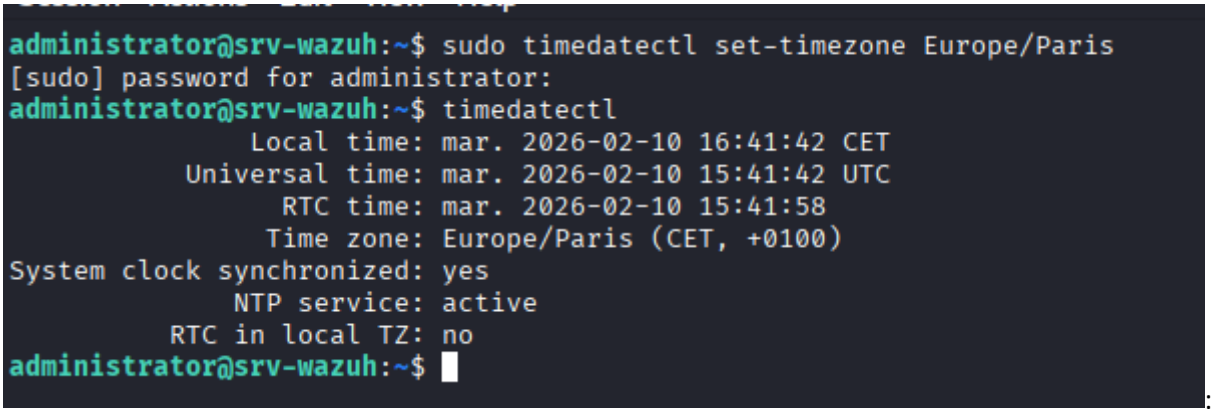
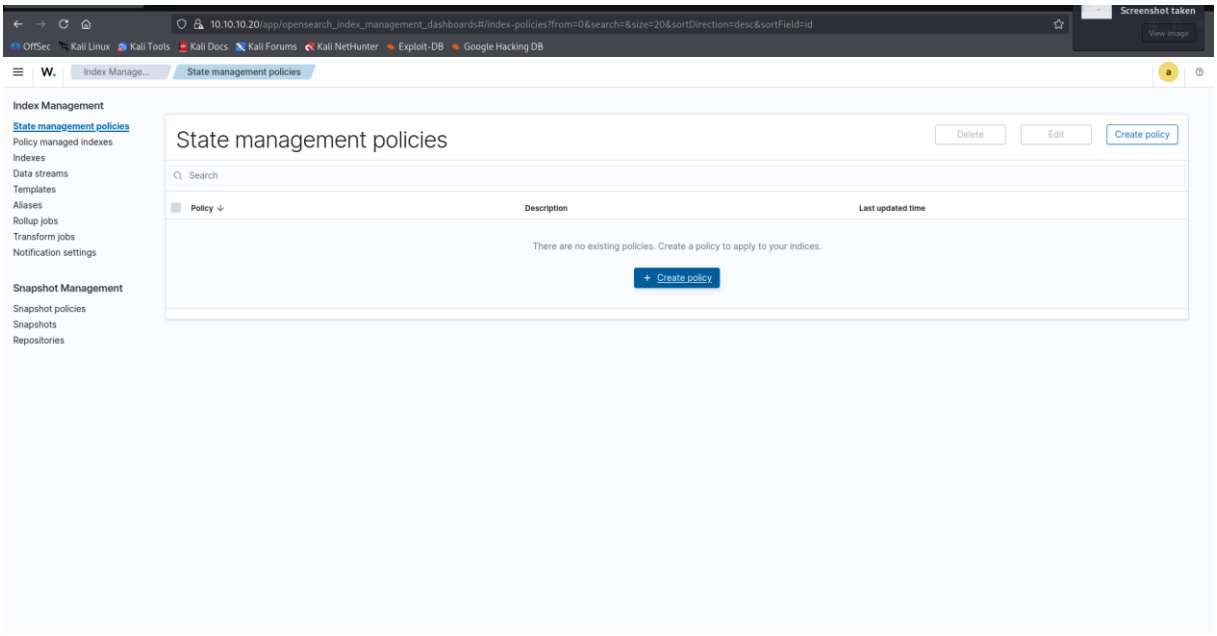
Procédure Configuration de Base Wazuh :

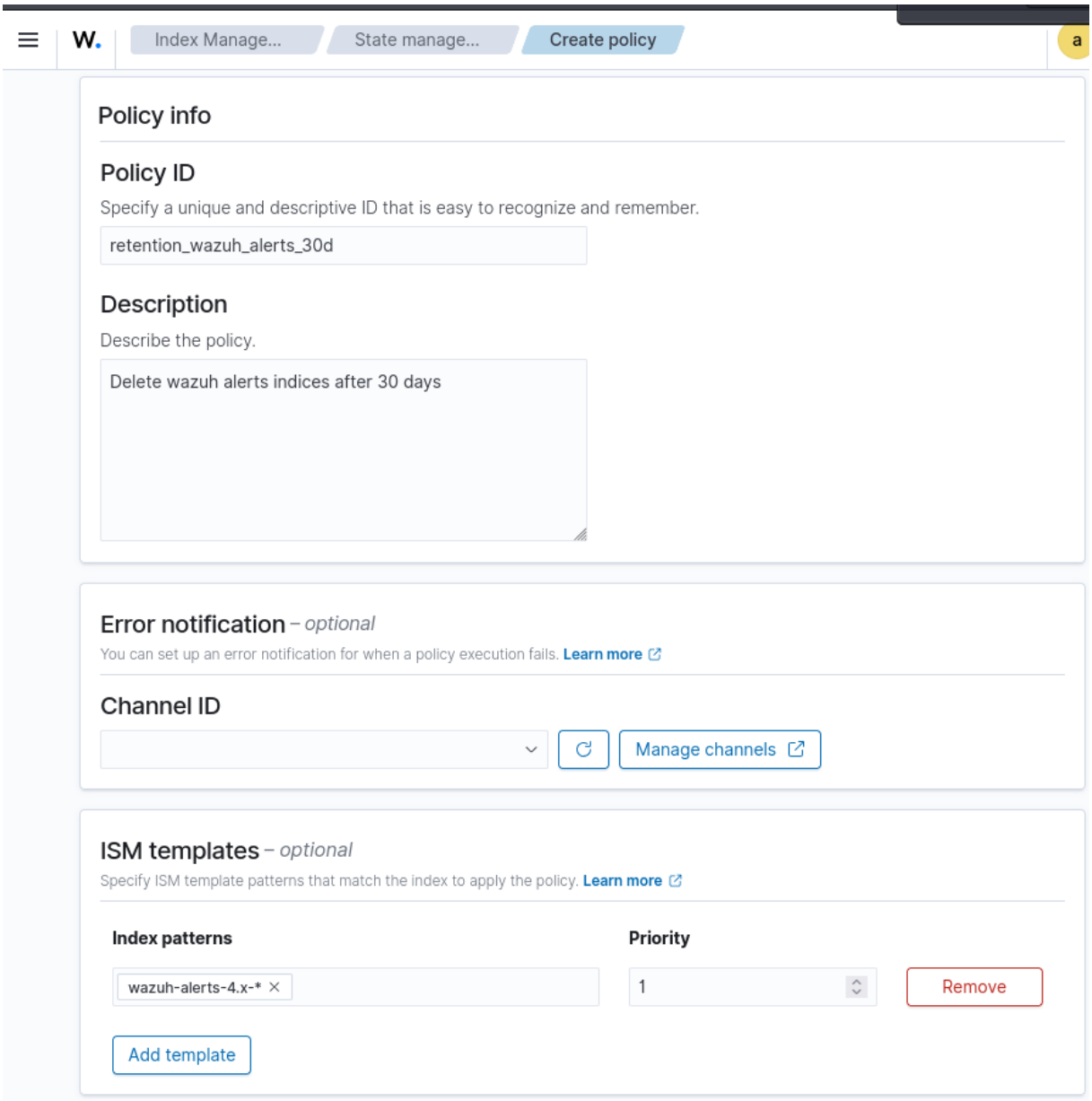
Avant tout on vérifie qu'on n'est la bonne timezone c'est très important pour la corrélation on fait c'est commande « sudo timedatectl set-timezone Europe/Paris » et « timedatectl »



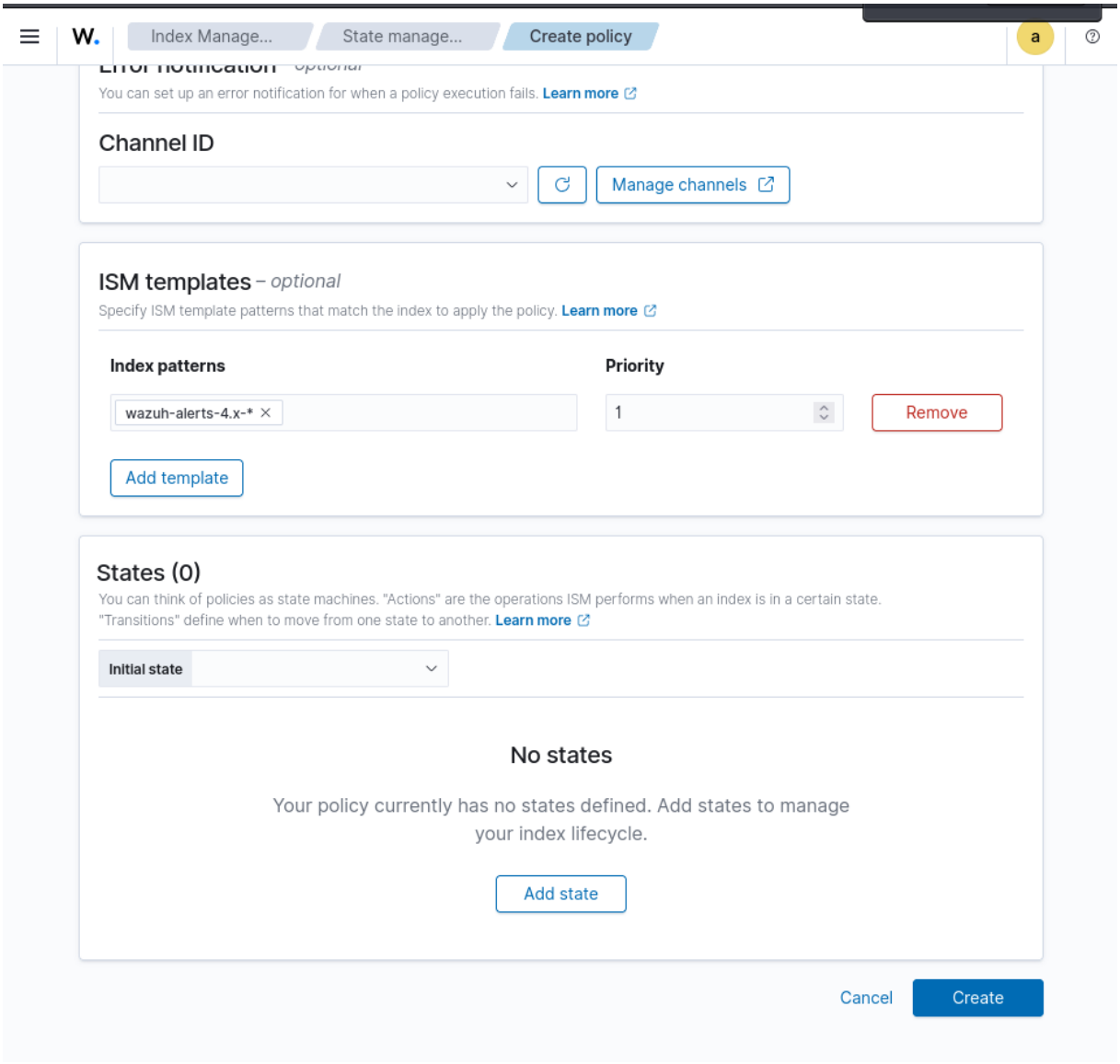
Ensuite on configure la rétention propre (c'est supprimer les logs trop vieux) rdv dans la dashboard wazuh dans Indexer Management → State Management Policies cliquer sur create policies :



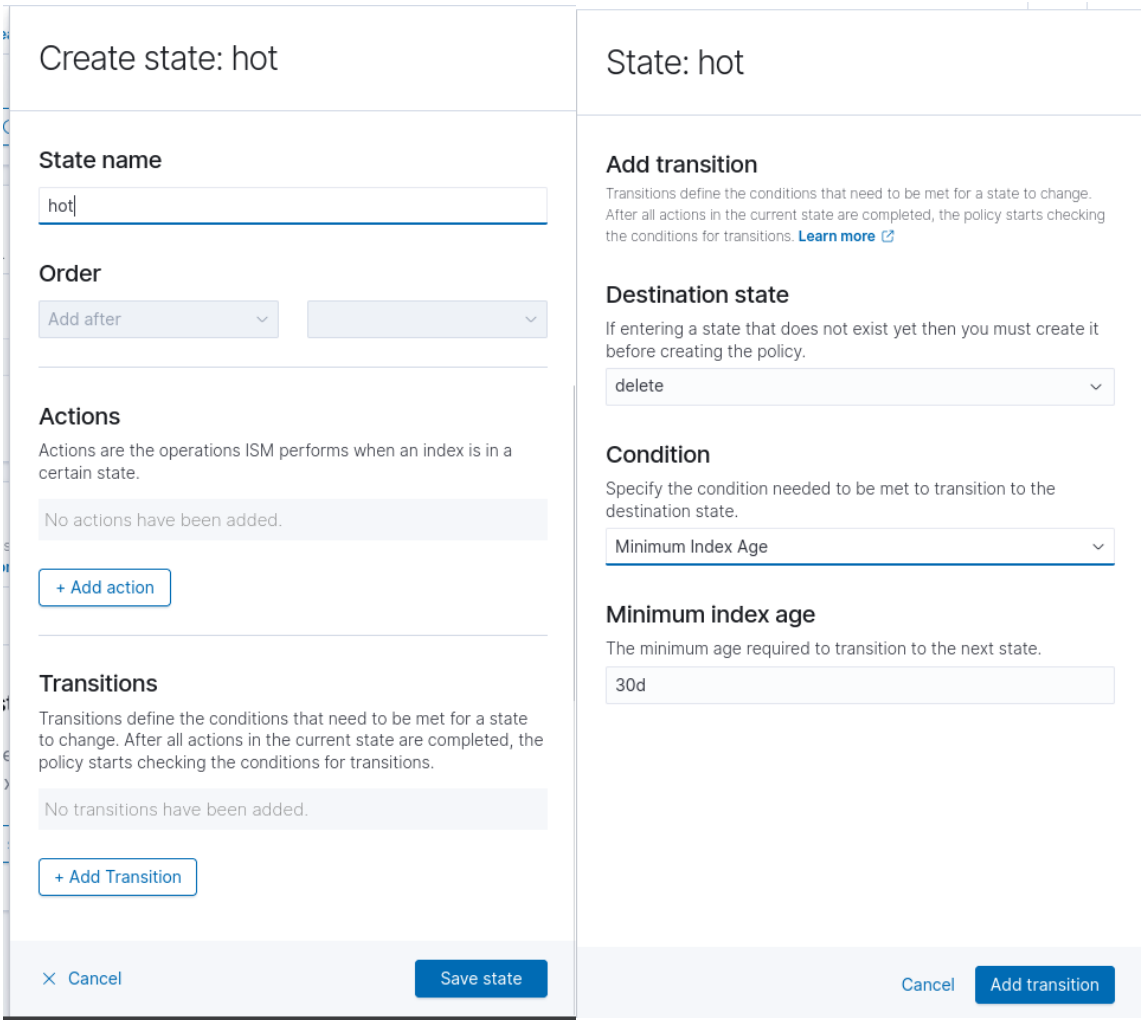
Ensuite vous arriver ici : remplisser les case comme moi :



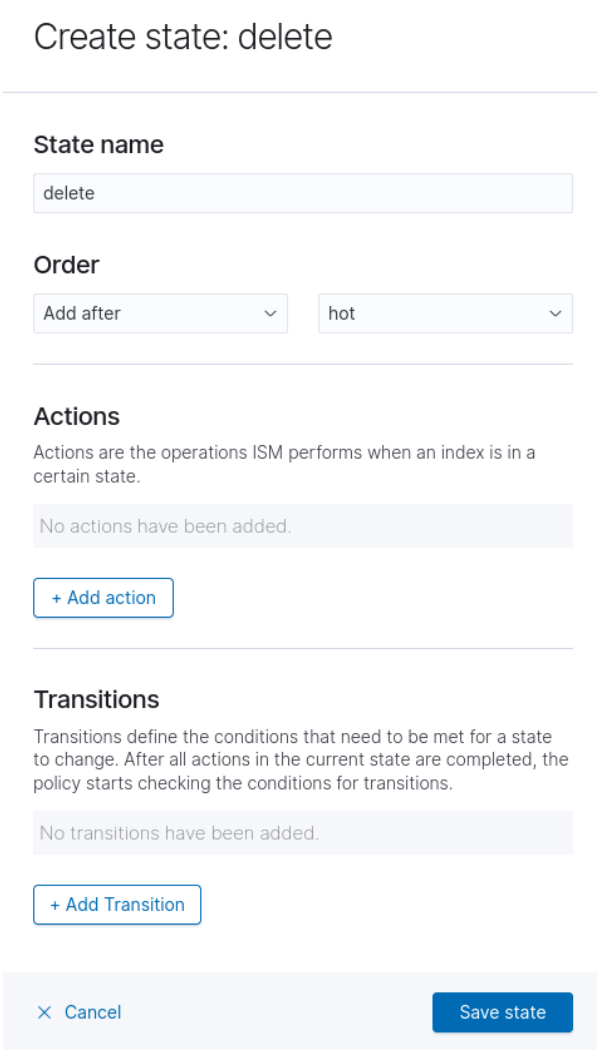
Ensuite cliquer sur Add State tout en bas :

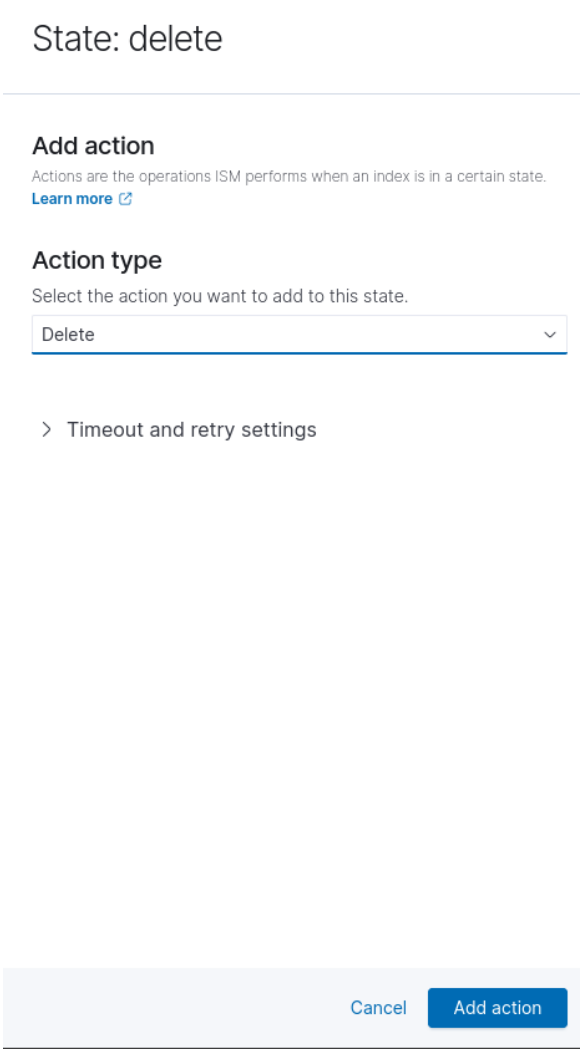

Index Manage...
State manage...
Create policy
a
You can set up an error notification for when a policy execution fails. Learn more
Channel ID
Manage channels
ISM templates – optional
Specify ISM template patterns that match the index to apply the policy. Learn more
Index patterns
Priority
wazuh-alerts-4.x-*
1
Remove
Add template
States (0)
You can think of policies as state machines. "Actions" are the operations ISM performs when an index is in a certain state. "Transitions" define when to move from one state to another. Learn more
Initial state
No states
Your policy currently has no states defined. Add states to manage your index lifecycle.
Add state
Cancel
Create

On lui donne un nom et cliquer sur add transition et remplissez comme ci-dessous (ici on vas supprimer les indexs tous les 30 Jours) et cliquer sur add transiton et add State :

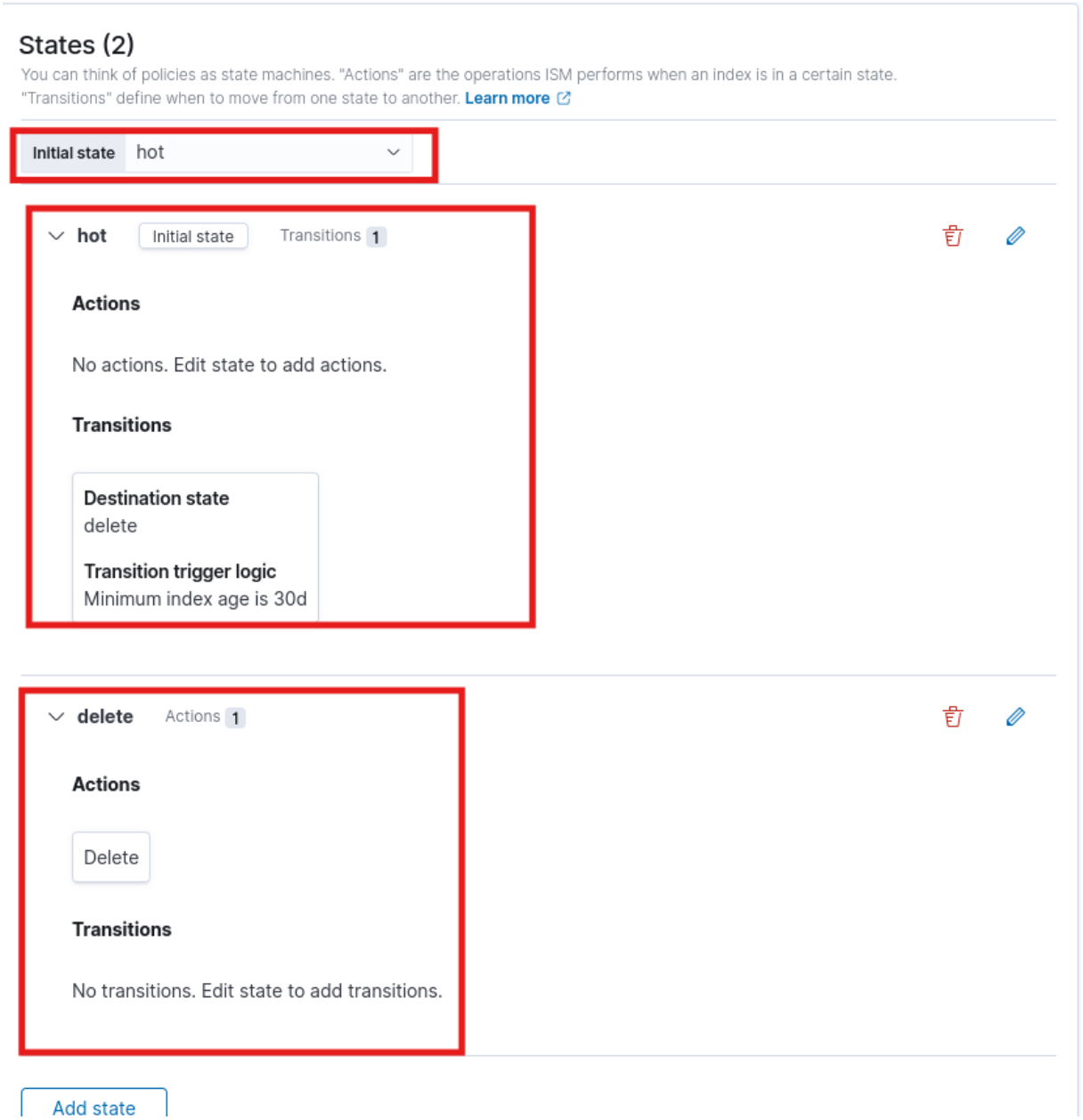


On cree un nouveau State cliquer sur add action et remplissez avec les valeur ci-dessous ensuite fait add action et save state ：

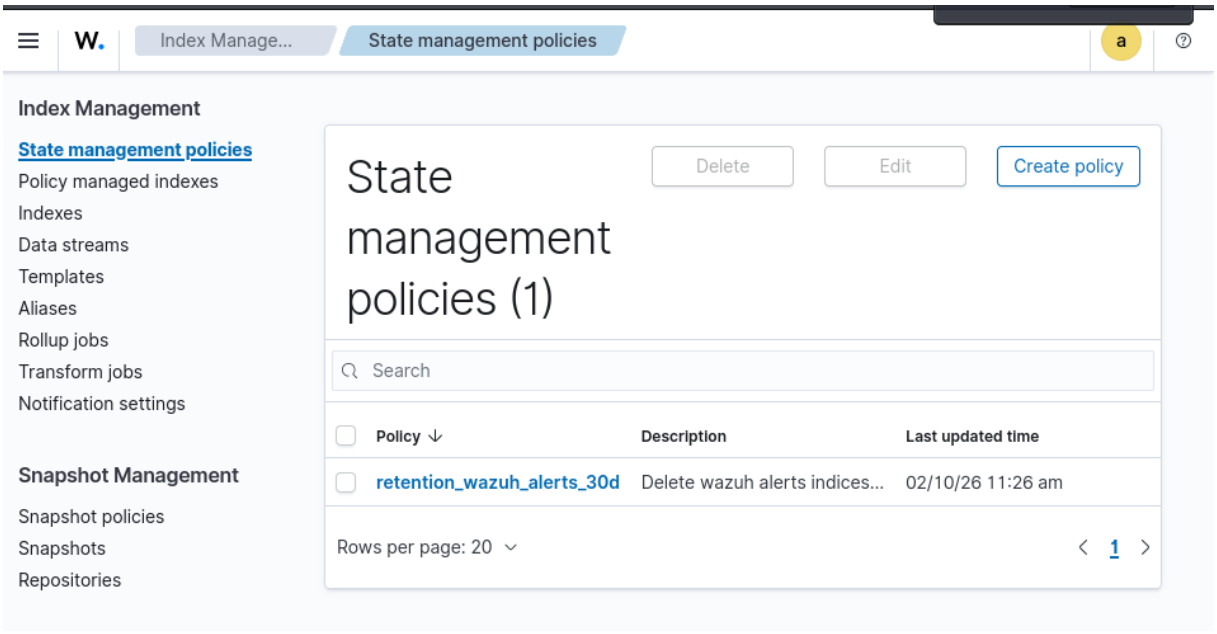




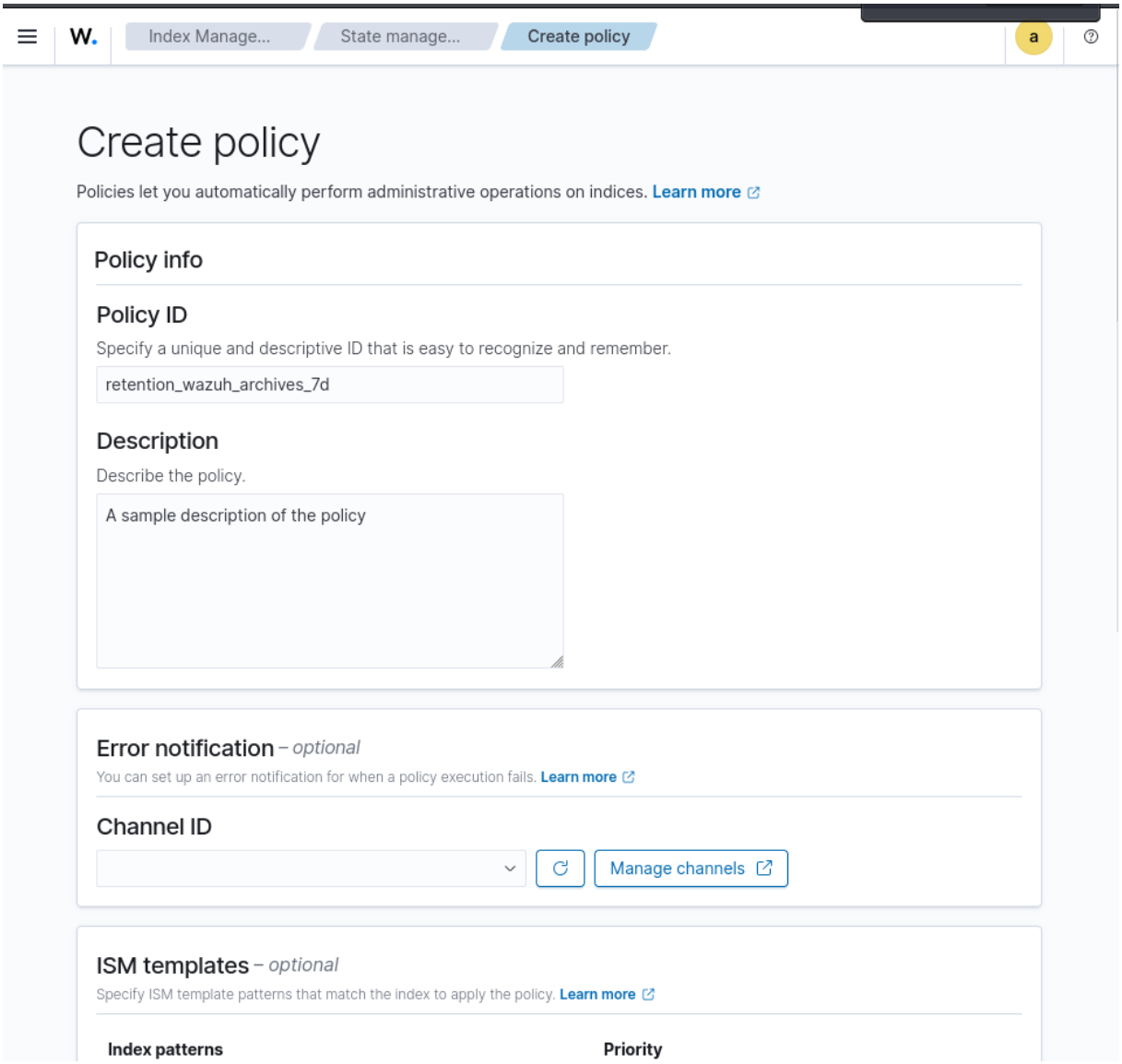
Vous devriez avoir ceci faite ensuite Create :



Si ça réussi wazuh devrait vous emmenez sur cette page :



Maintenant faite la même chose mais pour les archive tous les 7 jours ce sera supprimer voici la conf :



Pour les State voici la conf :

States (2)

You can think of policies as state machines. "Actions" are the operations ISM performs when an index is in a certain state. "Transitions" define when to move from one state to another. Learn more

Initial state: hot

hot

Initial state | Transitions 1

Actions

No actions. Edit state to add actions.

Transitions

Destination state
delete

Transition trigger logic
Minimum index age is 7d

delete

Actions 1

Actions

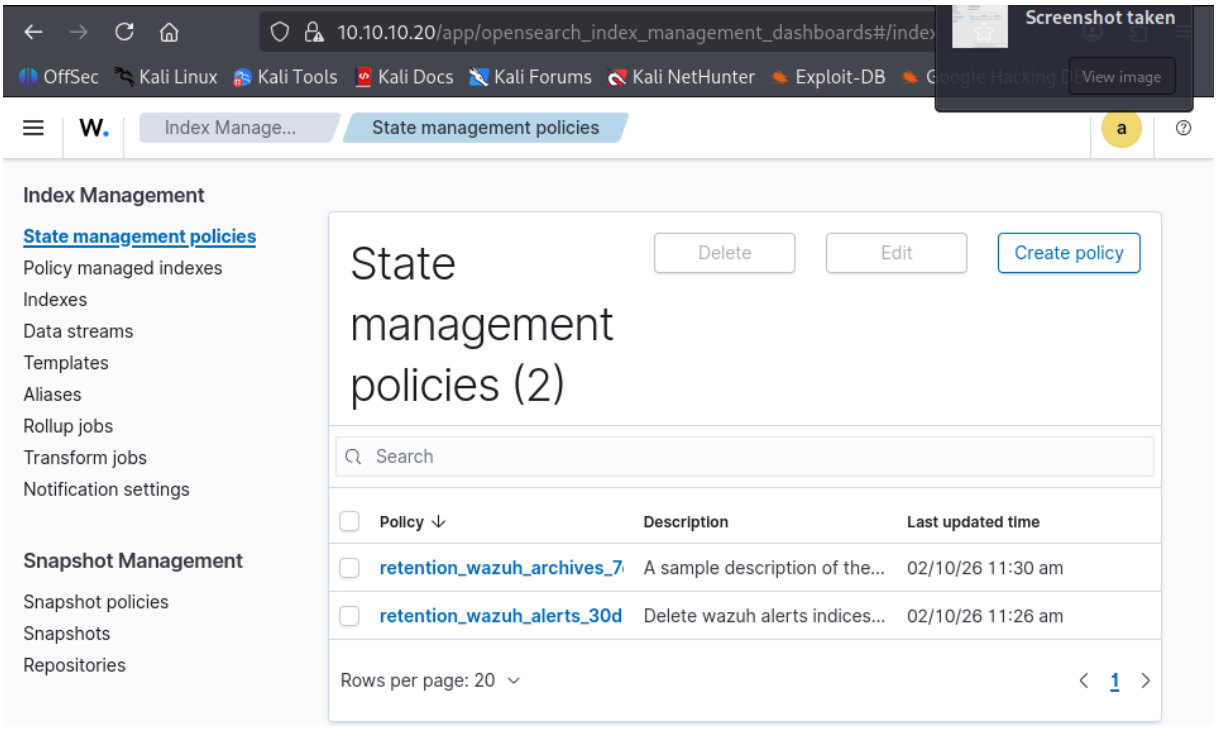
Delete

Transitions

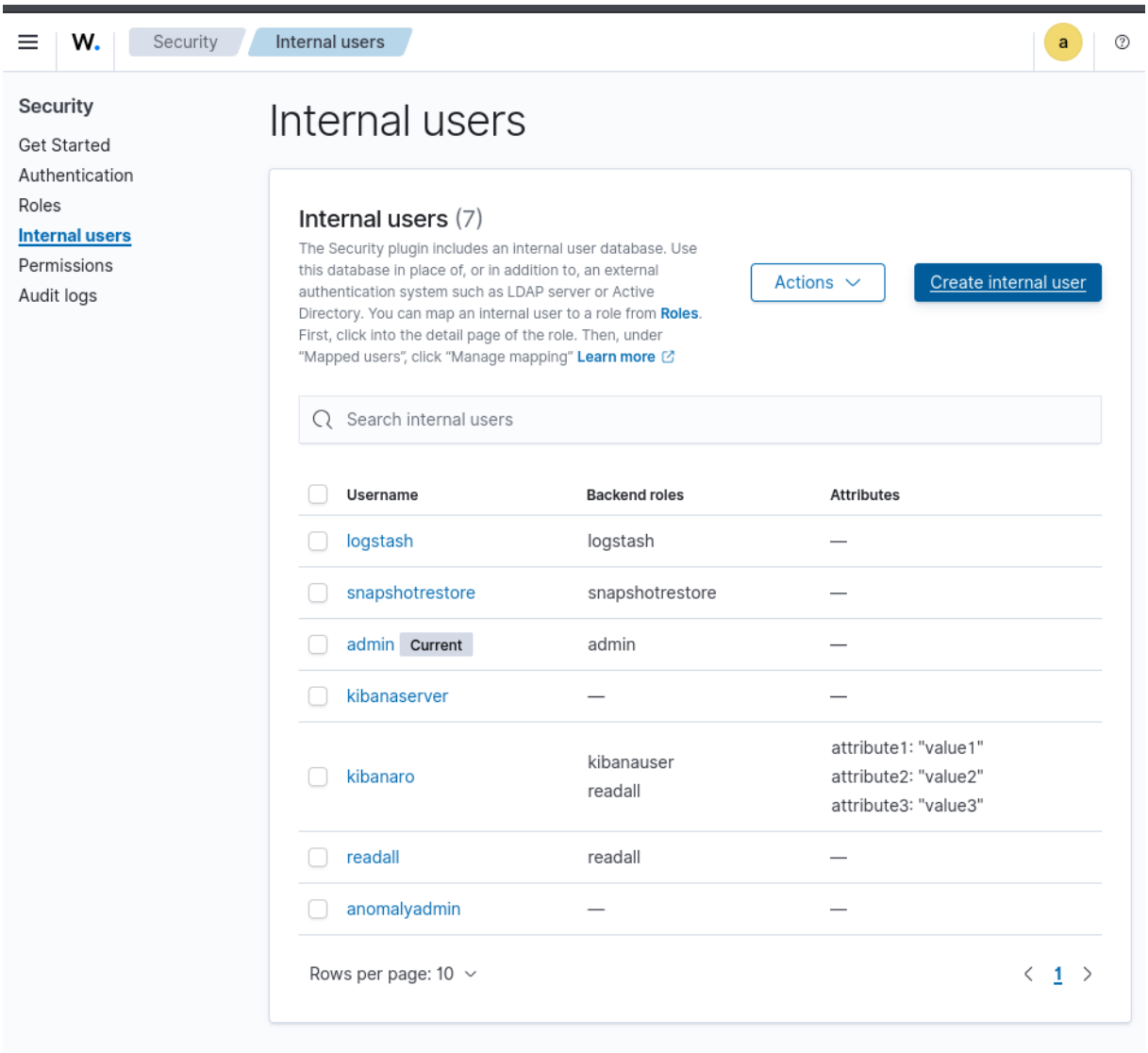
No transitions. Edit state to add transitions.

Add state

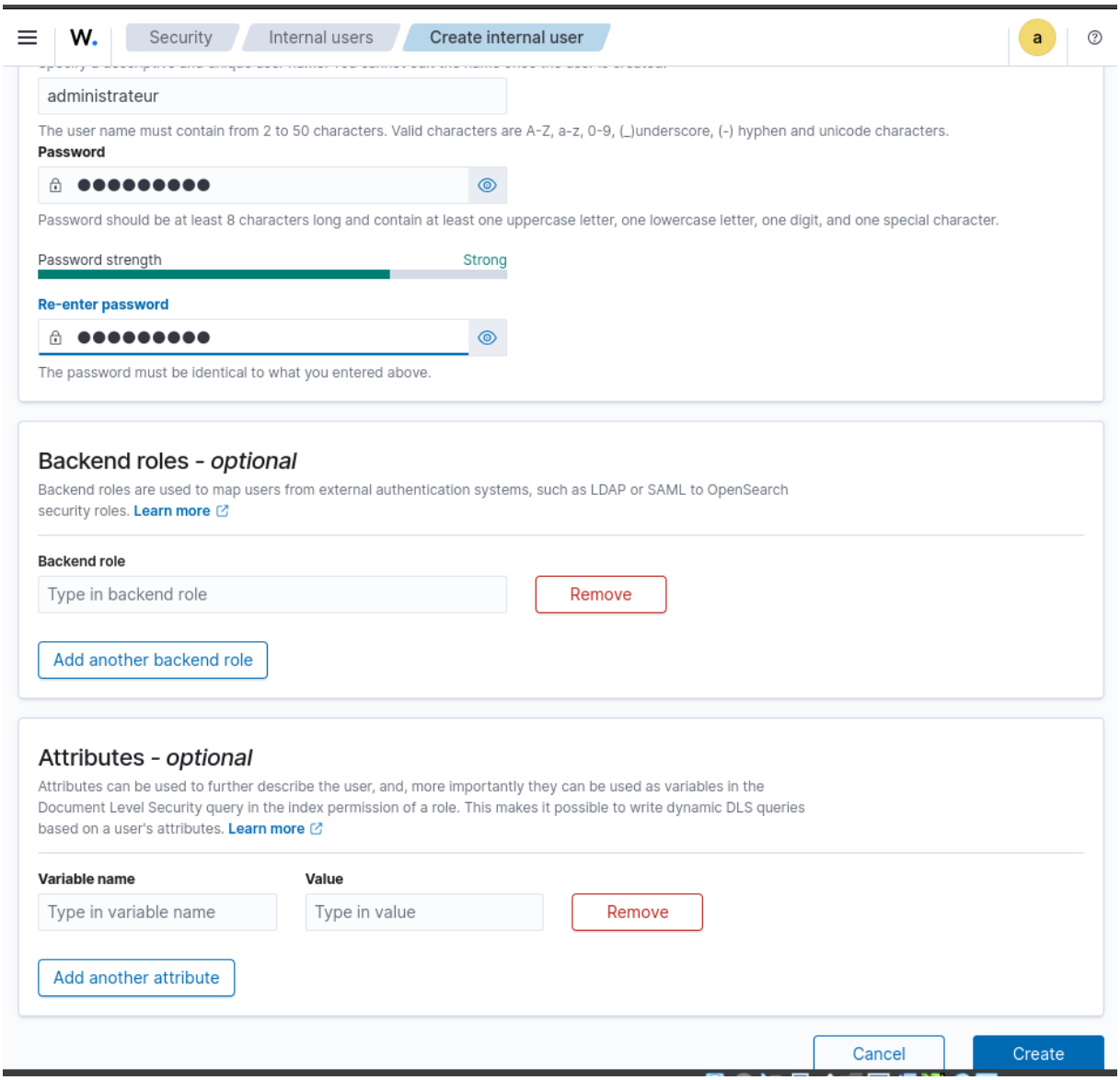
Vous devriez avoir cette conf :



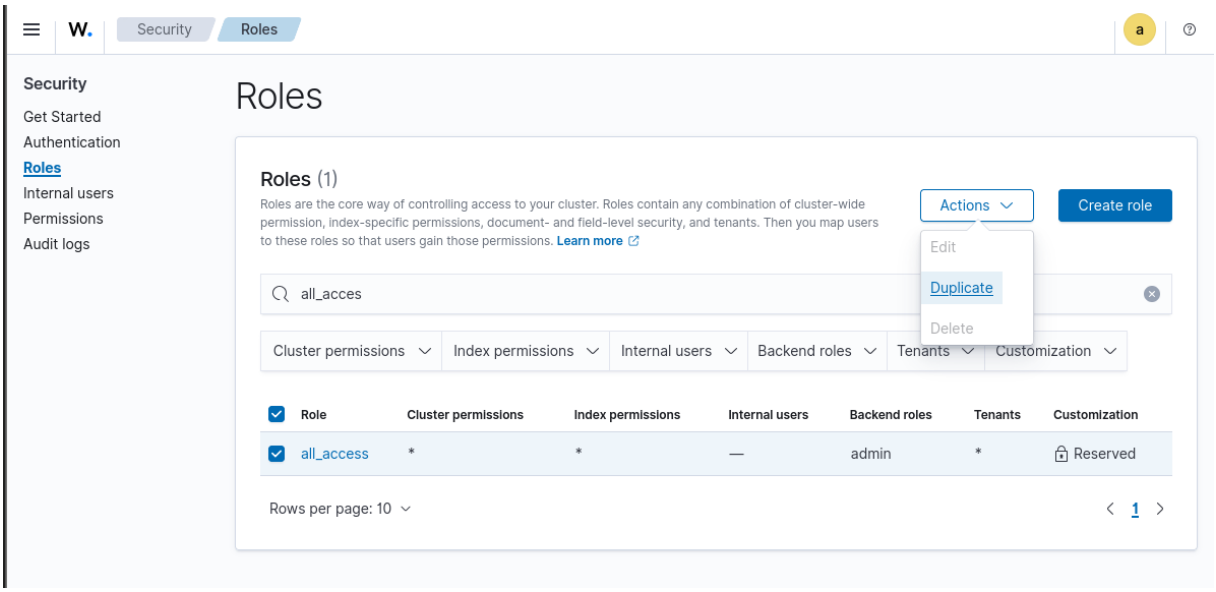
Ensuite on vas créer un nouvel utilisateur qu'on nommera administrateur : rdv dans indexer Management → Internal Users → create internal user


Security
Internal users
a
Security
Get Started
Authentication
Roles
Internal users
Permissions
Audit logs
Internal users
Internal users (7)
The Security plugin includes an internal user database. Use this database in place of, or in addition to, an external authentication system such as LDAP server or Active Directory. You can map an internal user to a role from Roles. First, click into the detail page of the role. Then, under "Mapped users", click "Manage mapping" Learn more
Actions
Create internal user
Search internal users
Username
Backend roles
Attributes
logstash
logstash
—
snapshotrestore
snapshotrestore
—
admin
Current
admin
—
kibanaserver
—
—
kibanaro
kibanauser
readall
attribute1: "value1"
attribute2: "value2"
attribute3: "value3"
readall
readall
—
anomalyadmin
—
—
Rows per page: 10
1

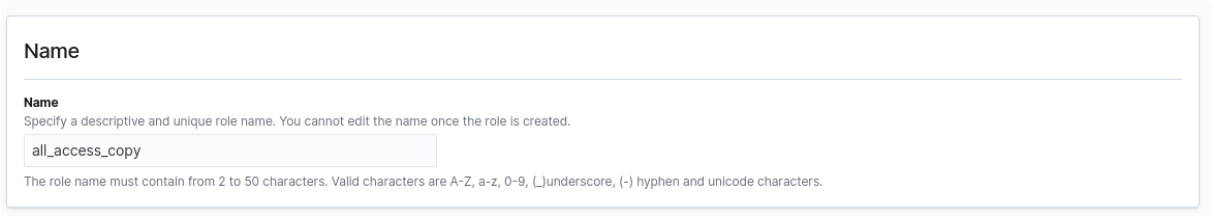
Donner lui un mdp fort et cliquer sur create :



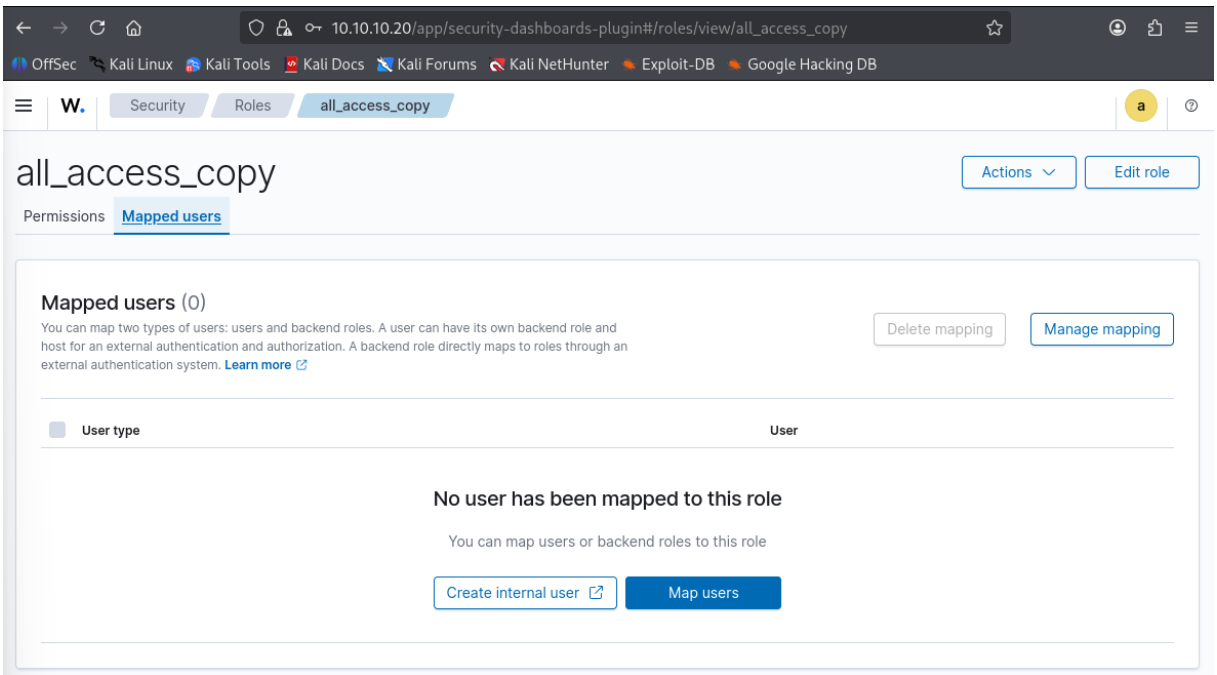
Ensuite cliquer sur Rôles et rechercher All Access, sélectionner le cliquer sur action et duplicate :



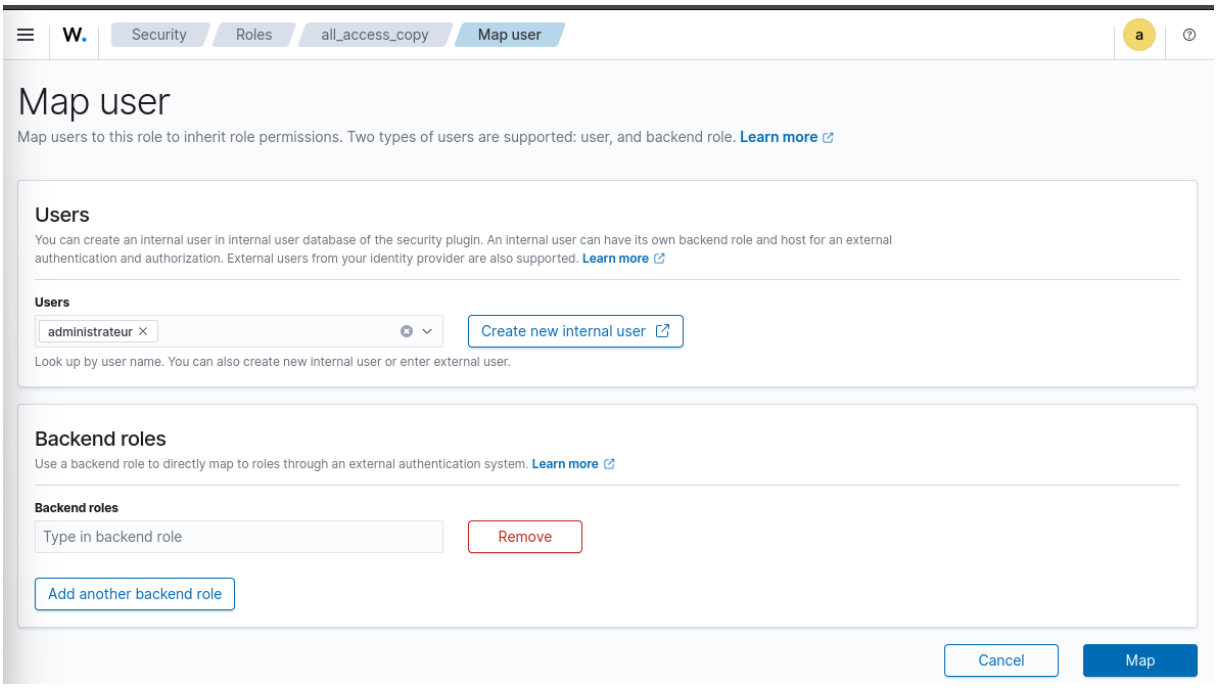
Renommer le all_access_administrateur et cliquer sur create:



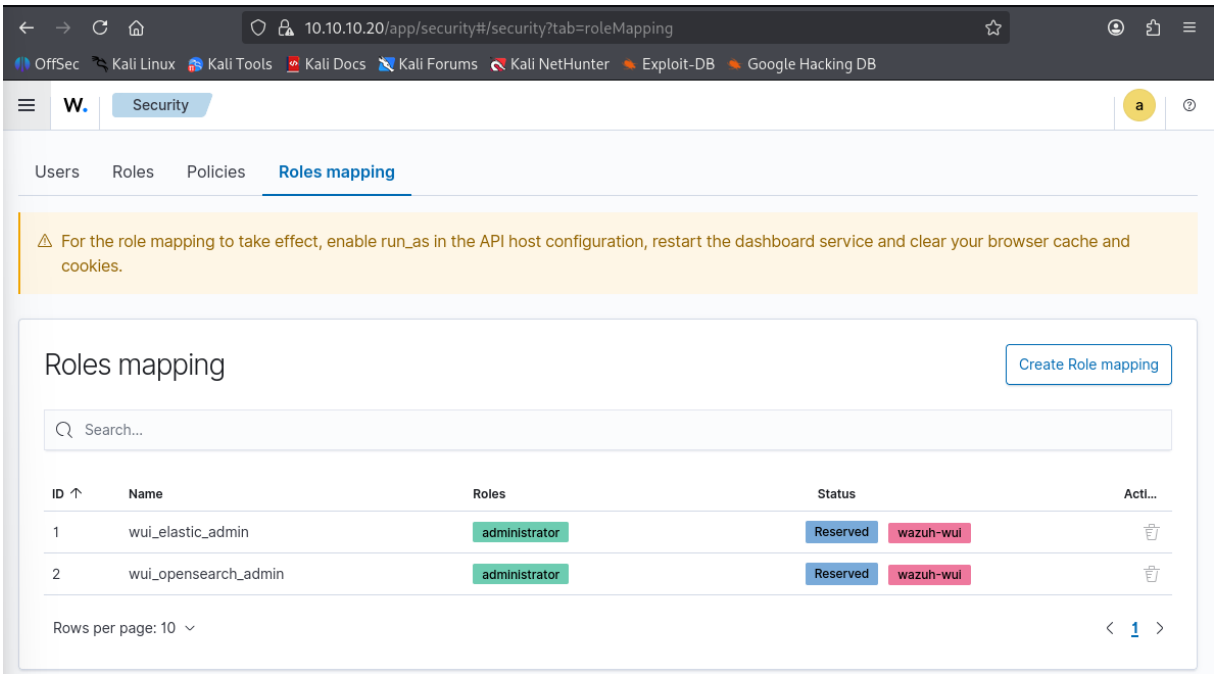
Cliquer ensuite sur Mapped Users et Map Users :



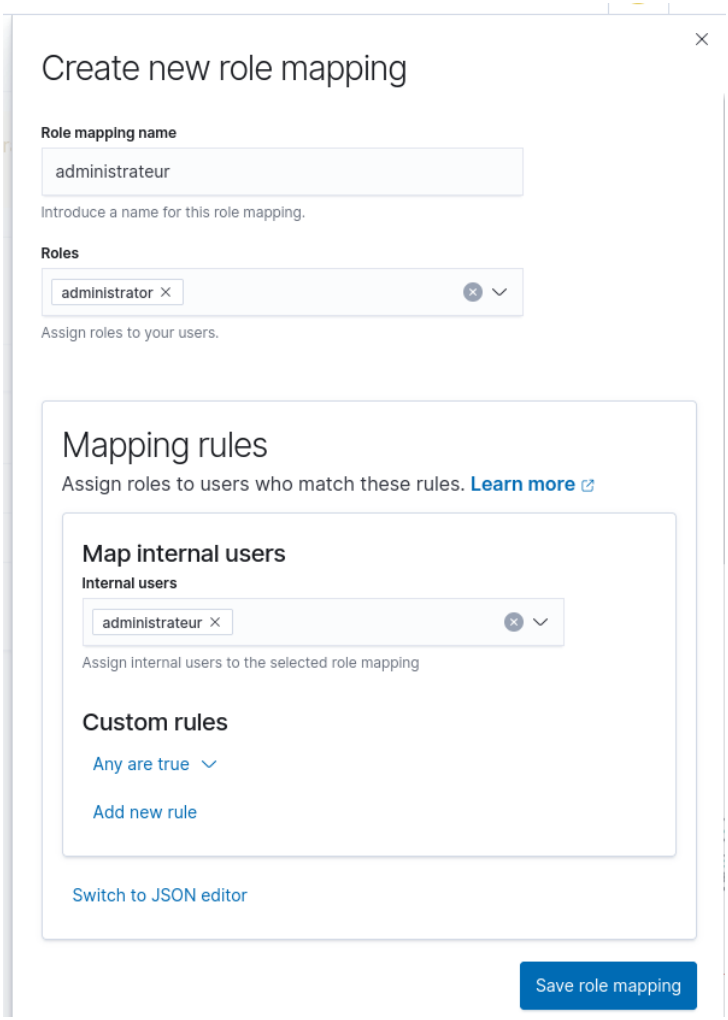
Sélectionner administrateur puis Map :



Rdv ensuite dans Server Managment → security → roles mapping et create Role Mapping :



Ensuite faite la meme configuration que ci-dessous et Save Role Mapping :

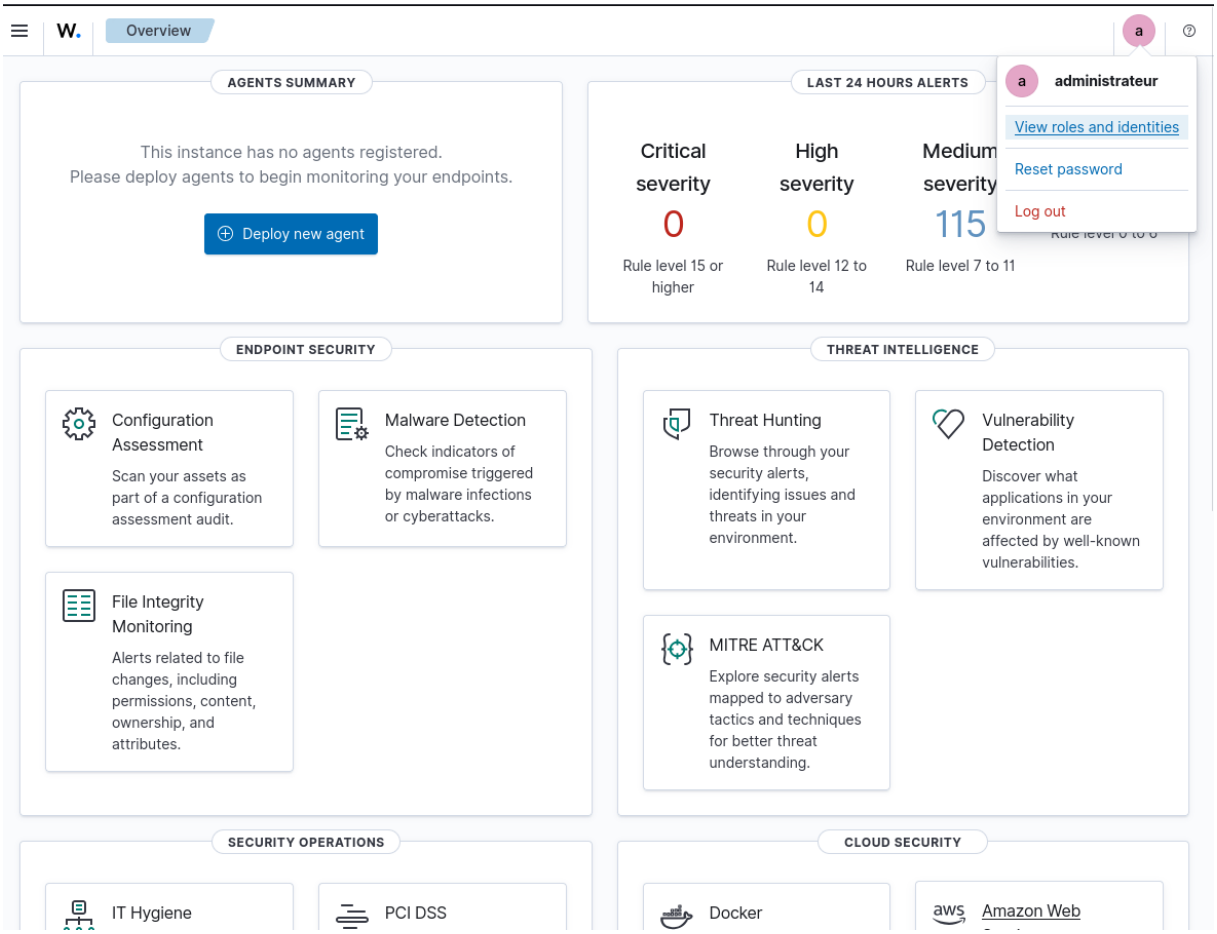


Ensuite dans l'invite de de wazuh copier cette commande « sudo nano /usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml » et rdv tout en bas du fichier pour modifier run_as et m'était le en True sauvegarder et relancer wazuh-dashboard: sudo systemctl restart wazuh-dashboard

```
hosts:
  - default:
      url: https://127.0.0.1
      port: 55000
      username: wazuh-wui
      password: "Q6Kv+tMpO+AXV*Yidy6tukrfEa3yZd11"
      run_as: true
```

```
administrator@srv-wazuh:~$ sudo systemctl restart wazuh-dashboard
administrator@srv-wazuh:~$
```

Vous pouvez maintenant vous déconnecter et vous reconnecter avec votre compte administrateur qui aura les meme permission que l'utilisateur admin :



Et voila la configuration de base de wazuh et terminer bravo ! la prochaine étape c'est d'installer les agents sur différente machine Windows ou linux. Référé vous a la procédure Installation des agents.