Service Openstack Cloud de la DSI INRAE

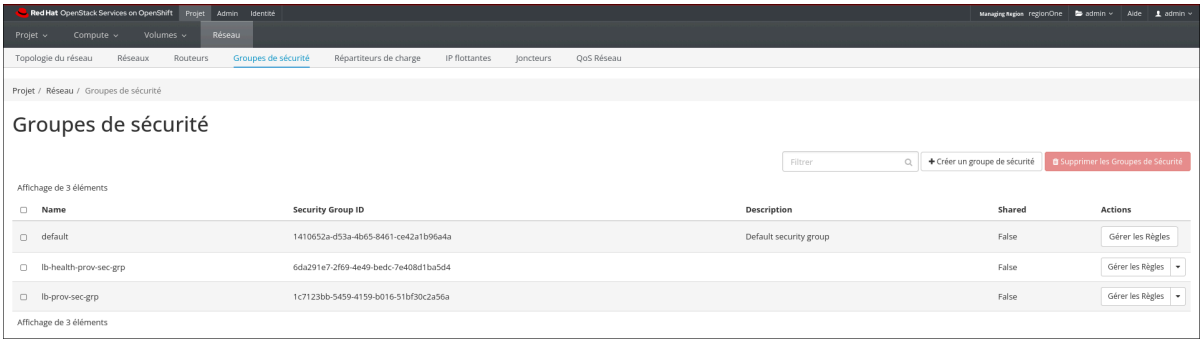
Version 0.0.1

Gérer les groupes de sécurités

⚠ 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/

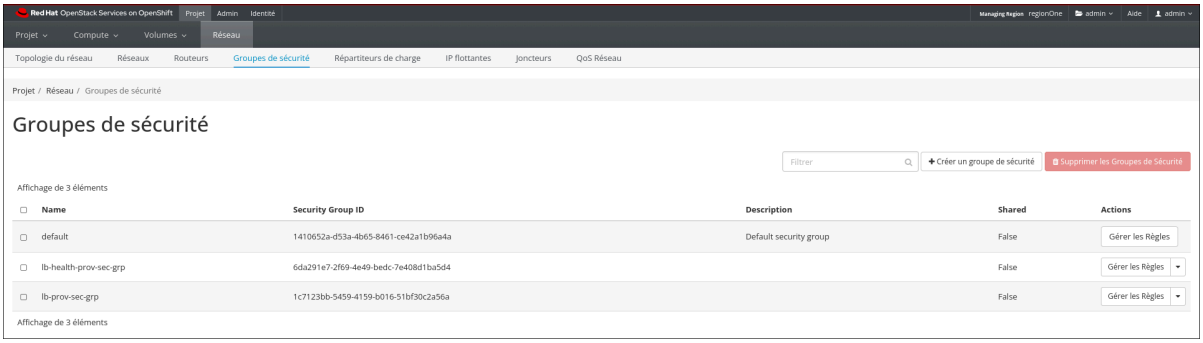
Gestion des security group

Pour gérer les groupes de sécurités, placer vous dans la section **Projet** en haut à gauche, puis dans l'onglet **Réseau** et enfin, cliquer sur **Groupes de sécurité**.

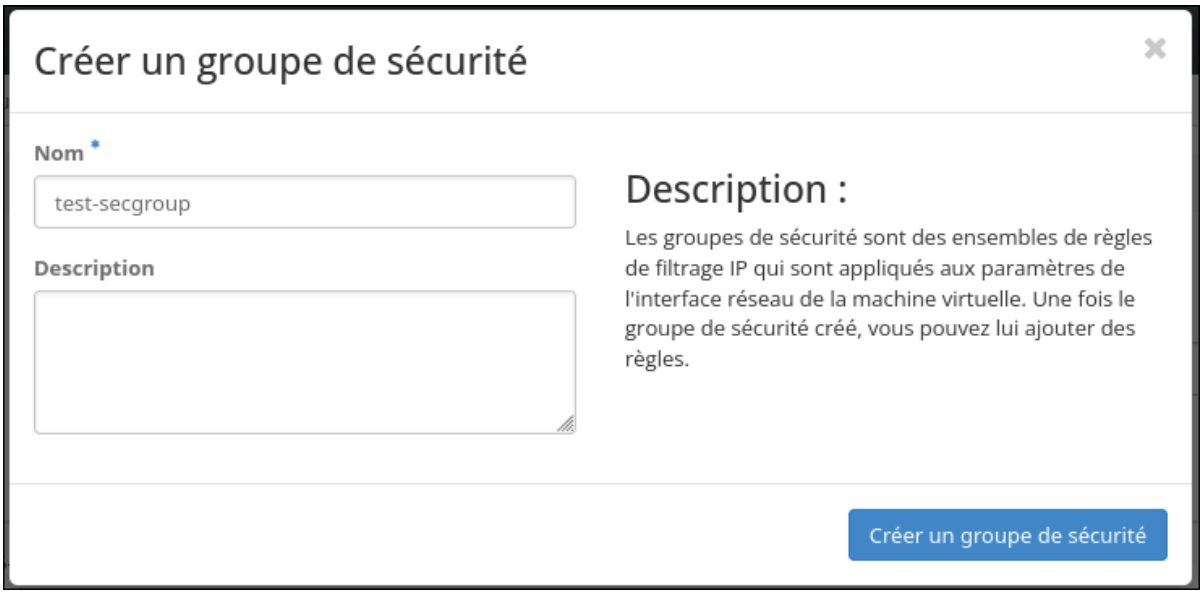


Creation d'un security group

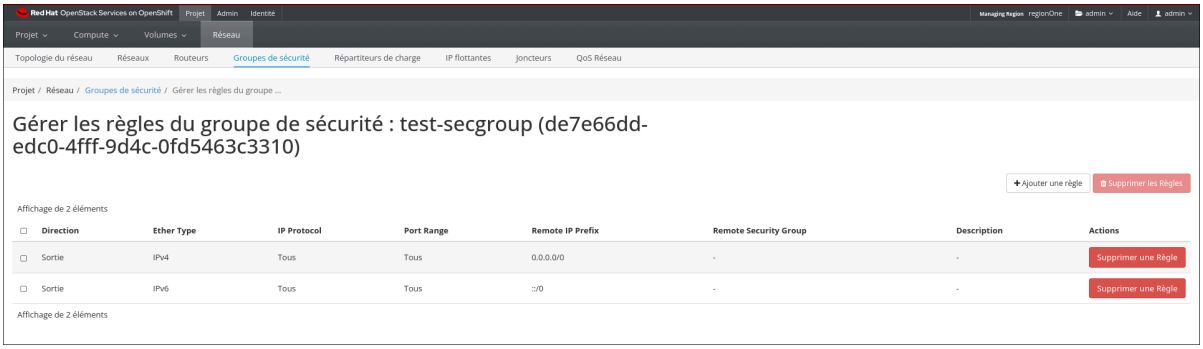
Pour la création de groupe de sécurité, choisir **Créer un groupe de sécurité**



Renseigner le nom de votre groupe de sécurité, vous pourrez aussi ajouter une description si vous le souhaiter. Puis cliquer sur **Créer un groupe de sécurité**

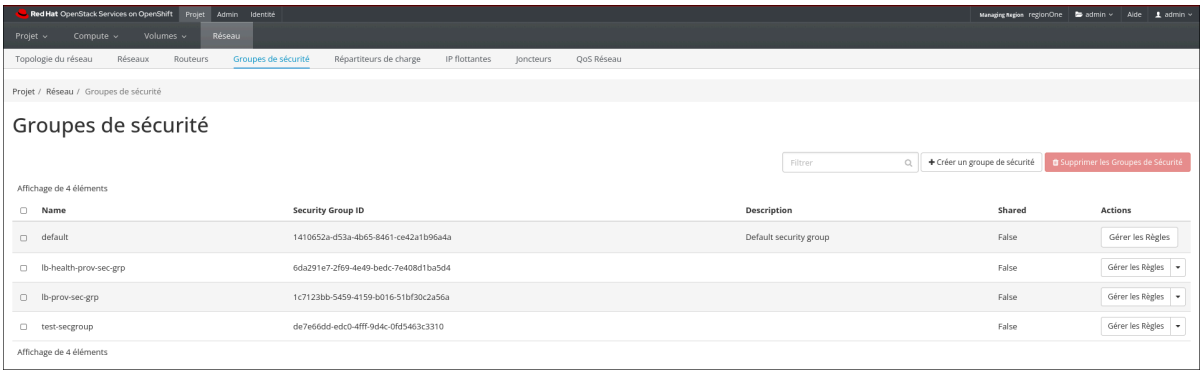


Une fois le groupe de sécurité crée, vous verrez la liste des règles de votre nouveau groupe de sécurité (ces règles sont les règles par défaut)

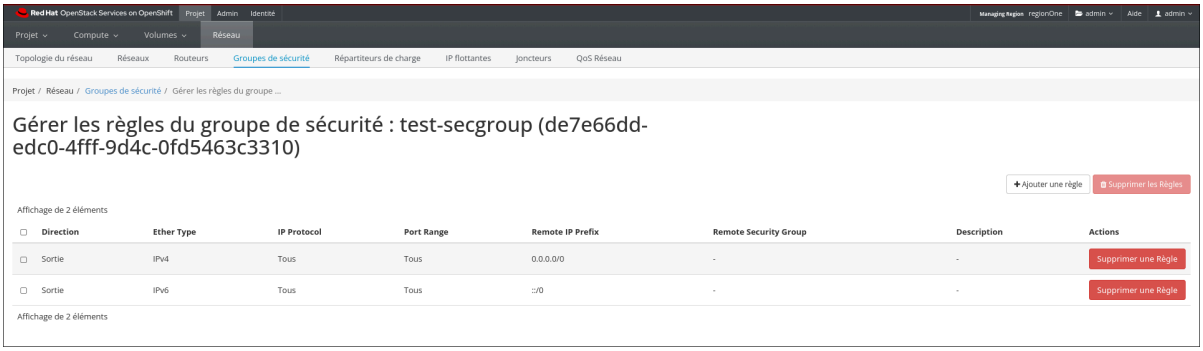


Gestion des regles dans un security group

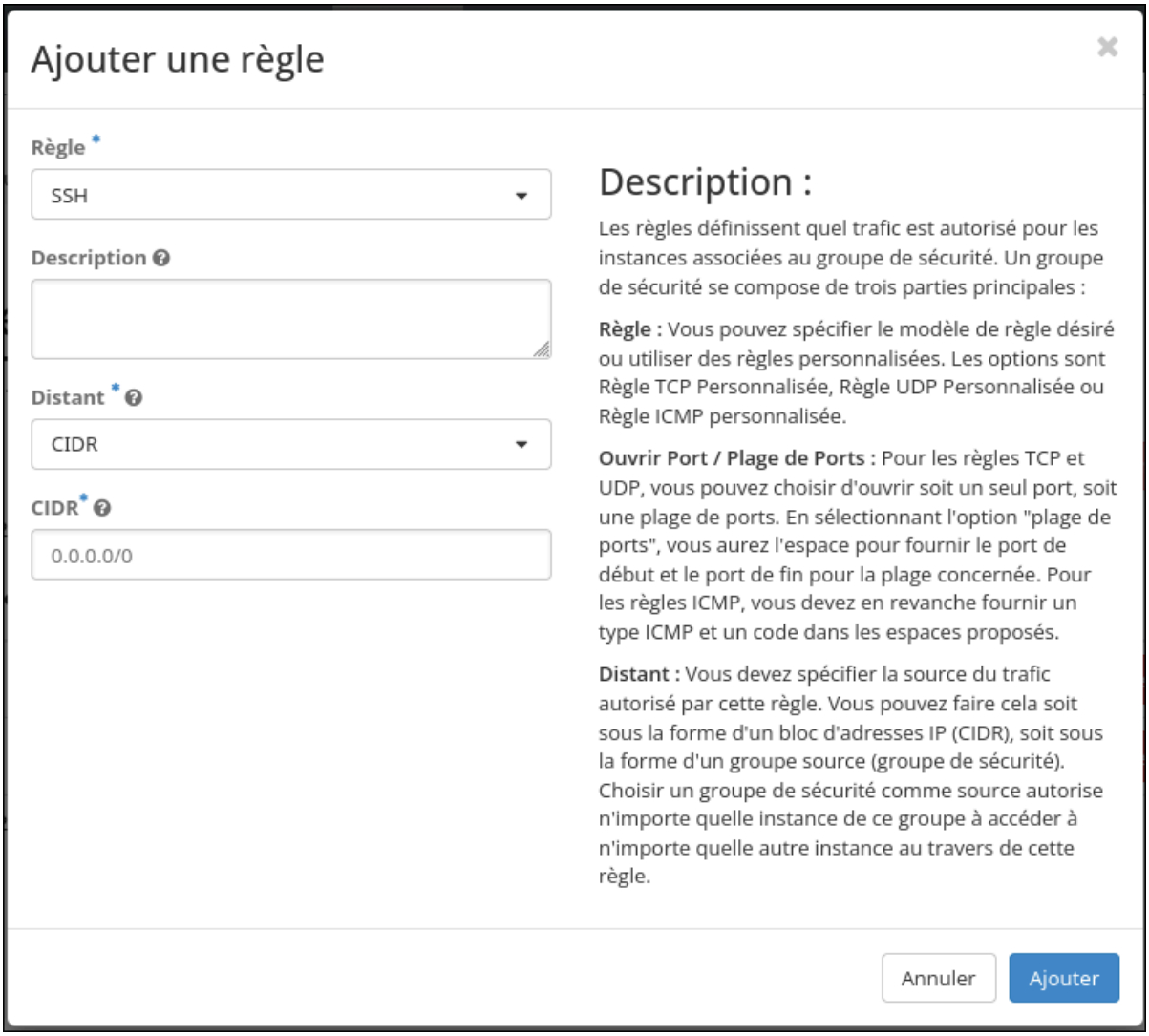
Pour la gestion des règles du groupe de sécurité, choisir **Gérer les règles** tout à droite de la ligne du groupe de sécurité que vous voulez éditer



Depuis cette fenêtre, vous pourrez gérer les règles de sécurité du secgroup. Par exemple, pour ajourer une règle, choisir **Ajouter une règle**



On pourra par exemple créer une règle pour autoriser les connexions SSH aux instances du projet en choisissant le protocol SSH dans le menu déroulant de la fenêtre qui vient de s'ouvrir. Puis choisir **Ajouter**


Ajouter une règle
Règle *
SSH
Description
Distant *
CIDR
CIDR*
0.0.0.0/0
Description :
Les règles définissent quel trafic est autorisé pour les instances associées au groupe de sécurité. Un groupe de sécurité se compose de trois parties principales :
Règle : Vous pouvez spécifier le modèle de règle désiré ou utiliser des règles personnalisées. Les options sont Règle TCP Personnalisée, Règle UDP Personnalisée ou Règle ICMP personnalisée.
Ouvrir Port / Plage de Ports : Pour les règles TCP et UDP, vous pouvez choisir d'ouvrir soit un seul port, soit une plage de ports. En sélectionnant l'option "plage de ports", vous aurez l'espace pour fournir le port de début et le port de fin pour la plage concernée. Pour les règles ICMP, vous devez en revanche fournir un type ICMP et un code dans les espaces proposés.
Distant : Vous devez spécifier la source du trafic autorisé par cette règle. Vous pouvez faire cela soit sous la forme d'un bloc d'adresses IP (CIDR), soit sous la forme d'un groupe source (groupe de sécurité). Choisir un groupe de sécurité comme source autorise n'importe quelle instance de ce groupe à accéder à n'importe quelle autre instance au travers de cette règle.
Annuler
Ajouter