
SPLUNK

Version 1.0 le 8 avril 2019

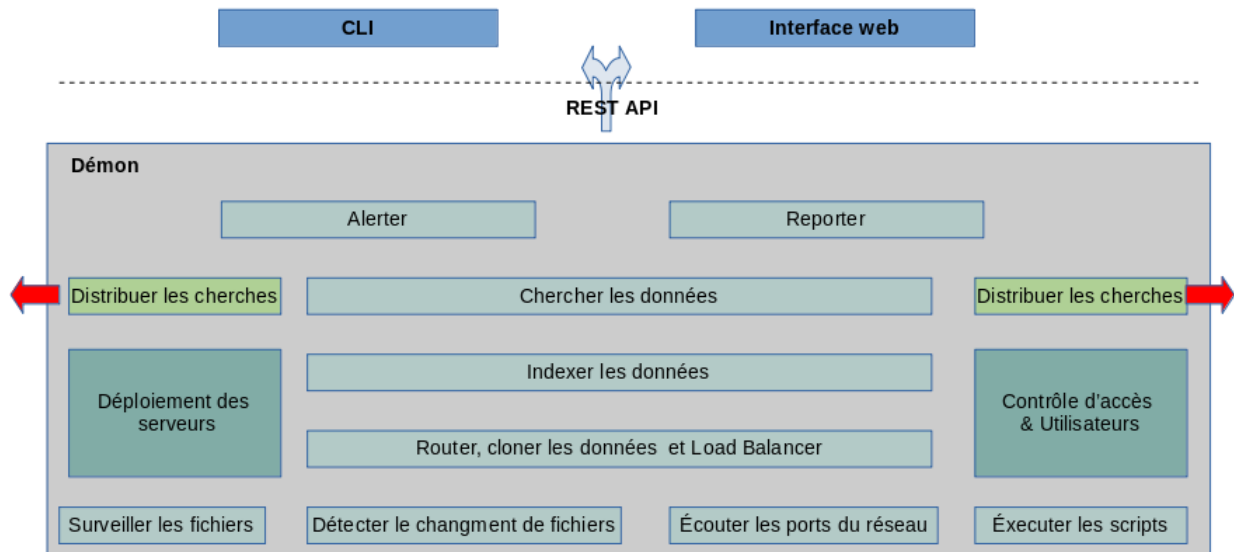
SOMMAIRE

I. Introduction du SPLUNK	3
II. Architecture du SPLUNK	3
III. Mise en place du SPLUNK	3
III.1. installation et configuration du Splunk ES	
III.2. installation de configuration des 3 Splunk agents	
III.3. configuration du serveur Splunk	
IV. SPL	
IV.1 faire un exemple (identifier @IP_src @IP_dest suspectes) pour chercher une enquête	
IV.1 faire un exemple (identifier le temps suspect) pour chercher une enquête	
V. Définition des scénarios de comportements anormaux	
V.1 N°1 scénario	
V.2 N°2 scénario	
V.3 N°3 scénario	
V.4 N°4 scénario	
V.5 N°5 scénario	
VI. Implémentation des scénarios	
VI.1 N°1 scénario	
VI.1.1 Génération d'une alerte	
VI.1.2 Exécution des règles de remédiation	
VI.2 N°2 scénario	
VI.2.1 Génération d'une alerte	
VI.2.2 Exécution des règles de remédiation	
VI.3 N°3 scénario	
VI.3.1 Génération d'une alerte	
VI.3.2 Exécution des règles de remédiation	
VI.4 N°4 scénario	
VI.4.1 Génération d'une alerte	
VI.4.2 Exécution des règles de remédiation	
VI.5 N°5 scénario	
VI.5.1 Génération d'une alerte	
VI.5.2 Exécution des règles de remédiation	

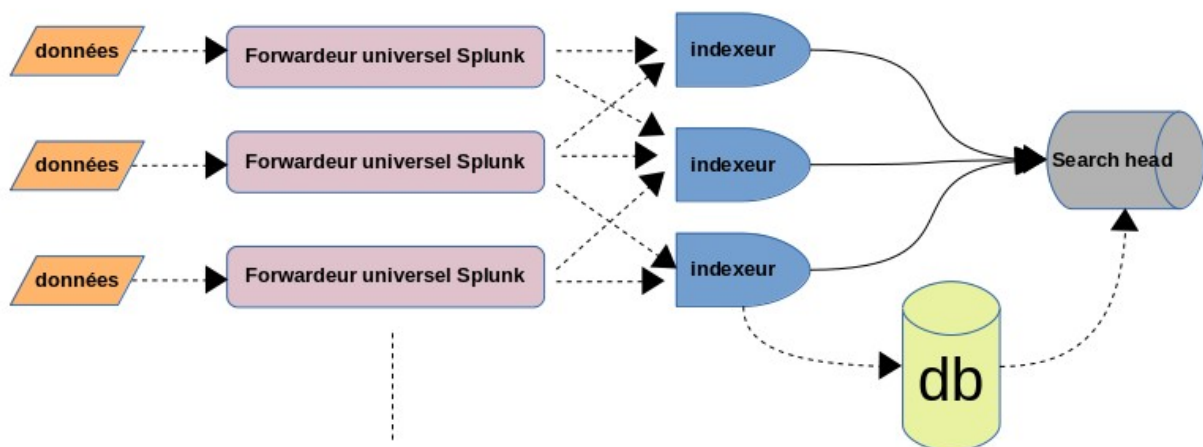
I. Introduction du SPLUNK

Splunk est un outil de SIEM qui gère des événements 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 reçues, 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 exécutent 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'
```

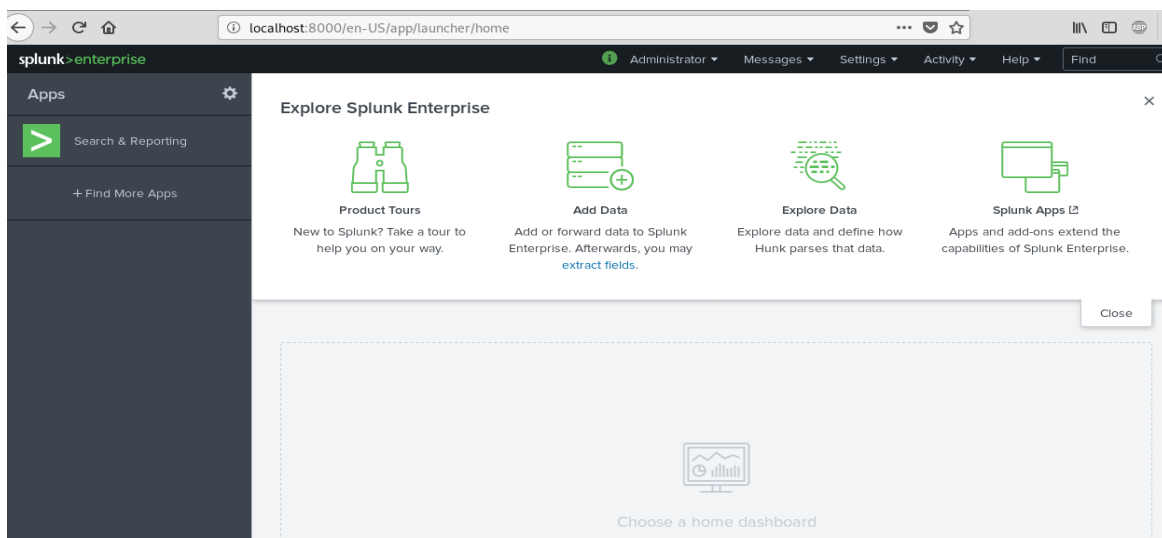
Pour la suite on la suit:

```
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

Sous Linux

De retour sur le forwarder universel, vous pouvez télécharger la dernière version d'après votre système. Ou vous pouvez directement exécuter la ligne suivante:

```
wget -O splunkforwarder-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=universalforwarder&filename=splun  
kforwarder-7.2.5.1-962d9a8e1586-linux-2.6-amd64.deb&wget=true'
```

Pour la suite l'installer:

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

Et enfin pour démarrer un forwarder universel sur la machine, saisir la commande suivante:

```
/opt/splunkforwarder/splunk start --accept-license
```

Voilà, pour la configuration, identifier le serveur splunk par @IP et Port N°:

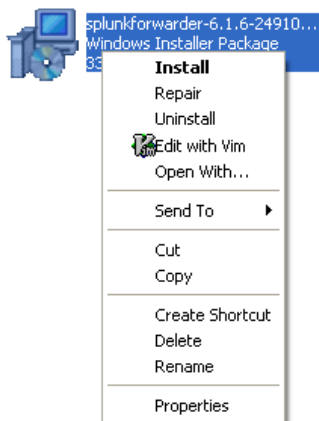
```
/opt/splunkforwarder/splunk add forward-server 192.168.1.xx:9997
```

Puis ajouter un dossier ou un fichier en surveillance, qui sera automatiquement envoyé au serveur Splunk:

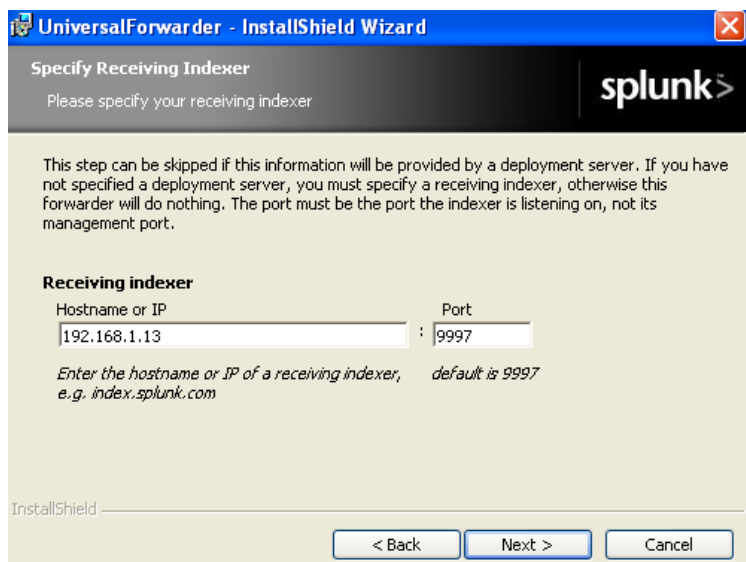
```
/opt/splunkforwarder/splunk add monitor /var/log/syslog -index syslog
```

Sous Windows

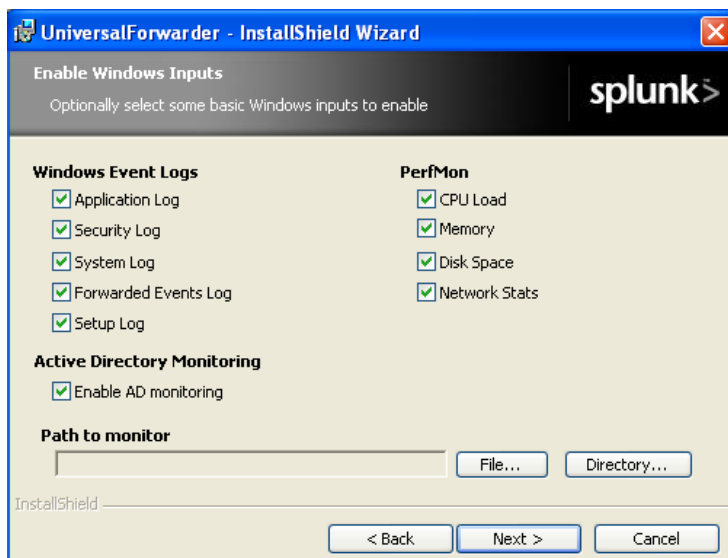
L'installation sous windows nécessite de télécharger l'exécutable sur le site du Splunk. Il s'agit d'un fichier .msi.



Pour la suite lancer l'installation par **install**. Vous pouvez choisir quels logs Forwardeur surveillera. Un écran vousn proposera de configurer un serveur du Splunk avec @IP et le port.



Puis vous pouvez ajouter des fichiers ou paths en surveillance, qui seront automatiquement envoyés au serveur Splunk.



III.3. configuration du serveur Splunk

Comme toujours, activer le port d'écoute sur le serveur splunk afin de recevoir des données du forwarder.

Add new
Forwarding and receiving » Receive data » Add new

Configure receiving
Set up this Splunk instance to receive data from forwarder(s).

Listen on this port *

For example, 9997 will receive data on TCP port 9997.

Puis vérifier que le hôte distant soit affiché ci-dessous:

Data Summary

Hosts (2) Sources (7) Sourcetypes (7)

filter

Host ▾		Count ▾	Last Update ▾
kali		14	4/10/19 1:36:48.000 PM
xp		3,549	4/11/19 10:54:52.000 AM

Voilà, c'est terminé. Les logs commencent à remplir l'index selon lequel vous pouvez lancer des SPL recherches.

IV. SPL

IV.1 faire un exemple (**identifier @IP_src @IP_dest suspectes**) pour chercher une enquête

IV.1 faire un exemple (**identifier le temps suspect**) pour chercher une enquête

V. Définition des scénarios de comportements anormaux

V.1 N°1 scénario

Un serveur SSH, muni des fichiers controversés d'échange, est pris en contrôle par un attaquant en brute-force. Le pire c'est que quelques fichiers similaires soient exposés au public.

V.2 N°2 scénario

La connexion à la page d'accueil de site web d'entreprise est tellement lente et instable que des visiteurs ne peuvent pas faire des courses sur Internet. L'administrateur a vérifié la performance du serveur web Apache en état de bon fonctionnement mais en surcharge.

V.3 N°3 scénario

L'administrateur a accédé à la base de données le weekend. Mais en réalité, il n'en a pas fait sans aucun doute.

V.4 N°4 scénario

Un employé a parfois trouvé le ralentissement des performances du réseau entre les deux hôtes internes ou (un interne et un externe).

V.5 N°5 scénario

Lorsque une clé usb est insérée, un très grand nombre des fichiers sont copiés immédiatement sans afficher des fenêtres de copier- coller. En même temps le logiciel antivirus rien n'a affiché.