BloodHound

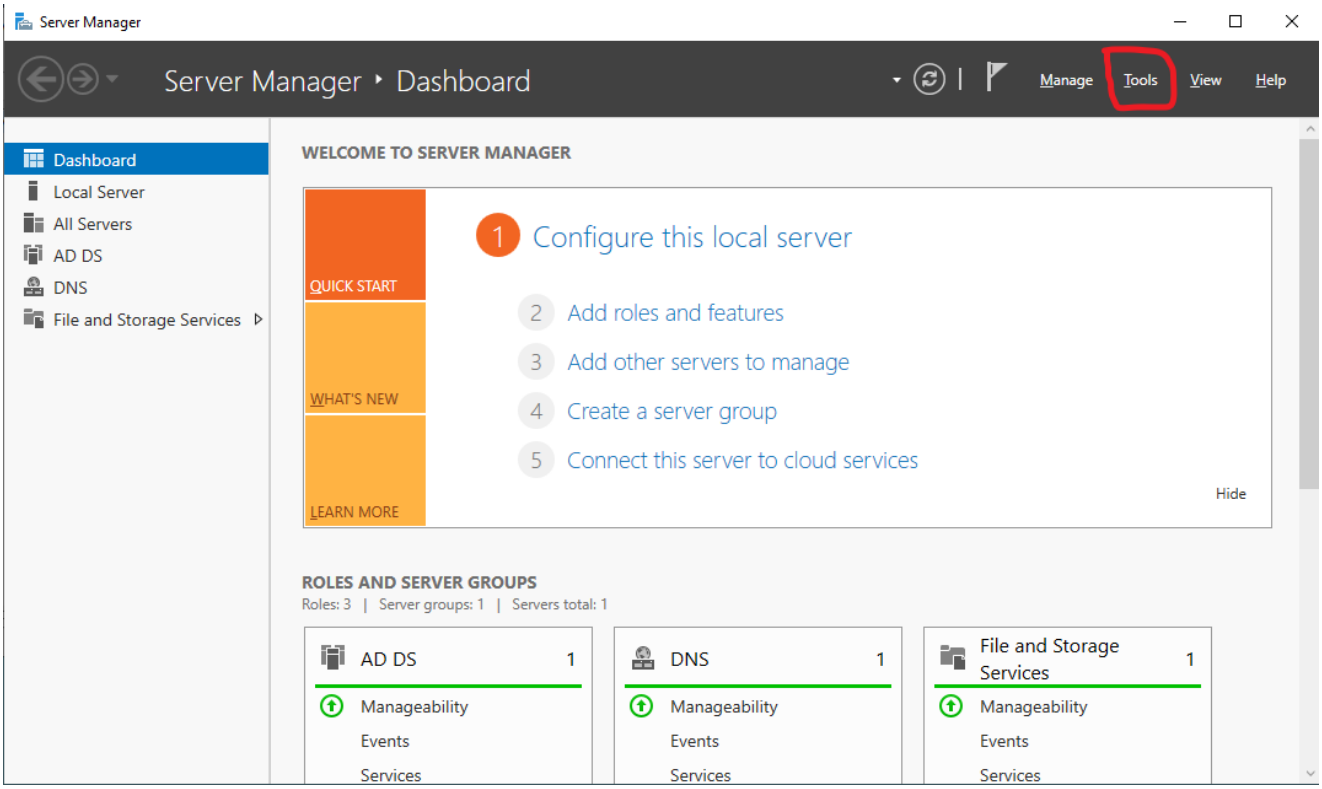
BloodHound est un outil open source qui permet d'analyser les chemins d'attaques au sein d'un Active Directory.

Introduction

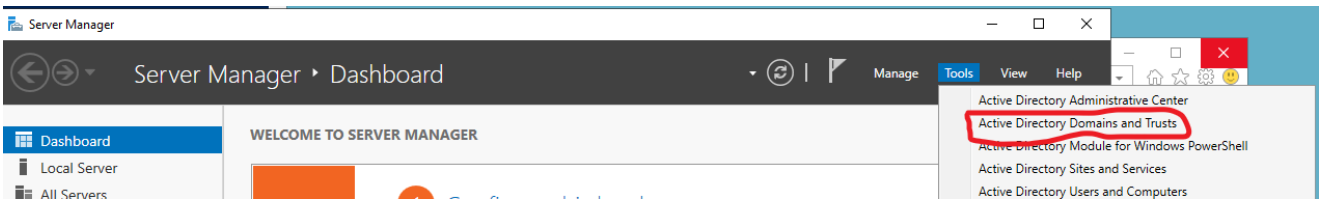
En premier temps il faut bien vérifier que le GOAD s'est bien lancé.
Pour se faire l'on va aller dans le Server Manager d'un DC pour vérifier que celui-ci possede bien un active directory domains.

Vérification lancement GOAD

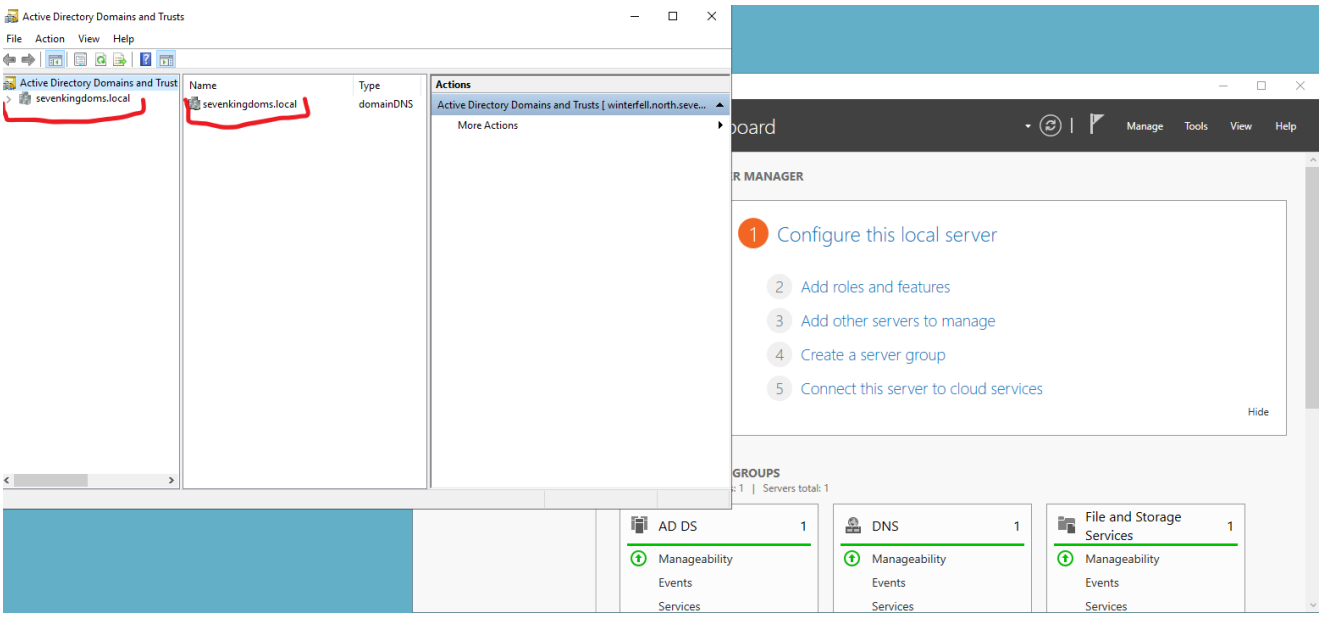
Lorsque le Server Manager est lancé il faut ensuite aller dans l'onglet "Tools"



Ceci fait nous voulons voir les domains ratachés à cette machine.
Pour se faire il faut aller dans "Active Direvtory Domains And Trust"



Nous pouvons voir que le DC possede bien un Domain, ainsi cela veut donc dire que m'installation s'est bien effectué.



Installation

Pour installer BloodHound il suffit de la ncer la commande suivante sur une debian:

```
sudo apt install bloodhound
```

Il faut ensuite installer neo4j. C'est une base de données de graphes hautement performante qui stocke et traite des données sous forme de graphes.

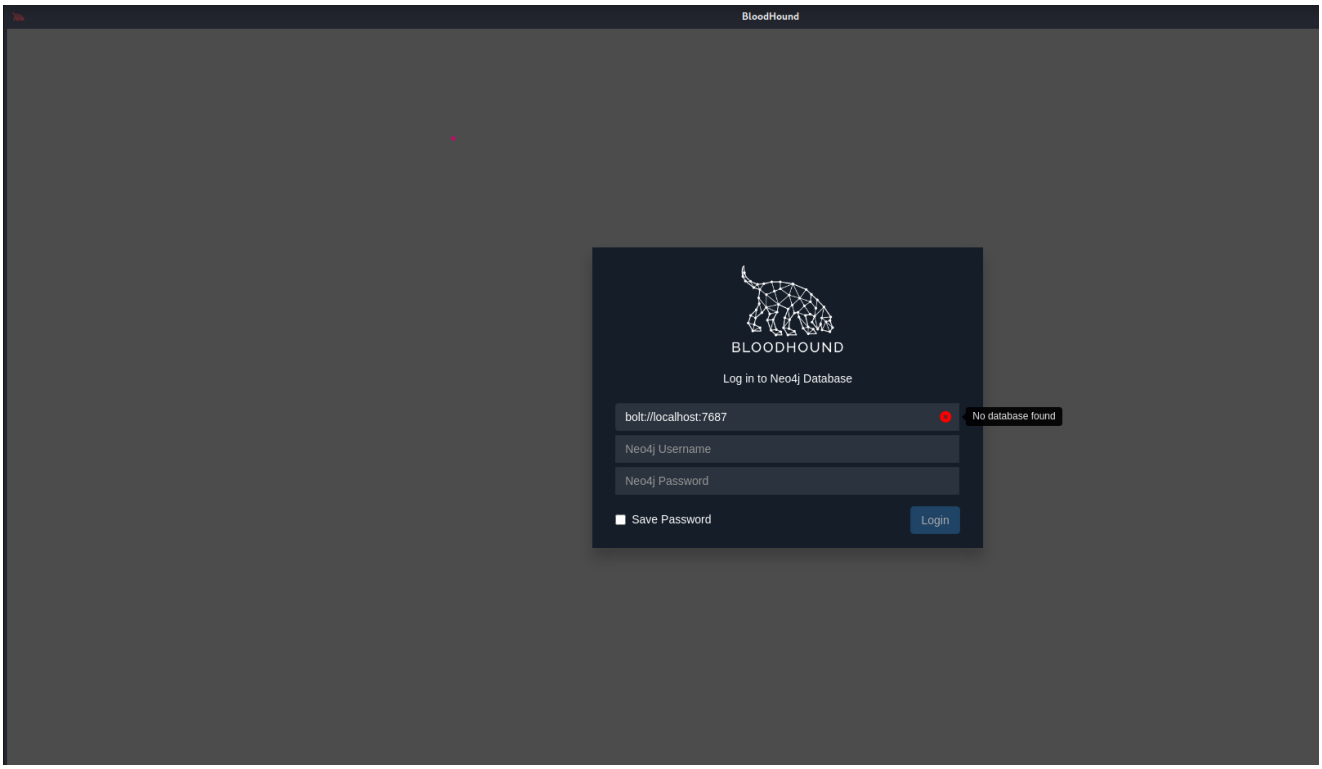
```
sudo apt install neo4j
```

Il faut ensuite lancer neo4j avec la commande:

```
sudo neo4j start
```

Ceci fait un lien https localhost s'affiche, il faut maintenant aller sur le lien, modifier le mots de passe. Puis il faut lancer le server.

Apres avoir lancer bloodhound nous pouvons voir que une page de connexion s'affiche:

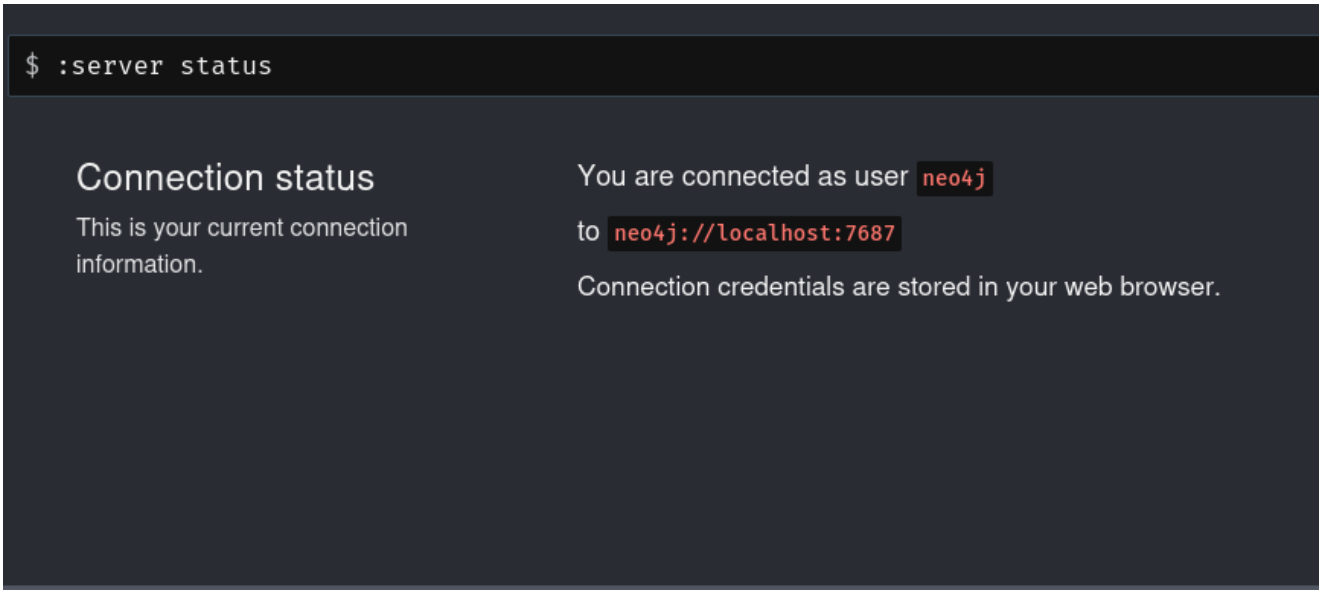


On peut voir qu'il faut renseigner le lien du neo4j, l'utilisateur ainsi que son mots de passe modifié précédemment.

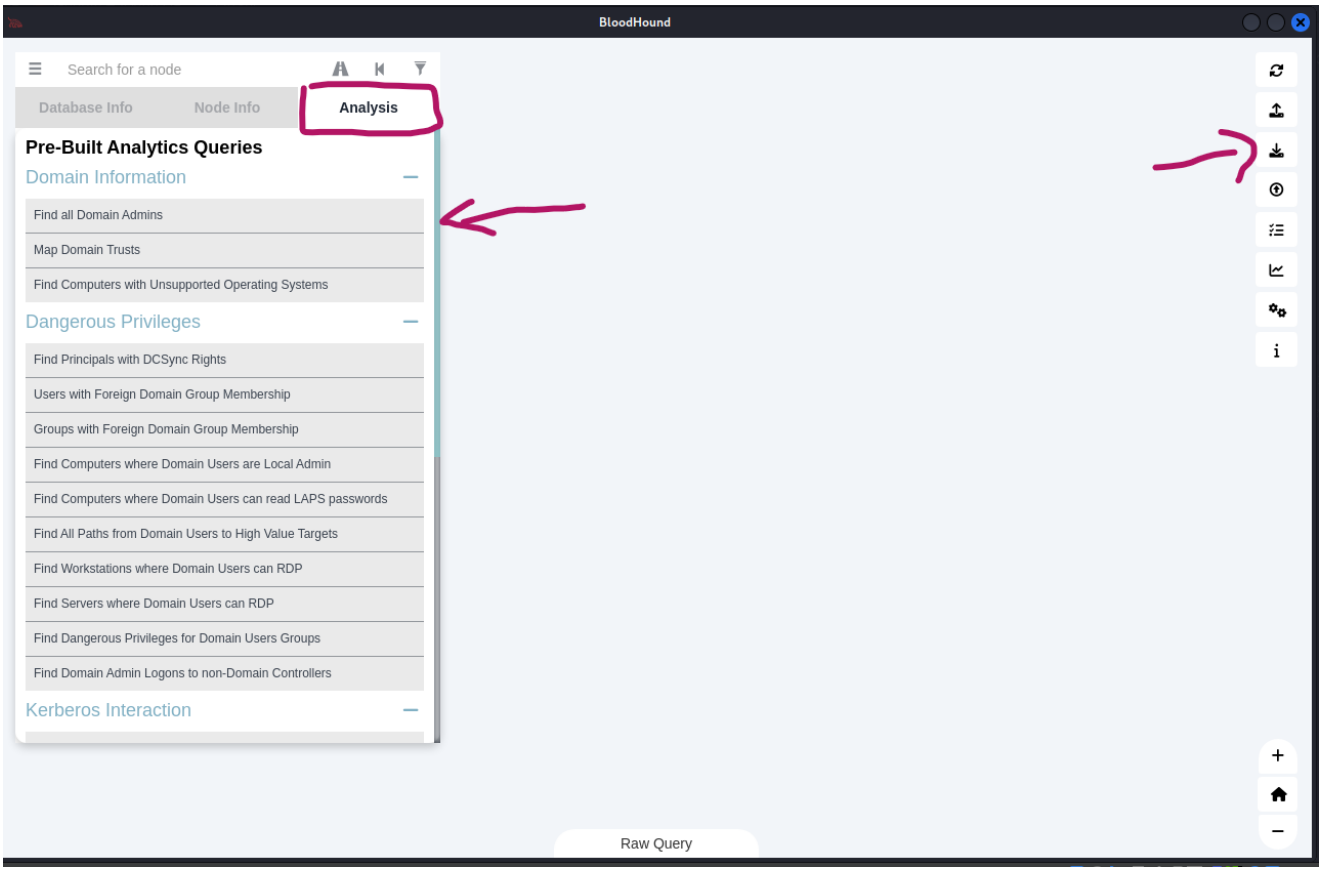
SharpHound

SharpHound est un composant spécifique du projet BloodHound. Il s'agit d'une série de scripts PowerShell utilisés pour collecter des données sur les relations et les autorisations au sein d'un environnement Active Director.

Mise en place finale



Apres avoir renseigné toutes les infos il suffit de se log, une page apparait, sur celle-ci un menu à droite est affiché.
Il faut ensuite selectionner le logo importer et importer par la suite les datas.



Ceci fait nous allons dans "Analysis" dans le menu principal puis selectionnons le graph que nous voulons, ici nous selctionnons le "Find All Domains Admins".