

ELK Documentation

This is a document to show the setup of ELK in the cloud:

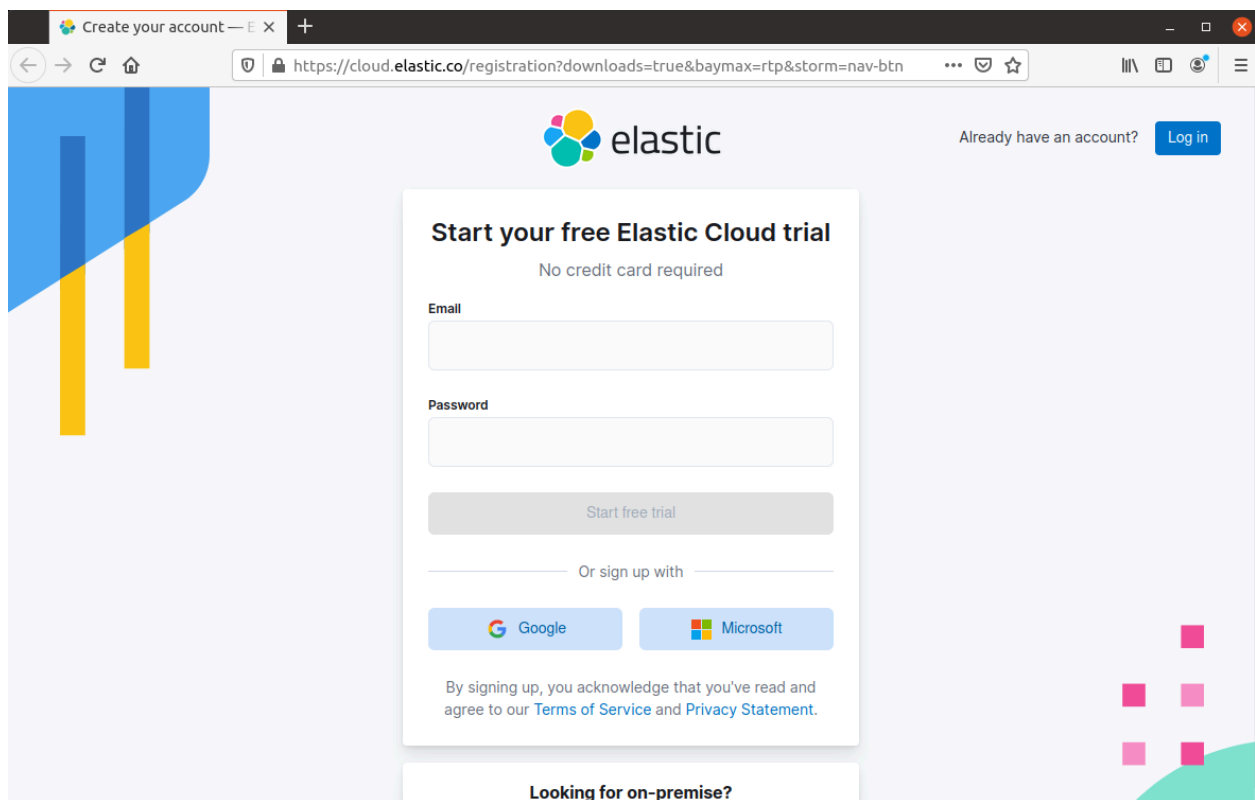
E - Elasticsearch

L - Logstash

K - Kibana

ELK is a SIEM that enables defenders to detect attacks and conduct threat hunting.

Step 1: Create an account using [this link](https://cloud.elastic.co/registration?downloads=true&baymax=rtp&storm=nav-btn)

A screenshot of a web browser showing the Elastic Cloud registration page. The browser's address bar displays the URL: https://cloud.elastic.co/registration?downloads=true&baymax=rtp&storm=nav-btn. The page features the Elastic logo at the top center. To the right of the logo, there is a link "Already have an account?" and a "Log in" button. The main content area is a white card titled "Start your free Elastic Cloud trial" with the subtext "No credit card required". Below this, there are input fields for "Email" and "Password". A "Start free trial" button is positioned below the password field. Further down, there is a section "Or sign up with" with buttons for "Google" and "Microsoft". At the bottom of the card, a small text states: "By signing up, you acknowledge that you've read and agree to our Terms of Service and Privacy Statement." Below the registration card, there is a link "Looking for on-premise?". The background of the page is light purple with abstract blue and yellow shapes on the left and pink and teal shapes on the right.

After logging in, fill in all the details and proceed ahead.

Step 2: Create an ELK instance

Give the deployment some name and click “Create Deployment”

Create your first deployment

A deployment includes Elasticsearch, Kibana, and other Elastic Stack features, allowing you to store, search, and analyze your data.

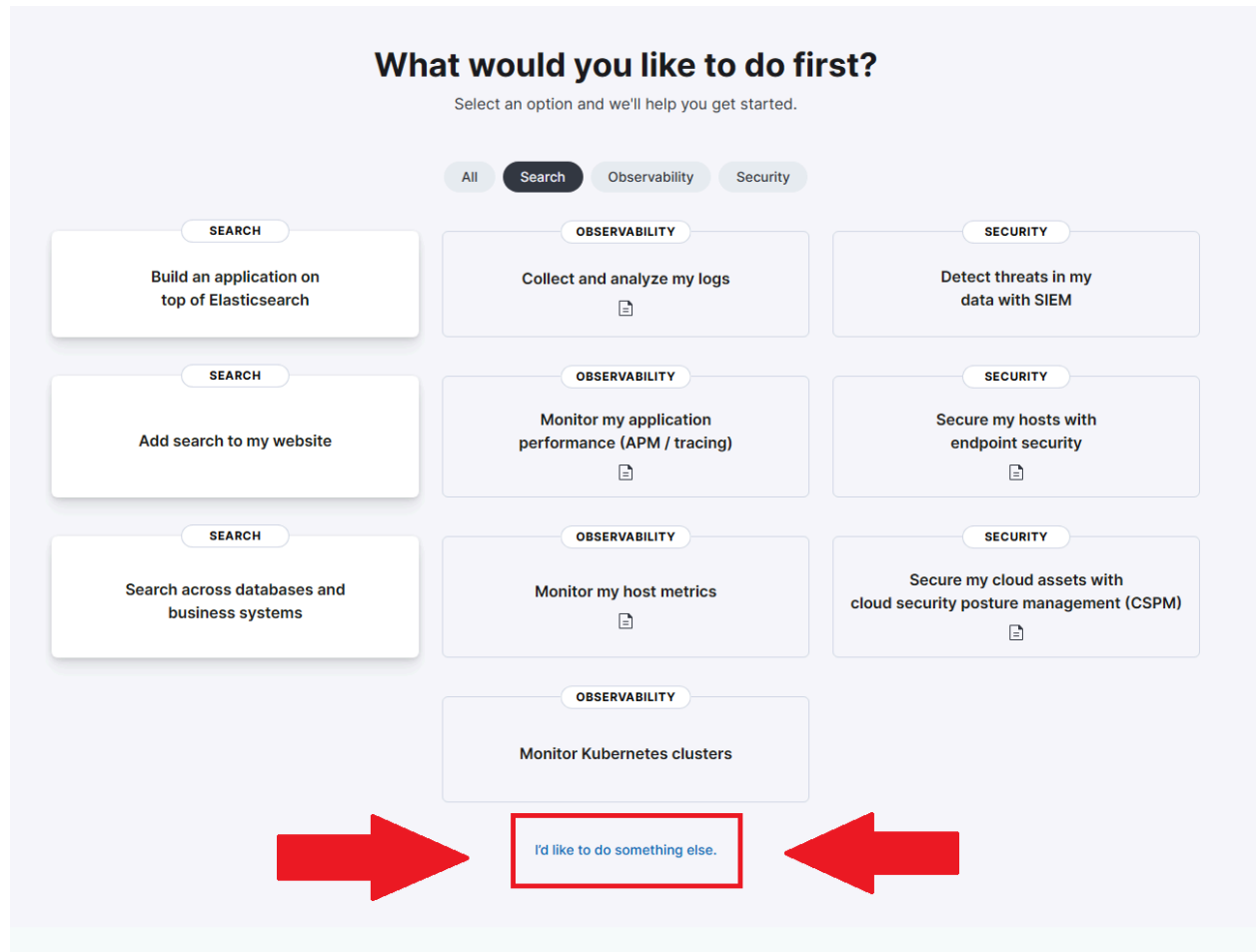
Name

My deployment

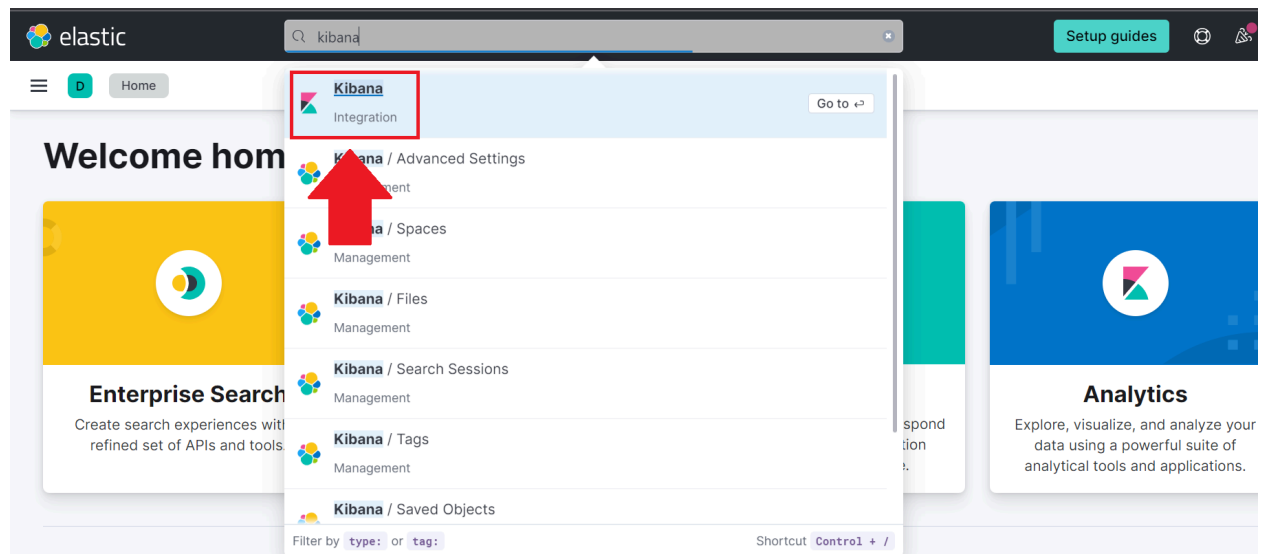


GCP Iowa (us-central1) [Edit settings](#)
Storage optimized, 8.8.1

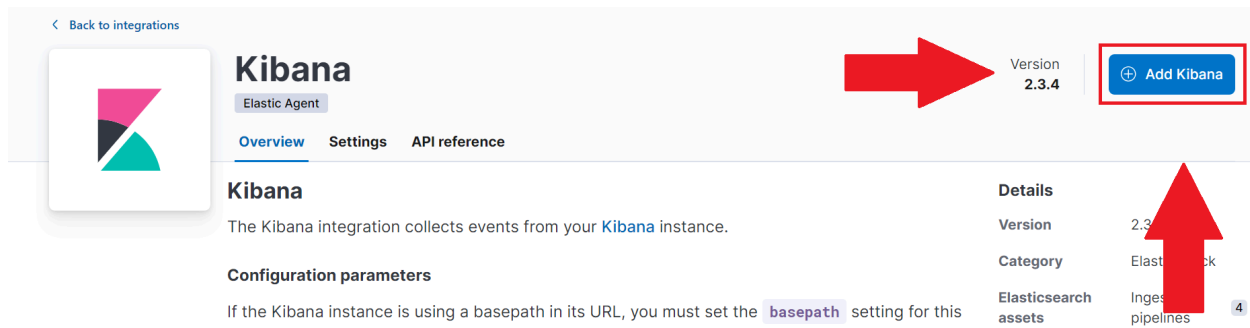
Create deployment



At the top of the search bar, search for "Kibana"



Once Kibana is selected, click on Add Kibana



Back to integrations

Kibana

Elastic Agent

Overview Settings API reference

The Kibana integration collects events from your [Kibana](#) instance.

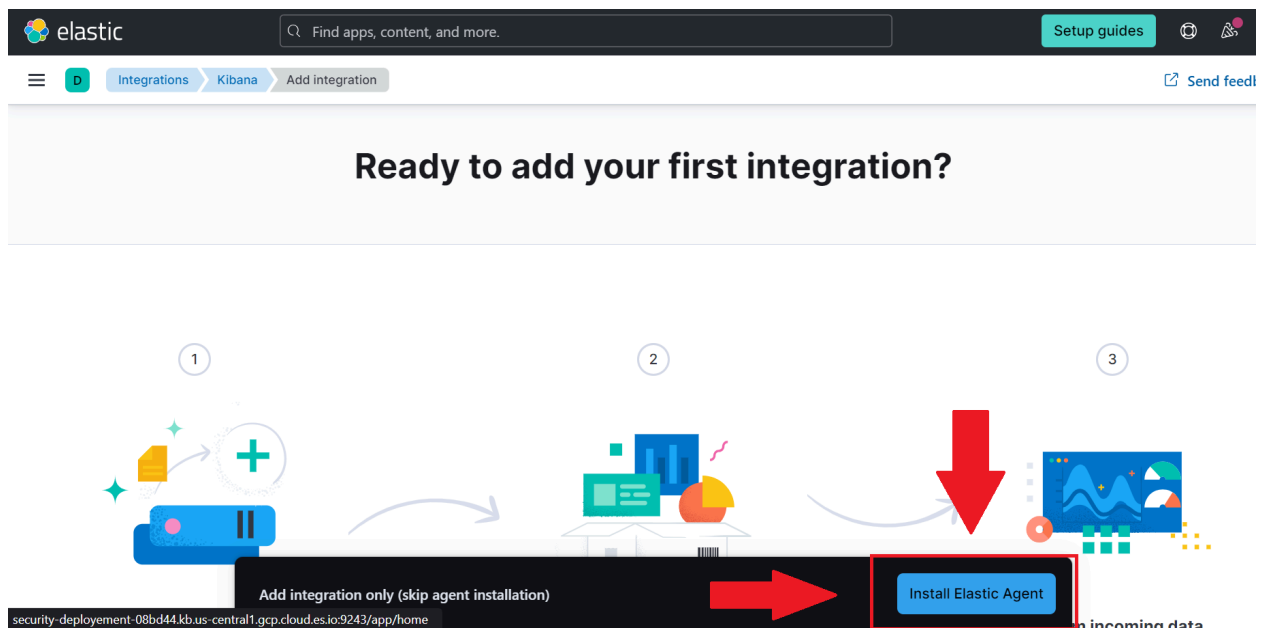
Configuration parameters

If the Kibana instance is using a basepath in its URL, you must set the `basepath` setting for this

Details

Version	2.3.4
Category	Elasticsearch
Elasticsearch assets	Ingest pipelines 4

We will next be prompted to "Install Elastic Agent" This is what we are going to put on our machine that monitors what's happening. Click "Install Elastic Agent"



elastic

Find apps, content, and more.

Setup guides

Integrations Kibana Add integration

Send feed

Ready to add your first integration?

1 2 3

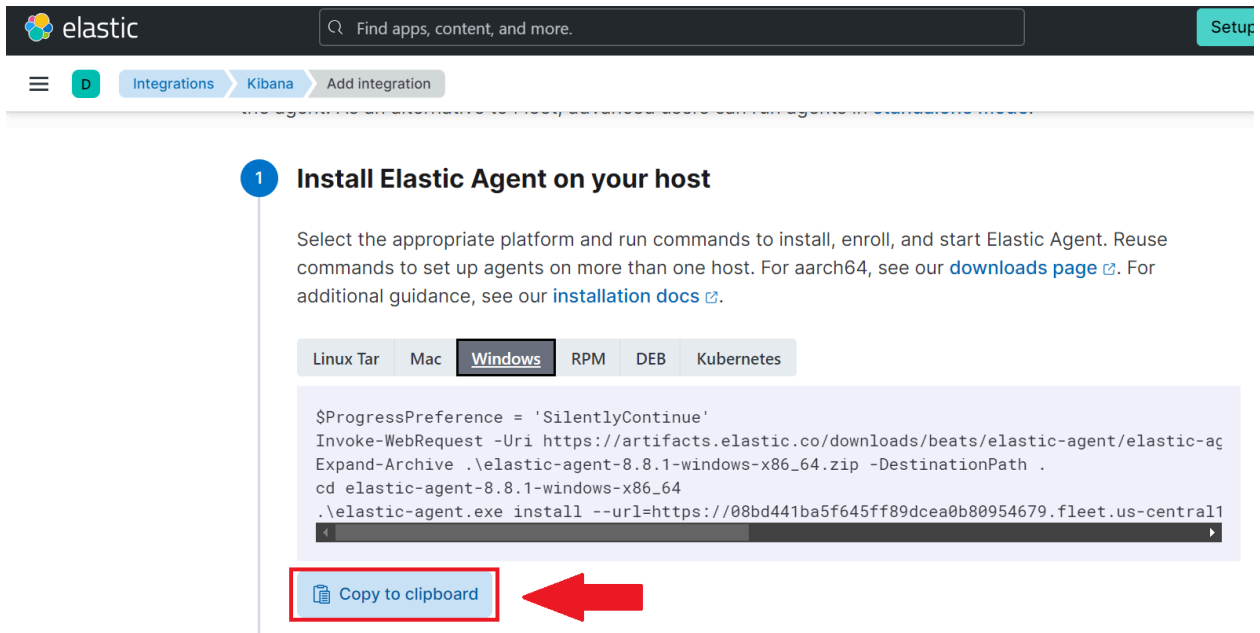
Add integration only (skip agent installation)

Install Elastic Agent

security-deployment-08bd44.kb.us-central1.gcp.cloud.es.io:9243/app/home

incoming data

Next, we add the Elastic Agent to our host machine. I am selecting Windows



The screenshot shows the Elastic Agent installation page. At the top, there's a navigation bar with the Elastic logo, a search bar, and a 'Setup' button. Below the navigation bar, there's a breadcrumb trail: 'Integrations > Kibana > Add integration'. The main heading is '1 Install Elastic Agent on your host'. Below this, there's a paragraph explaining the installation process. Then, there's a tabbed interface with tabs for 'Linux Tar', 'Mac', 'Windows' (which is selected), 'RPM', 'DEB', and 'Kubernetes'. Below the tabs, there's a code block containing the installation commands for Windows. At the bottom of the code block, there's a 'Copy to clipboard' button, which is highlighted with a red box and a red arrow pointing to it.

```
$ProgressPreference = 'SilentlyContinue'  
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.8.1-windows-x86_64.zip -DestinationPath .  
Expand-Archive .\elastic-agent-8.8.1-windows-x86_64.zip -DestinationPath .  
cd elastic-agent-8.8.1-windows-x86_64  
.\elastic-agent.exe install --url=https://08bd441ba5f645ff89dcea0b80954679.fleet.us-central1
```

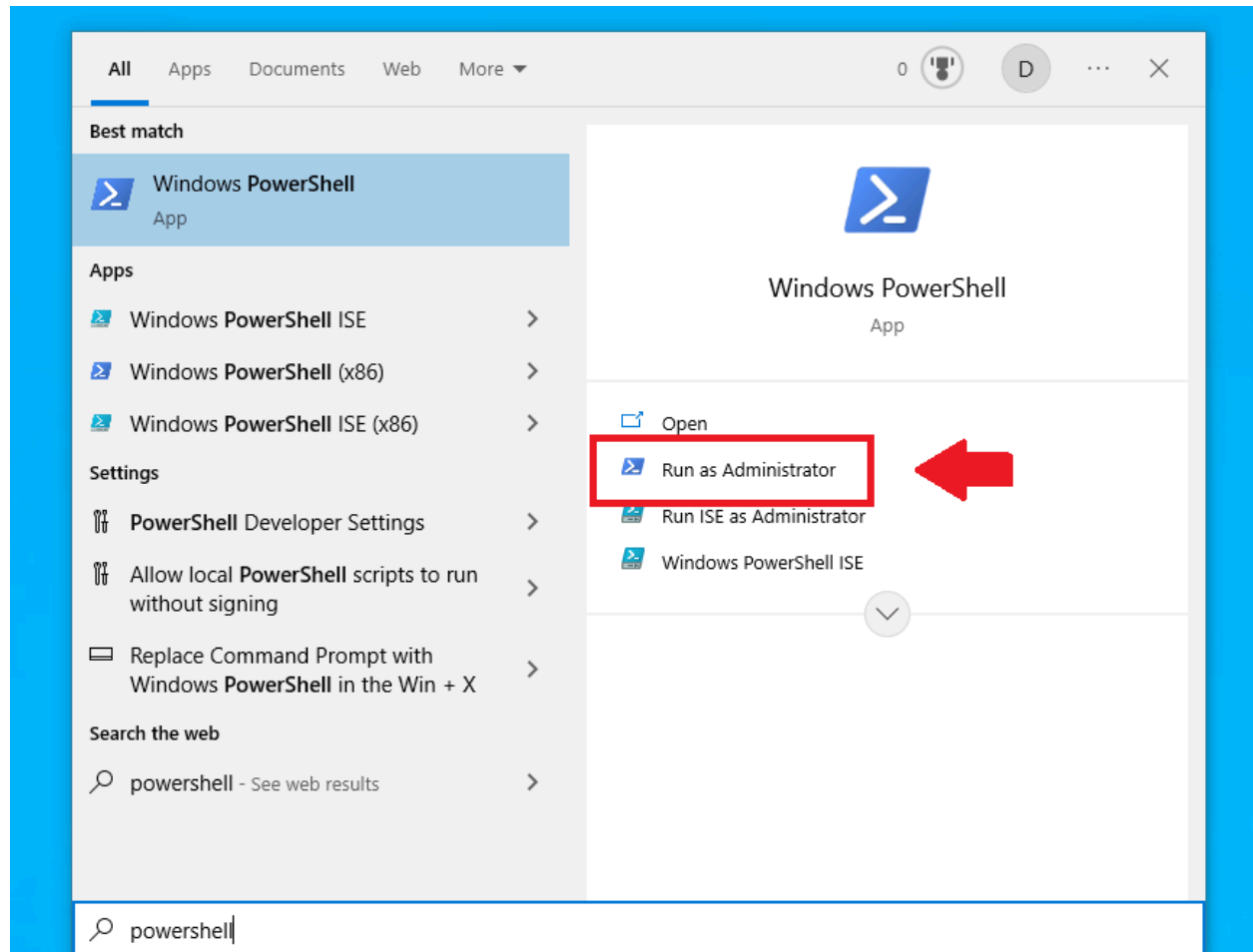
Copy to clipboard

Note: We should hold on to this command because we will be using it in the future. I just saved it in a notepad file called agent.txt

The ELK stack is now configured and we have our connection information saved. Part two will cover how to install and configure an Elastic Agent.

Step 3: Downloading the Elastic Agent

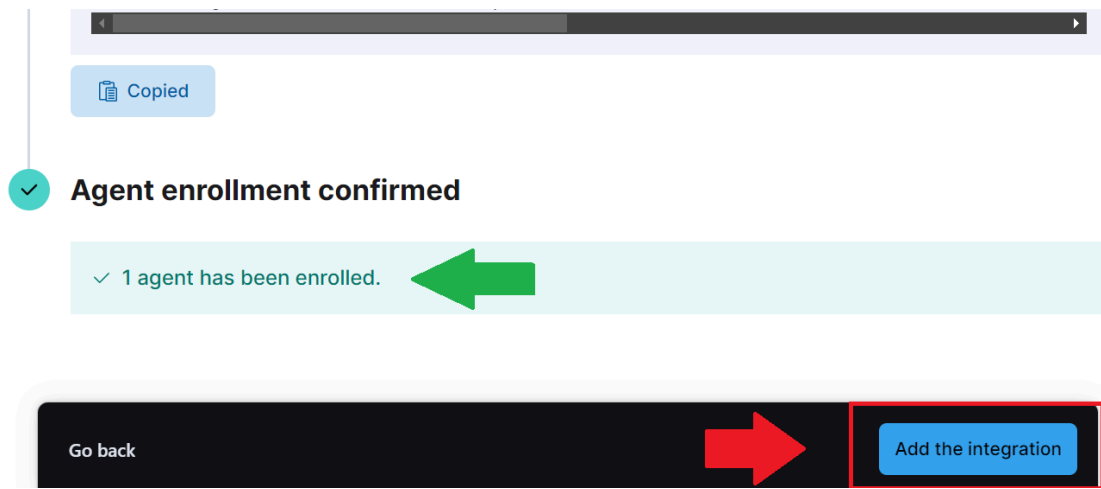
Press the Windows button search “Powershell” and run it as administrator



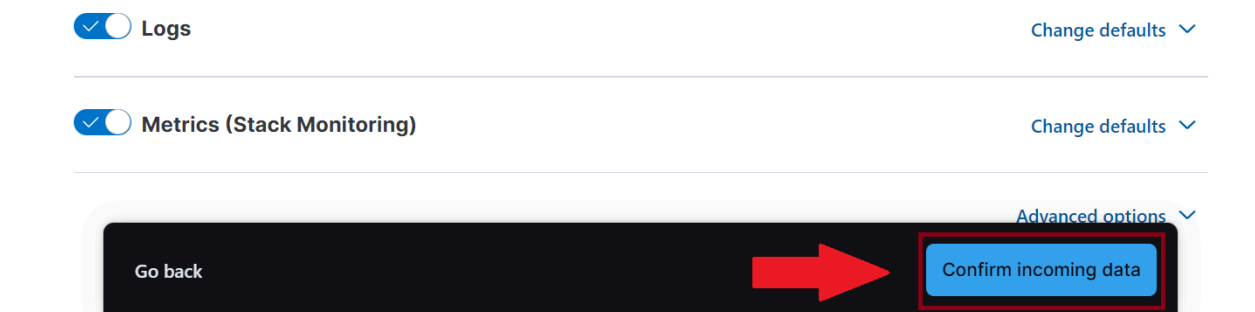
Once PowerShell is opened, copy and paste the agent information that we have copied one by one. Enter “Y” wherever prompted

```
PS C:\Windows\system32> $ProgressPreference = 'SilentlyContinue'
PS C:\Windows\system32> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.8.1-windows-x86_64.zip -OutFile elastic-agent-8.8.1-windows-x86_64.zip
PS C:\Windows\system32> Expand-Archive .\elastic-agent-8.8.1-windows-x86_64.zip -DestinationPath .
PS C:\Windows\system32> cd elastic-agent-8.8.1-windows-x86_64
PS C:\Windows\system32> .\elastic-agent.exe install --url=https://08bd441-5f645ff80dcaa0b80954679.fleet.us-central1.amazonaws.com/elastic-agent-8.8.1-windows-x86_64 --fleet-url=https://08bd441-5f645ff80dcaa0b80954679.fleet.us-central1.amazonaws.com/elastic-agent-8.8.1-windows-x86_64 --enroll-key=08bd441-5f645ff80dcaa0b80954679
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to install? [Y/n] y
{"log.level":"info","@timestamp":"2023-06-13T14:32:32.750-0700","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":470},"message":"Starting Elastic Agent"}
{"log.level":"info","@timestamp":"2023-06-13T14:32:39.966-0700","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":276},"message":"Successfully enrolled the Elastic Agent."}
Elastic Agent has been successfully installed.
PS C:\Windows\system32\elastic-agent-8.8.1-windows-x86_64>
```

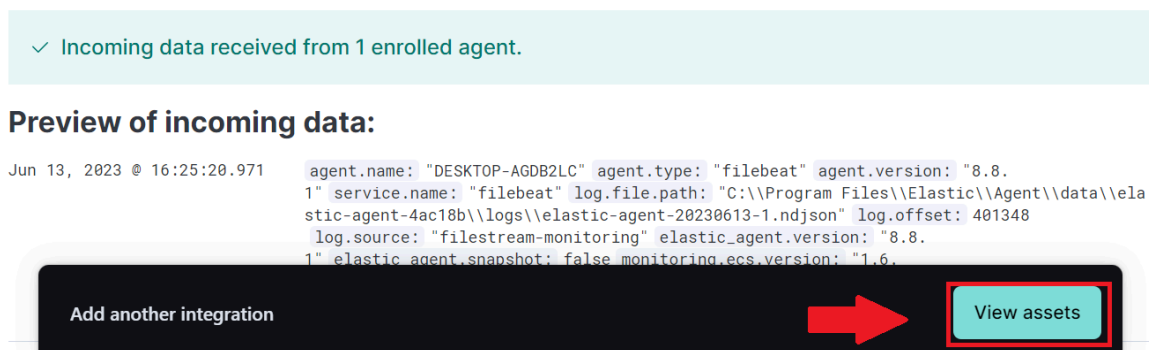
Go back to the browser and you can see “1 agent has been enrolled” click on “Add the integration”



On the next page leave everything default and click "Confirm Incoming Data".

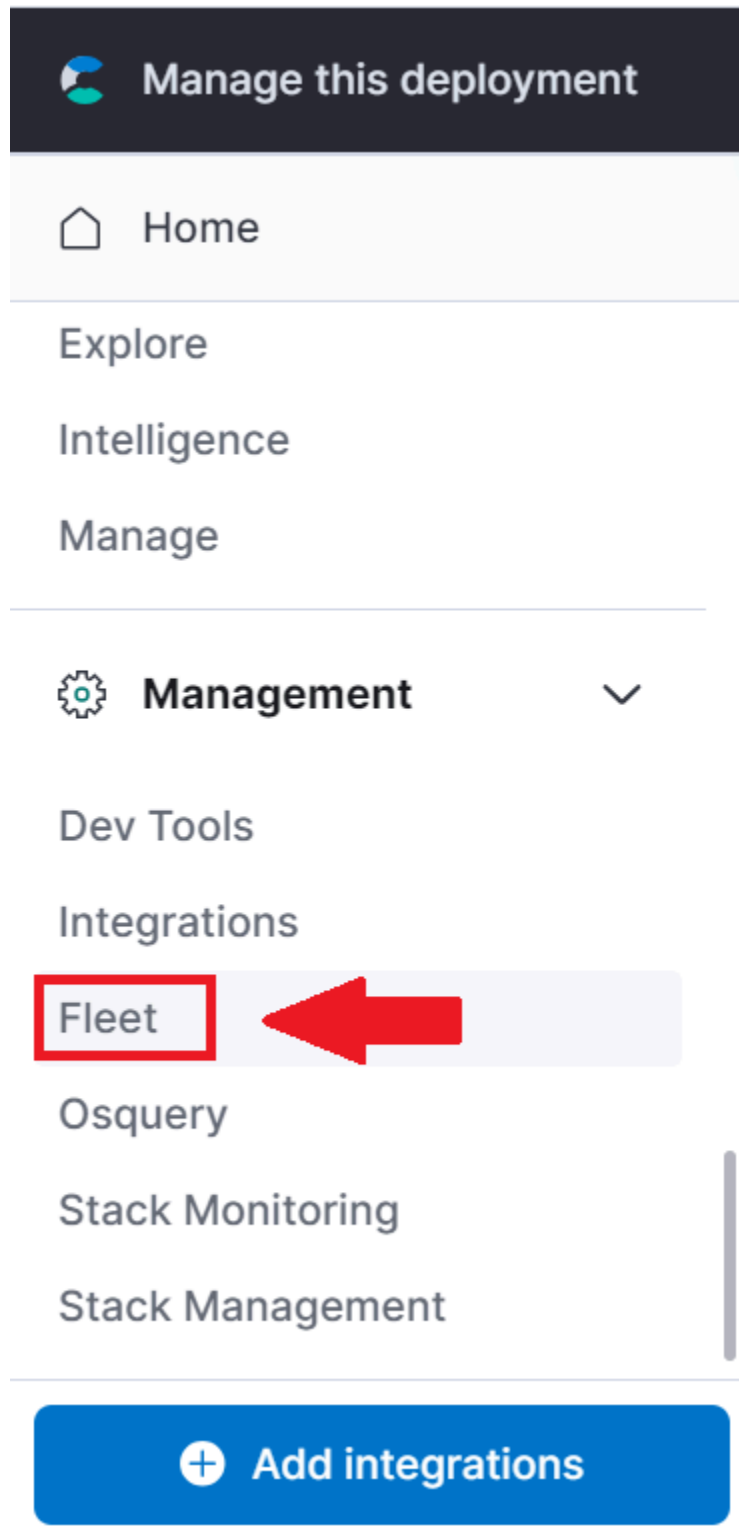


The browser will take a few seconds to confirm the machine is connected, once thats finished click "View Assets"



Step 4: Check the Fleet

Go to the hamburger menu, navigate to Management, and click on “Fleet”



Make sure that the device is connected

<input type="checkbox"/>	Status	Host	Agent policy	CPU ⓘ	Memory ⓘ	Last activity	Version	Actions
<input type="checkbox"/>	Healthy	DESKTOP-AGDB2LC	My first agent policy rev. 2	94 %	88 MB	23 seconds ago	8.8.1	...

Our Elastic Agent is installed and configured to be connected to our ELK instance in the cloud.

Step 5: Download Sysmon

Use [this link](#) to download Sysmon

Microsoft | Docs Documentation Learn Q&A Code Samples

Sysinternals Downloads Community Resources

Docs / Sysinternals / Downloads

Filter by title

Security Utilities

Autologon

LogonSessions

NewSID

PsLoggedOn

PsLogList

RootkitRevealer

Sysmon

> System Information

> Miscellaneous

Sysinternals Suite

Community

> Resources

Software License Terms

Licensing FAQ

Download PDF

Sysmon v13.10

04/21/2021 • 14 minutes to read • +2

By Mark Russinovich and Thomas Garnier

Published: April 21, 2021

[Download Sysmon](#) (2.9 MB)

Introduction

System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using [Windows Event Collection](#) or [SIEM](#) agents and subsequently analyzing them, you can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

Note that *Sysmon* does not provide analysis of the events it generates, nor does it attempt to protect or hide itself from attackers.

Is this page helpful?

Yes No

In this article

[Introduction](#)

[Overview of Sysmon](#)

[Capabilities](#)

[Screenshots](#)

[Usage](#)

[Examples](#)

[Events](#)

[Configuration files](#)

[Configuration Entries](#)

[Event filtering entries](#)

Once downloaded, extract the contents to the Downloads folder

After it's done, click on the Windows icon type "Powershell" and run it as administrator.

In your PowerShell window, enter the following command. You will need to substitute [USER] for the user you are using on your local system.

```
cd C:\Users\[USER]\Downloads\Sysmon\
```

The following command will install and start Sysmon as a service.

```
.\Sysmon.exe -i -n -accepteula
```

The output would look like this:

```
PS C:\Windows\system32> cd C:\Users\Chris\Downloads\Sysmon
PS C:\Users\Chris\Downloads\Sysmon> .\Sysmon.exe -i -n -acceptula

System Monitor v15.12 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Usage:
Install:          Sysmon.exe -i [<configfile>]
Update configuration: Sysmon.exe -c [<configfile>]
Install event manifest: Sysmon.exe -m
Print schema:     Sysmon.exe -s
Uninstall:        Sysmon.exe -u [force]
  -c Update configuration of an installed Sysmon driver or dump the
      current configuration if no other argument is provided. Optionally
      take a configuration file.
  -i Install service and driver. Optionally take a configuration file.
  -m Install the event manifest (done on service install as well)).
  -s Print configuration schema definition of the specified version.
      Specify 'all' to dump all schema versions (default is latest)).
  -u Uninstall service and driver. Adding force causes uninstall to proceed
      even when some components are not installed.

The service logs events immediately and the driver installs as a boot-start driver to capture activity from early in
the boot that the service will write to the event log when it starts.

On Vista and higher, events are stored in "Applications and Services Logs/Microsoft/Windows/Sysmon/Operational". On
older systems, events are written to the System event log.

Use the '-? config' command for configuration file documentation. More examples are available on the Sysinternals
website.

Specify -accepteula to automatically accept the EULA on installation, otherwise you will be interactively prompted to
accept it.

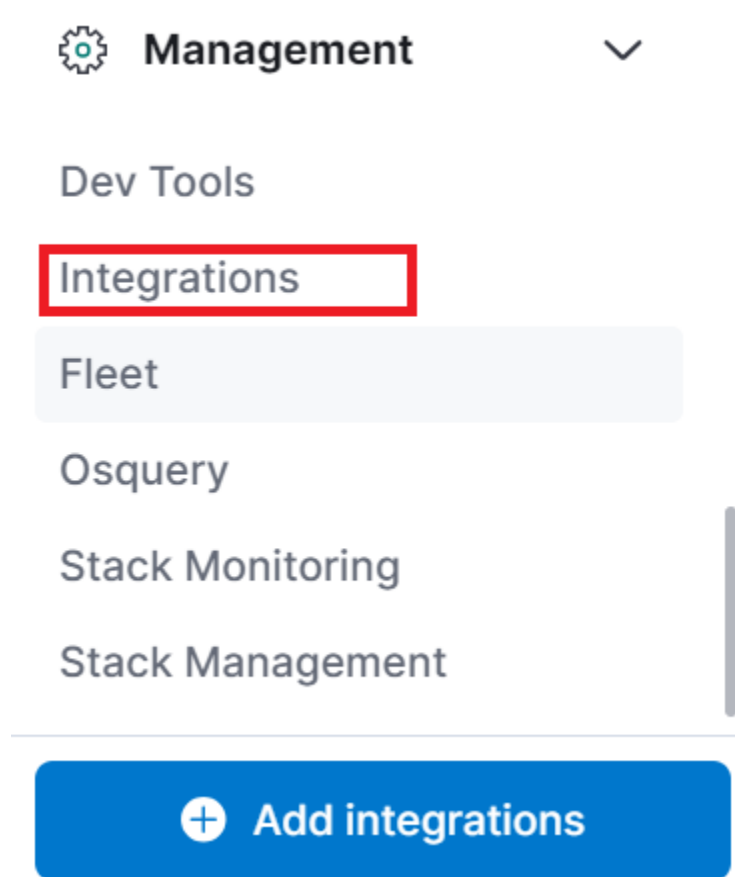
Neither install nor uninstall requires a reboot.

PS C:\Users\Chris\Downloads\Sysmon>
```

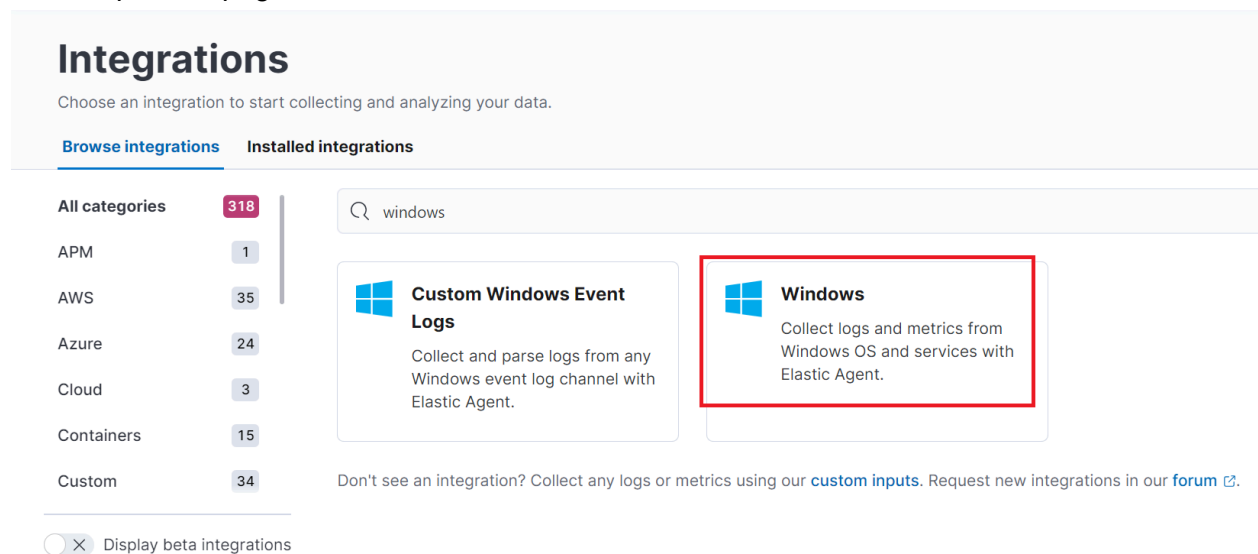
Now that Sysmon is running on our system, we need to configure our Elastic agent to gather these logs. Sign into your cloud account.

[Elastic Cloud Login](#)

Navigate to "Integrations" through the navigation menu.



At the top of the page enter "windows" into the search bar. Select "Windows"



Add the Windows Integration

By default, the Sysmon logs channel should be active. This can be checked under the "Collect events from the following Windows event log channels:" section of the "Add Integration" page.

☒ **Collect events from the following Windows event log channels:** ^

☒ Forwarded
Collect ForwardedEvents channel logs

☒ Powershell
Windows Powershell channel

☒ Powershell Operational
Microsoft-Windows-
Powershell/Operational channel

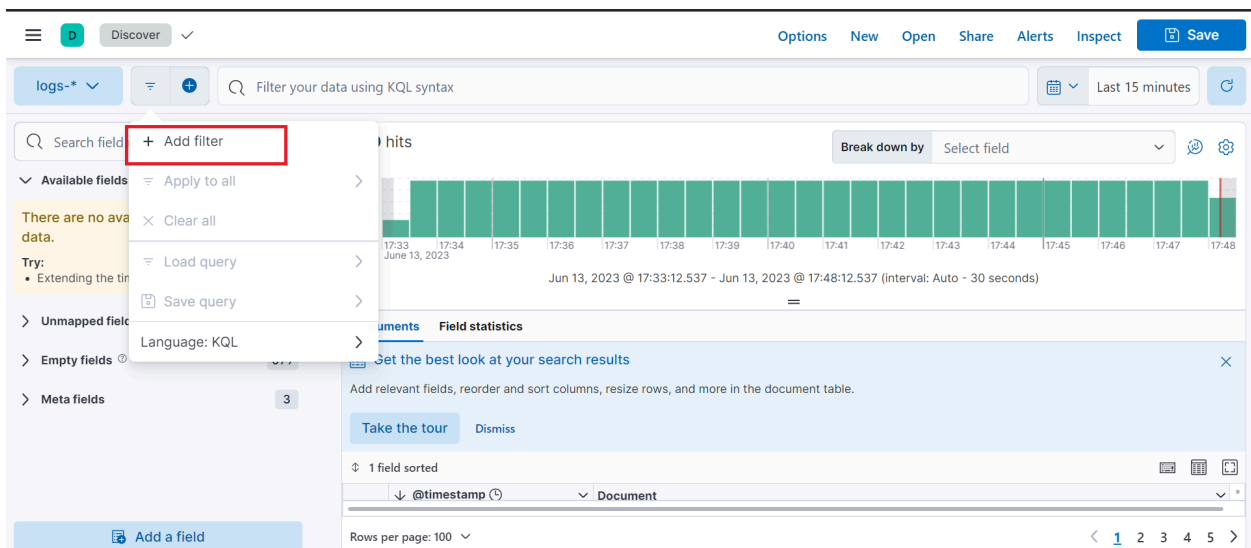
☒ Sysmon Operational
Collect Microsoft-Windows-
Sysmon/Operational channel logs

Click Save and Continue

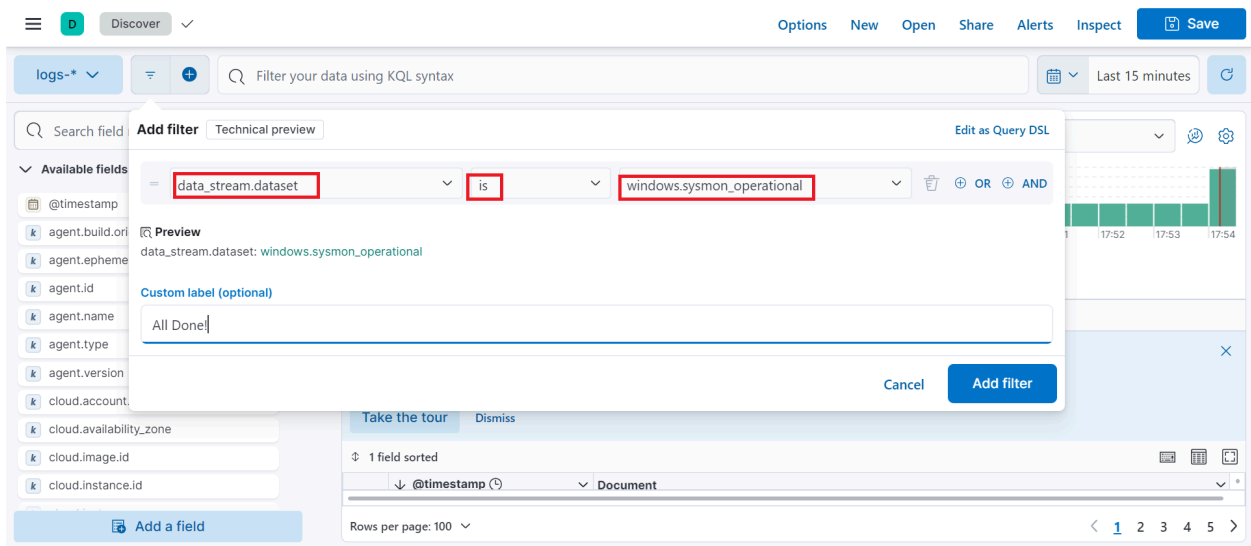
When prompted click "Add elastic agent to your hosts".

Now that we've configured the ELK in the cloud, play around and make some log activities like making a few Google searches, adding files, deleting files, moving files, etc.

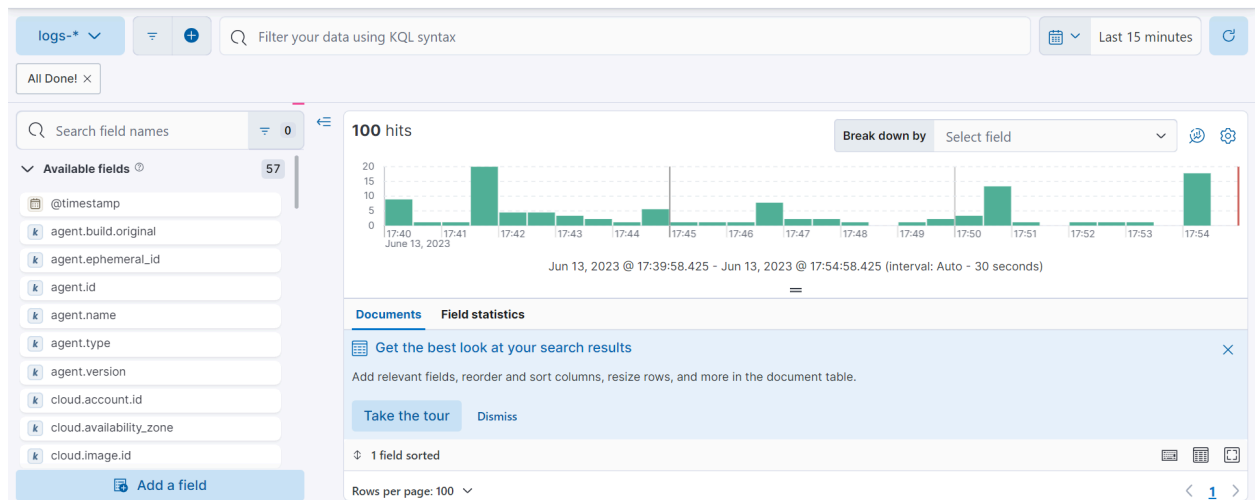
After you have created some log activity, navigate to "Discover" by accessing the hamburger menu on the top left.



Set a filter on your data to limit your results to sysmon data. This can be done by searching the "data_stream.dataset" field for "windows.sysmon_operational" data. Then click "add filter". Your filter should now be set.



If you have a result and not an error, your Sysmon data is being collected and sent to Elastic.



Note: I have only used the Elasticsearch and Kibana of ELK and the Logstash isn't being implemented