

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.
- Les 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

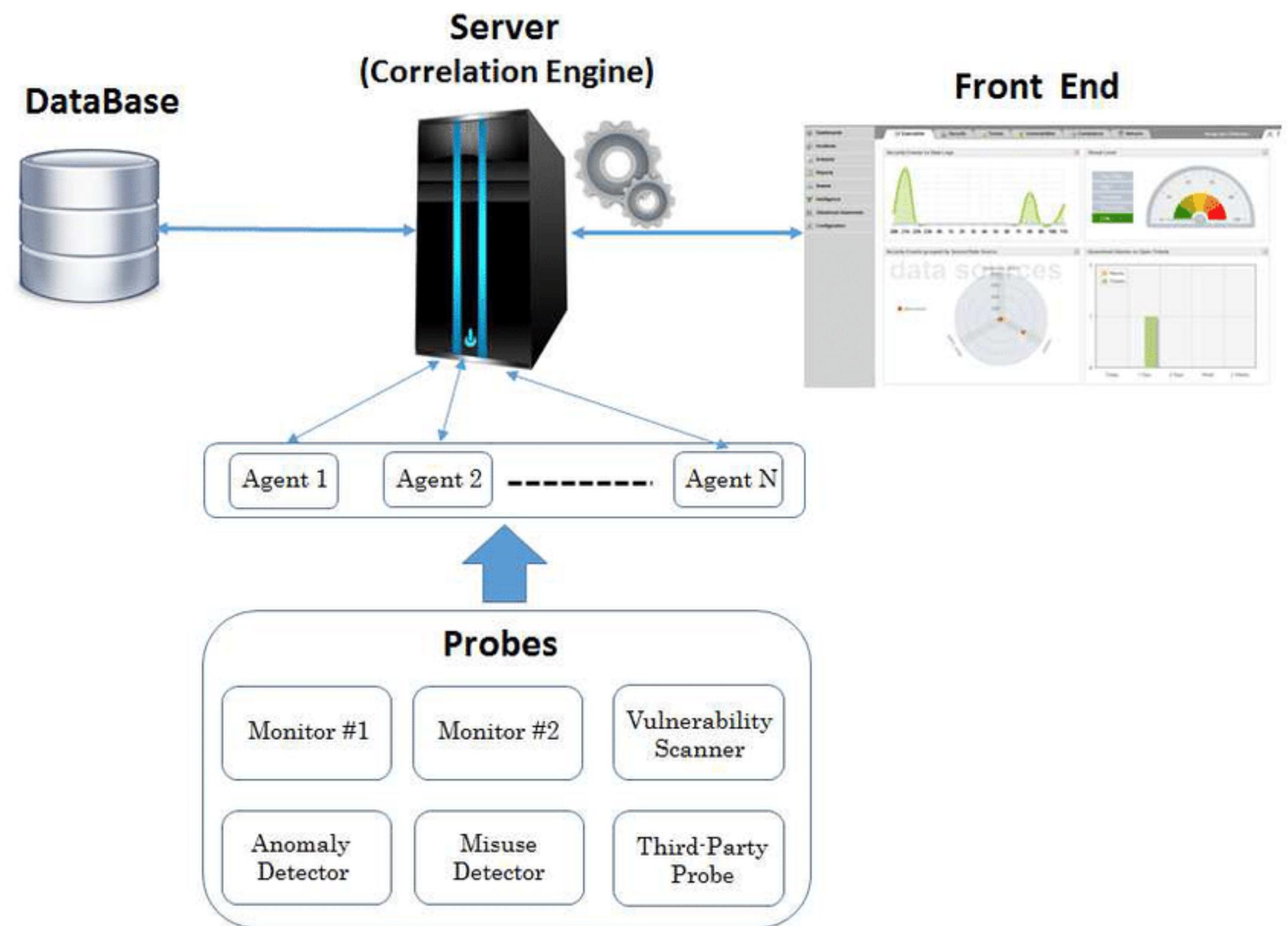
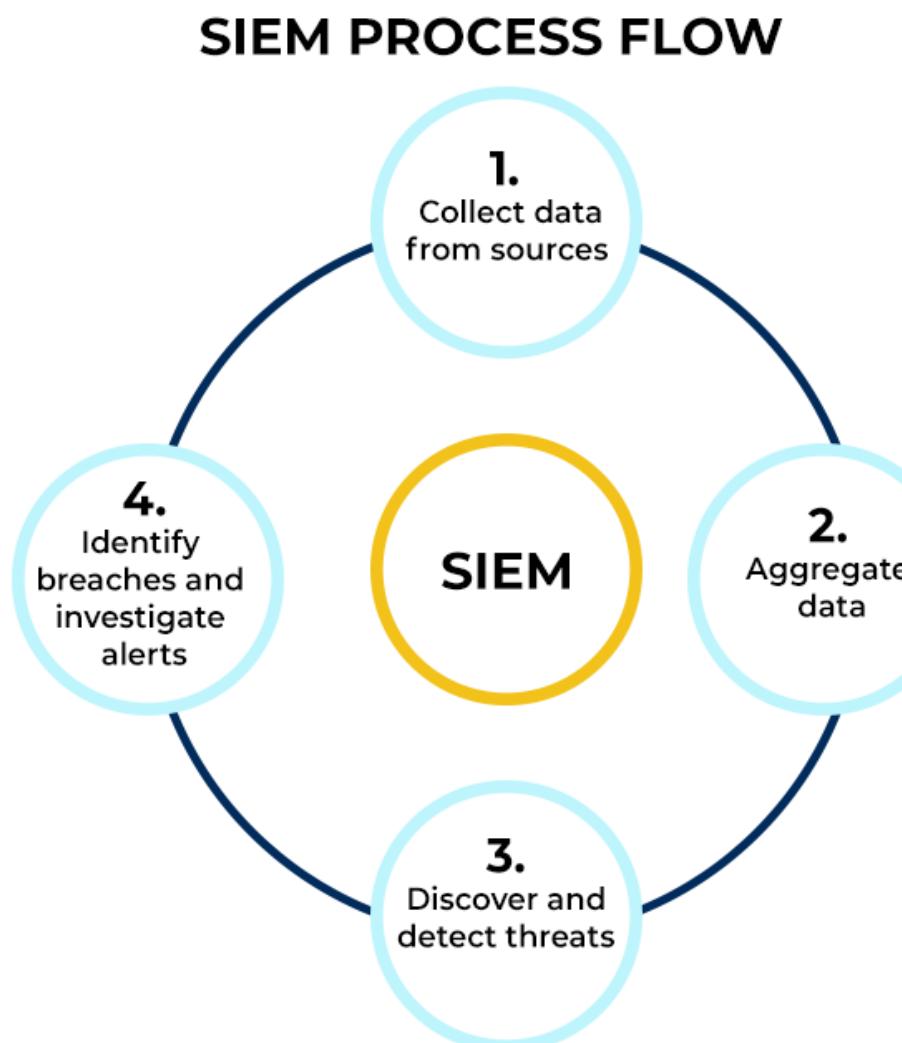
- **Elastic Security**
- **Graylog**
- **IBM QRadar**
- **Splunk**
- **InsightsIDR**

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)



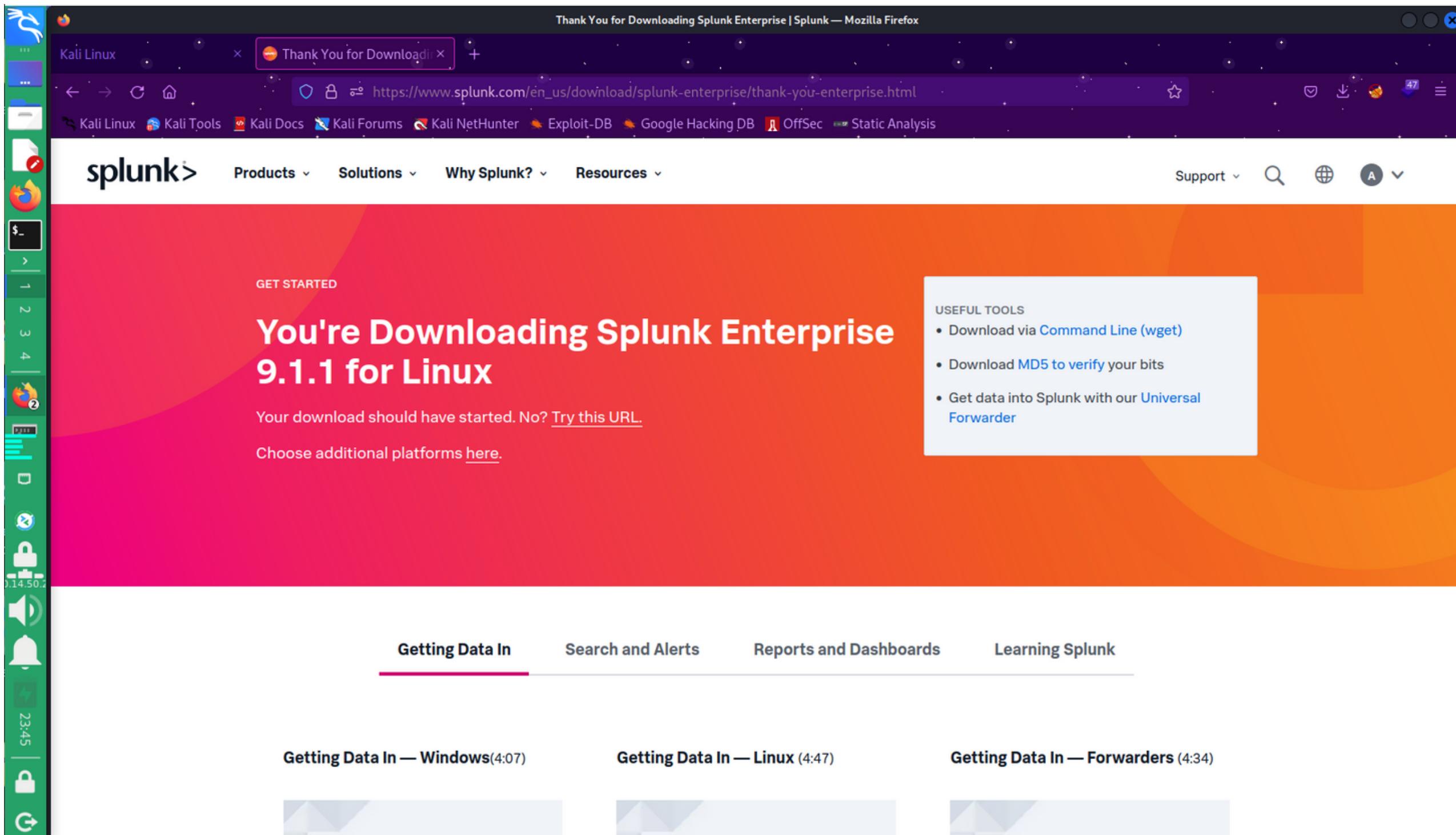
SIEM OVERVIEW



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

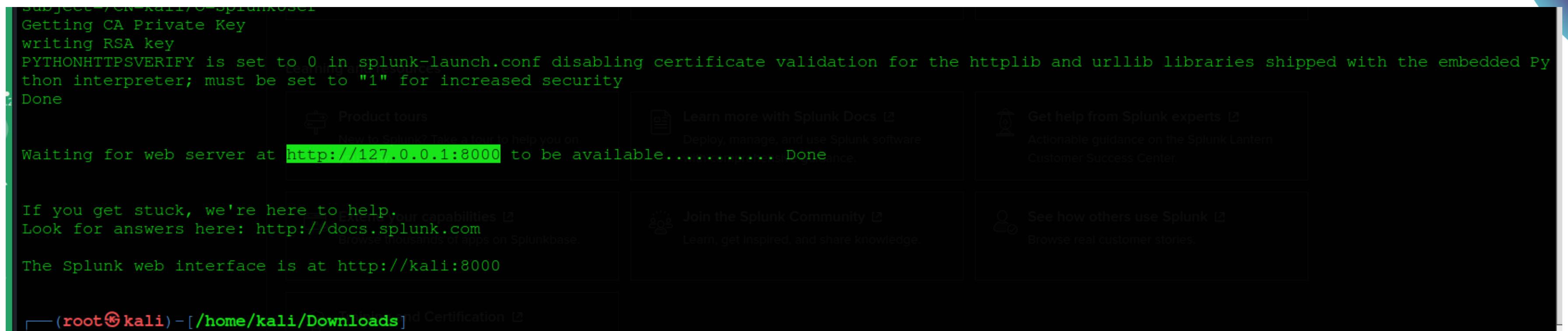
- EXEMPLE ON LINUX

```
Subject: CN=kali,O=SplunkSCL
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done

Waiting for web server at http://127.0.0.1:8000 to be available.....Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com
The Splunk web interface is at http://kali:8000

[root@kali] - [/home/kali/Downloads]
```



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.

```
[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

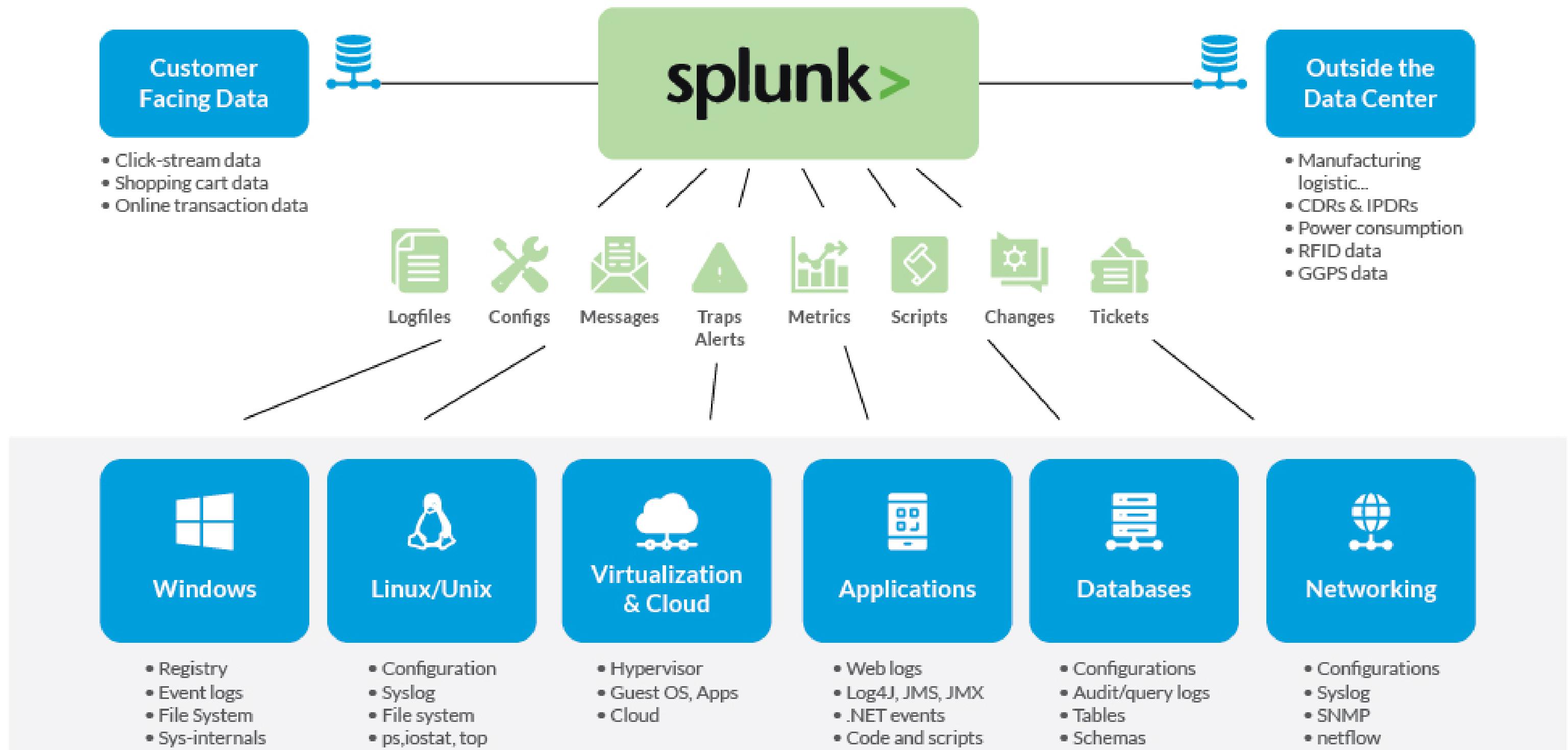
Splunk Enterprise on Linux

- SPLUNK INTERFACE

The screenshot shows the Splunk Enterprise interface on a Linux system. The top navigation bar includes the 'splunk>enterprise' logo, a 'Find' search bar, and links for 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. On the left, a sidebar titled 'Apps' lists 'Search & Reporting', 'Splunk Secure Gateway', 'Upgrade Readiness App', and a 'Find more apps' link. The main content area displays a 'Hello, Administrator' message and several 'Quick Links': 'Add data', 'Search your data', 'Visualize your data', 'Add team members', 'Manage permissions', and 'Configure mobile devices'. Below these are sections for 'Learning and resources' with links to 'Product tours', 'Learn more with Splunk Docs', 'Get help from Splunk experts', 'Extend your capabilities', 'Join the Splunk Community', 'See how others use Splunk', and 'Training and Certification'.

Splunk Enterprise on Linux

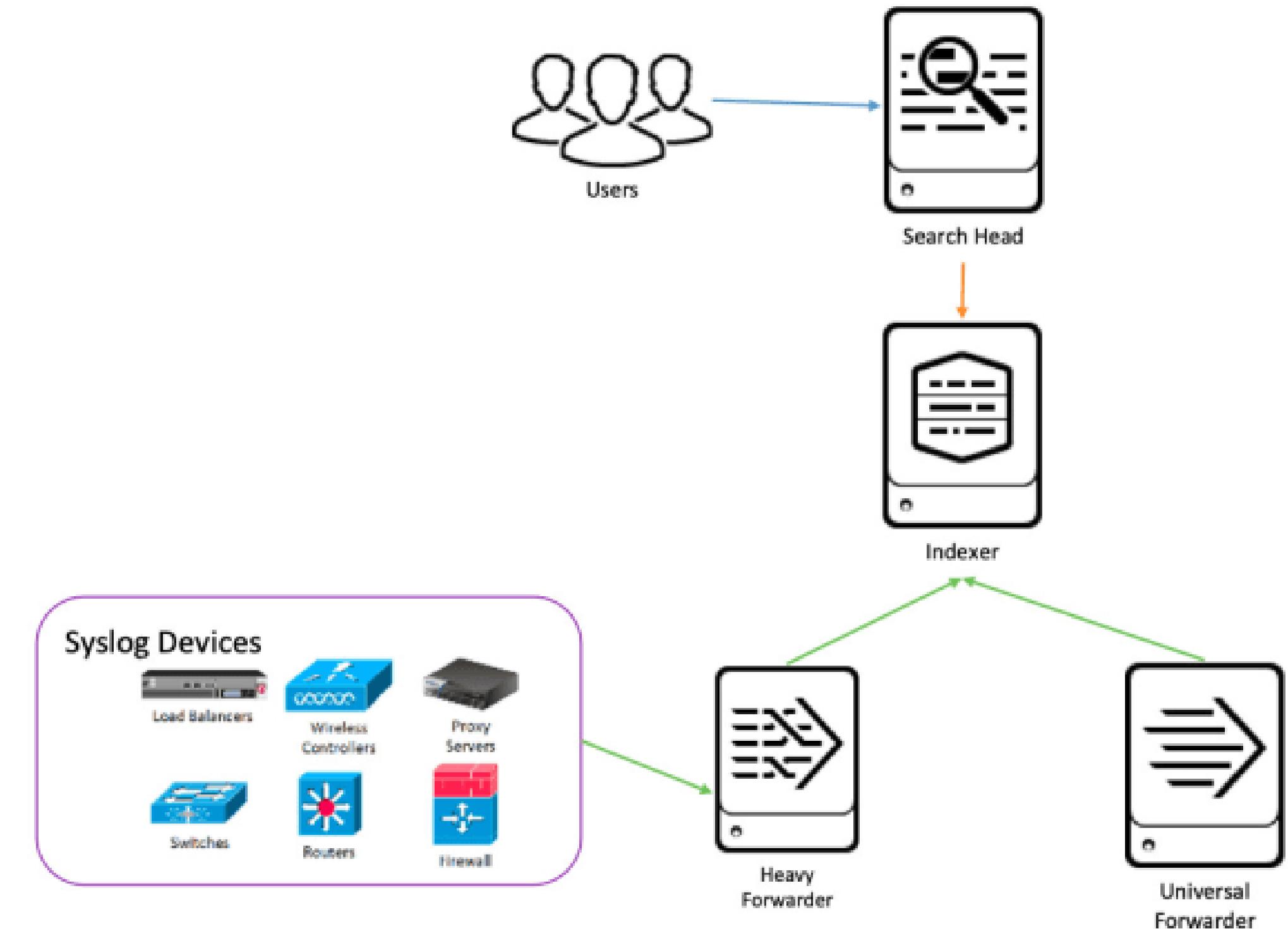
- EXPLICATION



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.



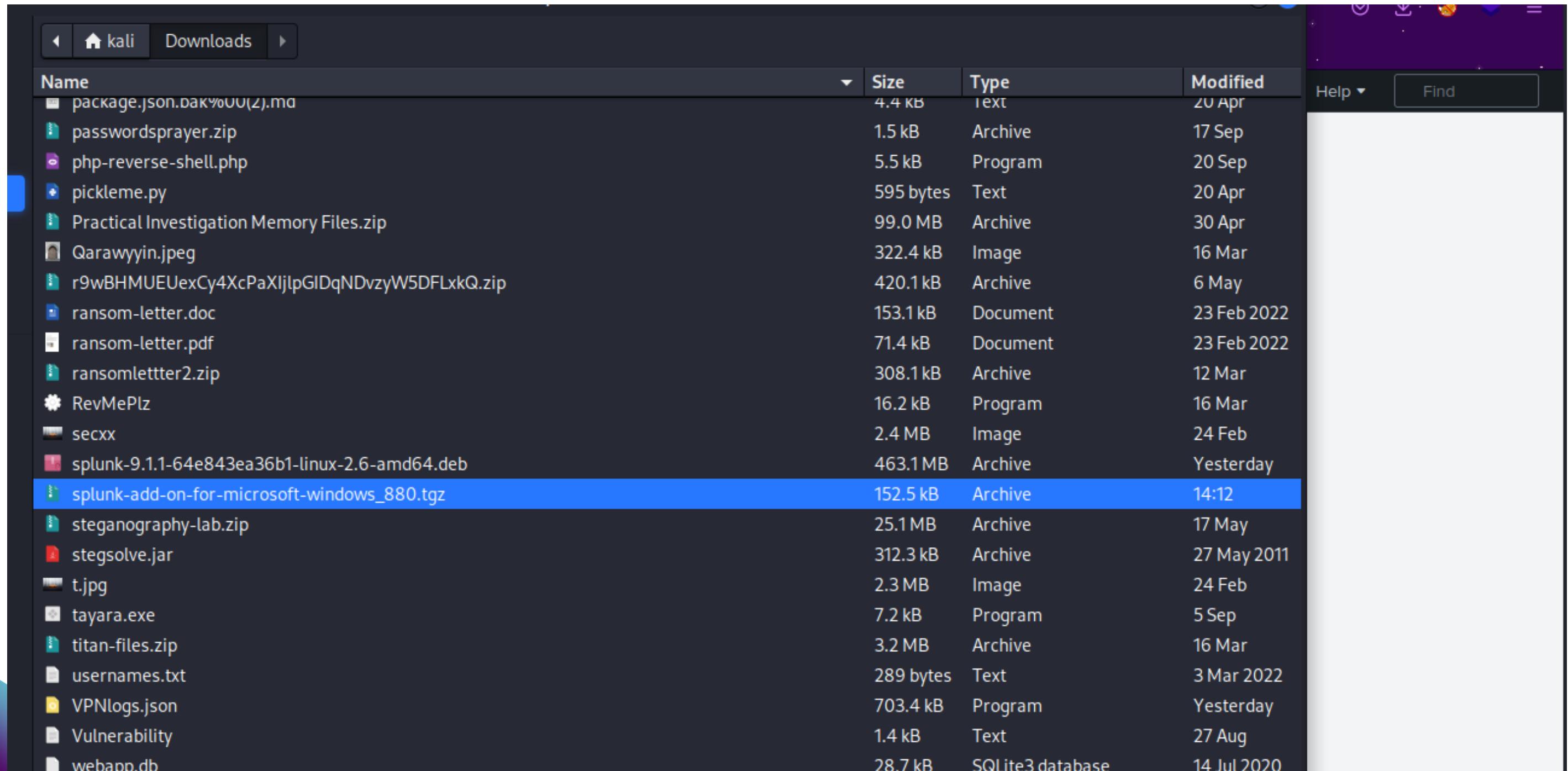
Splunk Enterprise on Linux

- DANS LA MACHINE QUI ANALYSE LES DONNES

The screenshot shows the Splunk Enterprise interface on a Kali Linux desktop. The top navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Static Analysis, and a user account icon. The main menu has items for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Static Analysis, and Apps. The Apps menu is currently selected, showing a sub-menu with 'splunk>enterprise' and 'Upload app'. The 'Upload app' screen displays a form titled 'Install App From File' with instructions for uploading .spl or .tar.gz files. It includes a 'Browse...' button, a file selection field showing 'No file selected.', and a checkbox for upgrading an existing app. Below the form are 'Cancel' and 'Upload' buttons. To the right, a sidebar shows a download history with two entries: 'splunk-add-on-for-microsoft-windows_880.tgz' (Completed — 149 KB) and 'splunk-9.1.1-64e843ea36b1-linux-2.6-amd64.deb' (Completed — 442 MB). A 'Show all downloads' link is also present.

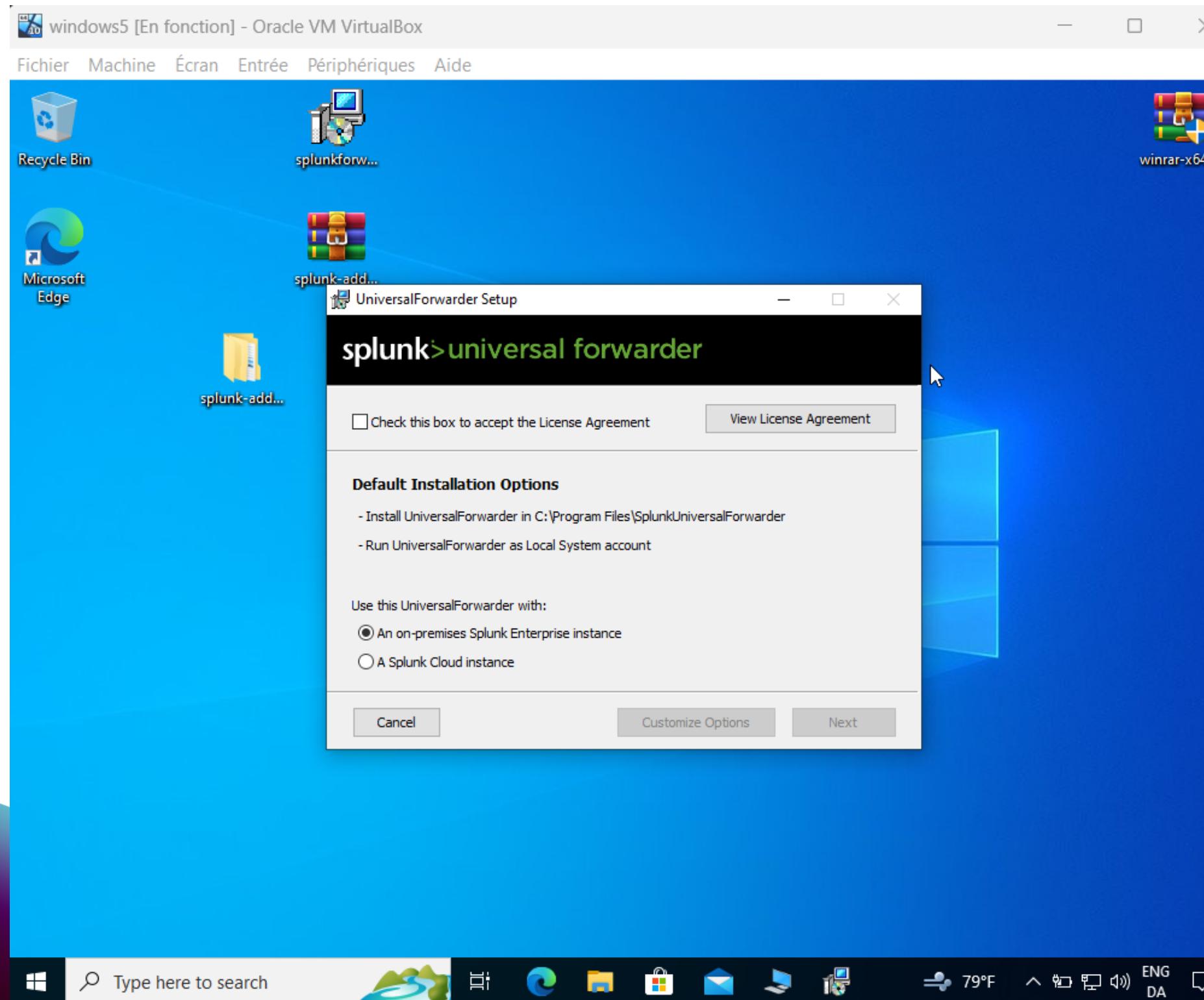
Splunk Enterprise on Linux

- 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.



```
Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\windows2>ipconfig

Windows IP Configuration

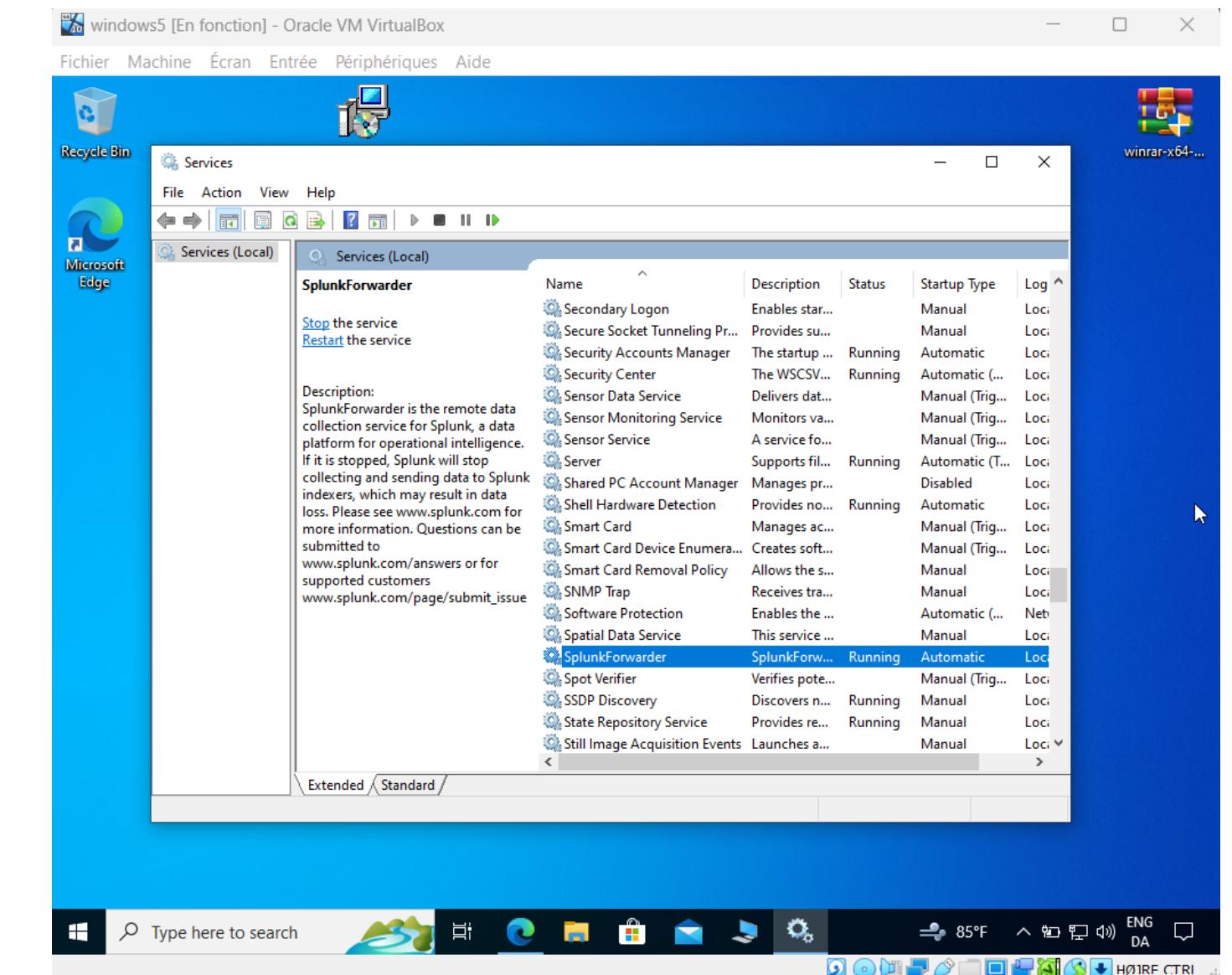
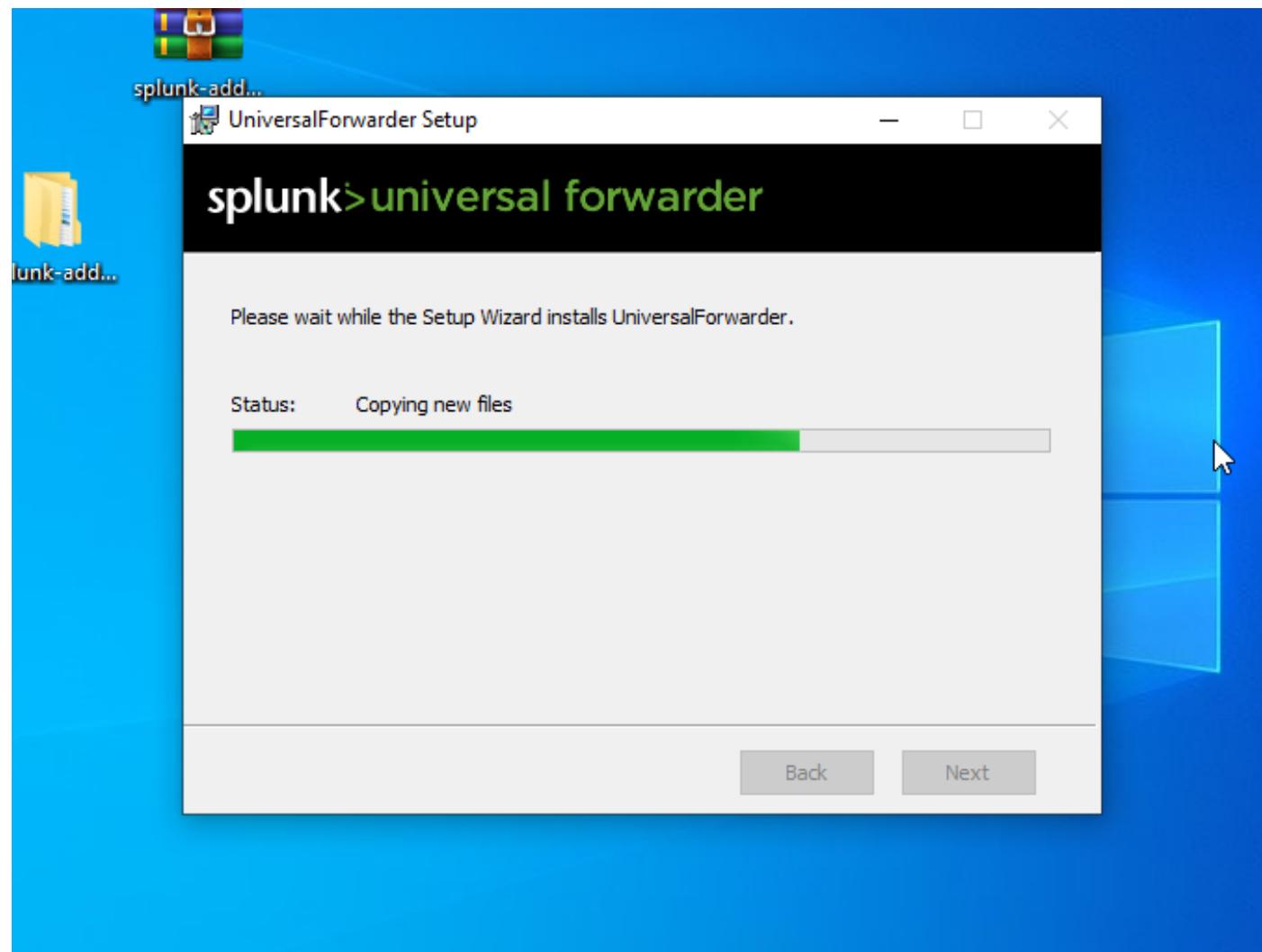
Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . . . . .
  Link-local IPv6 Address . . . . . fe80::6819:5ac8:5a53:d62%6
  IPv4 Address . . . . . 192.168.1.127
  Subnet Mask . . . . . 255.255.255.0
  Default Gateway . . . . . 192.168.1.111

C:\Users\windows2>
```

Machine cible (windows 10)

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

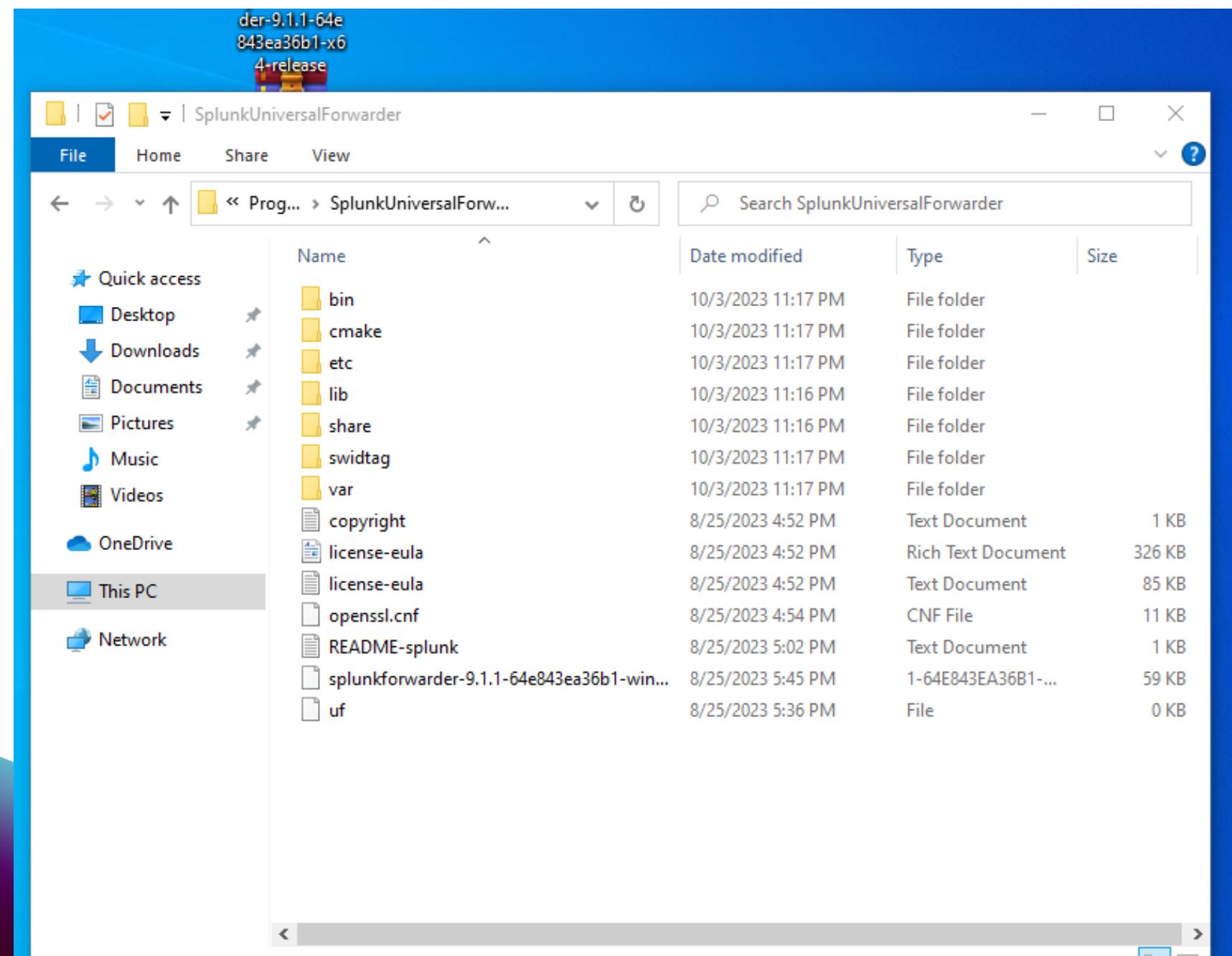


Software Protection	Enables the ...	Automatic (...)	Netw...
Spatial Data Service	This service ...	Manual	Loca...
SplunkForwarder	SplunkForw...	Running	Automatic
Spot Verifier	Verifies pote...	Manual (Trig...)	Loca...
SSDP Discovery	Discovers n...	Running	Manual

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.



The screenshot shows a Notepad window titled "inputs - Notepad" with the following configuration file content:

```
## SPDX-FileCopyrightText: 2021 Splunk, Inc. <sales@splunk.com>
## SPDX-License-Identifier: LicenseRef-Splunk-8-2021
## DO NOT EDIT THIS FILE!
## Please make all changes to files in
## To make changes, copy the section/st
## into ../local and edit there.
## 

##### OS Logs #####
[WinEventLog://Application]
disabled = 1
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=true

[WinEventLog://Security]
disabled = 1
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=true

[WinEventLog://System]
disabled = 1
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=true
```

Three sections of the configuration file are circled with black ovals:

- [WinEventLog://Application]
- [WinEventLog://Security]
- [WinEventLog://System]

Splunk Enterprise on Linux

- DANS LA MACHINE QUI ANALYSE LES DONNES

The screenshot shows the Splunk Enterprise web interface with a dark theme. The top navigation bar includes the 'splunk>enterprise' logo, 'Apps', 'Administrator' (logged in), 'Messages', 'Settings', and 'Activity'. On the left, a vertical sidebar lists icons for 'Forwarding and receiving', 'Forward data', 'Receive data', 'Forwarding defaults', 'Configure forwarding', 'Configure receiving', and 'Add new'.

Forwarding and receiving

Forward data

Set up forwarding between two or more Splunk instances.

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data

Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

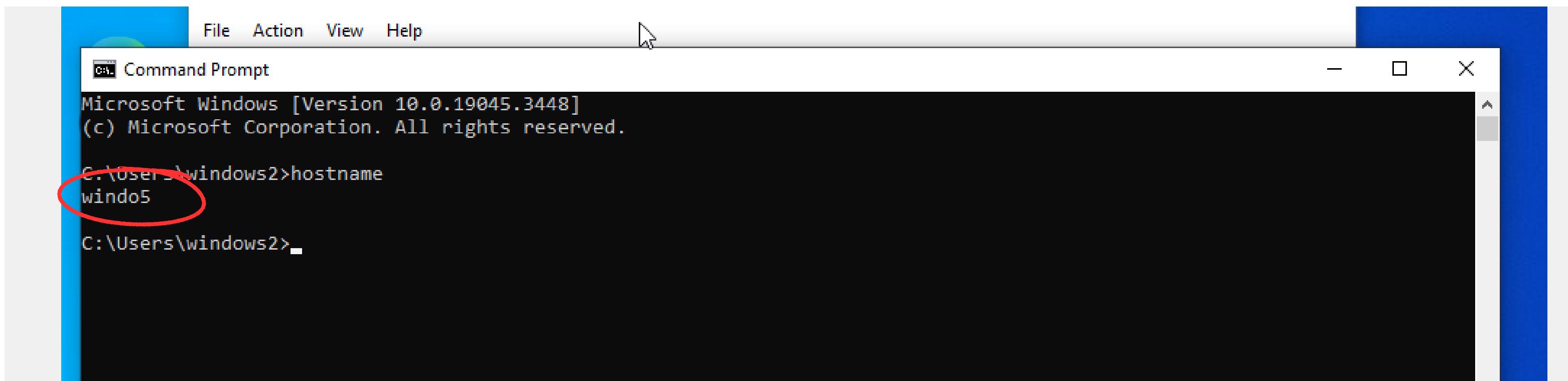
Splunk Enterprise on Linux

- DANS LA MACHINE QUI ANALYSE LES DONNES

The screenshot shows a web-based configuration interface for Splunk Enterprise. On the left, there is a vertical toolbar with icons for Home, Search, Reports, Dashboards, and Settings. The main area has a header "Add new" and a breadcrumb trail "Forwarding and receiving » Receive data » Add new". A central modal window titled "Configure receiving" contains the instruction "Set up this Splunk instance to receive data from forwarder(s.)". It features a text input field labeled "Listen on this port" with the value "9997" highlighted by a blue border. Below the input field is a explanatory note: "For example, 9997 will receive data on TCP port 9997." At the bottom right of the modal are two buttons: "Cancel" and "Save".

Machine cible (windows 10)

■ vérification

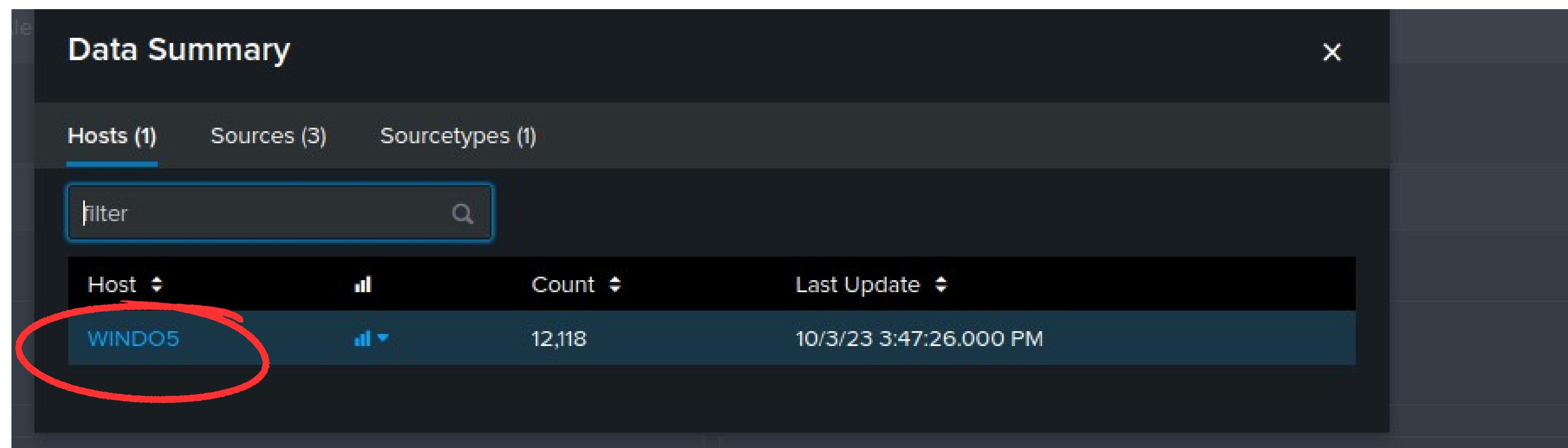


```
File Action View Help
Command Prompt
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\windows2>hostname
windo5

C:\Users\windows2>
```

A screenshot of a Windows Command Prompt window. The title bar says "Command Prompt". The window shows the following text:
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.
C:\Users\windows2>hostname
windo5
C:\Users\windows2>
The line "windo5" is circled in red.



Data Summary

Hosts (1) Sources (3) Sourcetypes (1)

filter

Host	Count	Last Update
WINDO5	12,118	10/3/23 3:47:26.000 PM

A screenshot of a "Data Summary" interface. It shows a table with one host entry. The table has columns: Host, Count, and Last Update. The host entry is "WINDO5" with a count of "12,118" and a last update of "10/3/23 3:47:26.000 PM". The row for "WINDO5" is circled in red.

Splunk Enterprise on Linux

• RECUPERATION DES DONNES DE LA MACHINE WIND05

The screenshot shows the Splunk Enterprise search interface. At the top, there's a navigation bar with links for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The main title is "New Search". On the right side of the search bar, there are buttons for "Save As", "Create Table View", and "Close". Below the search bar, it says "Last 24 hours" and has a search icon. The event count is 1,504 events (from 10/2/23 3:00:00.000 PM to 10/3/23 3:49:04.000 PM) with "No Event Sampling". There are buttons for "Job", "Smart Mode", and other search controls.

The main area displays the search results. The first event is:

Time	Event
10/3/23 2:52:23 PM	host = WIND05 source = WinEventLog:Application sourcetype = WinEventLog LogName=Application EventCode=1001 EventType=4 ComputerName=windo5.bench.local Show all 43 lines

The second event is:

Time	Event
10/3/23 2:52:23 PM	host = WIND05 source = WinEventLog:Application sourcetype = WinEventLog LogName=Application EventCode=8198 EventType=2 ComputerName=windo5.bench.local Show all 15 lines

The third event is:

Time	Event
10/3/23 2:52:23 PM	host = WIND05 source = WinEventLog:Application sourcetype = WinEventLog LogName=Application EventCode=1003 EventType=4 ComputerName=windo5.bench.local Show all 65 lines

On the left side, there are two panels: "SELECTED FIELDS" and "INTERESTING FIELDS". The "SELECTED FIELDS" panel lists "host" (1), "source" (3), and "sourcetype" (1). The "INTERESTING FIELDS" panel lists various fields like "Account_Domain" (6), "Account_Name" (10), "action" (5), "app" (3), "body" (100+), "category" (37), "ComputerName" (1), "dest" (3), "dest_nt_domain" (6), "dest_nt_host" (3), "dvc" (1), "dvc_nt_host" (1), "Error_Code" (4), "event_id" (100+), "EventCode" (97), "eventtype" (27), and "EventType" (5).

Splunk Enterprise on Linux

• RECUPERATION DES DONNES DE LA MACHINE WIND05

The screenshot shows the Splunk Enterprise search interface with the URL `127.0.0.1:8000/en-US/app/search/search?q=search%20host%3DWIND05%20authentication_method%3DKerberos%20Authentication_Package%3DKerberos&display.page`. The search results table displays an event from host WIND05 with the following details:

Type	Field	Value	Actions
Selected	Logon_ID	0x0	▼
	Security_ID	NULL SID	▼
	host	WIND05	▼
	source	WinEventLog:Security	▼
	sourcetype	WinEventLog	▼
Event	Account_Domain	-	▼
	Account_Name	-	▼
	Authentication_Package	Kerberos	▼
	Caller_Process_ID	0x0	▼
	Caller_Process_Name	-	▼
	ComputerName	windo5.bench.local	▼
	Error_Code	0xC0000133	▼
	EventCode	4625	▼
	EventType	0	▼
	Failure_Reason	An Error occurred during Logon.	▼
	Key_Length	0	▼
	Keywords	Audit Failure	▼
	LogName	Security	▼
	Logon_Process	Kerberos	▼
	Logon_Type	3	▼
	Message	An account failed to log on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Kerberos Authentication Failed	▼

Splunk Enterprise on Linux

• RECUPERATION DES DONNES DE LA MACHINE WIND05

The screenshot shows the Splunk Enterprise interface with a search results page. The top navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, and Static Analysis. The search results are displayed in a table with columns for Time and Event. A red oval highlights the 'TaskCategory' field, which is set to 'Logon'. The 'Event' column contains detailed logon information, including the subject account, security ID, logon type (3), and authentication method (Kerberos). A large portion of the event body is visible, describing the failure of a logon attempt. Below the main table, there is a summary of additional fields and an option to extract new fields.

Time	Event
	<p>TaskCategory ▾ Logon</p> <p>Transited_Services ▾ -</p> <p>Type ▾ Information</p> <p>Workstation_Name ▾ -</p> <p>action ▾ failure</p> <p>app ▾ win:remote (remote)</p> <p>authentication_method ▾ Kerberos</p> <p>body ▾ An account failed to log on. Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Whic... h Logon Failed: Security ID: NULL SID Account Name: Account Domain: Failure Information: Failure Reason: An Error occurred during Logon. St... atus: 0xC0000133 Sub Status: 0x0 Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Nam... e: - Source Network Address: - Source Port: - Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the co... mputer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most com... monly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind o... f logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account... and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstatio... n name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about t... his specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name in... dicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0... if no session key was requested.</p>
	<p>category ▾ Logon</p> <p>dest ▾ windo5.bench.local</p> <p>dest_nt_host ▾ windo5.bench.local</p> <p>dvc ▾ windo5.bench.local</p> <p>dvc_nt_host ▾ WIND05</p> <p>event_id ▾ 12835</p> <p>eventtype ▾ endpoint_services_processes</p>

Hide Fields All Fields List Format 20 Per Page

src 1 src_ip 1 src_nt_domain 1 src_port 2 status 2 subject 2 Subject_Account_Domain 1 Subject_Account_Name 1 Subject_Logon_ID 1 Subject_Security_ID 1 ta_windows_action 2 tag 7 tag::app 2 tag::eventtype 5 TaskCategory 1 Transited_Services 1 Type 1 user 2 vendor 1 vendor_product 1 Virtual_Account 1 Workstation_Name 1 6 more fields Extract New Fields

Splunk Enterprise on Linux

- RECUPERATION DES DONNES DE LA MACHINE WIND05

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for Apps, Settings, Activity, Help, and a search bar labeled 'Find'. Below the navigation is a secondary header with 'splunk>enterprise' and a user icon for 'Administrator'. The main area is titled 'New Search' and contains a search bar with the query 'host=WIND05 authentication_method=Kerberos Authentication_Package=Kerberos app="win:local" category=Logon'. It displays 6 events from October 3, 2023, to October 4, 2023. On the right, a context menu is open over the search bar, with the 'Existing Dashboard' option circled in red. The bottom half of the screen shows a table of event details with columns for Time, Event, and various selected fields like host, Logon_ID, Security_ID, source, and sourcetype.

Time	Event
10/4/23 6:43:27 AM	LogName=Security EventCode=4624 EventType=0 ComputerName=windo5.bench.local Show all 70 lines Logon_ID = 0x0 Logon_ID = 0x1223E4D Security_ID = NULL SID Security_ID = NT AUTHORITY\SYSTEM host = WIND05 source = WinEventLog:Security sourcetype = WinEventLog
10/4/23 6:43:24 AM	LogName=Security EventCode=4624 EventType=0 ComputerName=windo5.bench.local Show all 70 lines Logon_ID = 0x0 Logon_ID = 0x1222ECE Security_ID = NULL SID Security_ID = NT AUTHORITY\SYSTEM host = WIND05 source = WinEventLog:Security sourcetype = WinEventLog
10/3/23 11:58:10 PM	Logon_ID = 0x0 Logon_ID = 0x1222ECE Security_ID = NULL SID Security_ID = NT AUTHORITY\SYSTEM host = WIND05 source = WinEventLog:Security sourcetype = WinEventLog

SELECTED FIELDS

- a host 1
- a Logon_ID 7
- a Security_ID 2
- a source 1
- a sourcetype 1

INTERESTING FIELDS

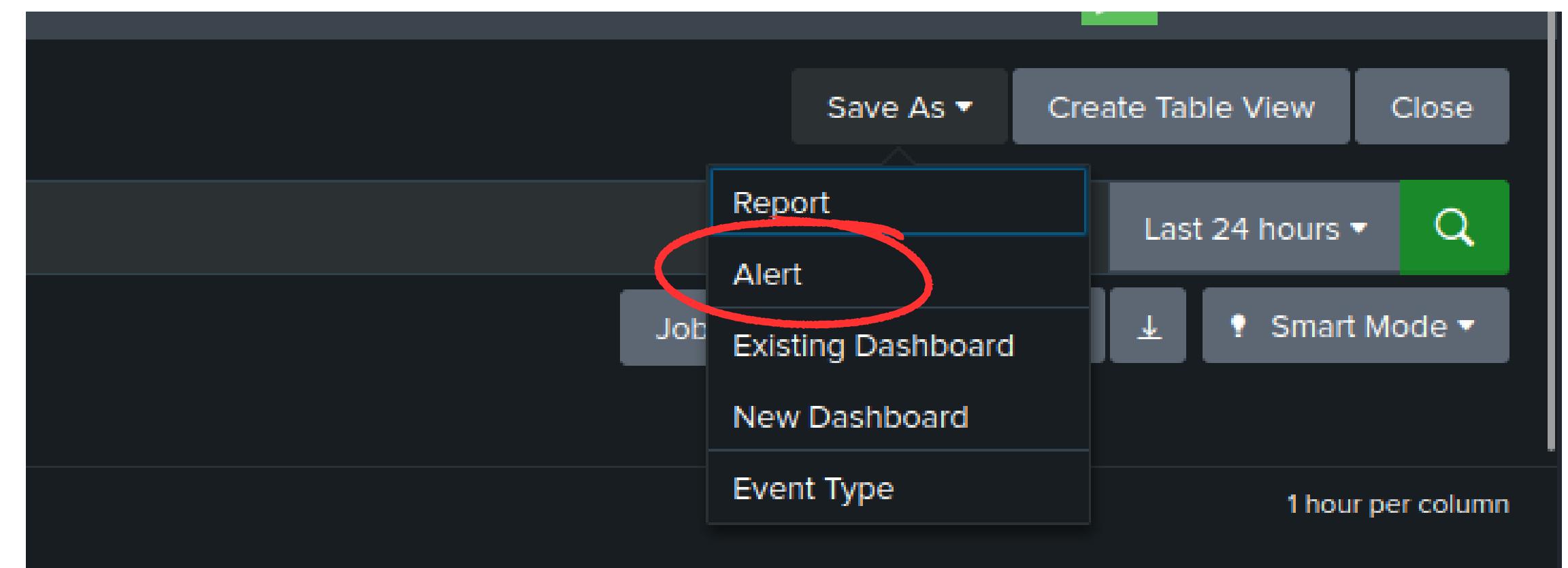
- a Account_Domain 2
- a Account_Name 2
- a action 1
- a app 1
- a authentication_method 1
- a Authentication_Package 1
- a body 6
- a category 1
- a ComputerName 1

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.

```
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**