

Installation de la version d'essai de Splunk Enterprise

Introduction :

Splunk est un SIEM côté en bourse (donc ça fait pro) qui propose depuis 2003 une plateforme unifiée de sécurité et d'observabilité. La solution est très connue (et reconnue) par de nombreuses entreprises américaines et la fiabilité n'est pas à re-démontrer. Cependant, le prix peut vite refroidir : 1000\$/an. Heureusement pour nous, il est possible de télécharger une version d'essai de Splunk qui permet l'aggrégation de 500Mo de logs par jour gratuitement, c'est ce qu'on va installer.

Installation :

Il faut d'abord se rendre sur le site de Splunk puis créer un compte pour vendre nos données :

```
https://www.splunk.com/en_us/download/splunk-enterprise.html?locale=en_us
```

On installe les bons paquets nécessaires :

```
apt install -y sudo curl && usermod -aG sudo deb-user
```

Pour éviter de redevoir faire un compte, je met ici le lien au cas où :

```
wget https://download.splunk.com/products/splunk/releases/9.1.2/linux/splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb
```

On peut finalement lancer le .deb :

```
sudo dpkg -i splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb
```

Puis le supprimer pour libérer de l'espace :

```
sudo rm splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb
```

On rajoute le bon PATH :

```
export PATH=$PATH:/opt/splunk/bin && su -c "export PATH=$PATH:/opt/splunk/bin"
```

Puis on lance notre instance Splunk et on génère un mot de passe :

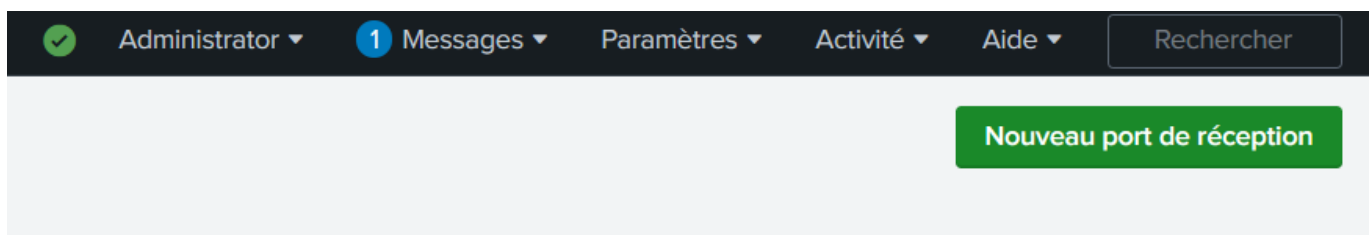
```
sudo /opt/splunk/bin/splunk start --accept-license  
--answer-yes --no-prompt --gen-and-print-passwd
```

On fait en sorte que le serveur écoute en HTTPS :

```
sudo /opt/splunk/bin/splunk enable web-ssl && sudo /opt/splunk/bin/splunk set web-  
port 443 && sudo /opt/splunk/bin/splunk restart
```

Il faut aller ouvrir un port pour démarrer le service d'indexage :


```
https://10.202.0.153/fr-FR/manager/search/data/inputs/tcp/cooked
```



Puis :

A screenshot of the 'Configurer la réception' (Configure Reception) form in the Splunk web interface. The form title is 'Configurer la réception'. Below it, the text reads 'Paramétrer cette instance Splunk pour recevoir les données des forwarders.' There is a label 'Écouter ce port *' followed by a text input field containing '9000'. Below the input field, a note says 'Par exemple, 9997 recevra les données sur le port TCP 9997.' At the bottom right of the form, there are two buttons: 'Annuler' (Cancel) and 'Enregistrer' (Save).

On a alors notre port d'ouvert :

Réception des données		
Transmission et réception » Réception des données		
Affichage de 1-1 objet sur 1		
<input type="text" value="filtre"/> 		
Écouter ce port ↕	Statut ↕	Actions
9000	Activé Désactiver	Supprimer
<		

On peut alors faire un script Ansible pour déployer les différents agents sur les machines distantes :

```
---
- name: Déploiement de l'agent Splunk.
  hosts: all
  gather_facts: false
  tasks:
    - name: Télécharge l'agent Splunk.
      win_shell: |
        [Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
        Invoke-WebRequest -Uri
https://download.splunk.com/products/universalforwarder/releases/9.1.2/windows/spl
unkforwarder-9.1.2-b6b9c8185839-x64-release.msi -OutFile "C:\tmp\splunkforwarder-
9.1.2-b6b9c8185839-x64-release.msi" -UseBasicParsing

        # On change les IPs ICI !
    - name: Installe l'agent Splunk.
      win_shell: |
        $Serv_splunk = "10.202.0.153:9000"
        msixexec.exe /i "C:\tmp\splunkforwarder-9.1.2-b6b9c8185839-x64-release.msi"
RECEIVING_INDEXER="$Serv_splunk" WINEVENTLOG_APP_ENABLE=1 WINEVENTLOG_SEC_ENABLE=1
WINEVENTLOG_SYS_ENABLE=1 WINEVENTLOG_FWD_ENABLE=1 WINEVENTLOG_SET_ENABLE=1
ENABLEADMON=1 PERFMON=cpu,memory,network,diskspace SPLUNKUSERNAME=admin
SPLUNKPASSWORD=cvbn123456 USE_LOCAL_SYSTEM=1 PRIVILEGESECURITY=1
AGREETOLICENSE=Yes /quiet

    - name: Démarre l'agent Splunk.
      win_shell: |
        NET START SplunkForwarder
```

Pour lancer le script Ansible :

```
ansible-playbook -i Ansible/inventaire.ini Ansible/script.yml
```

Si quelque chose se passe mal, on peut alors désinstaller les agents avec également un script Ansible :

```

---
- name: Supprime les agents Splunk
  hosts: all
  gather_facts: false
  tasks:
    - name: Arrête le Forwarder Splunk...
      win_shell: |
        NET STOP SplunkForwarder

    - name: Supprime le Forwarder Splunk...
      win_shell: |
        msixexec /x "C:\tmp\splunkforwarder-9.1.2-b6b9c8185839-x64-release.msi"

```

Pour le lancer :

```
ansible-playbook -i Ansible/inventaire.ini Ansible/desinstall.yml
```

On peut alors conclure en allant voir les informations remontées dans notre serveur Splunk, par exemple par rapport à Kerberos :

The screenshot shows the Splunk Enterprise Search & Reporting interface. The search bar contains 'kerberos' and the results show 26,681 events from 05/12/2023 14:00:00,000 to 06/12/2023 14:38:56,000. The interface includes a navigation bar with 'Recherche', 'Analytics', 'Jeux de données', 'Rapports', 'Alertes', and 'Tableaux de bord'. The search results are displayed in a table with columns for 'Durée' and 'Événement'. The first event is dated 06/12/2023 14:38:47,000 and details a Kerberos authentication process. The second event is dated 06/12/2023 14:38:38,000 and also details a Kerberos authentication process. The interface includes a sidebar for 'Masquer les champs' and 'CHAMPS INTÉRESSANTS'.

Durée	Événement
06/12/2023 14:38:47,000	12/06/2023 05:38:47 AM ... 45 lines omitted ... Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: - Afficher toutes les 70 lignes host = WINTERFELL source = WinEventLog:Security sourcetype = WinEventLog:Security
06/12/2023 14:38:38,000	12/06/2023 05:38:38 AM ... 45 lines omitted ... Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos