

TP N°2

Elastic Cloud

Étape 1 : Installation de ELK dans le cloud

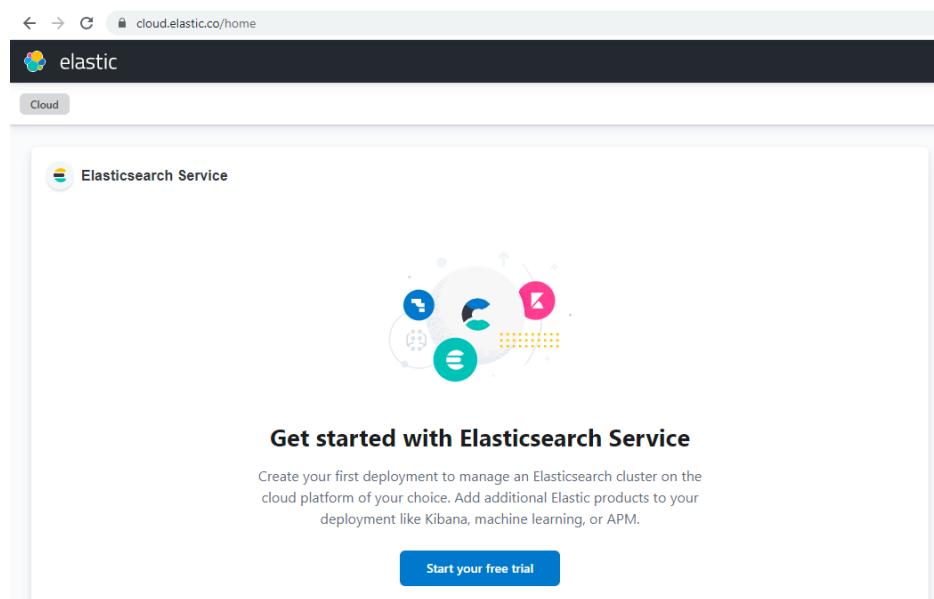
ELK combine trois technologies et fournit une solution puissante lorsque vous travaillez avec un grand volume de données. De plus, nous sommes en mesure de configurer des règles SIEM pour nous alerter en tant que défenseurs des attaques contre notre organisation.

- ✓ E Elasticsearch
- ✓ L Logstash
- ✓ K Kibana

ELK permet aux défenseurs de détecter les attaques et de prévenir les menaces.

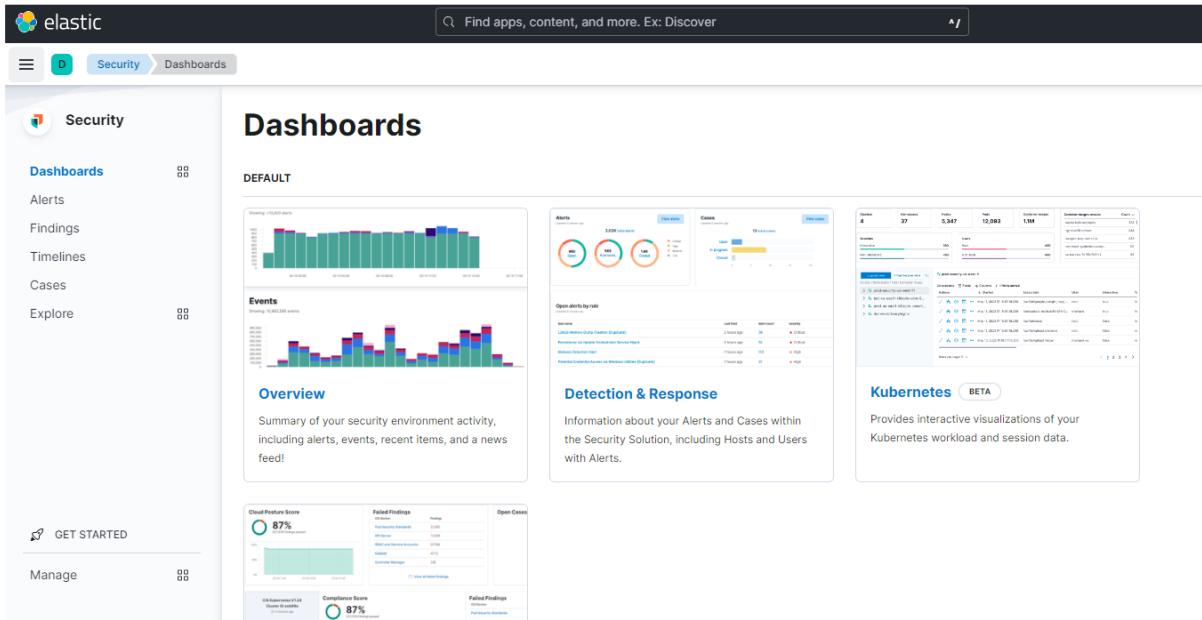
1. Créer un compte Elastic en utilisant le lien suivant (ce lien vous donnera un accès gratuit) :

<https://cloud.elastic.co/registration?settings=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJJsZW5ndGgiOiE1MCwic2l6ZSI6NDA5NiwiZGVmYXVsdF9zaXplIjoxMDI0fQ.dS6xq>



Pour nos besoins, nous devons avoir un nouveau déploiement personnalisé et nous voulons lancer une instance Elastic Security.

Nous avons maintenant une instance complète et fonctionnelle d'une instance ELK dans laquelle nous pouvons apprendre et expérimenter.

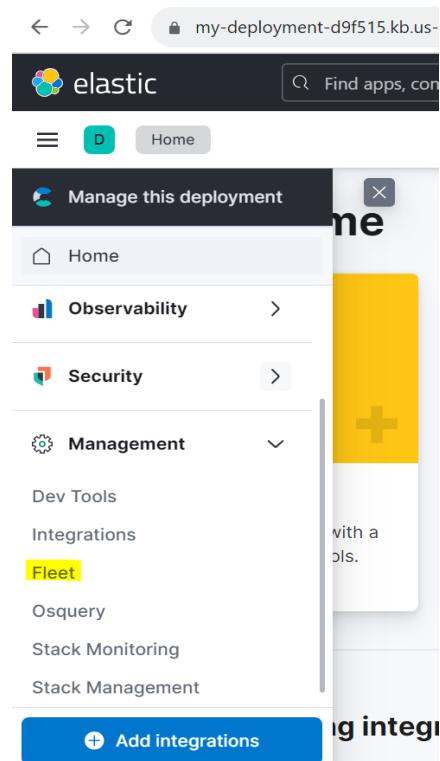


The screenshot shows the Elastic Security interface under the 'Security' tab. On the left, there's a sidebar with 'Dashboards', 'Alerts', 'Findings', 'Timelines', 'Cases', and 'Explore' sections. Below that is a 'GET STARTED' section with 'Manage'. The main area is titled 'Dashboards' and contains several cards:

- DEFAULT**: Shows a bar chart for 'Events' (Showing ~10,000 events) and a circular dashboard for 'Alerts' (~3,000 incidents).
- Overview**: A summary of security environment activity.
- Detection & Response**: Information about Alerts and Cases.
- Kubernetes (BETA)**: Provides interactive visualizations of Kubernetes workload and session data.

2. Configurer Fleet :

Kibana a une fonctionnalité pratique appelée « Fleet ». Cette fonctionnalité permet aux utilisateurs d'ajouter facilement des données à la stack ELK.



The screenshot shows the Kibana interface with a modal window titled 'Manage this deployment'. The modal lists several sections:

- Home
- Observability
- Security
- Management
- Dev Tools
- Integrations
- Fleet
- Osquery
- Stack Monitoring
- Stack Management

A blue button at the bottom right says '+ Add integrations'.

Dans le menu Fleet, recherchez l'onglet «Agents» :

The screenshot shows the Fleet interface with the Agents tab highlighted by a red box. Below the tabs, there is a section titled "Fleet (BETA)" with the sub-instruction "Manage Elastic Agents and their policies in a central location." To the right of this section is a blue button labeled "+ Add agent". The main area contains four cards: "Integrations" (Total available: 61), "Agent policies" (Total available: 1), "Agents" (Total agents: 0), and "Data streams" (Data streams: 0).

Ajouter un Agent :

The screenshot shows the Fleet interface with the Agents tab selected. At the bottom right, there is a prominent blue button labeled "Add agent" which is highlighted with a green box.

Choisir « Windows », et copier le code affiché :

The screenshot shows the "Install Elastic Agent on your host" step. The "Windows" tab is selected. Below it, a command line snippet is shown:

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.4.2-windows-x86_64.zip -OutFile elastic-agent-8.4.2-windows-x86_64.zip
Expand-Archive .\elastic-agent-8.4.2-windows-x86_64.zip -DestinationPath .
.\elastic-agent.exe install --url=https://o3eccod9de764f290ec9b64e9fa4c26.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=eFRBU21
```

Coller sur un bloc-note :

The screenshot shows a Microsoft Word document with the title "*Sans titre - Bloc-notes". It contains the following PowerShell command:

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.4.2-windows-x86_64.zip -OutFile elastic-agent-8.4.2-windows-x86_64.zip
Expand-Archive .\elastic-agent-8.4.2-windows-x86_64.zip -DestinationPath .
.\elastic-agent.exe install --url=https://o3eccod9de764f290ec9b64e9fa4c26.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=eFRBU21
```

La stack ELK est maintenant configurée et nos informations de connexion sont enregistrées. La deuxième étape couvrira l'installation et la configuration d'un agent Elastic.

Étape 2 : Installation de l'agent ELK sur une machine Windows

1. Télécharger l'agent à partir du lien suivant : <https://www.elastic.co/fr/downloads/elasticsearch-agent>
2. Extraire le fichier téléchargé et lancer la commande PowerShell sauvegardée à l'étape précédente d'installation.

Ouvrir « PowerShell » en tant qu'un administrateur :

```
PS C:\Users\Lenovo\Downloads\elastic-agent-8.4.2-windows-x86_64> ls

Répertoire : C:\Users\Lenovo\Downloads\elastic-agent-8.4.2-windows-x86_64

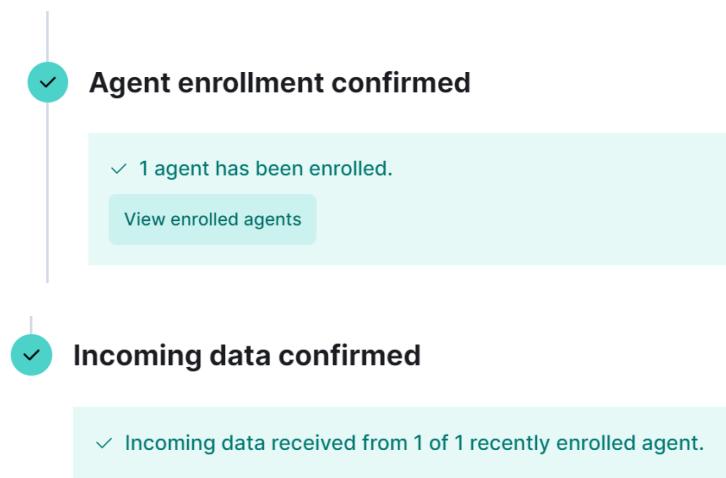
Mode                LastWriteTime       Length Name
----                -----          -----
d---- 14/09/2022 23:20                 data
d---- 14/09/2022 23:20           41 .build_hash.txt
d---- 14/09/2022 23:20           41 .elastic-agent.active.commit
d---- 14/09/2022 23:20        45134664 elastic-agent.exe
d---- 14/09/2022 23:20           9164 elastic-agent.reference.yml
d---- 14/09/2022 23:20           9127 elastic-agent.yml
d---- 14/09/2022 23:20           13675 LICENSE.txt
d---- 14/09/2022 23:20         943764 NOTICE.txt
d---- 14/09/2022 23:20           861 README.md

PS C:\Users\Lenovo\Downloads\elastic-agent-8.4.2-windows-x86_64>
```

3. Installer l'agent ELK avec la commande : .\elastic-agent.exe install --url=https://d9f515d32d0b45029612ac64e7daf0cc.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=aE9xNVBvd0JWSmpBTnVQTjF3R006NGZOVU01cmtTYXF5ZWhjMW5YaWpoZw==

```
PS C:\Users\Lenovo\Downloads\elastic-agent-8.4.2-windows-x86_64> .\elastic-agent.exe install --url=https://03ecc0d9de7646f290ec9b64e9fa4c26.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=eFRBU21ZTUjps5hSRWZ0amE5UhA623jyvJYSNH2TMBVQ7nfR6Gp1R1NQo=
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:Y
{"log.level": "info", "@timestamp": "2022-10-02T16:57:16.357+0200", "log.origin": {"file.name": "cmd/enroll_cmd.go", "file.line": "471"}, "message": "Starting enrollment to URL: https://03ecc0d9de7646f290ec9b64e9fa4c26.fleet.us-central1.gcp.cloud.es.io:443", "ecs.version": "1.6.0"}
{"log.level": "info", "@timestamp": "2022-10-02T16:57:17.627+0200", "log.origin": {"file.name": "cmd/enroll_cmd.go", "file.line": "271"}, "message": "Elastic Agent might not be running; unable to trigger restart", "ecs.version": "1.6.0"}
Successfully enrolled the Elastic Agent.
Elastic Agent has been successfully installed.
PS C:\Users\Lenovo\Downloads\elastic-agent-8.4.2-windows-x86_64>
```

Une fois l'installation terminée, nous avons la confirmation dans l'instance Elastic :



Il sera visible sur l'interface ELK :

The screenshot shows the 'Fleet' interface with the following details:

- Agents:** Agents management section.
- Metrics:** Ingest Overview Metrics and Agent Info Metrics.
- Buttons:** Agent activity, Add Fleet Server, Add agent.
- Search Bar:** Filter your data using KQL syntax.
- Filter Options:** Status (4), Tags (0), Agent policy (2), Upgrade available.
- Data Table:** Shows 2 agents:

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	desktop-uj063ge	Agent policy 1 rev. 1	17.36 %	195 MB	27 seconds ago	8.11.2	...
Healthy	2c7a434f6dc7	Elastic Cloud agent policy rev. 5	N/A	N/A	2 seconds ago	8.11.1	...

En cliquant sur l'agent ajouté, vous trouverez des informations sur l'agent ajouté :

The screenshot shows the 'Agent details' page for the agent 'desktop-uj063ge' with the following details:

- Agent details:** Selected tab.
- Logs:** Logs tab.
- Diagnostics:** Diagnostics tab.
- Overview:** General information about the agent.
- Metrics:** CPU: 13.94 %, Memory: 199 MB, Status: Healthy, Last activity: 8 seconds ago, Last checkin message: Running, Agent ID: 01c87757-2011-4611-9eb3-fda9e35c1bf3, Agent policy: Agent policy 1 rev. 1, Agent version: 8.11.2, Host name: desktop-uj063ge, Logging level: info, Agent release: stable, Platform: windows, Monitor logs: Enabled, Monitor metrics: Enabled, Tags: -.

Étape 3 : Configuration de Sysmon

Sysmon est un outil gratuit pour surveiller et enregistrer l'activité de Windows.

1.Télécharger Sysmon à partir du lien suivant : <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>

The screenshot shows the Microsoft Learn page for Sysmon v14.1 with the following details:

- Page Headers:** Learn / Sysinternals / Downloads /
- Title:** Sysmon v14.1
- Article Details:** Article • 09/29/2022 • 15 minutes to read • 9 contributors
- Author:** By Mark Russinovich and Thomas Garnier
- Published:** September 29, 2022
- Downloads:**
 - Download Sysmon (3.4 MB)
 - Download Sysmon for Linux (GitHub)
- Social Buttons:** Like, Share, Print.

Introduction

2. Extraire le fichier téléchargé et lancer la commande PowerShell sauvegardée à l'étape précédente d'installation :

```
PS C:\Users\Lenovo\Downloads> .\Sysmon64.exe -i -n -accepteula

System Monitor v14.1 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2022 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\Lenovo\Downloads>
```

3. Dans le menu Kibana, sélectionner “Integrations“ et ajouter Windows :

Revenez vers Fleet → Agent policies → Agent policy1 :

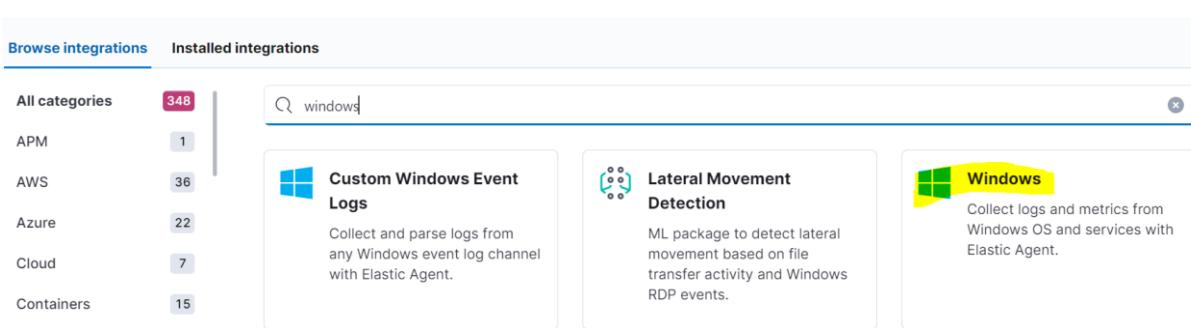
Name	Description	Last update...	Agents	Integrations	Actions
Agent policy 1 rev. 1		Dec 06, 2023	1	1	...
Elastic Cloud agent policy	Default agent policy for agents hosted on Elastic Cloud	Dec 04, 2023	1	2	...

Cliquer sur « add integration » :

Name ↑	Integration	Namespace	Actions
system-1	System v1.50.0	default	...

Chercher par « Windows », et cliquer sur :

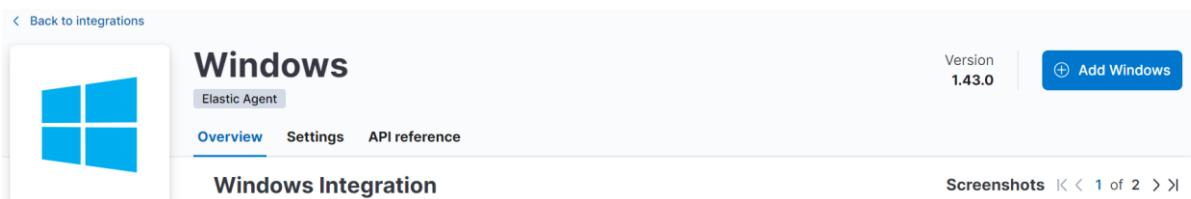
All categories	348	Search for integrations
APM	1	APM Collect performance metrics from your applications with Elastic APM.
AWS	36	Elastic Defend Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.
Azure	22	
Cloud	7	



The screenshot shows the 'Installed integrations' section of the Elastic Stack interface. A search bar at the top right contains the text 'windows'. Below it, there are three integration cards:

- Custom Windows Event Logs**: Collect and parse logs from any Windows event log channel with Elastic Agent.
- Lateral Movement Detection**: ML package to detect lateral movement based on file transfer activity and Windows RDP events.
- Windows**: Collect logs and metrics from Windows OS and services with Elastic Agent.

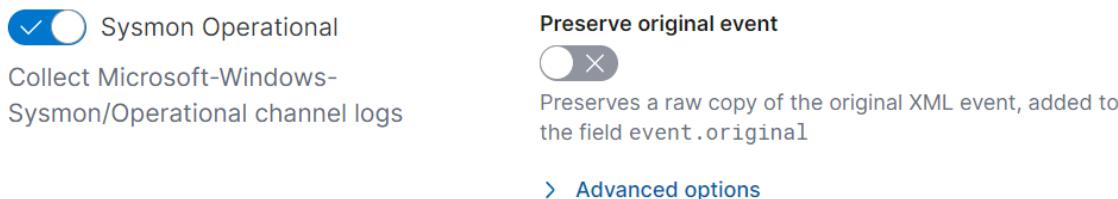
Cliquer sur « add windows » :



The screenshot shows the configuration page for the 'Windows' integration. It includes the following details:

- Icon**: Windows logo.
- Name**: Windows.
- Type**: Elastic Agent.
- Version**: 1.43.0.
- Add Windows** button.
- Overview**, **Settings**, and **API reference** tabs.
- Windows Integration** section.
- Screenshots** section.

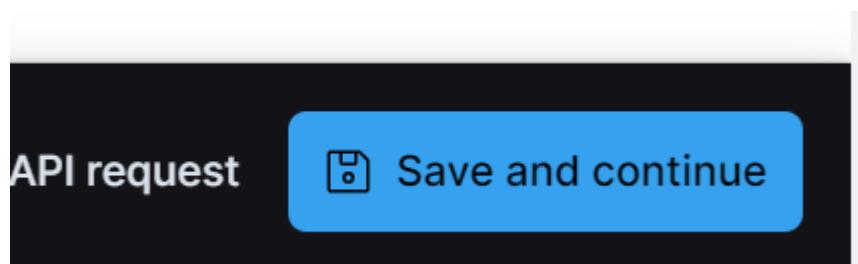
Vérifier si Sysmon est activé :



The screenshot shows the configuration options for the 'Sysmon Operational' integration:

- Sysmon Operational** switch: Enabled (checked).
- Collect Microsoft-Windows-Sysmon/Operational channel logs**.
- Preserve original event** switch: Disabled (unchecked).
- Description**: Preserves a raw copy of the original XML event, added to the field event.original.
- Advanced options** link.

Cliquer sur « save and continue » tout en bas :



Il sera visible dans l'integration :



The screenshot shows the 'Agent policy 1' configuration page:

- View all agent policies** link.
- Agent policy 1** name.
- Revision**: 2.
- Integrations**: 2.
- Agents**: 1 agent.
- Last updated on**: Dec 07, 2023.
- Actions** dropdown.
- Integrations** and **Settings** tabs.
- Search...** input field.
- Namespace** dropdown.
- Add integration** button.
- Table** showing integration details:

Name	Integration	Namespace	Actions
system-1	System v1.50.0	default	...
windows-1	Windows v1.43.0	default	...

On peut vérifier que le système windows, est maintenant intégré dans l'agent créé, en allant sur Fleet → desktop...

Overview	
CPU	4.12 %
Memory	221 MB
Status	Healthy
Last activity	13 seconds ago
Last checkin message	Running
Agent ID	01c87757-2011-4611-9eb3-fda9e35c1bf3
Agent policy	Agent policy 1 rev. 2
Agent version	8.1.2
Host name	desktop-uj063ge
Logging level	info
Agent release	stable

A ce stade, vous pouvez faire des manipulations sur le desktop avec l'agent : création des fichiers, modifications des fichiers, suppression des fichiers, faire des recherches google, ouvrir des programmes...

Après allez sur l'onglet : Analytics → discover pour vérifier les logs :

The screenshot shows the Databricks Analytics interface. At the top, there are three icons: a yellow one with three horizontal bars, a teal one with a white 'D', and a grey one labeled 'Analytics'. Below these is a dark header bar with a teal circular icon containing a white 'C' and the text 'Manage this deployment'. Underneath the header is a navigation bar with a house icon and the word 'Home'. The main content area has a title 'Analytics' with a dropdown arrow, followed by a 'Discover' button with a yellow background and black text. Below it are several menu items: 'Dashboard', 'Canvas', 'Maps', 'Machine Learning', 'Graph', and 'Visualize Library', each with a corresponding icon.

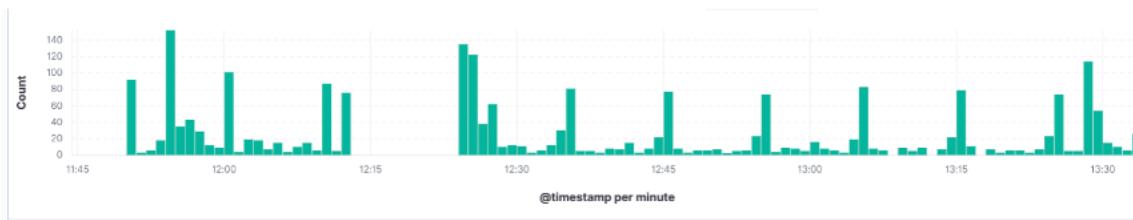
Cliquer sur logs :

En définissant notre source de données sur "logs-*". Définissez une contrainte de temps pour concentrer vos résultats. Nous pouvons ajouter un filtre sur nos données pour limiter vos résultats aux données Sysmon. Cela peut être fait en recherchant dans le champ "data_stream.dataset" les données "Windows.sysmon_operational".

The screenshot shows the Kibana Settings page with the following interface elements:

- A top navigation bar with the URL ".alerts-security.alerts-default,ap..." and a dropdown arrow.
- Two main actions: "Add a field to this data view" and "Manage this data view".
- A "Data views" section containing:
 - A search bar labeled "Find a data view" with a magnifying glass icon.
 - A list of data views:
 - "_alerts-security.alerts-def..." (selected, indicated by a checkmark and expanded to show sub-fields: ".kibana-event-log-*", "logs-*" (highlighted in yellow), and "metrics-*").
- A bottom banner with the text "Try ES|QL" and "Technical preview".

Si vous obtenez un résultat, et non une erreur, vos données Sysmon sont collectées et envoyées à Elastic.



Commencer à filtrer les champs, par exemple : agent.name, event.action, process.command_line

Ajouter aussi des filtres, par exemple :

Add filter Technical preview

Edit as Query DSL

= data_stream.dataset is windows.sysmon_operational

31 hits

Break down by Select field

December 7, 2023 @ 14:40:10.182 - Dec 7, 2023 @ 14:55:10.182 (interval: Auto - 30 seconds)

Documents Field statistics

Columns 1 field sorted

@timestamp	agent.name	event.action	process.command_line
Dec 7, 2023 14:55:03.350	DESKTOP-UJ063GE	Process creation	calc.exe
Dec 7, 2023 14:55:08.856	DESKTOP-UJ063GE	DNSEvent (DNS query)	-
Dec 7, 2023 14:54:48.734	DESKTOP-UJ063GE	Process creation	"C:\Windows\system32\cmd.exe"

Essayer aussi : winlog.event_id= "1" pour avoir que les event de type « process creation » :

logs-*

winlog.event_id:"1"

21 hits

Break down by Select field

December 7, 2023 @ 14:42:39.753 - Dec 7, 2023 @ 14:57:39.753 (interval: Auto - 30 seconds)

Documents Field statistics

Columns 1 field sorted

@timestamp	agent.name	event.action	process.command_line
Dec 7, 2023 14:46:03.655	DESKTOP-UJ063GE	Process creation	C:\Windows\system32\net1 stop HPAudioAnalytics
Dec 7, 2023 14:46:03.615	DESKTOP-UJ063GE	Process creation	net stop HPAudioAnalytics
Dec 7, 2023 14:46:03.339	DESKTOP-UJ063GE	Process creation	cmd.exe /C "net stop HPAudioAnalytics & net start HPAudioAnalytics"