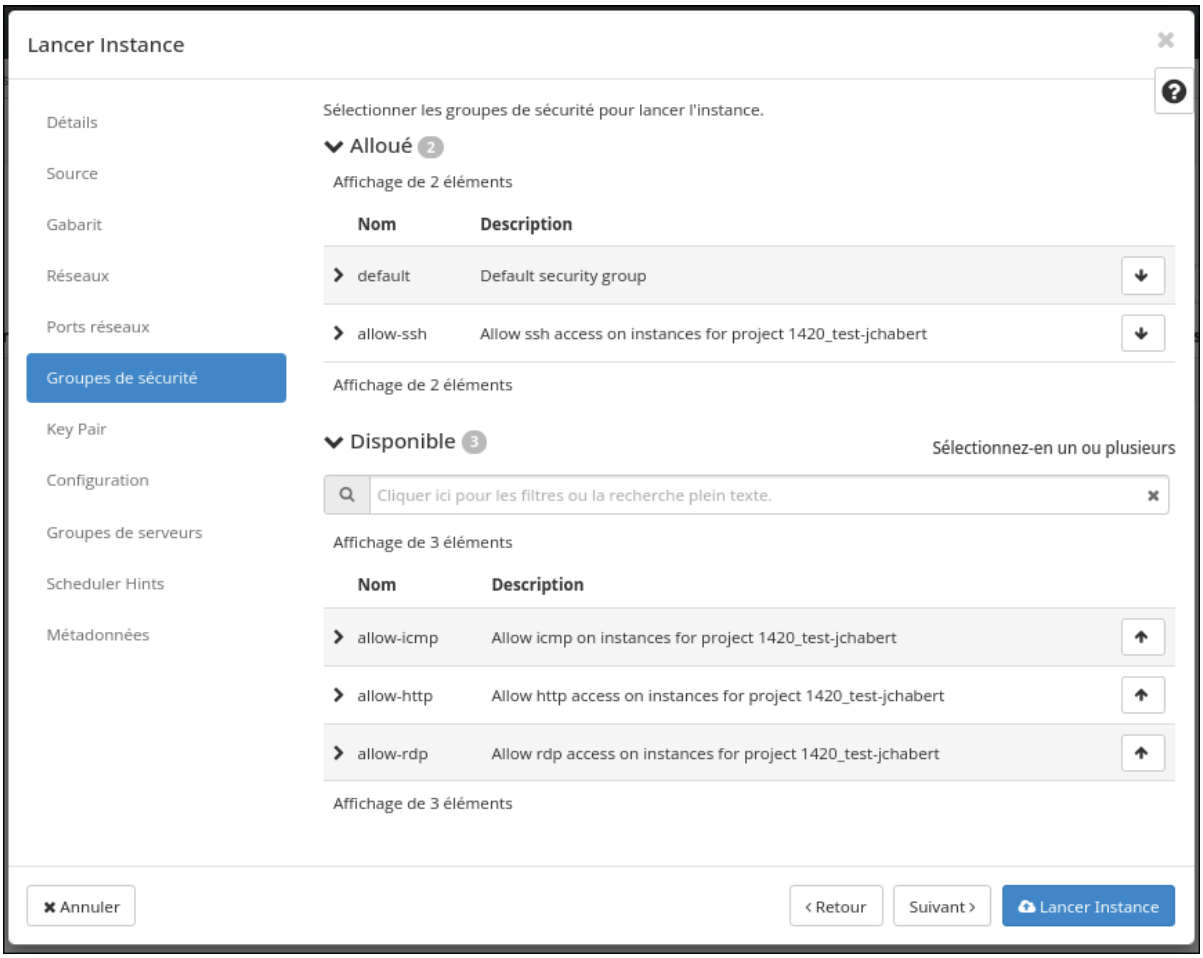
- Dans la vue **Gabarit** (Flavor), choisir un des gabarits proposés en cliquant sur la flèche de la ligne correspondante, pour le faire monter dans la section **Alloué**.



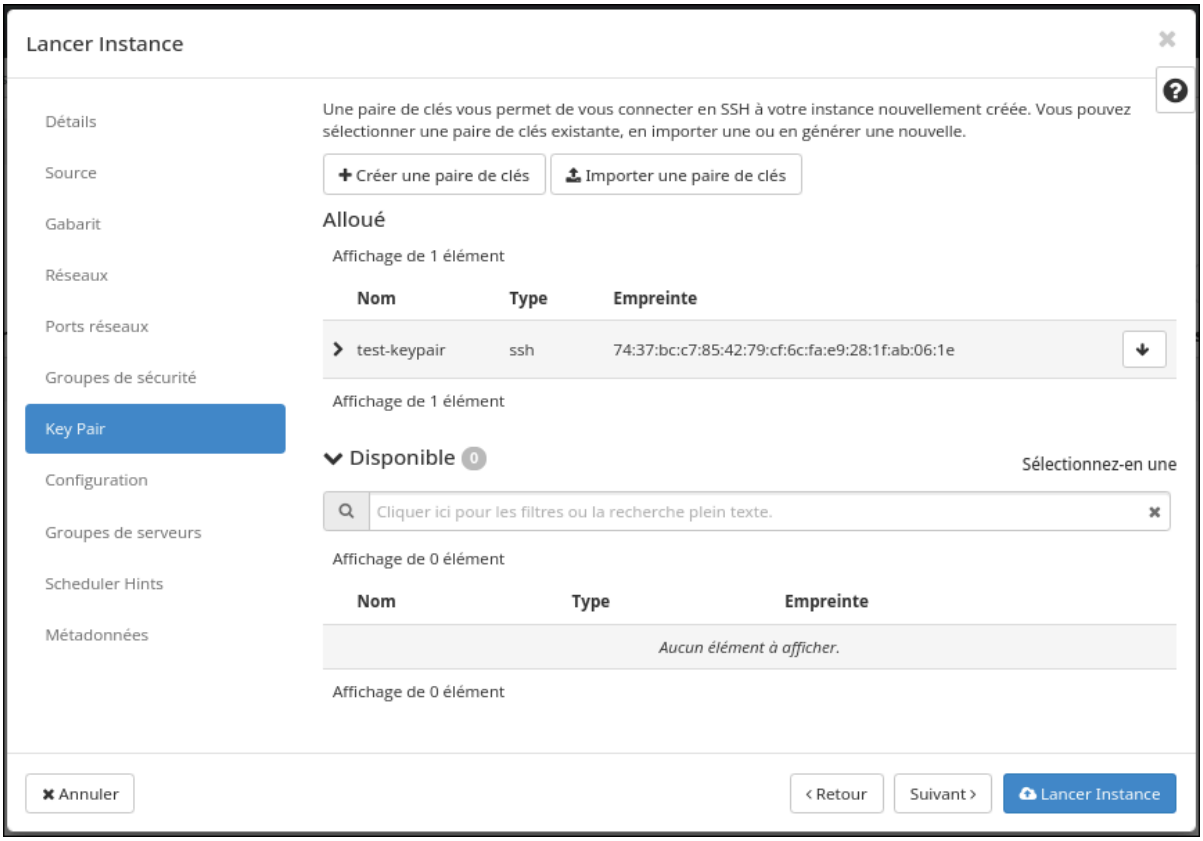
- Dans la vue **Réseaux**, choisir le réseau interne qui a été crée par défaut sur votre projet. Pour le rattacher à votre instance, cliquer sur la flèche de la ligne correspondante, pour le faire monter dans la section **Alloué**.



- On ne modifie pas les vues **Ports réseaux**
- Dans la vue **Groupe de sécurités**, vous pouvez voir les groupes de sécurité crées par default. Choisissez le group **allow_ssh** dans la liste pour autoriser les connexions SSH sur votre instance, et laisser le groupe **default**

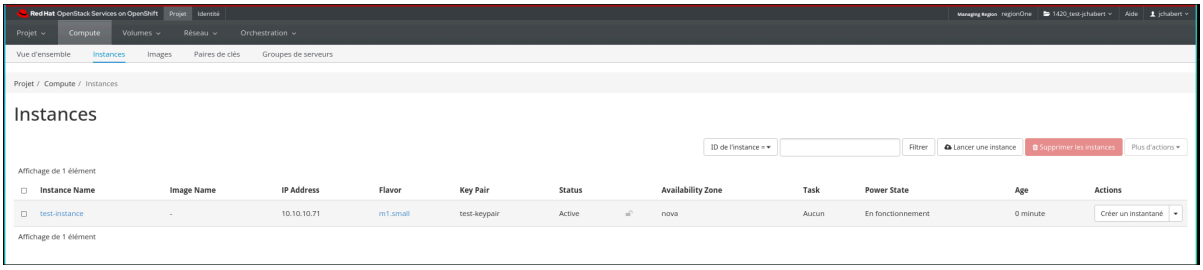


- Dans la vue **Key Pair**, vous pourrez choisir la clé publique crée précédemment en la sélectionnant (avec la flèche) pour qu'elle soit injectée dans la instance créée.



- Les vues suivantes peuvent être passées. Enfin cliquer sur le bouton **Lancer Instance**.

Une fois la tâche terminé, la machine peut alors démarrée :

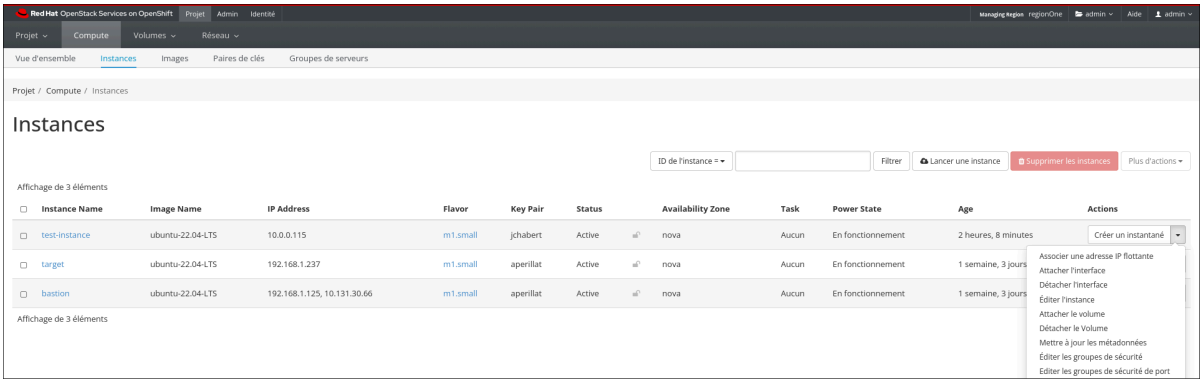


Ajout d'une ip flottante

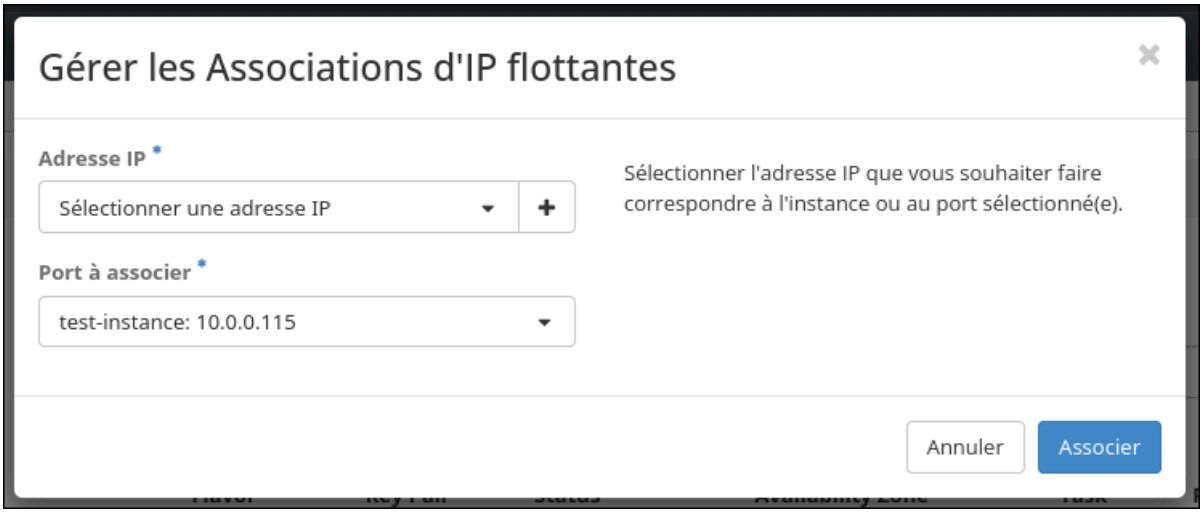
Une fois l'instance créée et démarrée pour pouvoir la rendre accessible il faut lui attribuer une ip flottante ou floating ips. Cette ip sera prise dans le pool d'adresses ip relative à la zone d'exposition, soit privée soit publique

> **Rappel**
>
> Un projet possède l'un des deux réseaux d'ip flottantes appelées external_priv et external_pub en fonction de ce qui a été choisi lors de sa création :
>
> - extenal_priv est une zone uniquement accessible depuis les sites INRAE et/ou au travers du VPN
> - external_pub est accessible à partir de tout internet ! Porter une attention particulière à définir des mots de passe robustes (SSH est ouvert à tout le monde)

Pour ajoutez une floating ip, placez vous dans la section **Projet** en haut a gauche, puis dans l'onglet **Compute** et enfin, cliquez sur **Instances**, ensuite cliquez sur le menu déroulant tout à droite de la ligne de votre instance, dans le menu sélectionnez **Associer une adresse ip flottante**

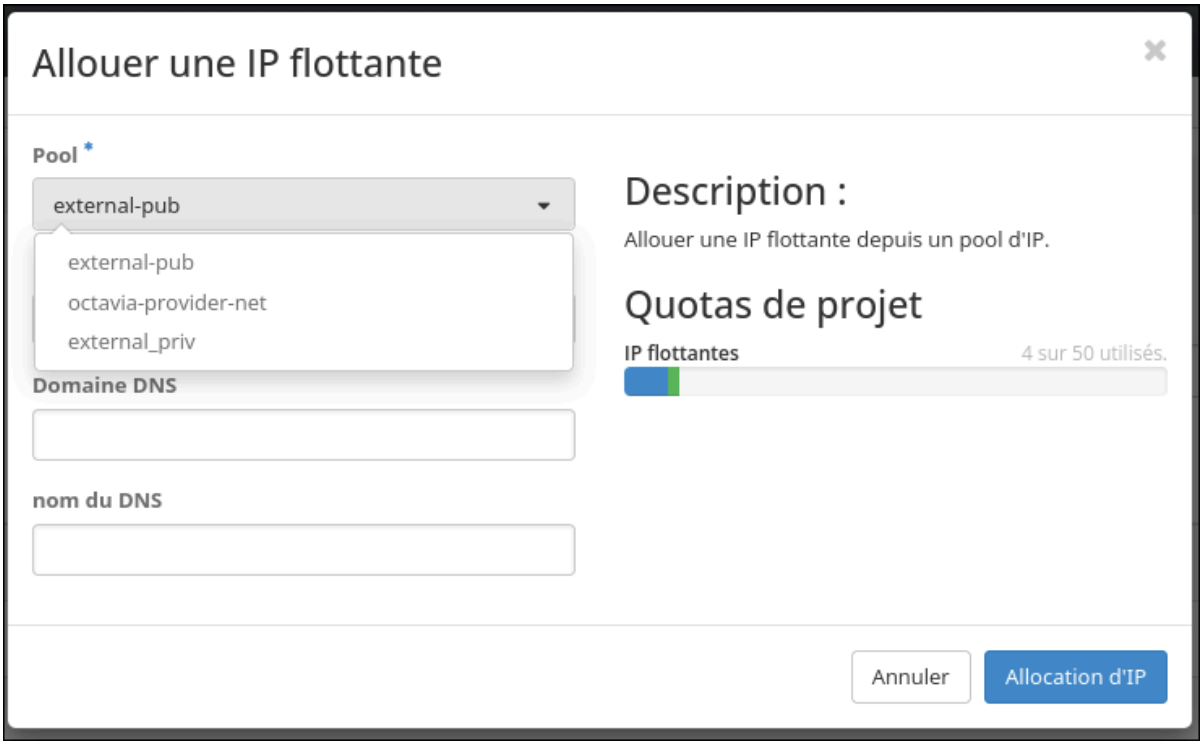


Une fenêtre s'ouvre et laisse le choix via une liste déroulante de choisir des ips flottantes précédemment utilisées ou en appuyant sur bouton **+** pour demander une nouvelle ip flottante.



Vous aurez le choix entre les deux réseaux d'ip flottantes, il faut faire attention de bien choisir celle qui correspond à la zone de sécurité sur laquelle est déployée l'instance.

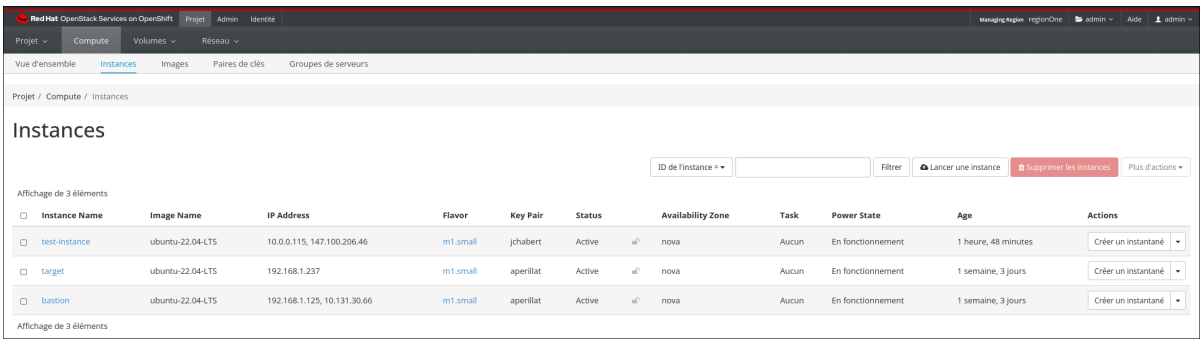
Le champ description peut être complété mais c'est facultatif et il suffit de cliquer sur **Allocation d'IP**



La prochaine fenêtre, montre l'ip flottante liée à l'ip privée de l'instance pour valider cette configuration il suffit de cliquer sur le bouton **Associer**



Lorsque l'adresse ip est associée à l'instance vous le verrez dans la vue des instances.



Accès à l'instance via SSH

Votre instance est maintenant déployée et accessible, pour vous y connecter en SSH, il fous faudra utiliser la commande suivante :

```
$> ssh -i <keypair_clef_prive> <login>@<floating_ip>
```

- keypair_clef_prive : Clef privée qui correspond à la clef publique utilisée lors de la création de l'instance
- login : utilisateur par défaut, qui depend de la distribution choisie - vous pourrez trouver cette information ici
- floating_ip : Ip flottante attachée à la machine

Dans notre exemple, on aura donc :

```
$> ssh -i Téléchargements/test-keypair.pem ubuntu@10.131.49.210
The authenticity of host '10.131.49.210 (10.131.49.210)' can't be
established.
ED25519 key fingerprint is:
SHA256:C7Fr16gjkVWPNeGnSu7WidkEnQp7qWRvQlWtqqy5oeU
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.131.49.210' (ED25519) to the list of known
hosts.
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-164-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed Mar 25 09:42:48 UTC 2026

  System load:  0.02              Processes:               122
  Usage of /:   8.2% of 19.20GB   Users logged in:         0
  Memory usage: 10%               IPv4 address for enp3s0: 10.10.10.71
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check
your Internet connection or proxy settings


Last login: Wed Mar 25 09:40:52 2026 from 147.100.186.79
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@test-instance:~$
```