Security information and event management

Mise en place d'une solution SIEM Splunk

PLAN

- Introduction
- Installing Splunk Enterprise on Linux
- Splunk Universal Forwarder
- Configuration et Récupération des Fichiers de Journalisation

INTRODUCTION

SIEM

- Un SIEM (Security information and event management, Système de gestion des informations et des événements de sécurité) collecte des logs et des événements afin de normaliser ces données pour une analyse ultérieure pouvant générer des visualisations, des alertes, des recherches, des rapports et bien plus encore.

- La avantages du SIEM en matière de détection des menaces et de conformité Le principal avantage des plates-formes SIEM est qu'elles collectent, agrègent, stockent et analysent les journaux et les données d'un grand nombre de sources en temps réel.

INTRODUCTION

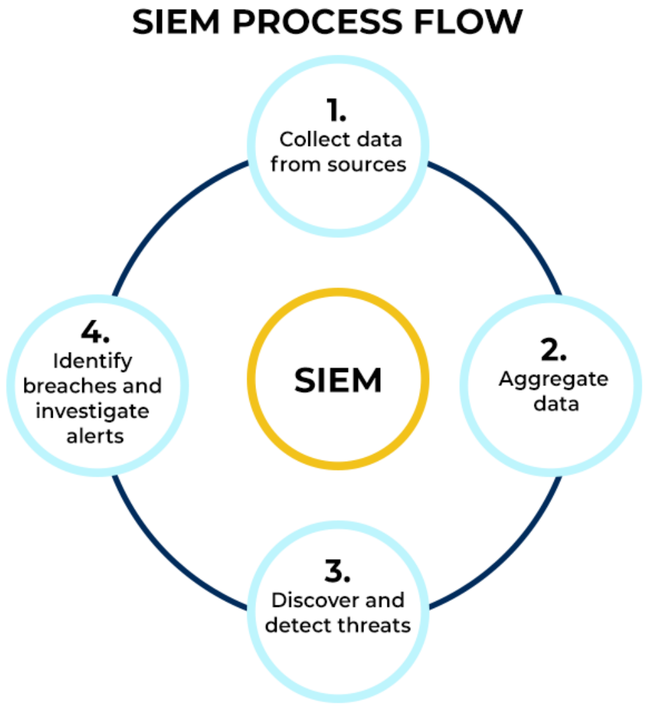
EXEMPLE SIEM

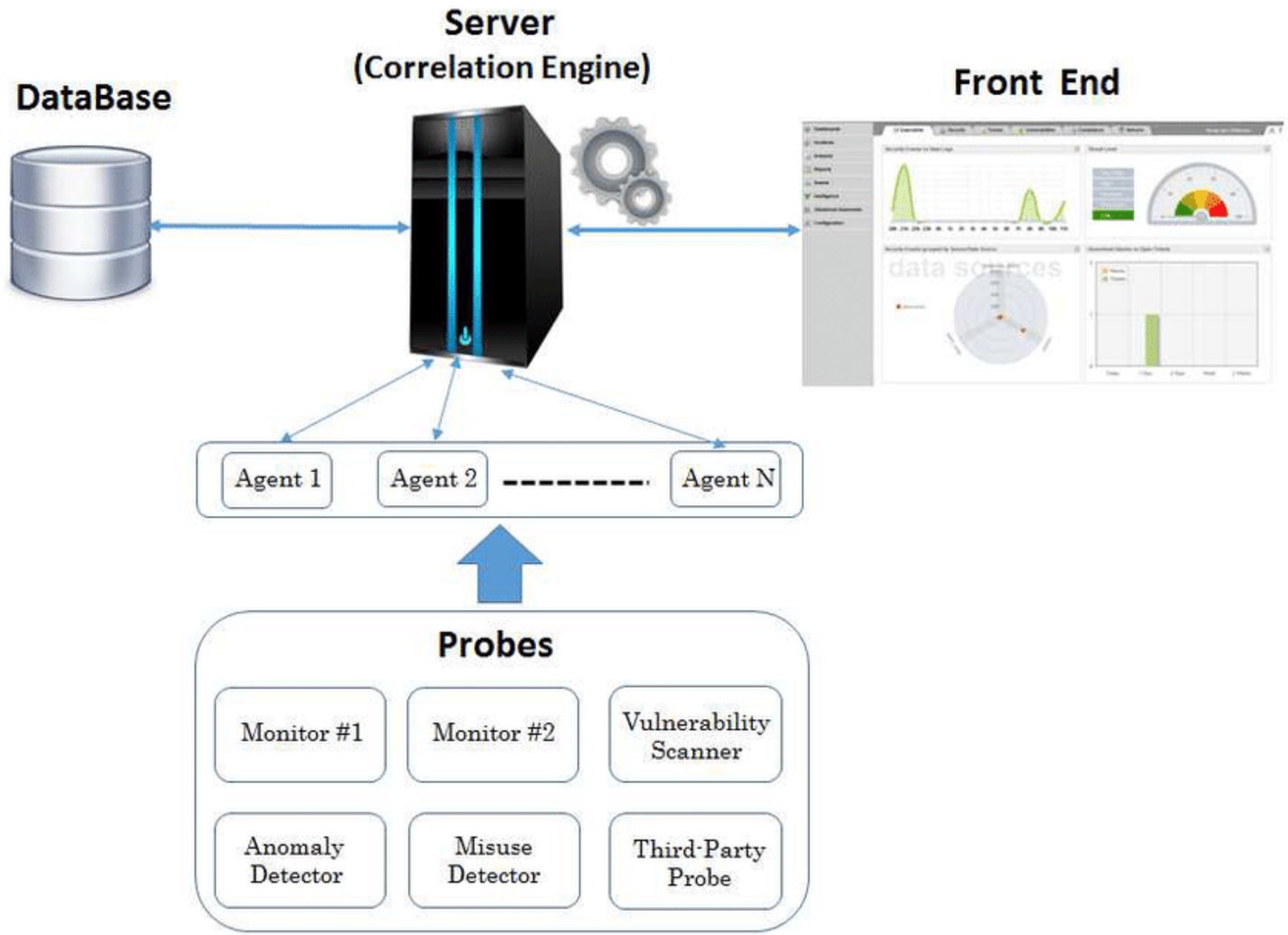
- **Elastic Security**
- **Graylog**
- **IBM QRadar**
- **Splunk**
- **InsightsIDR**

Quelle est la méthode utilisée par SIEM pour analyser les données ?

Le SIEM centralise les évènements et permet de détecter les menaces connues et inconnues en temps réel via du Machine Learning, de l'intelligence de sécurité et de l'analyse comportementale des utilisateurs et des entités (UEBA)

SIEM OVERVIEW

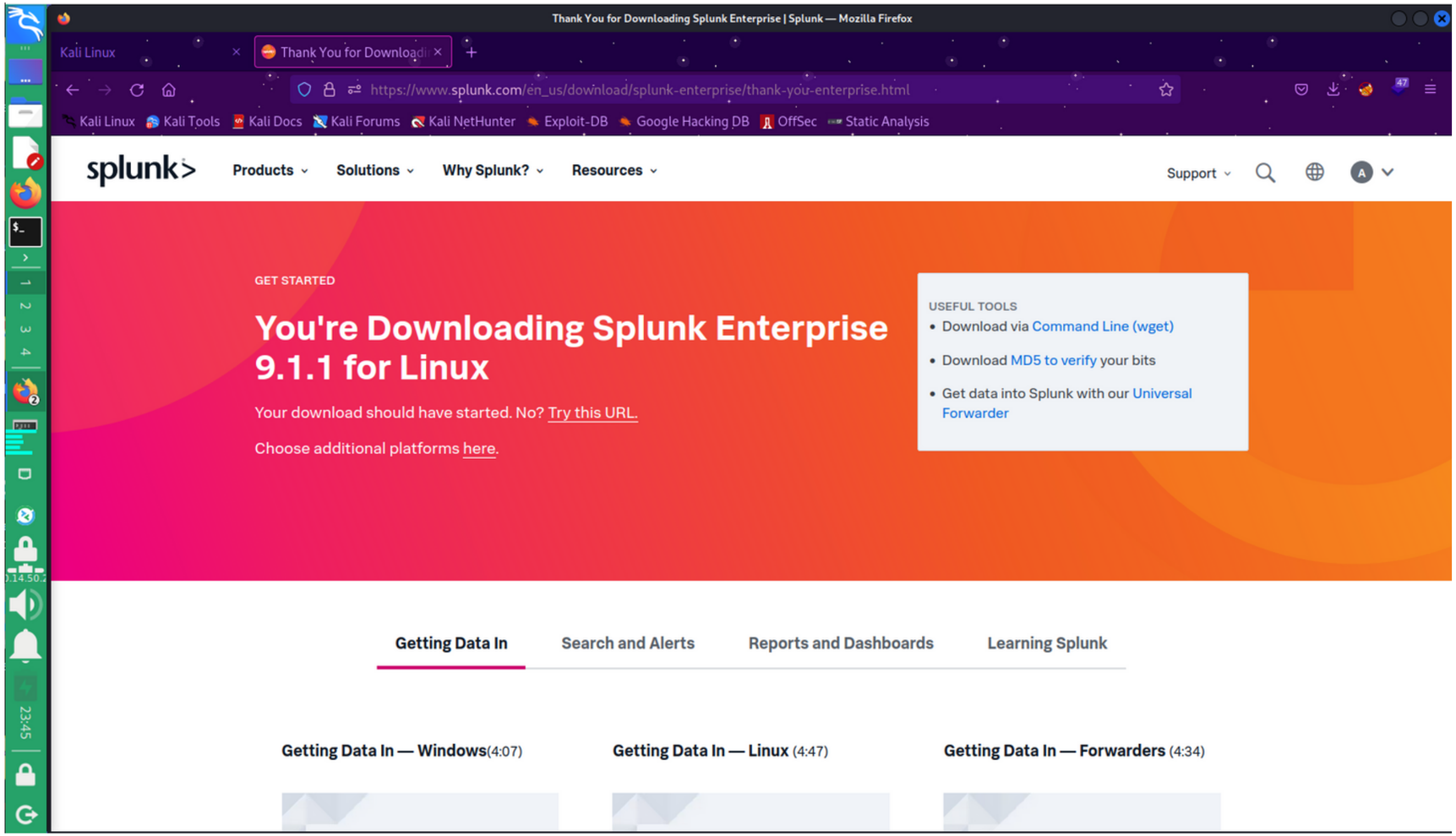




Installing Splunk Enterprise on Linux

Splunk Enterprise on Linux

- EXEMPLE ON LINUX



Splunk Enterprise on Linux

- EXEMPLE ON LINUX

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# dpkg -i ./splunk-9.1.1-64e843ea36b1-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 411901 files and directories currently installed.)
Preparing to unpack .../splunk-9.1.1-64e843ea36b1-linux-2.6-amd64.deb ...
Unpacking splunk (9.1.1+64e843ea36b1) ...
Setting up splunk (9.1.1+64e843ea36b1) ...
complete
```

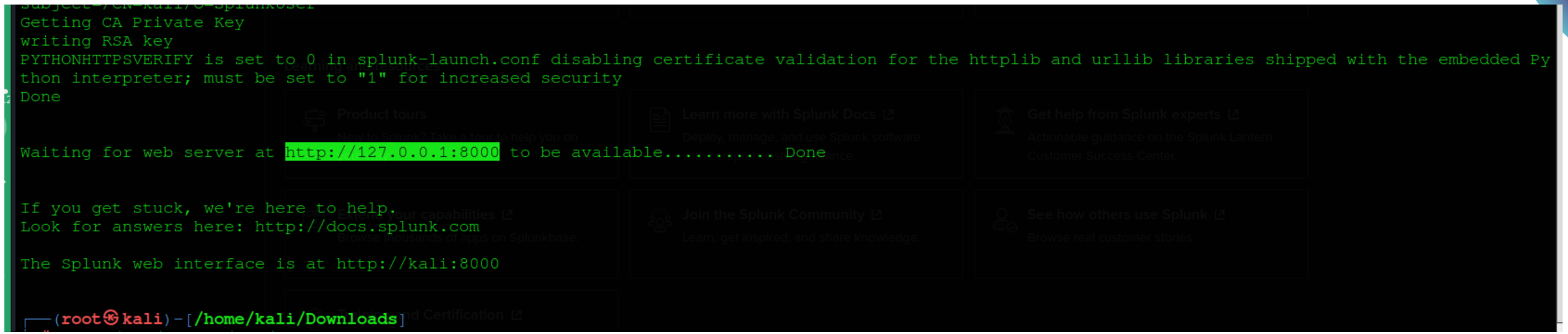
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# sudo /opt/splunk/bin/splunk start
sudo: unable to resolve host kali: Name or service not known
SPLUNK GENERAL TERMS

Last Updated: August 12, 2021

These Splunk General Terms ("General Terms") between Splunk Inc., a Delaware
corporation, with its principal place of business at 270 Brannan Street, San
Francisco, California 94107, U.S.A ("Splunk" or "we" or "us" or "our") and you
("Customer" or "you" or "your") apply to the purchase of licenses and
subscriptions for Splunk's Offerings. By clicking on the appropriate button,
or by downloading, installing, accessing or using the Offerings, you agree to
these General Terms. If you are entering into these General Terms on behalf of
Customer, you represent that you have the authority to bind Customer. If you
do not agree to these General Terms, or if you are not authorized to accept
the General Terms on behalf of the Customer, do not download, install, access,
```

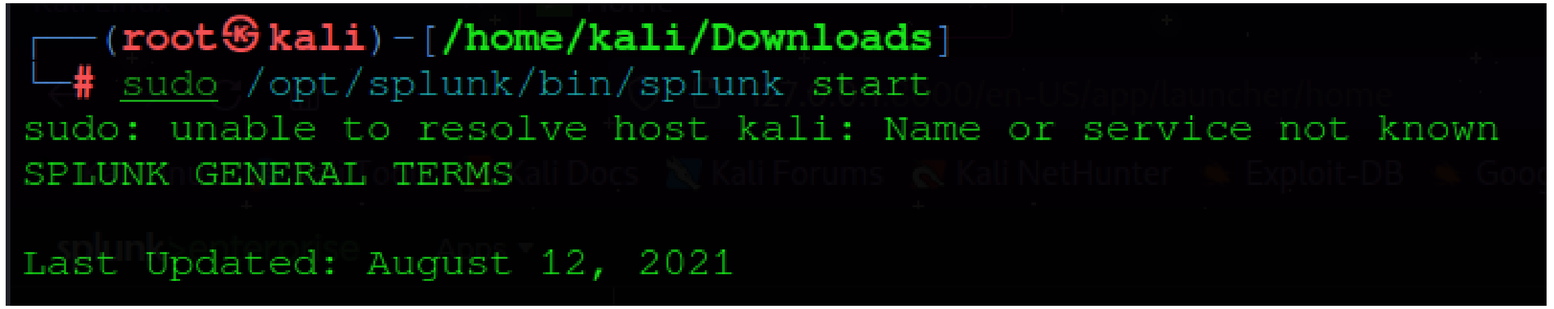
Splunk Enterprise on Linux

- EXEMPLE ON LINUX



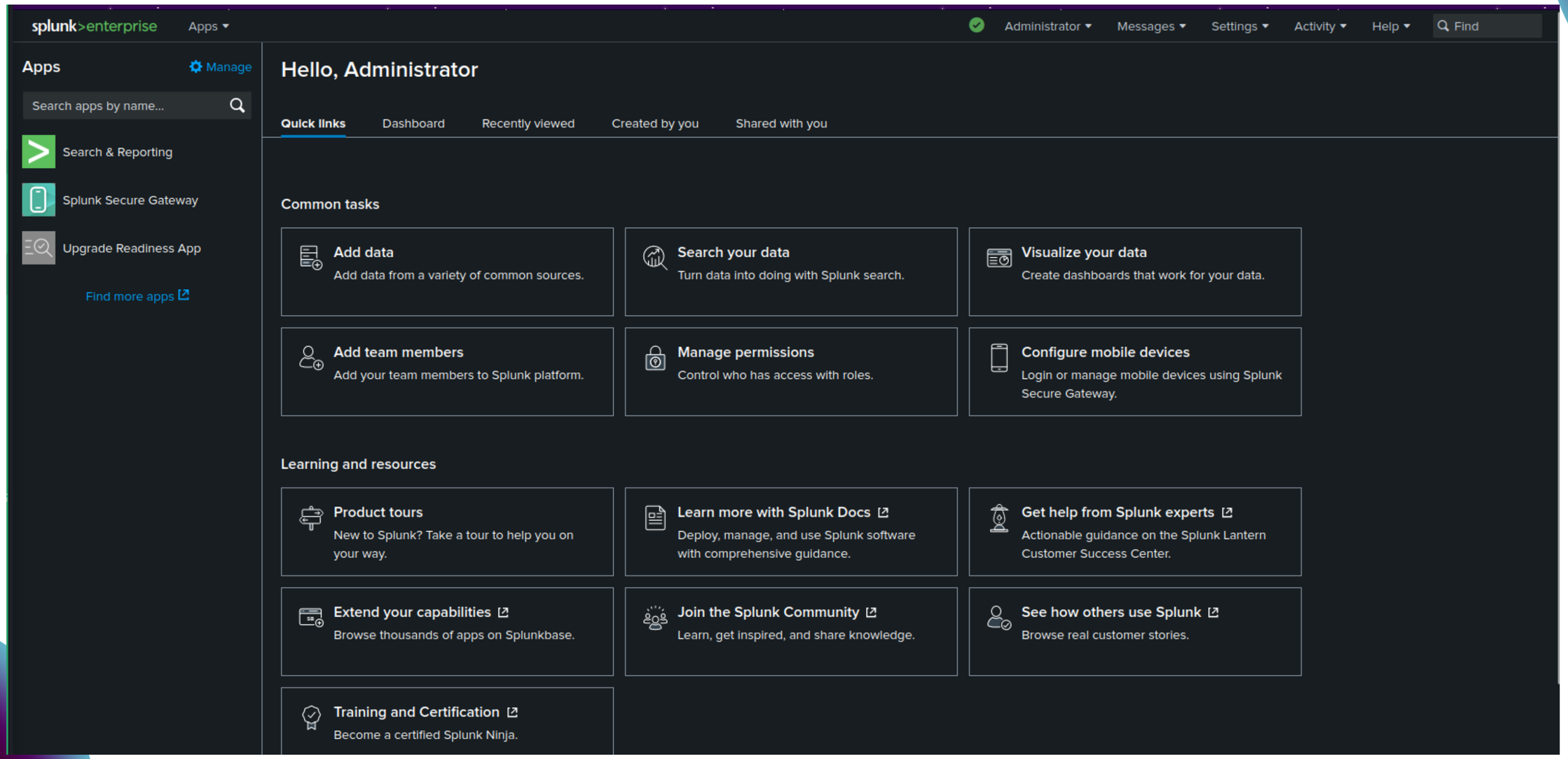
Lancement de SIEM Splunk : Comment y accéder via l'URL

Afin d'accéder à SIEM Splunk, il faut suivre l'URL appropriée après avoir lancé la commande adéquate.



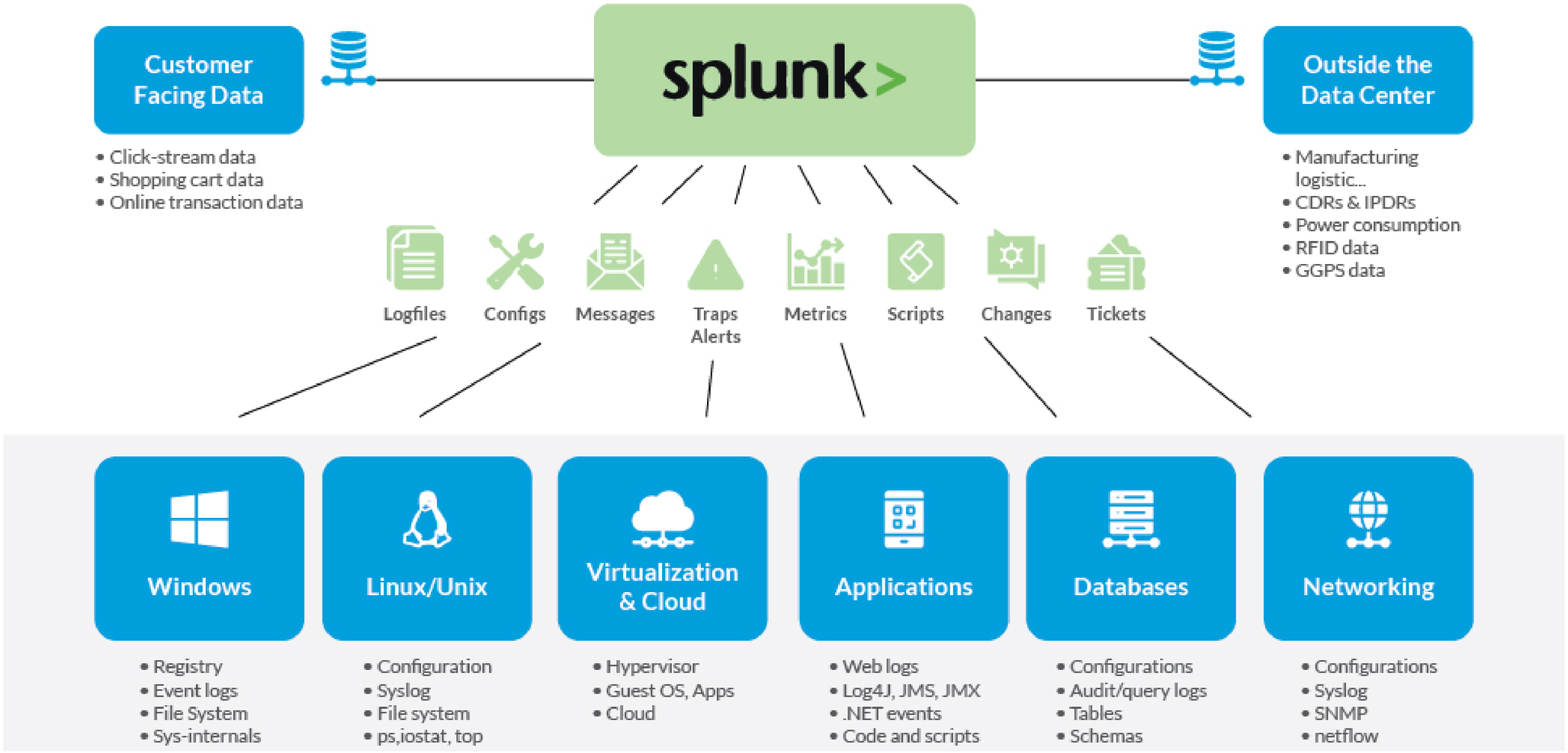
Splunk Enterprise on Linux

- SPLUNK INTERFACE



Splunk Enterprise on Linux

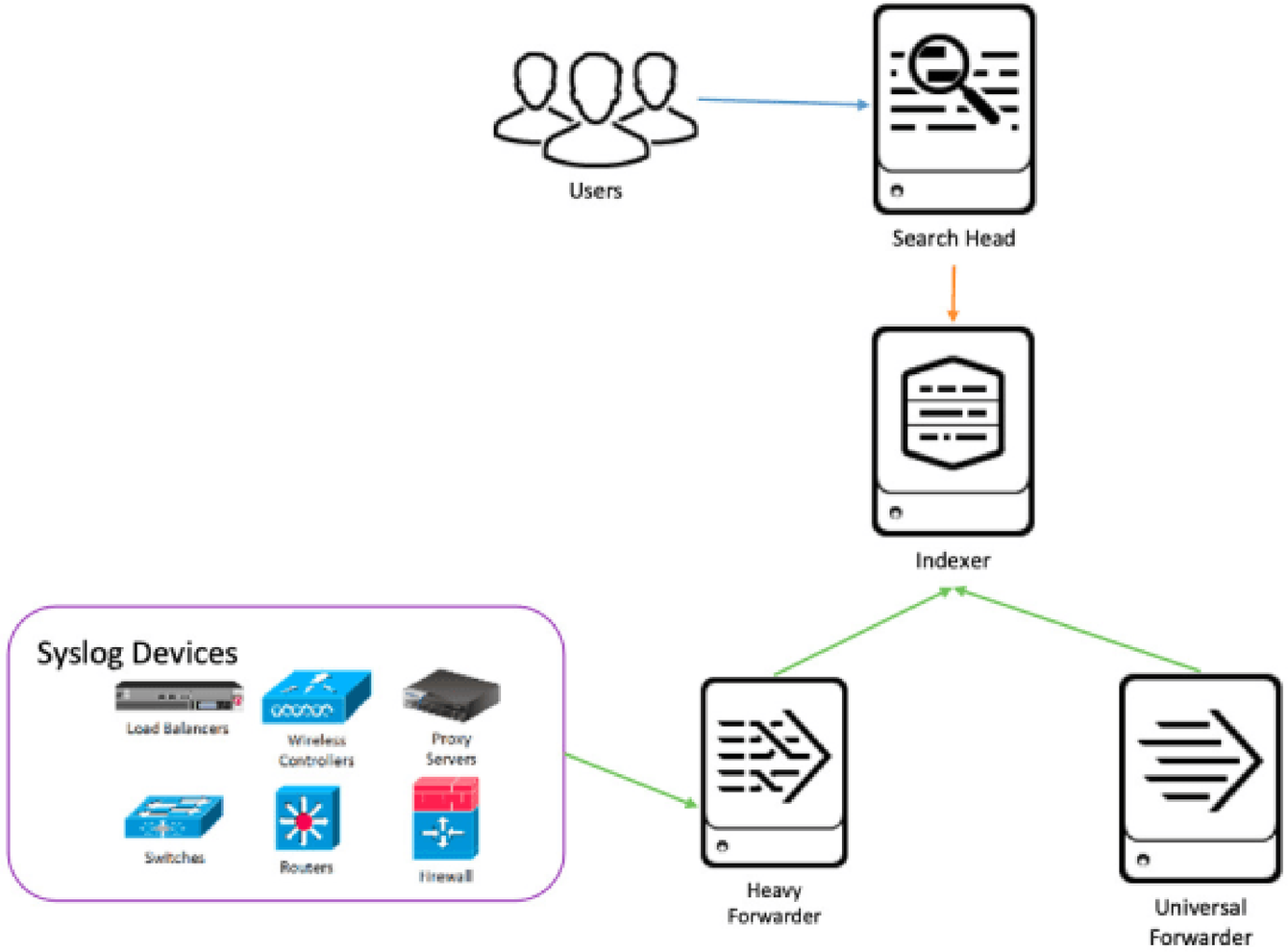
- EXPLICATION



Splunk Enterprise on Linux

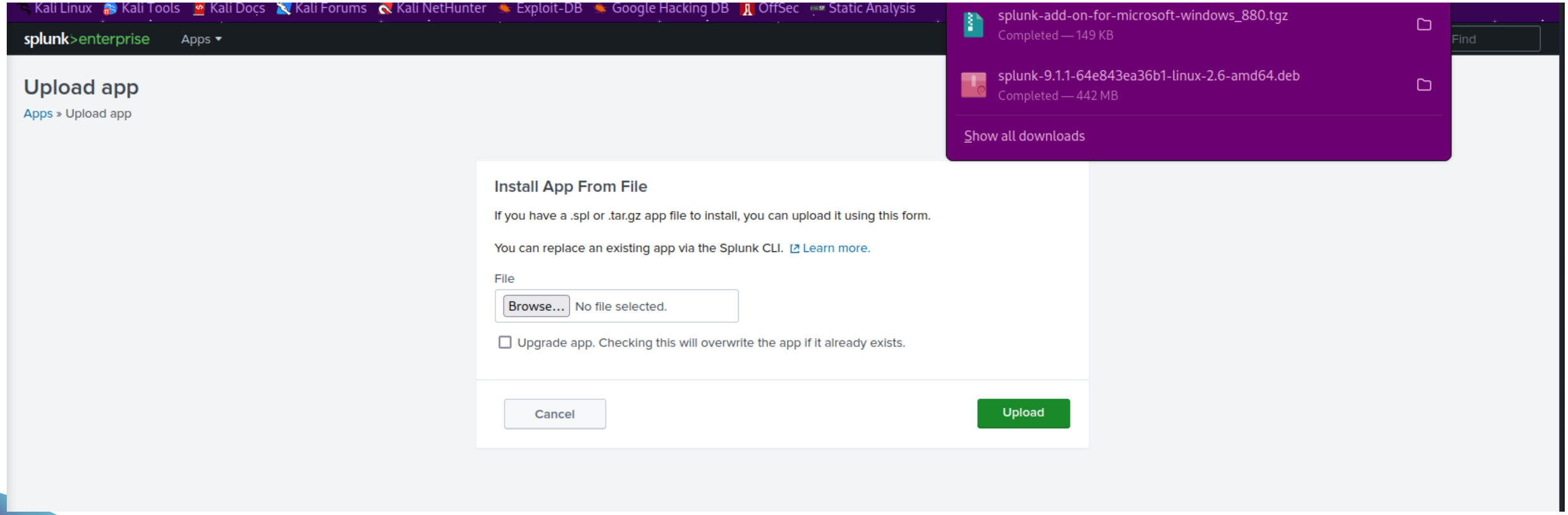
- EXPLICATION

- le Splunk Universal Forwarder agit comme un pont entre les sources de données dispersées et l'environnement Splunk, permettant ainsi la collecte, la sécurisation et la transmission efficace des données vers une plateforme centralisée pour l'analyse et la visualisation.



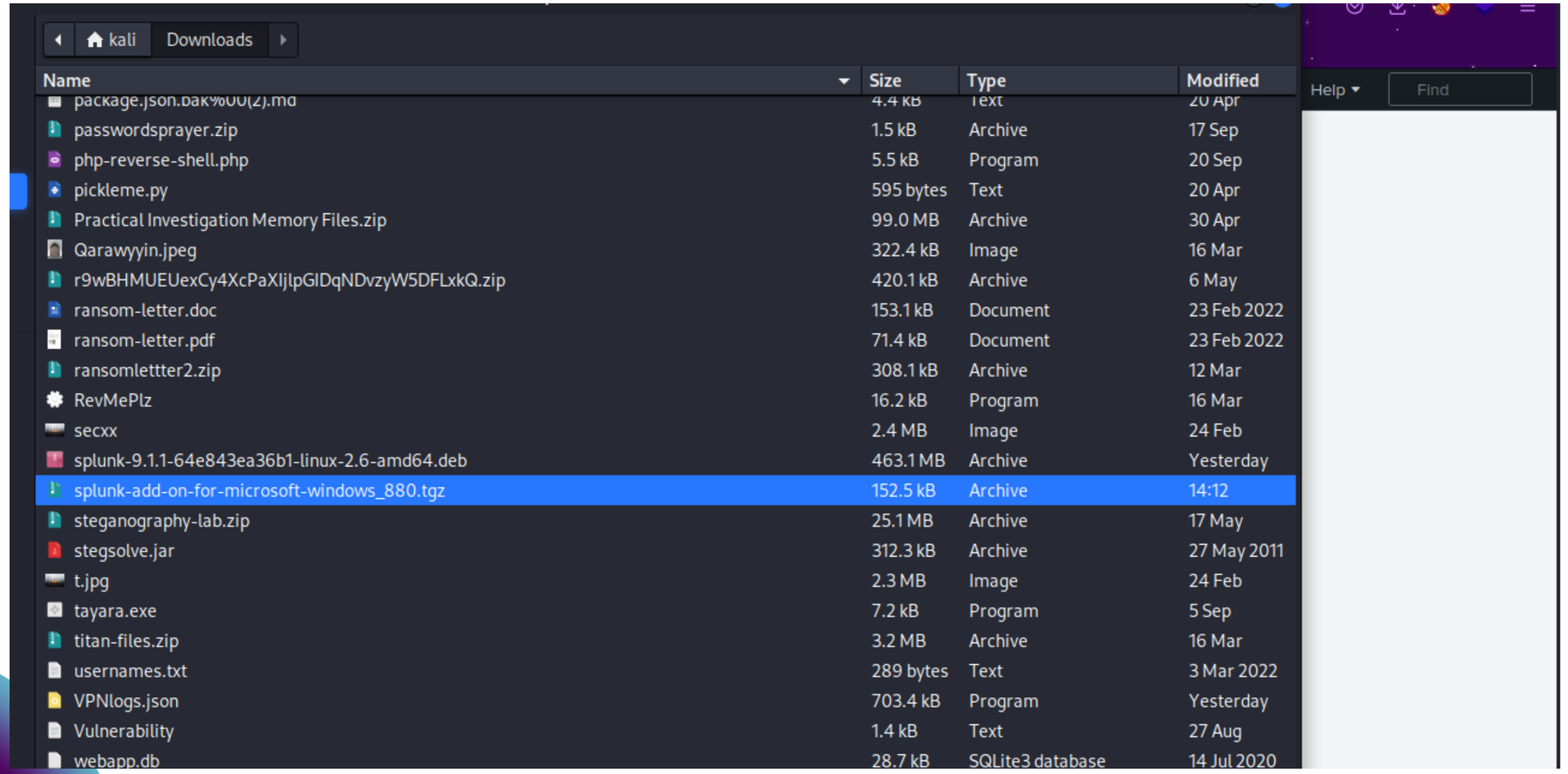
Splunk Enterprise on Linux

- DANS LA MACHINE QUI ANALYSE LES DONNES



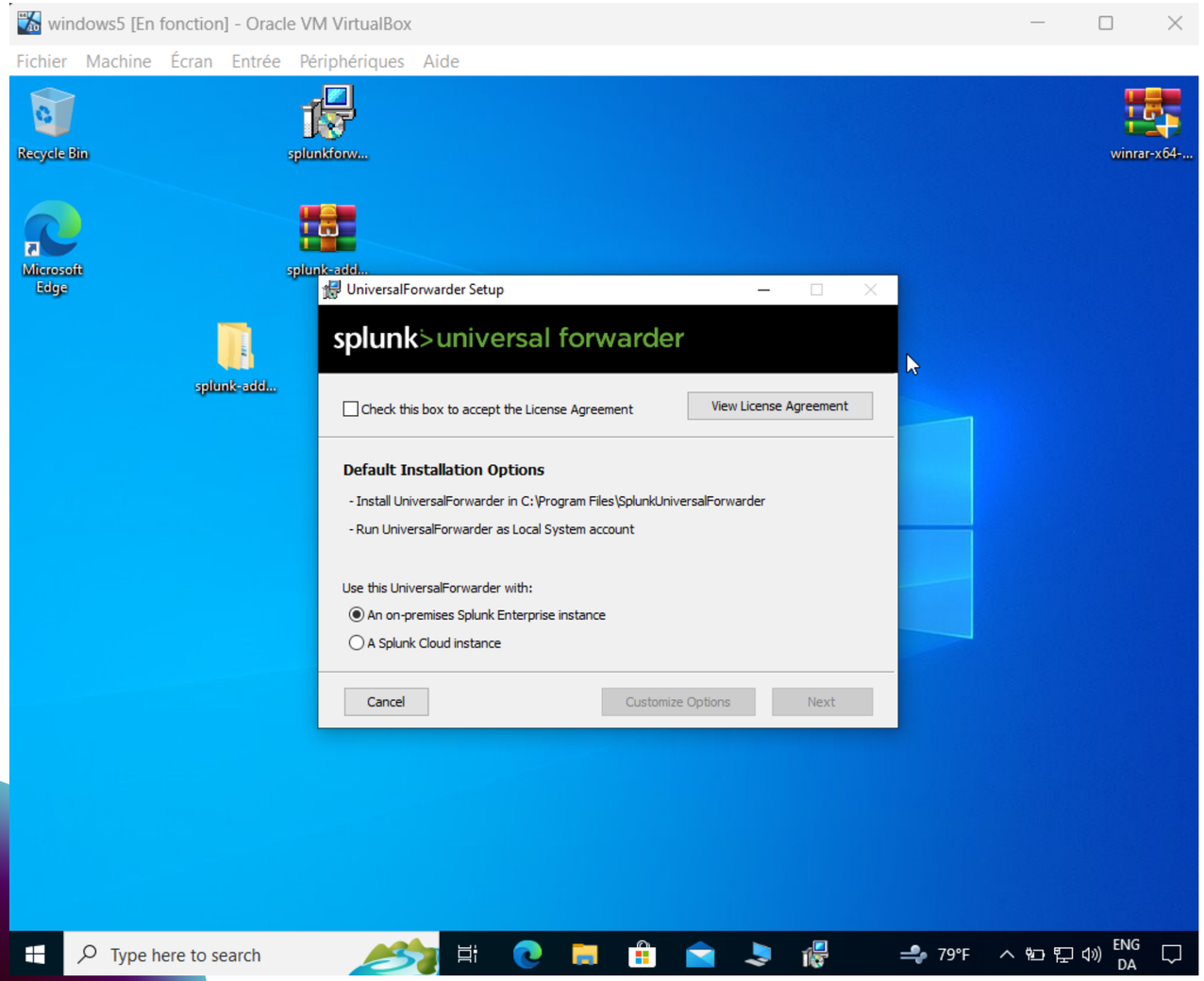
Splunk Enterprise on Linux

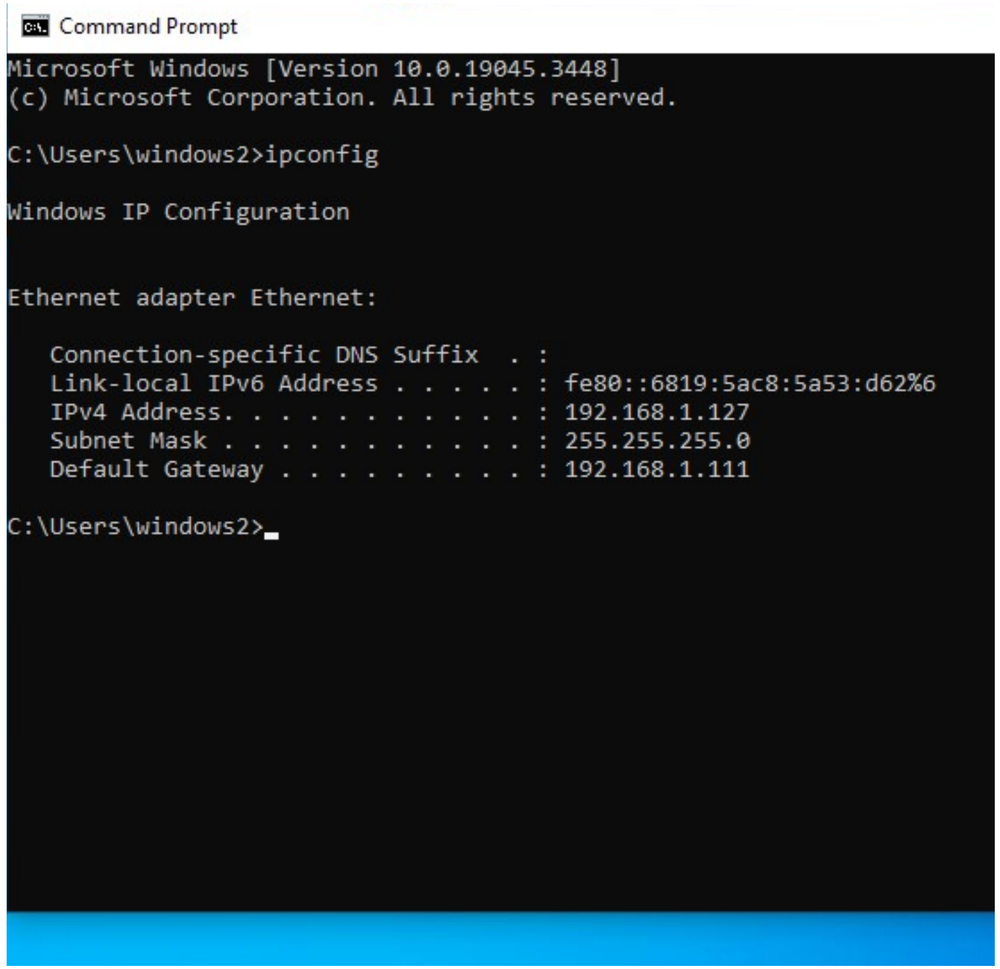
- DANS LA MACHINE QUI ANALYSE LES DONNES



Machine cible (windows 10)

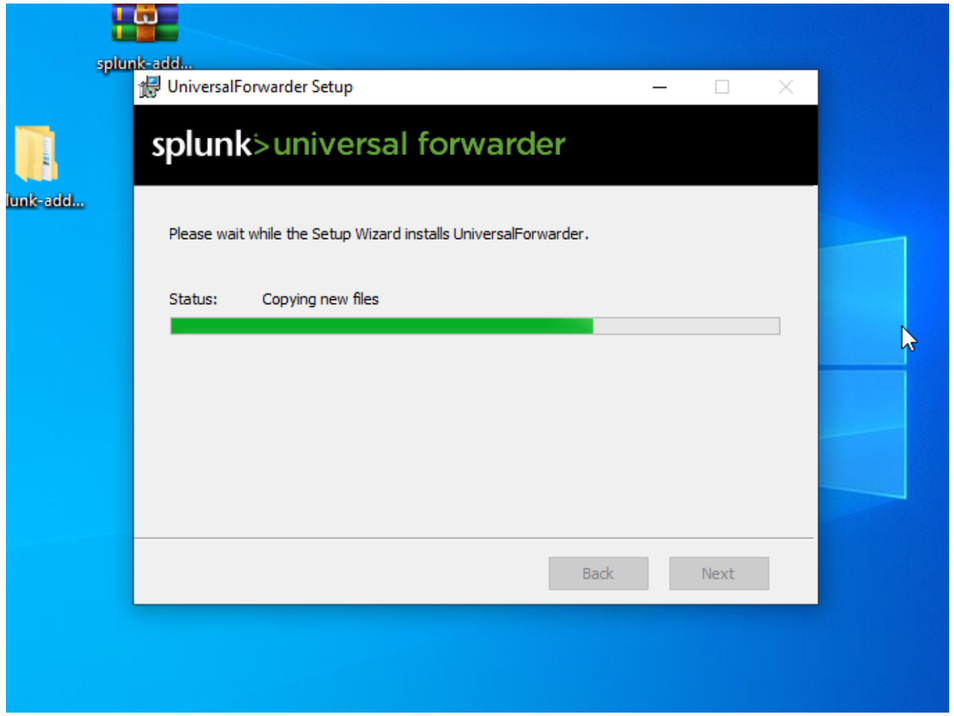
- Pour collecter les données, il faut installer le transfert universel Splunk sur la machine cible.

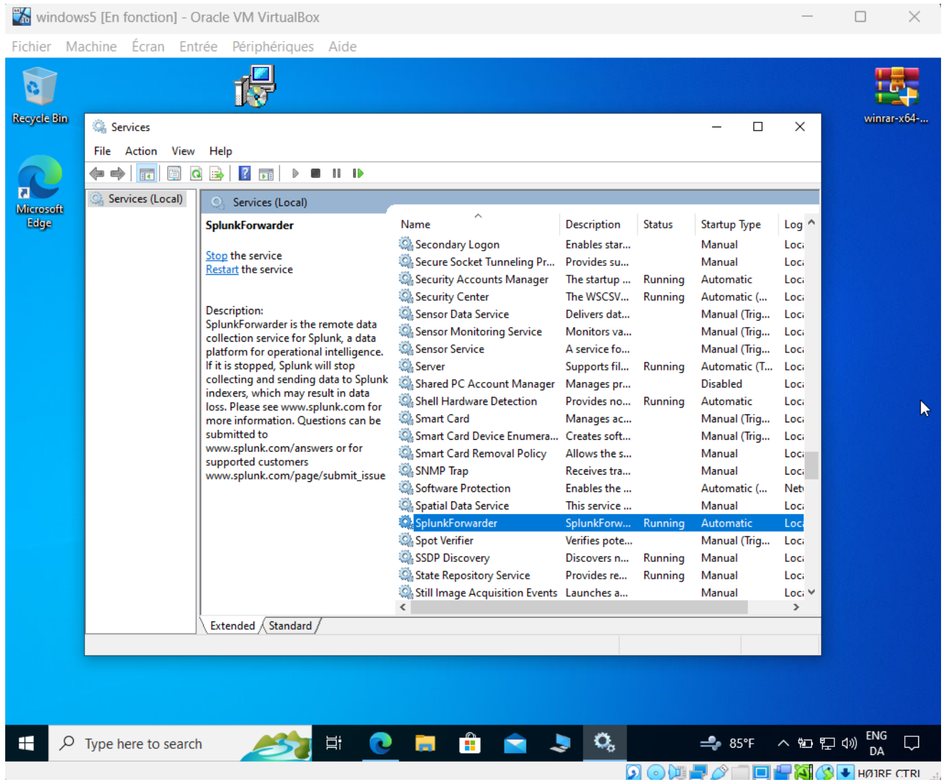


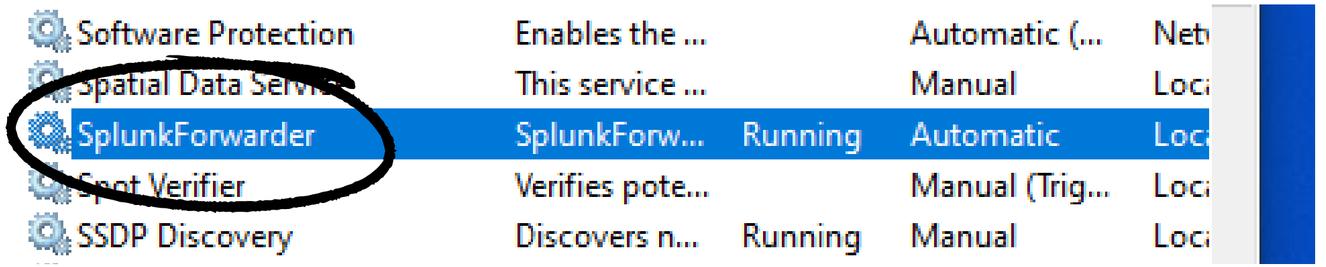


Machine cible (windows 10)

- Pour collecter les données, il faut installer le transfert universel Splunk sur la machine cible.



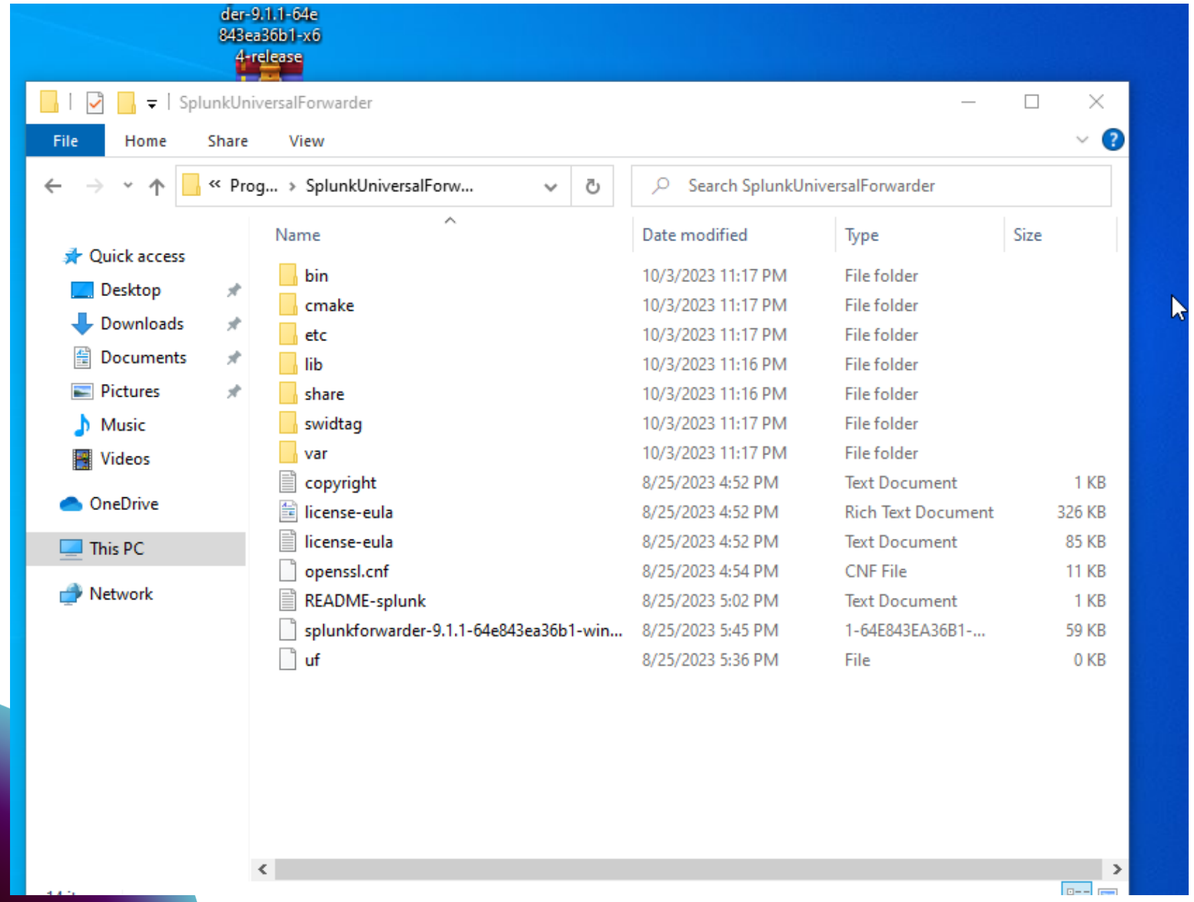


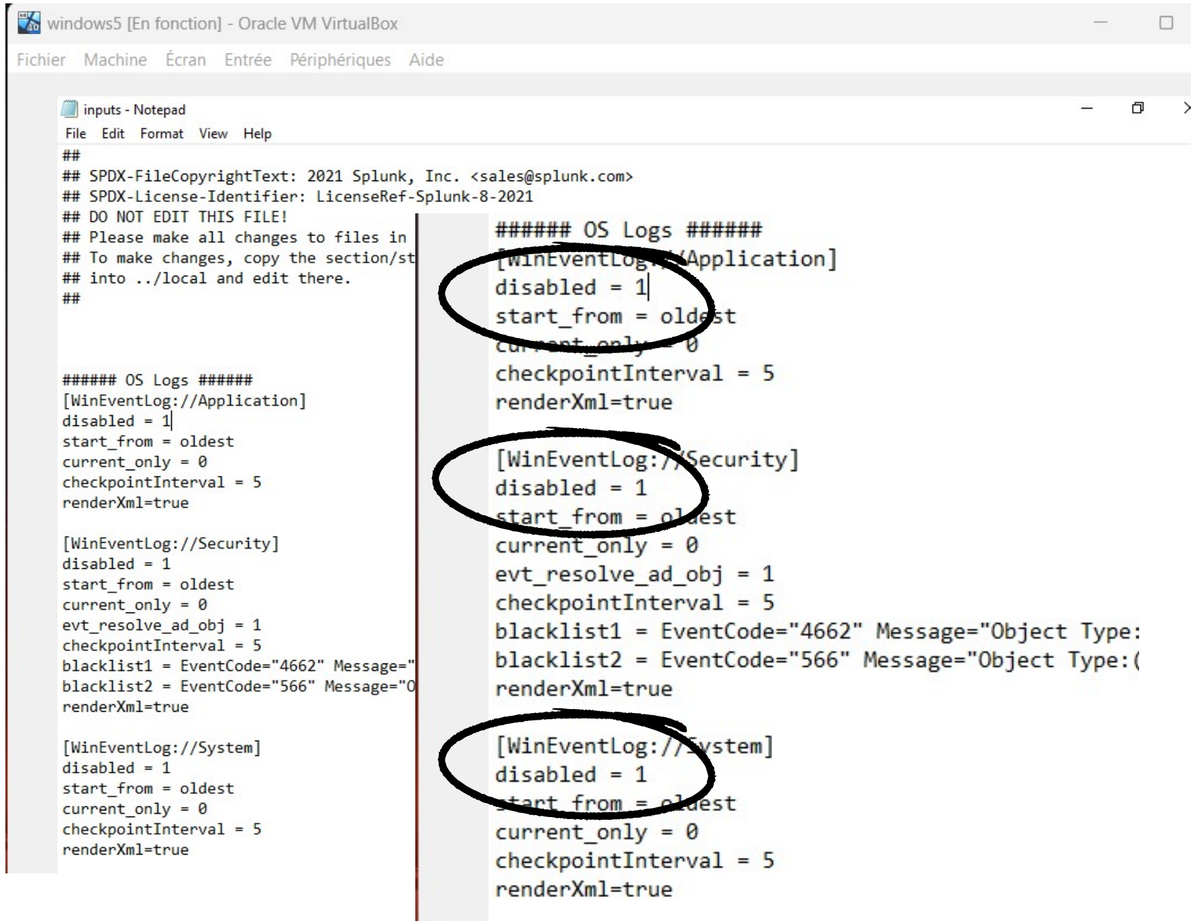


Machine cible (windows 10)

- Spécification des données transmises

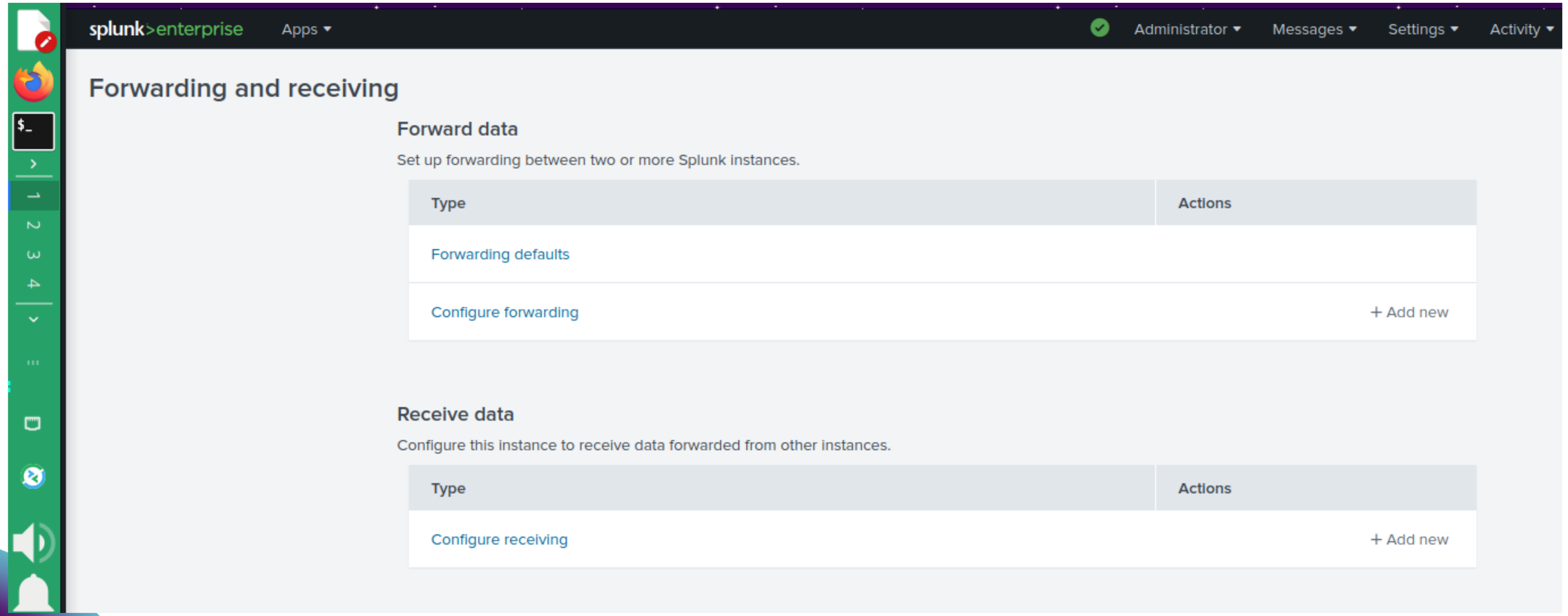
Spécification des types de données à transférer au centre Splunk Indexer pour analyse, après l'installation du Splunk Universal Forwarder.





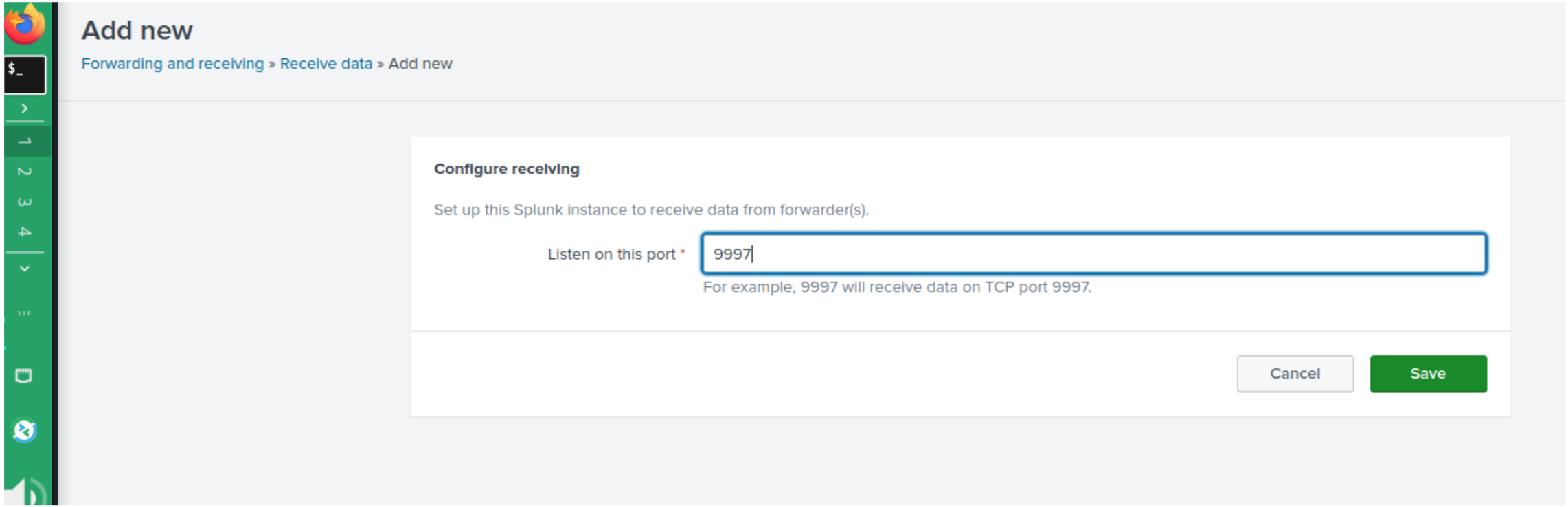
Splunk Enterprise on Linux

- DANS LA MACHINE QUI ANALYSE LES DONNES



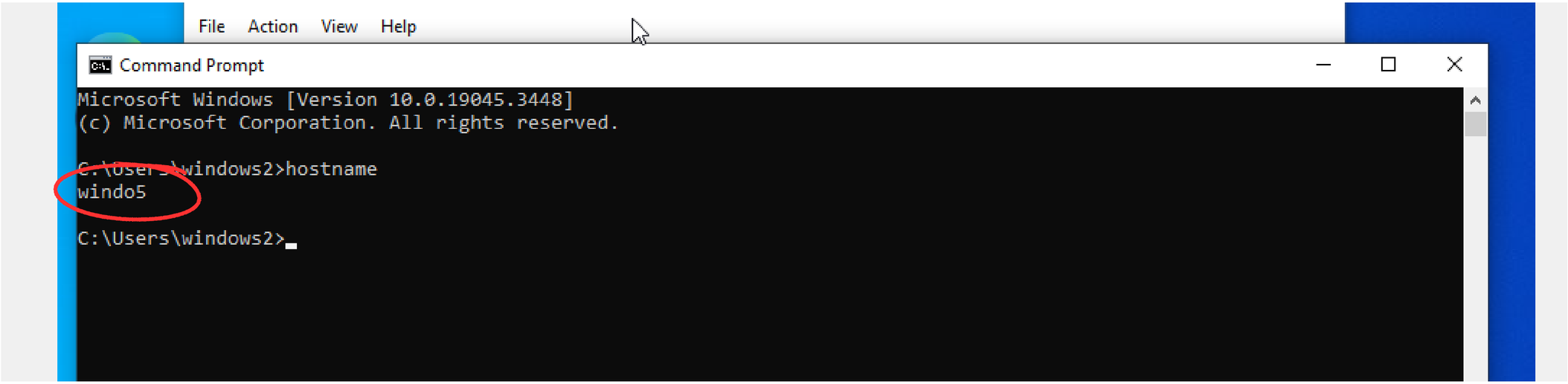
Splunk Enterprise on Linux

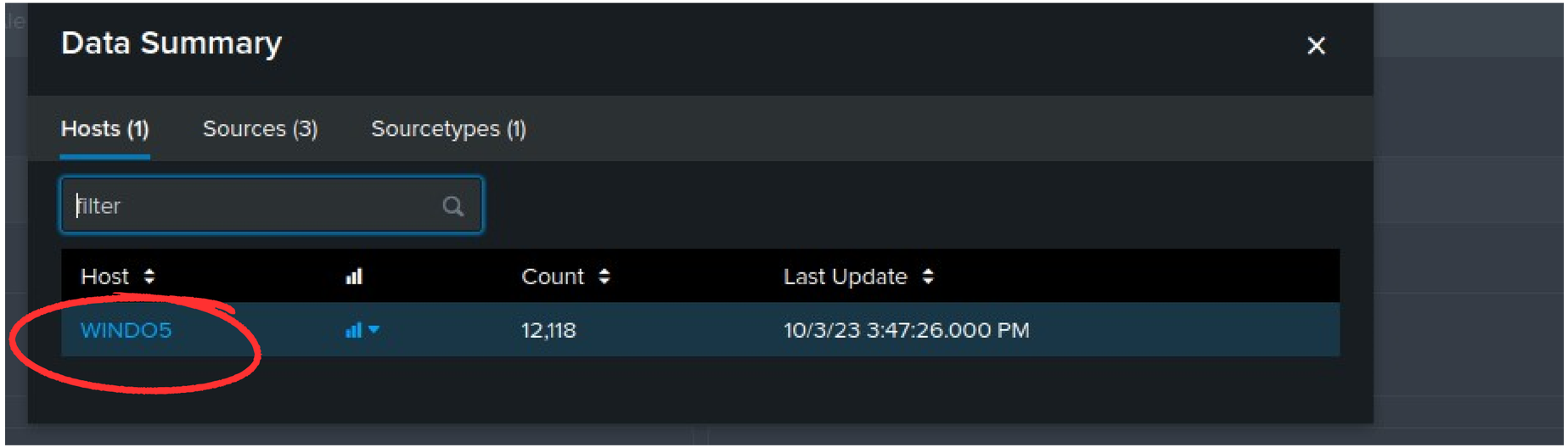
- DANS LA MACHINE QUI ANALYSE LES DONNES



Machine cible (windows 10)

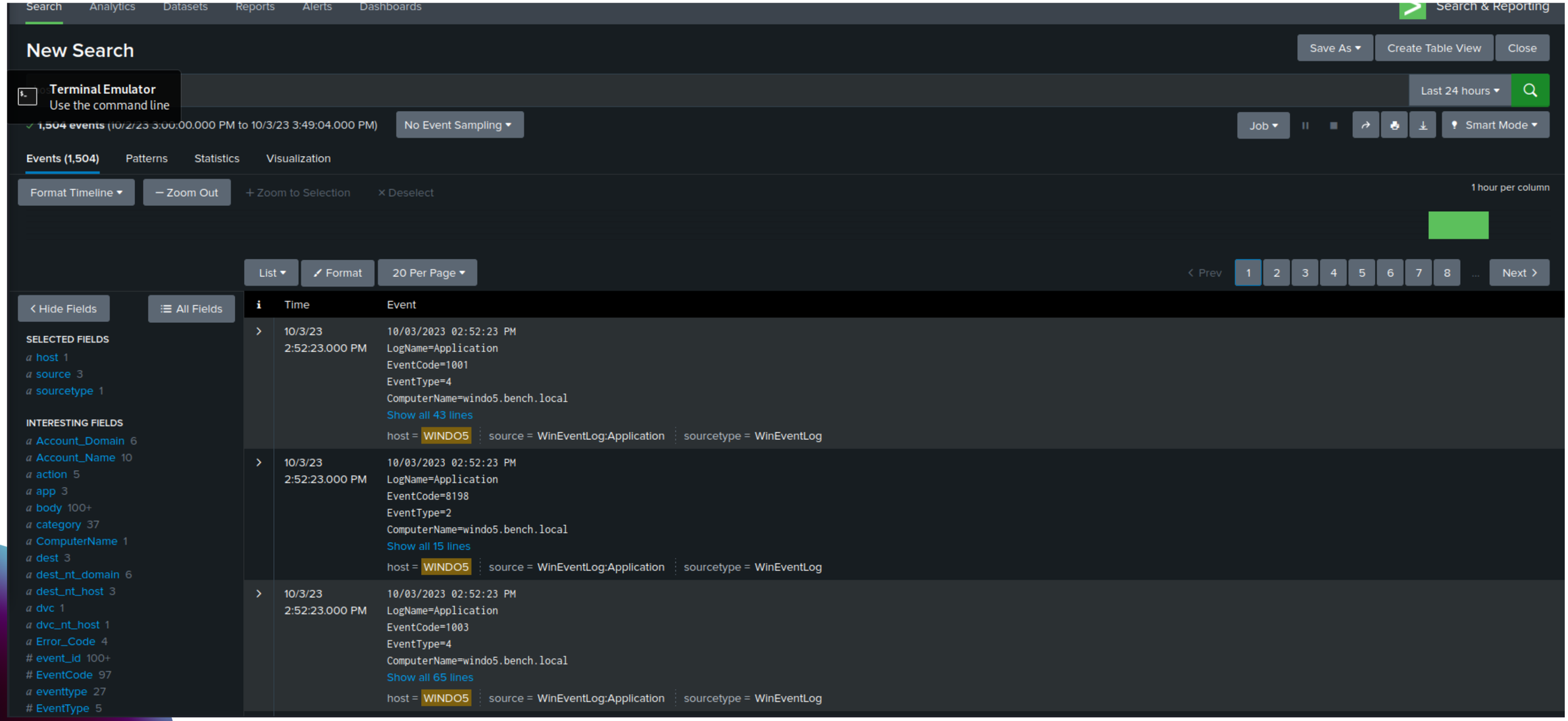
- vérification





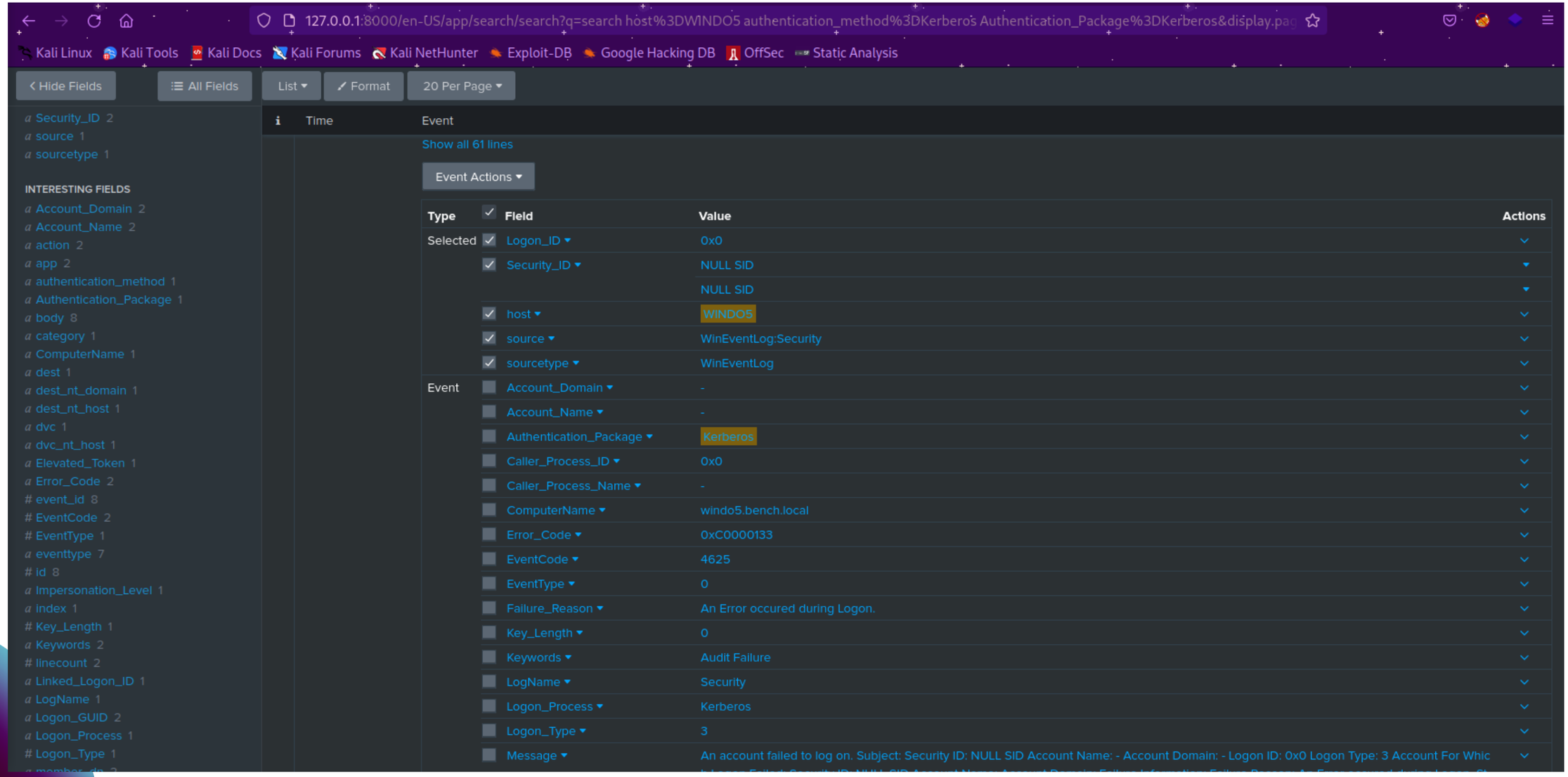
Splunk Enterprise on Linux

- RECUPEREATION DES DONNES DE LA MACHINE WINDO5



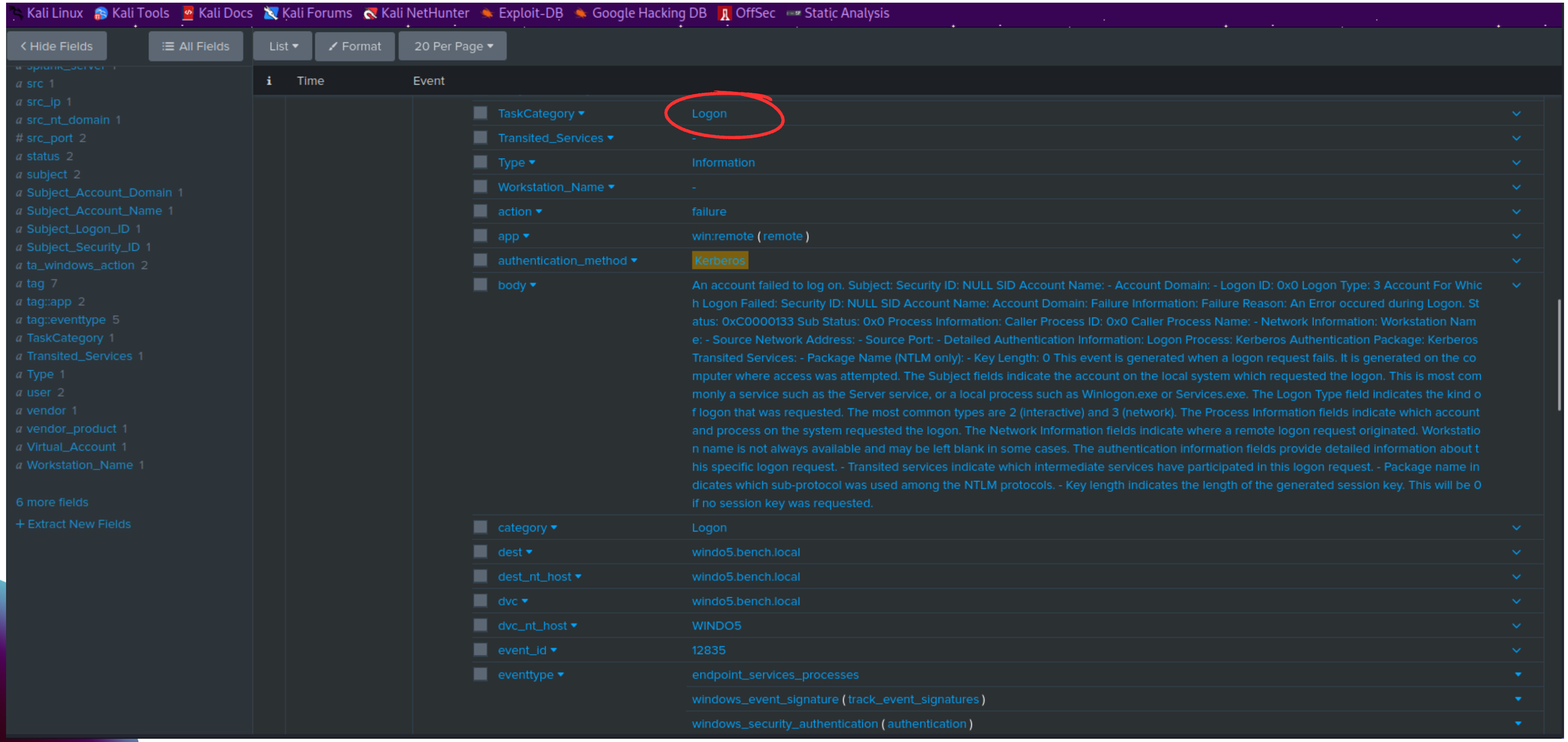
Splunk Enterprise on Linux

- RECUPEREATION DES DONNES DE LA MACHINE WINDO5



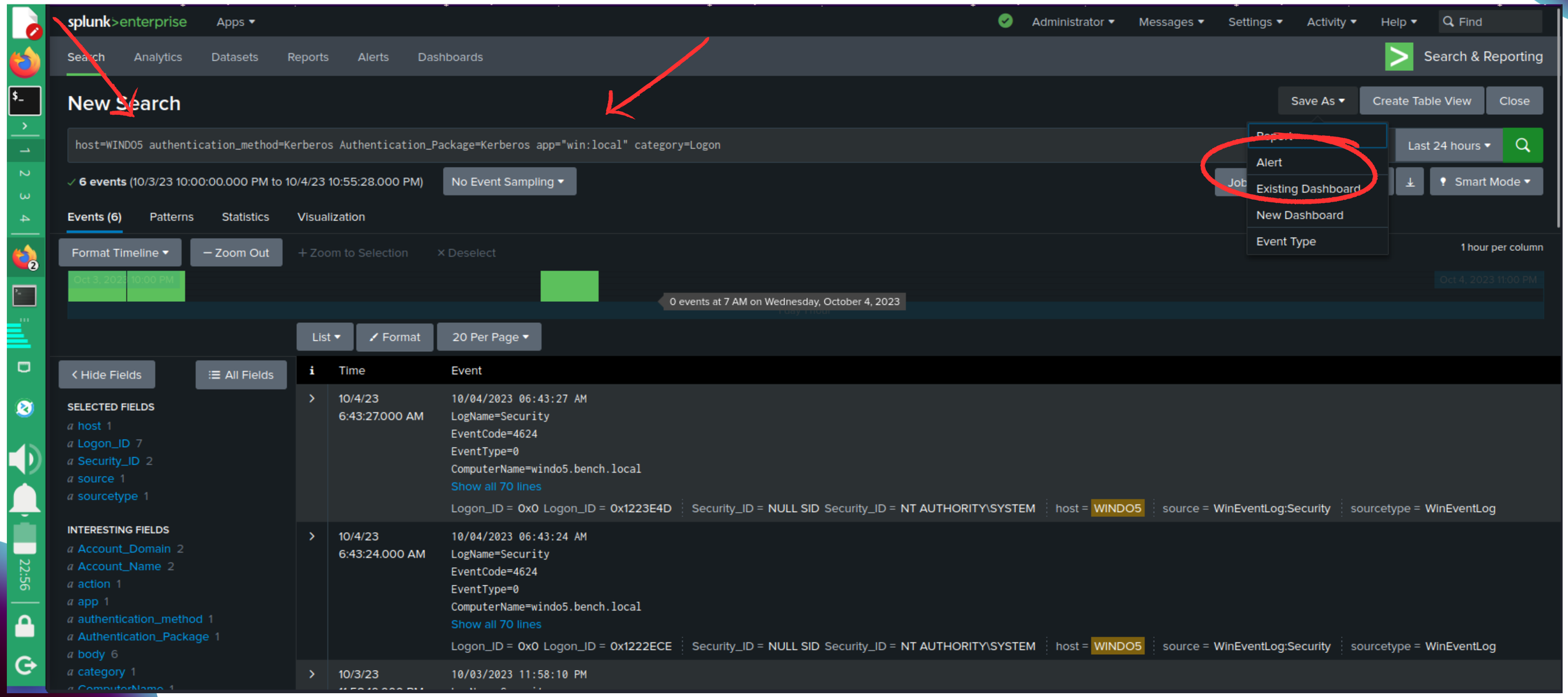
Splunk Enterprise on Linux

- RECUPEREATION DES DONNES DE LA MACHINE WINDO5



Splunk Enterprise on Linux

- RECUPEREATION DES DONNES DE LA MACHINE WINDO5

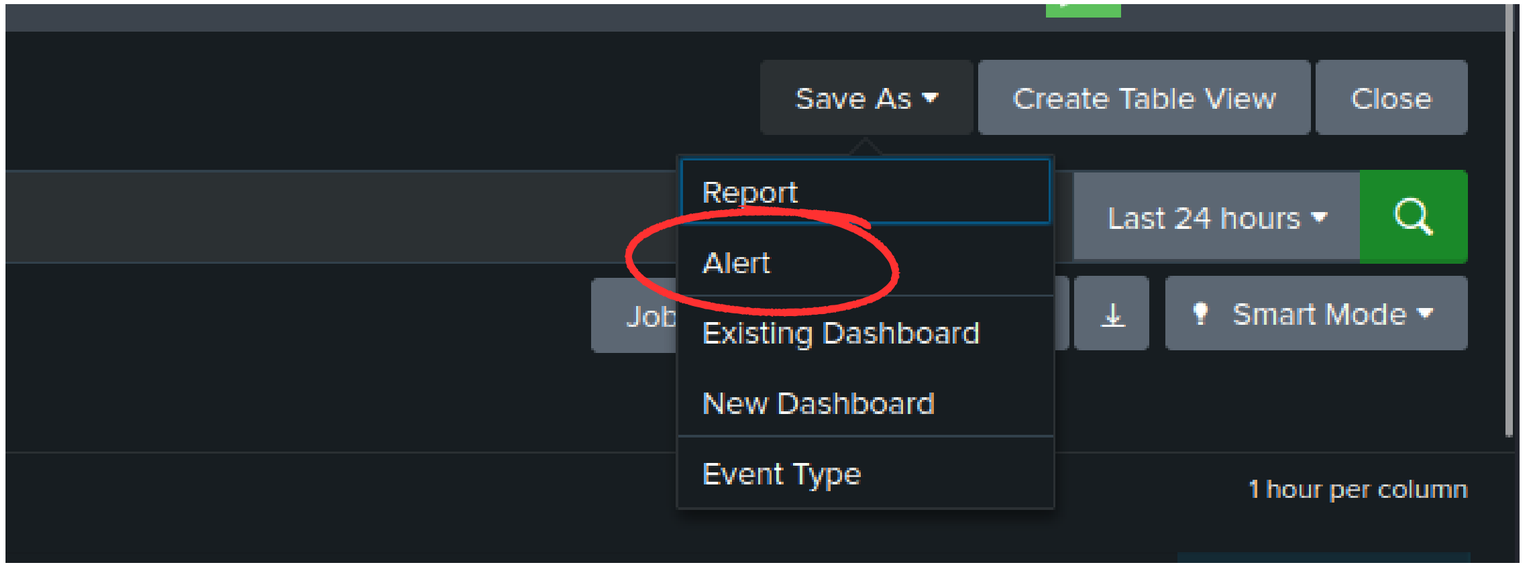


Splunk Enterprise on Linux

- CRÉATION D'UNE ALERTE POUR LES ÉCHECS DE CONNEXION

- Ce code en SPL (Splunk Processing Language) recherche dans les logs les actions de rejet (**action=reject**) et compte le nombre de rejets par adresse IP source. Ensuite, il filtre les résultats pour ne montrer que les adresses IP qui ont été rejetées au moins 5 fois. Ensuite, il utilise la commande **join** pour combiner les résultats de deux requêtes. La première requête compte le nombre de connexions rejetées, et la deuxième requête compte le nombre de connexions échouées pour chaque utilisateur. Enfin, il filtre les résultats pour ne montrer que les administrateurs qui ont eu plus de 10 connexions échouées, et envoie une alerte dans ce cas.

```splunk
index=your_index sourcetype=your_sourcetype action=reject
| stats count by src_ip
| where count>=5
| join type=left [ search index=your_index sourcetype=your_sourcetype action=fail ]
| stats count by user
| where count>=10 AND user=admin
```



MERCI POUR VOTRE ATTENTION