MARRAKECH
جامعة القاضي عياض
UNIVERSITÉ CADI AYYAD

كليـــــة العلوم السملالية - مراكش
FACULTÉ DES SCIENCES SEMLALIA - MARRAKECH

Filière : Licence en Networking, Système et Cybersécurité (S5)
Elément de Module : Digital Forensics
Année Universitaire : 2025/2026

TP N°2

Elastic Cloud

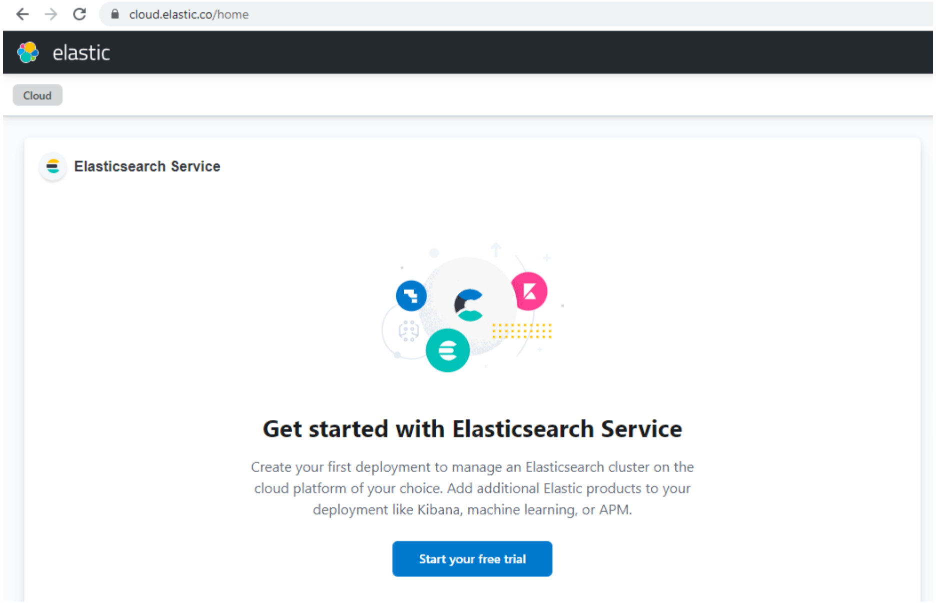
Étape 1 : Installation de ELK dans le cloud

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.eyJsZW5ndGgiOjE1MCwic2l6ZSI6NDA5NiwiZGVmYXVsdF9zaXplIjoxMDI0fQ.dS6xq

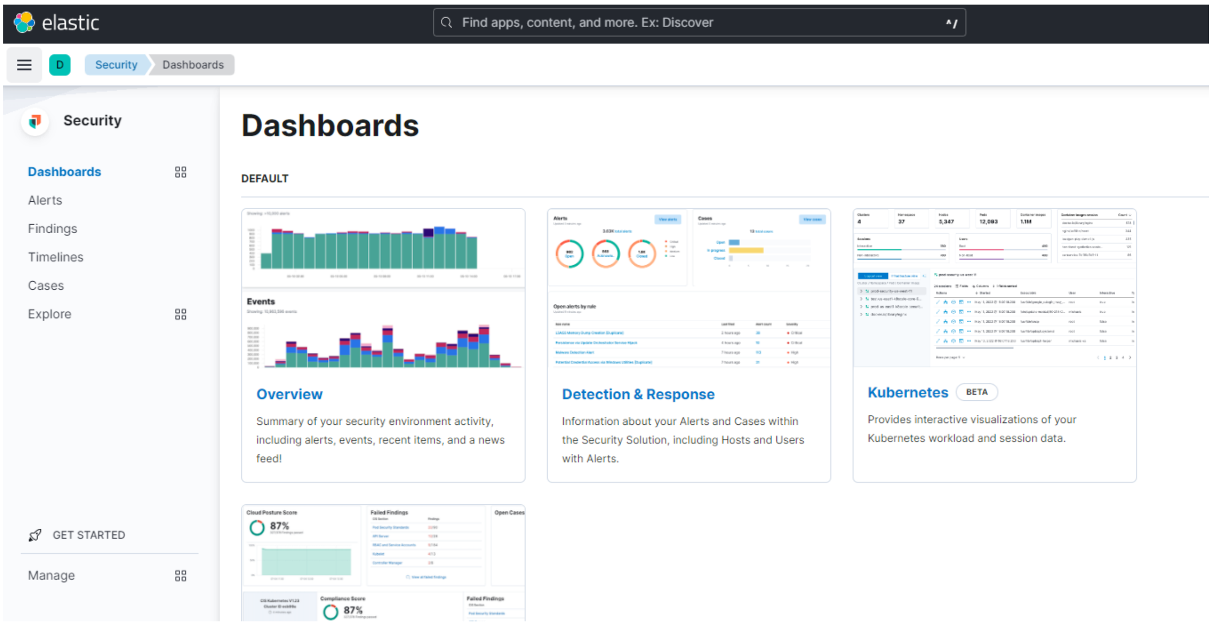


Get started with Elasticsearch Service

Create your first deployment to manage an Elasticsearch cluster on the cloud platform of your choice. Add additional Elastic products to your deployment like Kibana, machine learning, or APM.

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.



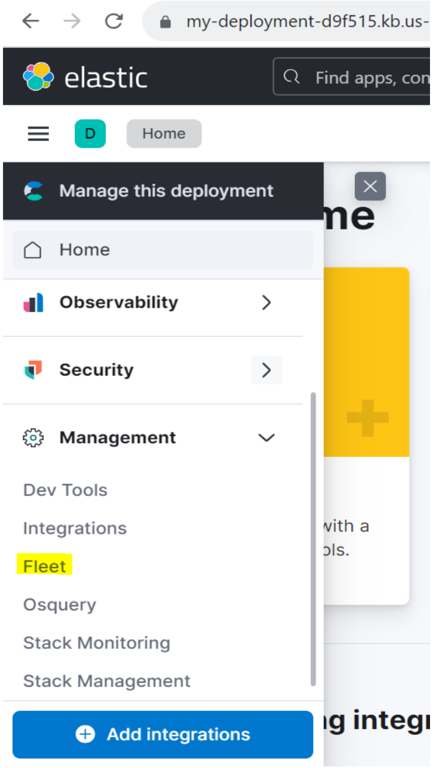
Summary of your security environment activity, including alerts, events, recent items, and a news feed!

Information about your Alerts and Cases within the Security Solution, including Hosts and Users with Alerts.

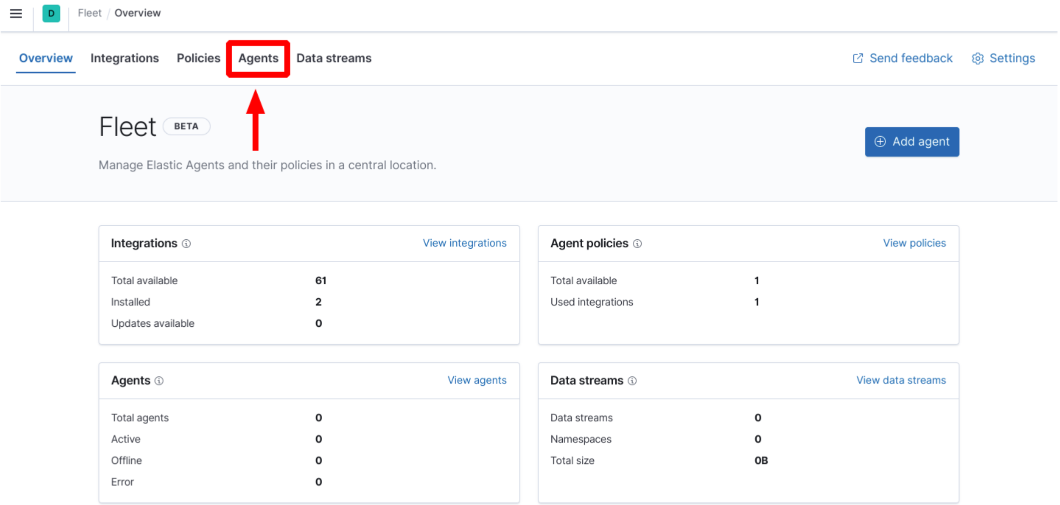
Provides interactive visualizations of your Kubernetes workload and session data.

2. Configurer Fleet :

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



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



Manage Elastic Agents and their policies in a central location.

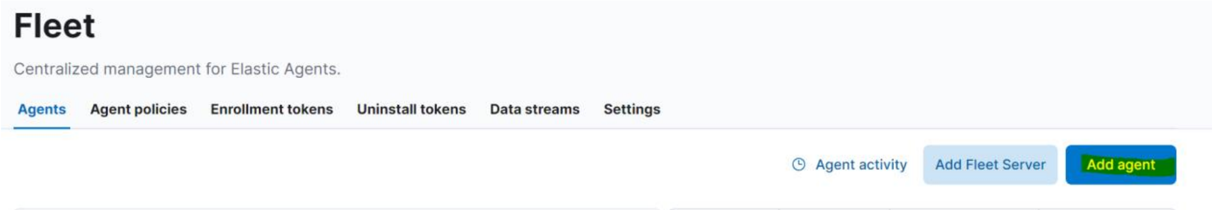
Integrations	View integrations
Total available	61
Installed	2
Updates available	0

Agent policies	View policies
Total available	1
Used integrations	1

Agents	View agents
Total agents	0
Active	0
Offline	0
Error	0

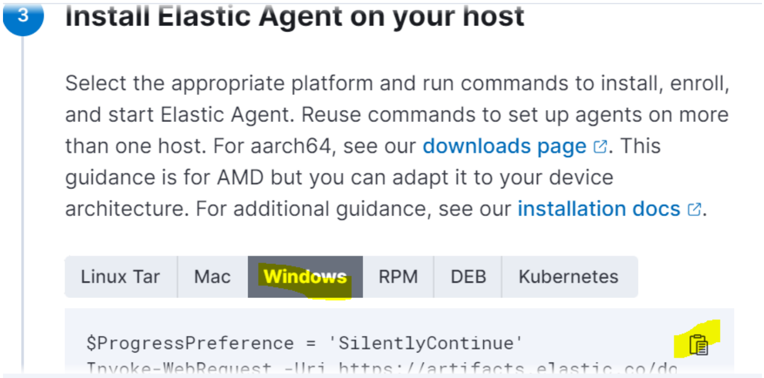
Data streams	View data streams
Data streams	0
Namespaces	0
Total size	0B

Ajouter un Agent :


Fleet

Centralized management for Elastic Agents.

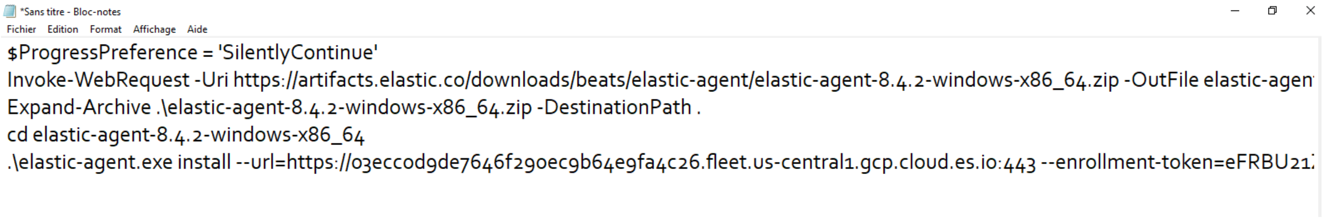
Choisir « Windows », et copier le code affiché :


3 Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our downloads page. This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our installation docs.

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/dc
```

Coller sur un bloc-note :



```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.4.2-windows-x86_64.zip -OutFile elastic-agen
Expand-Archive .\elastic-agent-8.4.2-windows-x86_64.zip -DestinationPath .
cd elastic-agent-8.4.2-windows-x86_64
.\elastic-agent.exe install --url=https://03eccod9de7646f290ec9b64e9fa4c26.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=eFRBU21
```

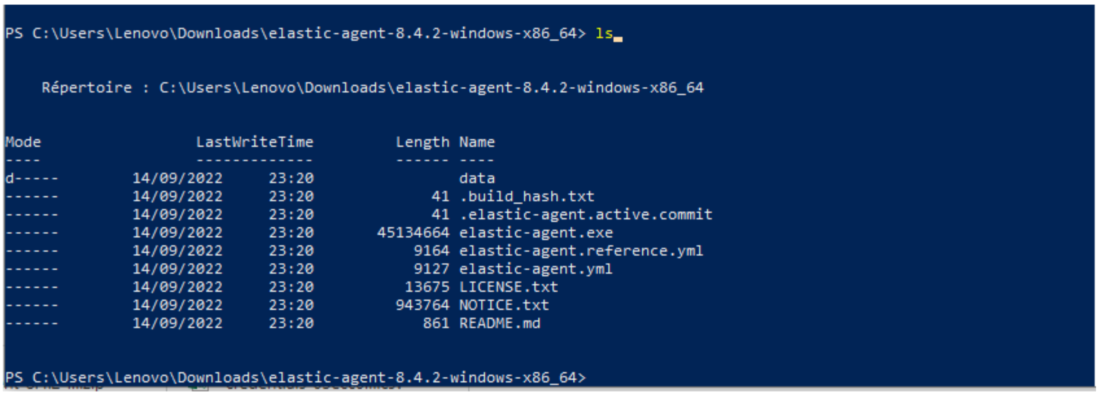
La stack ELK est maintenant configurée et nos informations de connexion sont enregistrées. La deuxième étape couvrira l'installation et la configuration d'un agent Elastic.

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/elastic-agent

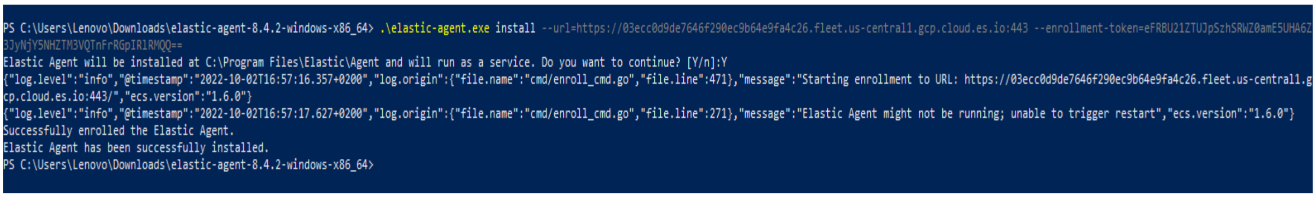
2. Extraire le fichier téléchargé et lancer la commande PowerShell sauvegardée à l'étape précédente d'installation.

Ouvrir « PowerShell » en tant qu'un administrateur :



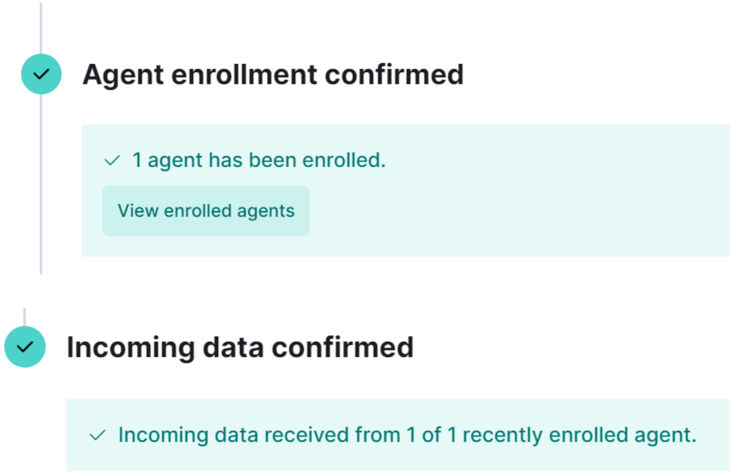
```
PS C:\Users\Lenovo\Downloads\elastic-agent-8.4.2-windows-x86_64> ls_


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


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        14/09/2022     23:20                data
------        14/09/2022     23:20             41 .build_hash.txt
------        14/09/2022     23:20             41 .elastic-agent.active.commit
------        14/09/2022     23:20       45134664 elastic-agent.exe
------        14/09/2022     23:20           9164 elastic-agent.reference.yml
------        14/09/2022     23:20           9127 elastic-agent.yml
------        14/09/2022     23:20          13675 LICENSE.txt
------        14/09/2022     23:20         943764 NOTICE.txt
------        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=eFRBU21ZTUJpSzhSRWZ0amE5UHA6Z
3JyNjY5NHZTM3VQTnFrRGpIR1RMQQ==
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.g
cp.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 :



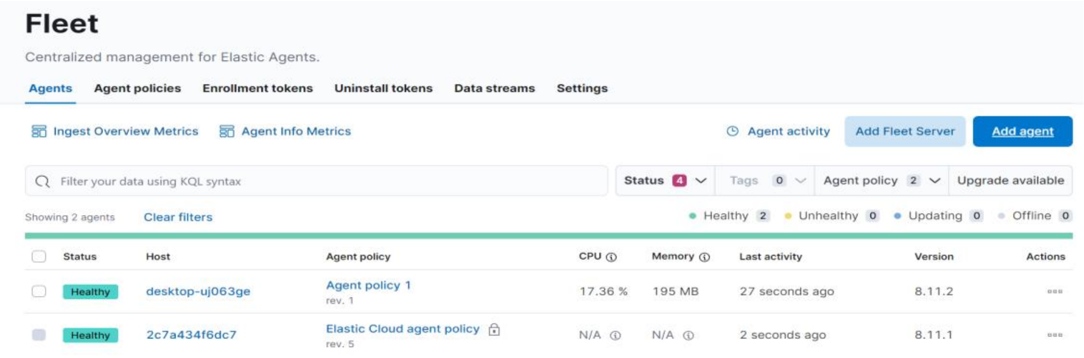
✓ Agent enrollment confirmed

✓ 1 agent has been enrolled.

✓ Incoming data confirmed

✓ Incoming data received from 1 of 1 recently enrolled agent.

Il sera visible sur l'interface ELK :



Fleet

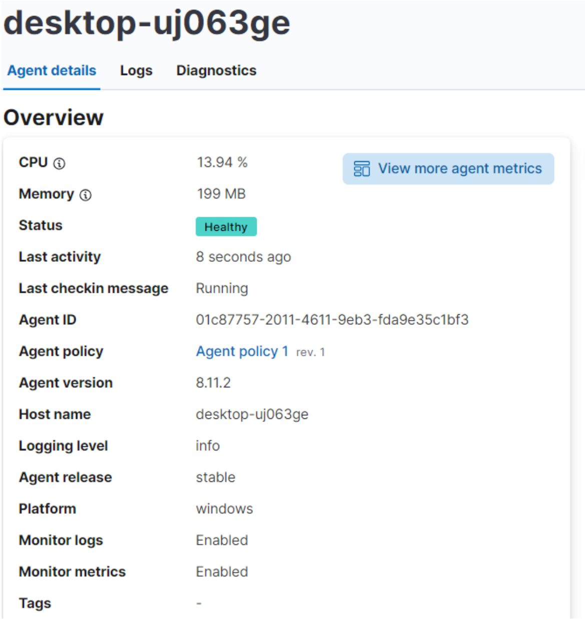
Centralized management for Elastic Agents.

Showing 2 agents

● Healthy 2 ● Unhealthy 0 ● Updating 0 ● Offline 0

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 :



desktop-uj063ge

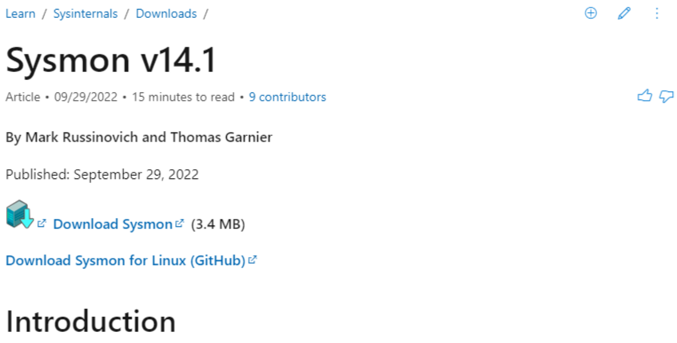
Overview

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



Learn / Sysinternals / Downloads /

Sysmon v14.1

Article • 09/29/2022 • 15 minutes to read • 9 contributors

By Mark Russinovich and Thomas Garnier

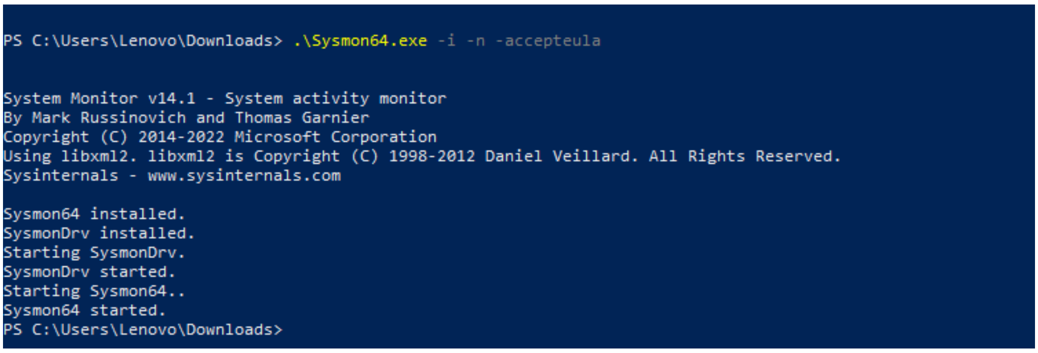
Published: September 29, 2022

Download Sysmon (3.4 MB)

Download Sysmon for Linux (GitHub)

Introduction

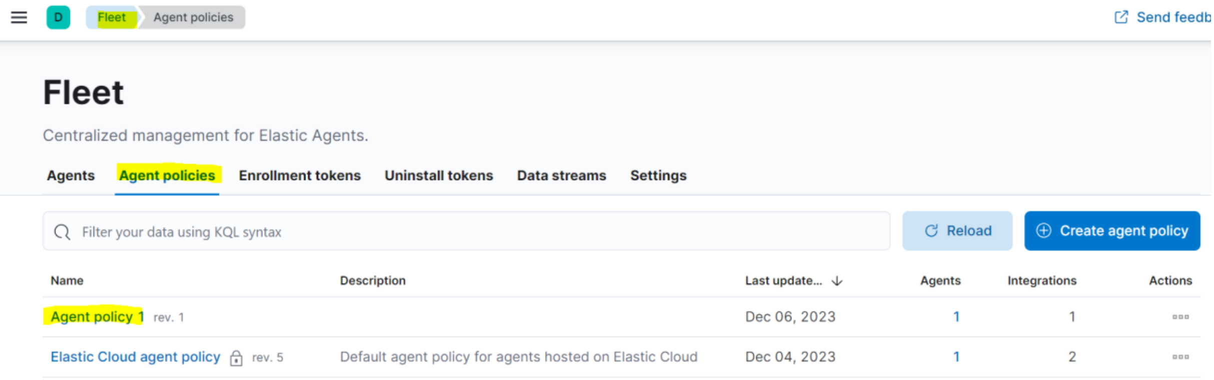
2. Extraire le fichier téléchargé et lancer la commande PowerShell sauvegardée à l'étape précédente d'installation :



```
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, séléctionner "Integrations" et ajouter Windows :

Revenez vers Fleet ➔ Agent policies ➔ Agent policy1 :

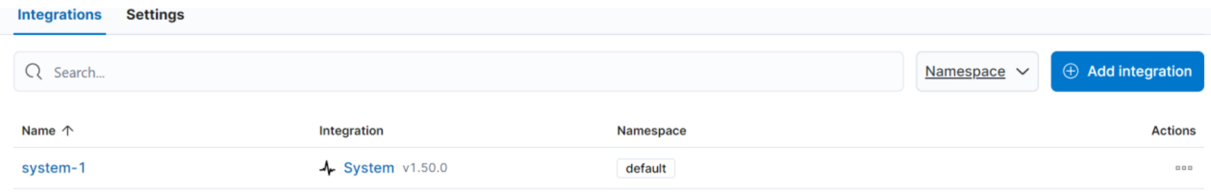


Fleet

Centralized management for Elastic Agents.

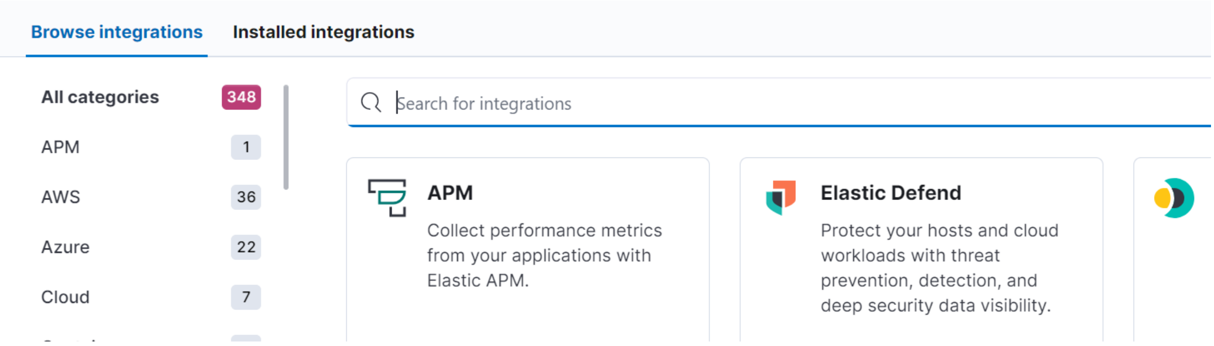
Name	Description	Last update... ↓	Agents	Integrations	Actions
Agent policy 1 rev. 1		Dec 06, 2023	1	1	···
Elastic Cloud agent policy rev. 5	Default agent policy for agents hosted on Elastic Cloud	Dec 04, 2023	1	2	···

Cliquer sur « add integration » :



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

Chercher par « Windows », et cliquer sur :

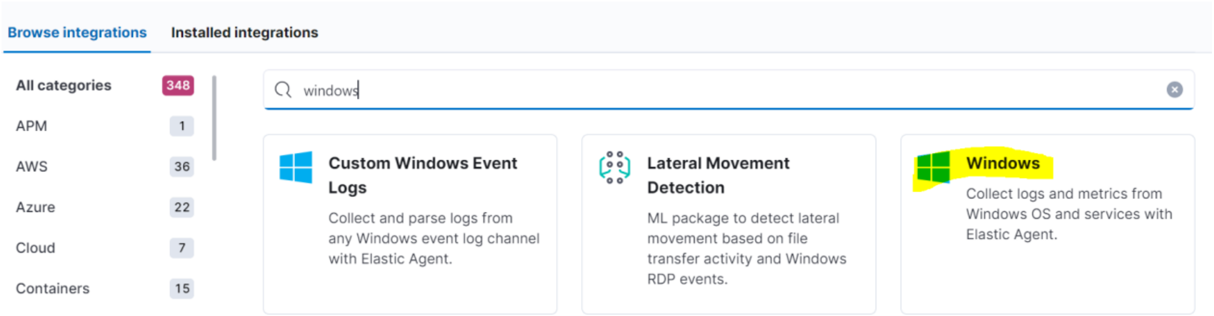


APM

Collect performance metrics from your applications with Elastic APM.

Elastic Defend

Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.



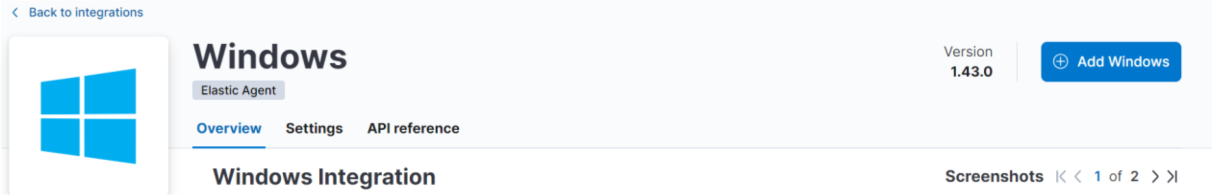
All categories	348
APM	1
AWS	36
Azure	22
Cloud	7
Containers	15

Custom Windows Event Logs — Collect and parse logs from any Windows event log channel with Elastic Agent.

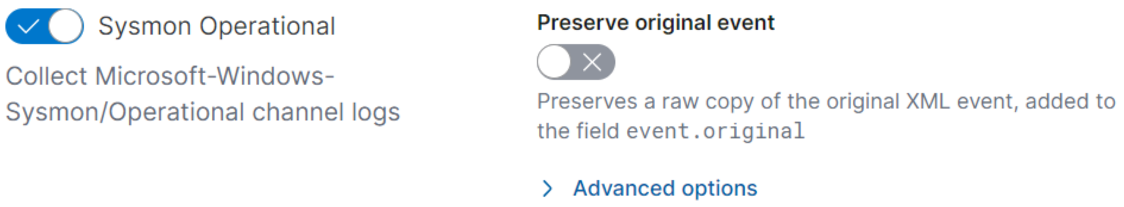
Lateral Movement Detection — ML package to detect lateral movement based on file transfer activity and Windows RDP events.

Windows — Collect logs and metrics from Windows OS and services with Elastic Agent.

Cliquer sur « add windows » :



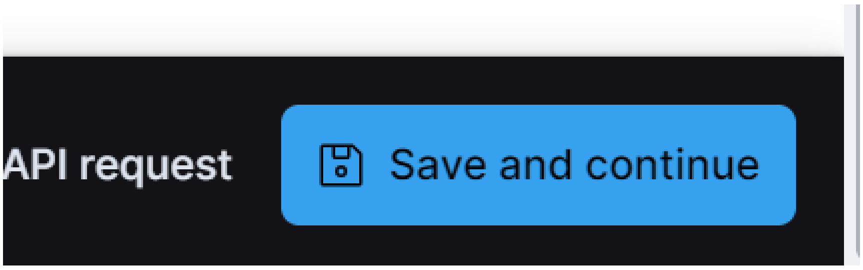
Vérifier si Sysmon est activé :



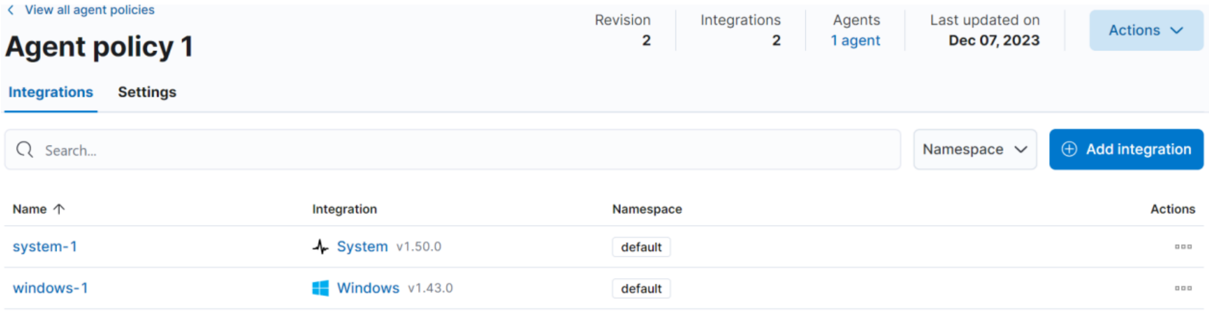
Collect Microsoft-Windows-Sysmon/Operational channel logs

Preserves a raw copy of the original XML event, added to the field `event.original`

Cliquer sur « save and continue » tout en bas :



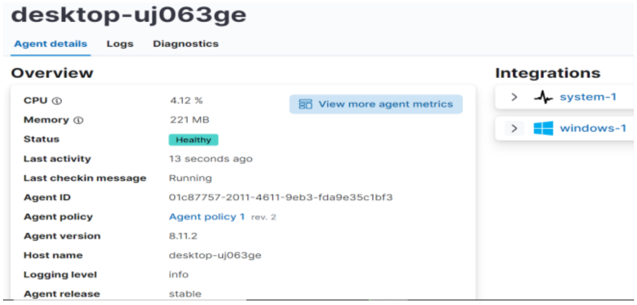
Il sera visible dans l'integration :



Revision	Integrations	Agents	Last updated on
2	2	1 agent	Dec 07, 2023

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…



desktop-uj063ge

Agent details | Logs | Diagnostics

Overview

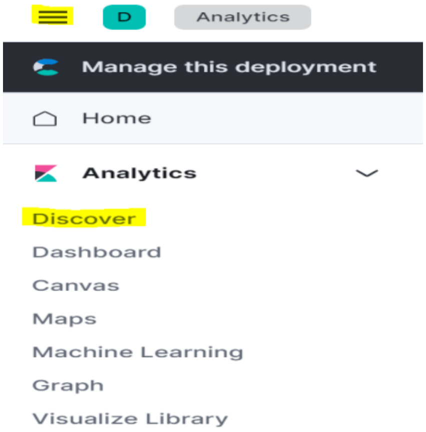
CPU ⓘ	4.12 %
Memory ⓘ	221 MB
Status	Healthy
Last activity	13 seconds ago
Last checkin message	Running
Agent ID	01c87757-2011-4611-9eb3-fda9e35c1bf3
Agent policy	Agent policy 1 rev. 2
Agent version	8.11.2
Host name	desktop-uj063ge
Logging level	info
Agent release	stable

Integrations

- system-1
- windows-1

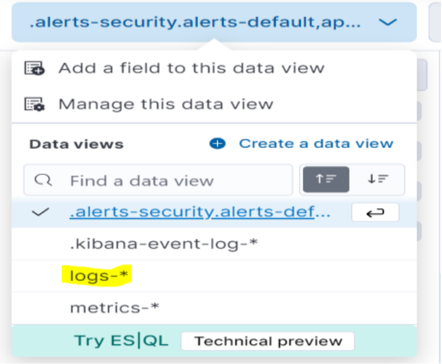
A ce stade, vous pouvez faire des manipulations sur le desktop avec l'agent : création des fichiers, modifications des fichiers, suppression des fichiers, faire des recherches google, ouvrir des programmes…

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

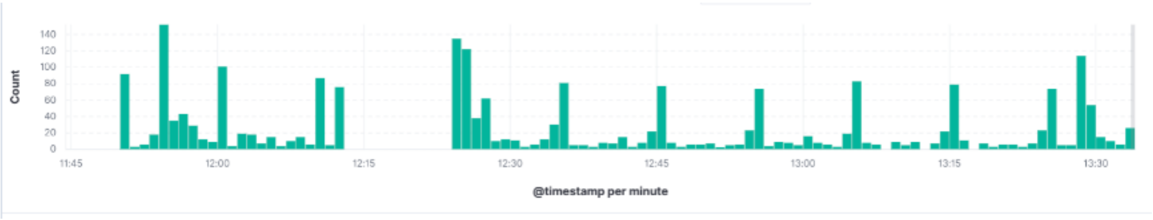


Cliquer sur logs :

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".

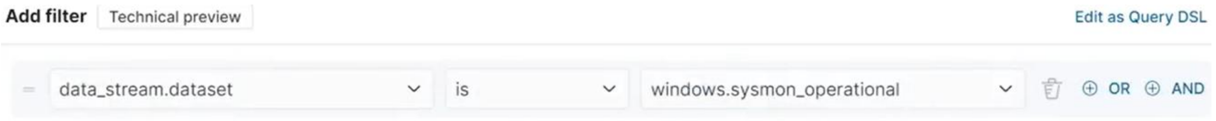


Si vous obtenez un résultat, et non une erreur, vos données Sysmon sont collectées et envoyées à Elastic.

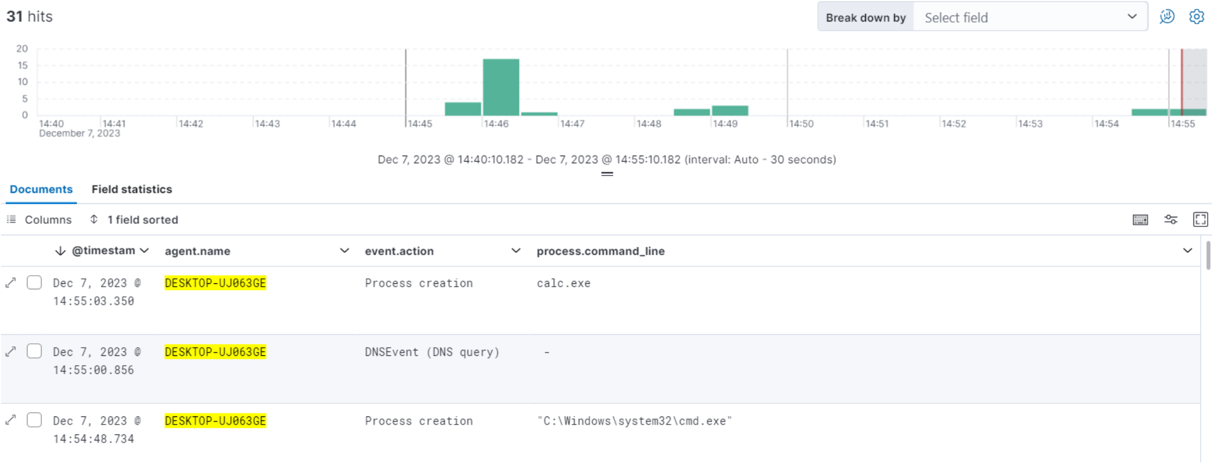


Commencer à filtrer les champs, par exemple : agent.name, event.action, proccess.commande_line

Ajouter aussi des filtres, par exemple :



data_stream.dataset is windows.sysmon_operational

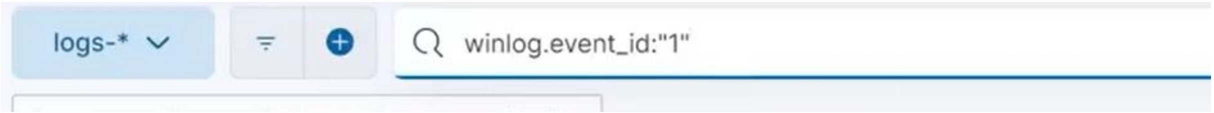


31 hits

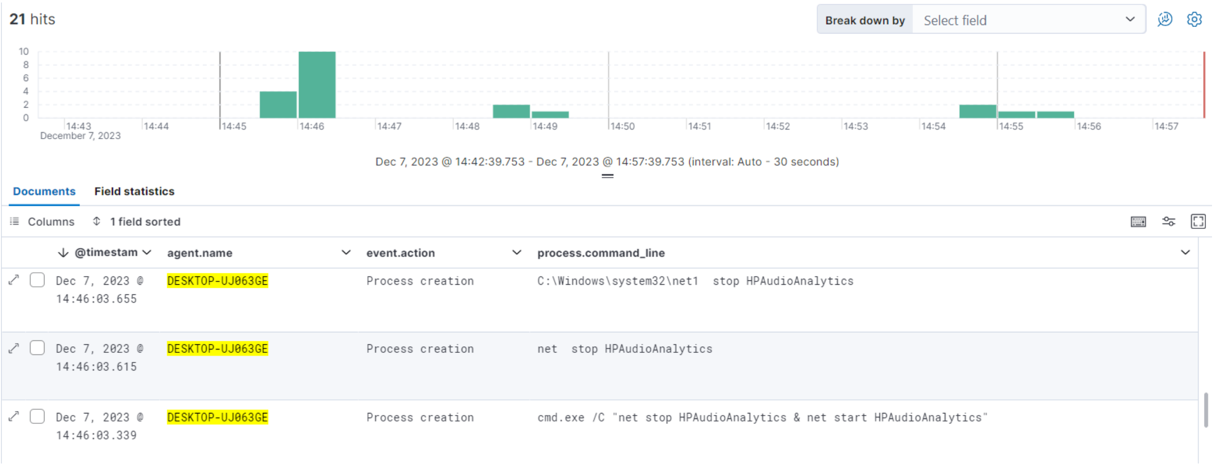
Dec 7, 2023 @ 14:40:10.182 - Dec 7, 2023 @ 14:55:10.182 (interval: Auto - 30 seconds)

@timestam	agent.name	event.action	process.command_line
Dec 7, 2023 @ 14:55:03.350	DESKTOP-UJ063GE	Process creation	calc.exe
Dec 7, 2023 @ 14:55:00.856	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 « proccess creation » :



winlog.event_id:"1"



21 hits

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

@timestam	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"