SPLUNK

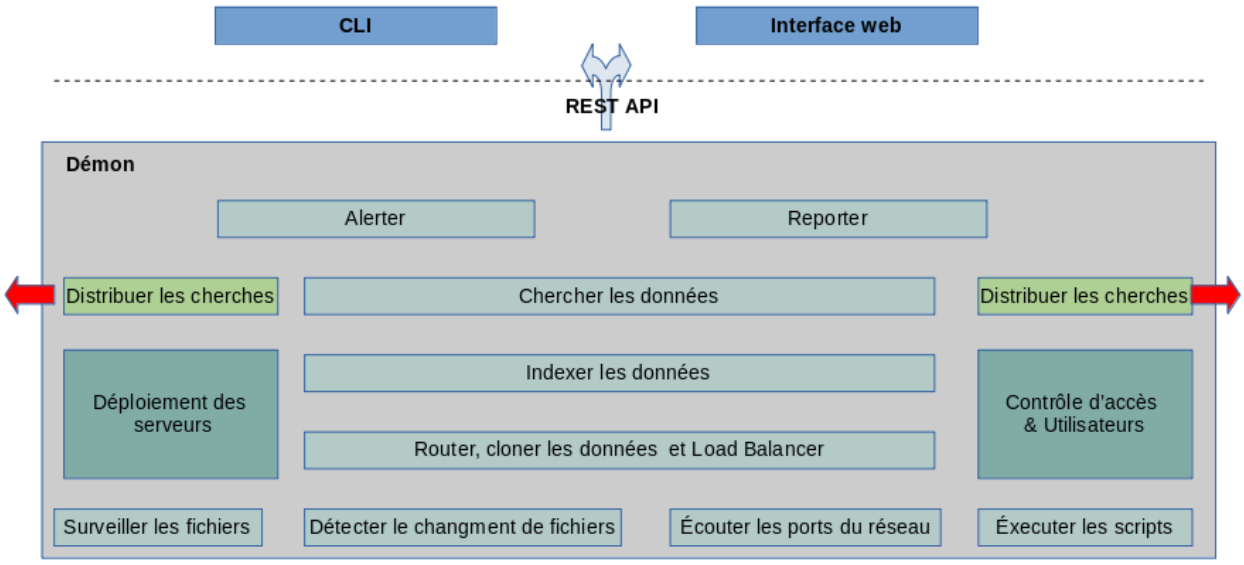
Version 1.0 le 8 avril 2019

SOMMAIRE

I. Introduction du SPLUNK

Splunk est un outil de SIEM qui gère des évènements du système d'information. Cet outil collecte, indexe et met en corrélation des données en temps réel dans des archives recherchables, permettant de générer des graphiques, des rapports, des alertes, des tableaux de bord et des infographies.

II. Architecture du SPLUNK



De manière simple, cet outil consiste à 3 parties: un CLI, une interface WEB et un démon qui réalise la collection, l'indexation et la recherche des données.

De manière précise, Il conclut 3 composants:

- Forwardeur: Il est un agent collecteur de logs chargé de transférer les données vers l'indexeur.
- Indexeur: Il analyse les données récues, les indexe selon une syntaxe spécifique et les stocke dans la disque.
- Search head: Il concrétise les recherches à travers toutes les données indexées. Ses serveurs executent CLI et Interface-web.

III. Mise en place du SPLUNK

III.1. Installation et configuration du Splunk ES

Pour la télécharger il suffit de s'inscrire et télécharger la version Splunk Entreprise. Ou vous pouvez directement exécuter la ligne suivante:

```
wget -O splunk-7.2.5.1-962d9a8e1586-linux-2.6-amd64.deb
'https://www.splunk.com/bin/splunk/DownloadActivityServlet?
architecture=x86_64&platform=linux&version=7.2.5.1&product=splunk&filename=splunk-7.2.5.1-
962d9a8e1586-linux-2.6-amd64.deb&wget=true'
```

Pour la suite on la suit:

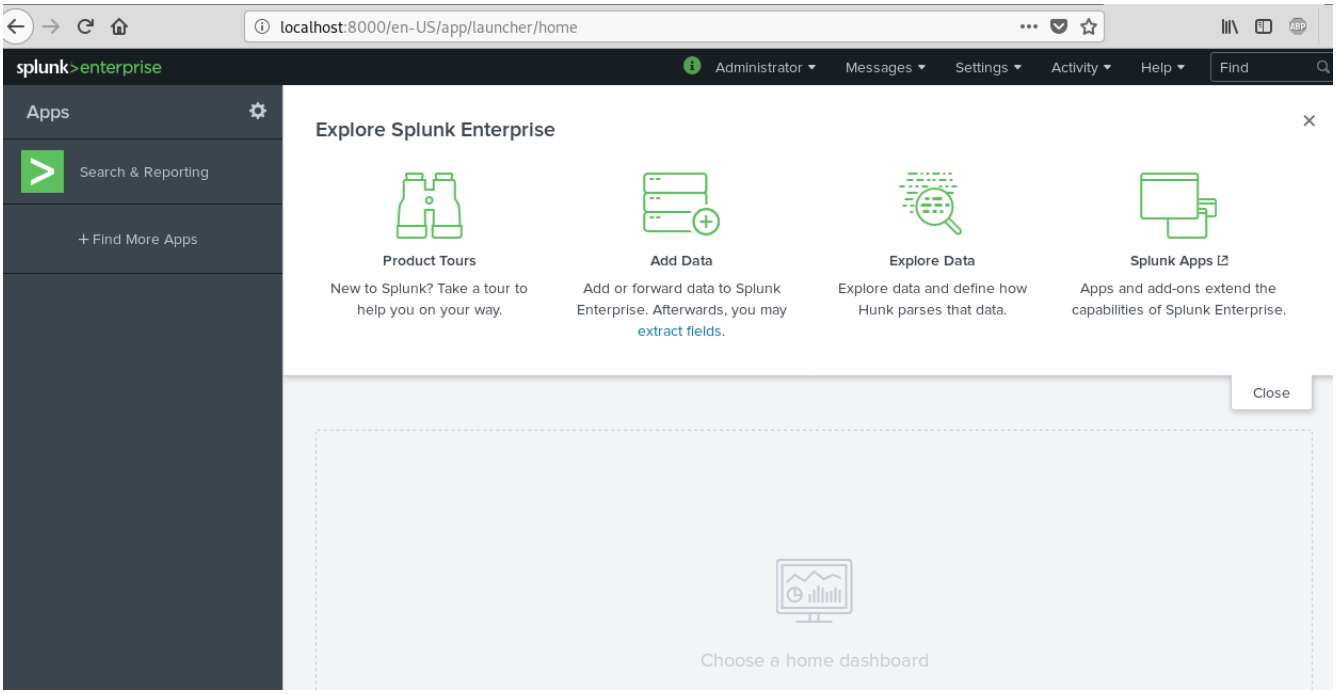
```
dpkg -i splunk-7.2.5.1-962d9a8e1586-linux-2.6-amd64.deb
```

Et enfin pour démarrer splunk sur la machine, on va saisir la commande suivante:

```
/opt/splunk/bin/splunk start
The Splunk web interface is at http://kali:8000
```

Voilà, ensuite vous pouvez ouvrir un navigateur et remplir la suivante pour obtenir la page d'accueil.

```
http://localhost:8000
```



III.2. Installation de configuration des 3 Splunk agents