Setting Up Elk in the Cloud

Introduction

ELK is a combination of three technologies that enables you to work with large data sets such as security logs and much more. ELK simply stands for Elasticsearch, Logstash, and Kibana, each of which are briefly described below:

- Elasticsearch: Elasticsearch is essentially the database for the logs.
- Logstash: Logstash is a data processing pipeline that ingests data from multiple sources, transforms it, and then sends it to a stash like Elasticsearch.
- Kibana: Kibana is the web interface to the Elasticsearch database. It is a data visualisation and exploration tool used for viewing, searching, and visualising data indexed in Elasticsearch.

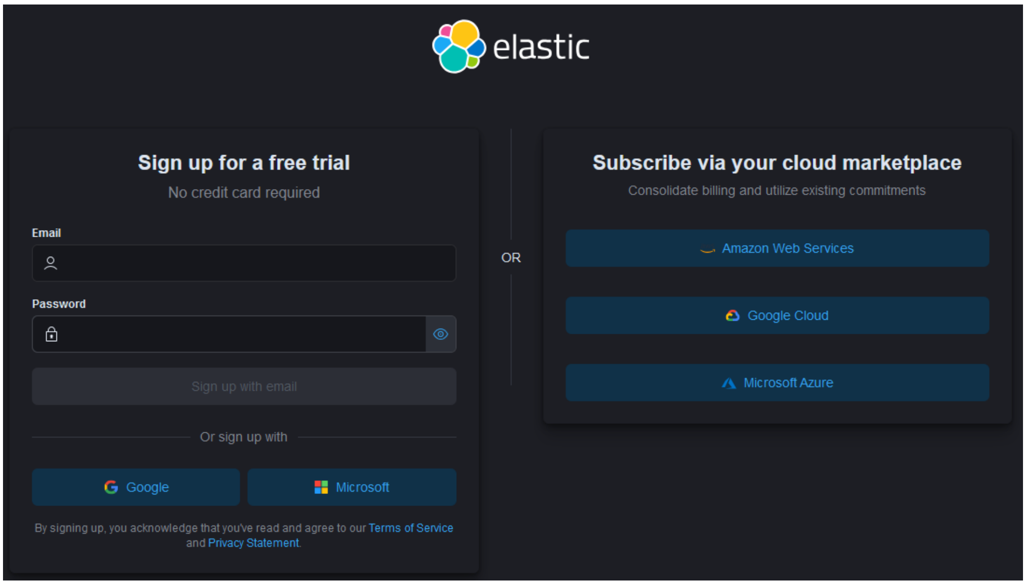
Together, the ELK stack allows for efficient data ingestion, storage, search, and visualisation. Please note, I am in no way proficient in this area of knowledge. I have some familiarity with using the ELK stack, however I have never deployed my own ELK stack, nor have I used ELK to investigate legitimate incidents. Therefore, I used the following amazing resources to help me deploy the ELK stack in the cloud:

- Primary resource, outlines a step-by-step tutorial on how to deploy ELK in the cloud for free.
- Video tutorial covering the same thing as the previous resource (by John Hammond)
- Video tutorial on how to deploy and configure a custom ELK stack locally
- Video tutorial on how to deploy and configure HELK, which is a custom implementation of ELK used for threat hunting

Signing up for a free Elastic cloud trial

Fortunately, to have fun and mess around with ELK you don't need to deploy your own servers/VMs or even spend money, Elastic Cloud is kind enough to provide a free 14-day trial without a credit card. You can sign up to the free trial here.

To start, create an account by entering an email address and password:



Sign up for a free trial

No credit card required

Email

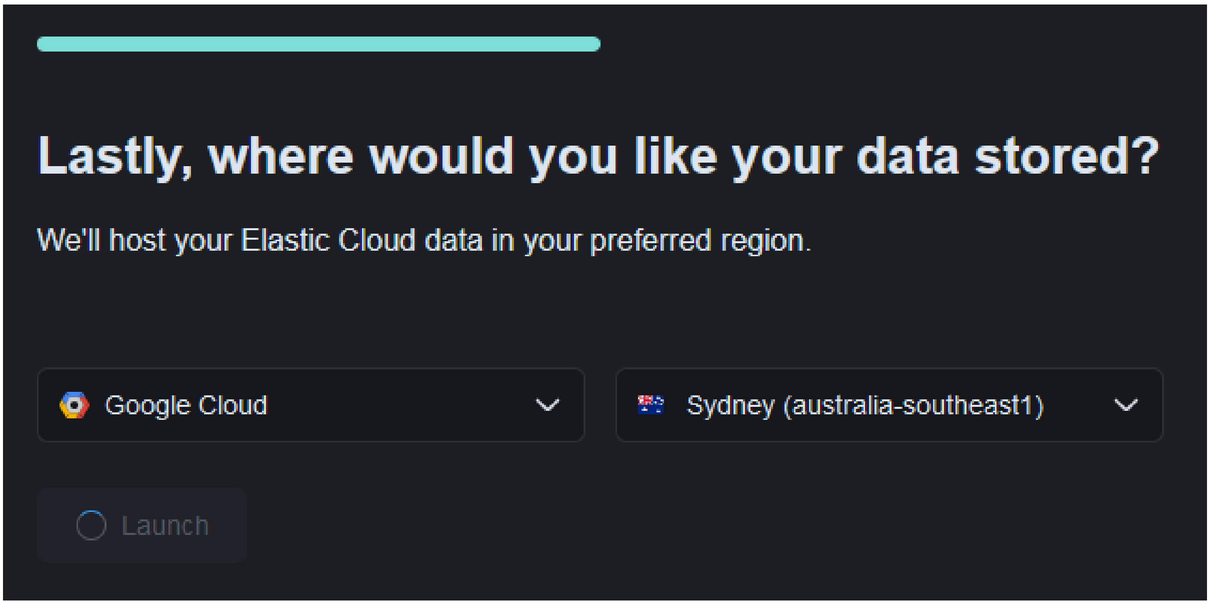
Password

By signing up, you acknowledge that you've read and agree to our Terms of Service and Privacy Statement.

Subscribe via your cloud marketplace

Consolidate billing and utilize existing commitments

Once you have verified your email address and logged in you will be required to fill out several forms, the information in these forms aren't really important. However, once you have completed this process and reached the last step, I recommend choosing a cloud provider closest to you. After doing so, simply click the launch button:



Lastly, where would you like your data stored?

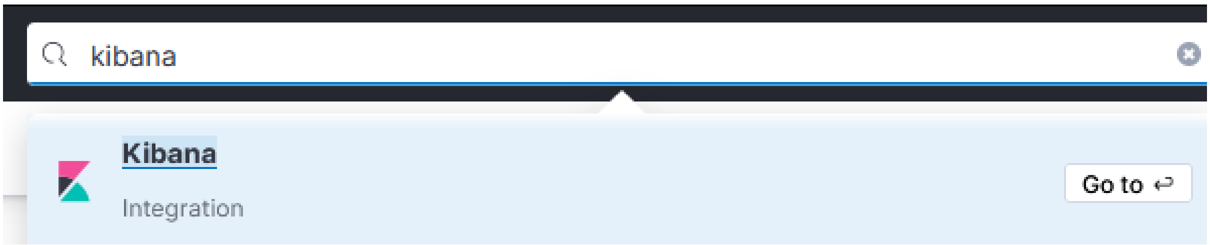
We'll host your Elastic Cloud data in your preferred region.

Google Cloud

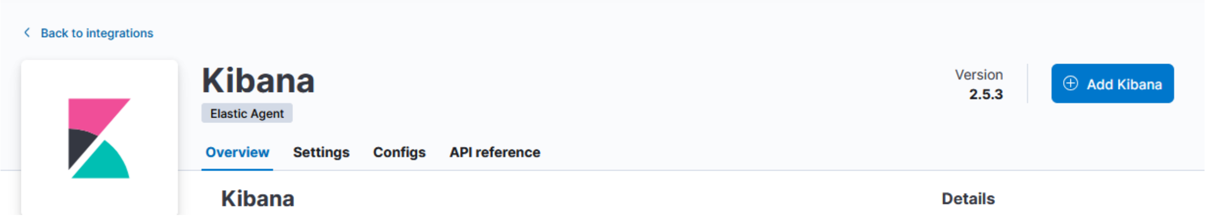
Sydney (australia-southeast1)

Start an ELK instance

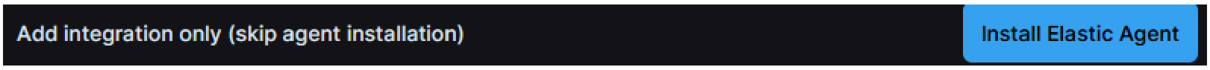
After the previous process has completed, you will be presented with an elastic landing page, simply search for Kibana at the top of the screen like as follows:



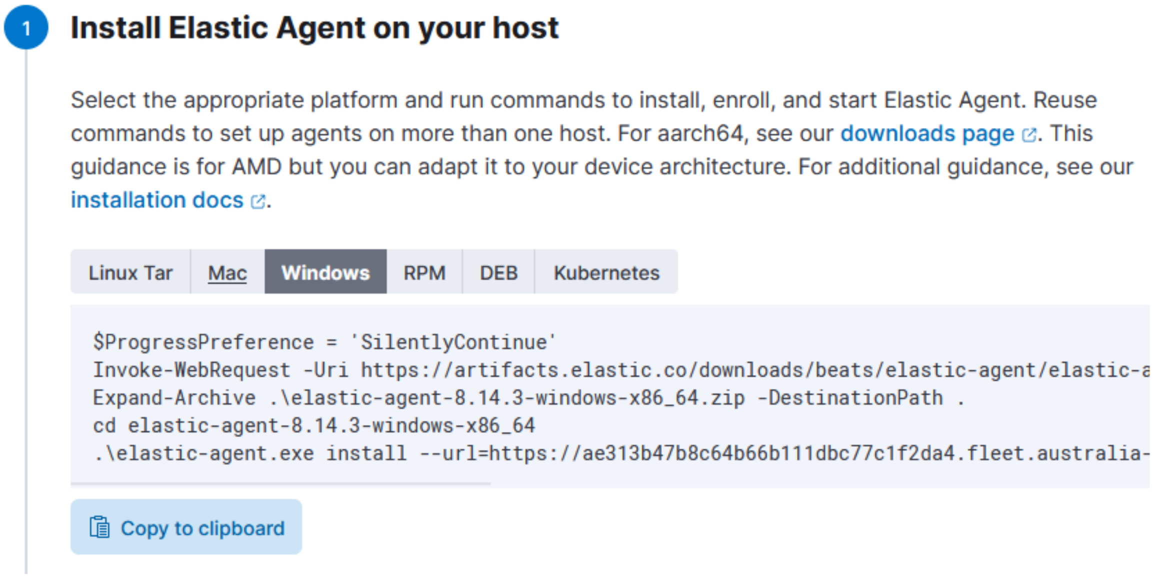
Hit enter or left-click. Then simply click the ‘Add Kibana’ button on the following page:



You will then be prompted to install Elastic Agent; this is what you are going to put on your machine to monitor what’s going on. Simply click the blue button:



Then select where you want the Elastic Agent (what host, i.e., Windows, Linux, etc). In this case, I am going to select Windows:



Install Elastic Agent on your host

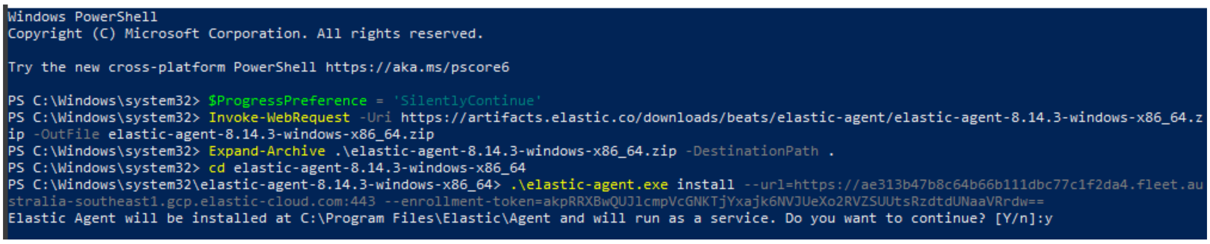
Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our downloads page. This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our installation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

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-a
Expand-Archive .\elastic-agent-8.14.3-windows-x86_64.zip -DestinationPath .
cd elastic-agent-8.14.3-windows-x86_64
.\elastic-agent.exe install --url=https://ae313b47b8c64b66b111dbc77c1f2da4.fleet.australia-
```

Also make sure to click the ‘Copy to clipboard’ button as this is what we enter on the machine we want to install the agent on.

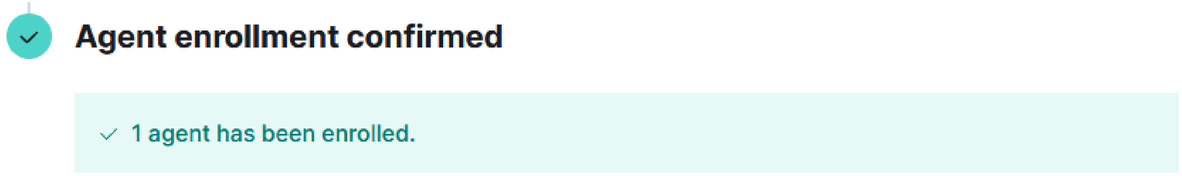
Download the Elastic Agent

Before diving into how to install the elastic agent on a machine, I want to note that I'm personally installing it on a freshly created Windows 10 VM. Whatever machine you install it on, if you want to follow along with me, make sure it's a Windows based machine because we will be installing Sysmon later to produce more detailed logs better tailored for cybersecurity. To install the agent on a Windows machine, enter the text you copied previously into a PowerShell instance that is running as administrator (also make sure to enter y and hit enter when prompted):



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> $ProgressPreference = 'SilentlyContinue'
PS C:\Windows\system32> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.14.3-windows-x86_64.z
ip -OutFile elastic-agent-8.14.3-windows-x86_64.zip
PS C:\Windows\system32> Expand-Archive .\elastic-agent-8.14.3-windows-x86_64.zip -DestinationPath .
PS C:\Windows\system32> cd elastic-agent-8.14.3-windows-x86_64
PS C:\Windows\system32\elastic-agent-8.14.3-windows-x86_64> .\elastic-agent.exe install --url=https://ae313b47b8c64b66b111dbc77c1f2da4.fleet.au
stralia-southeast1.gcp.elastic-cloud.com:443 --enrollment-token=akpRRXBwQUJ1cmpVcGNKTjYxajk6NVJUeXo2RVZSUUtsRzdtdUNaaVRrdw==
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
```

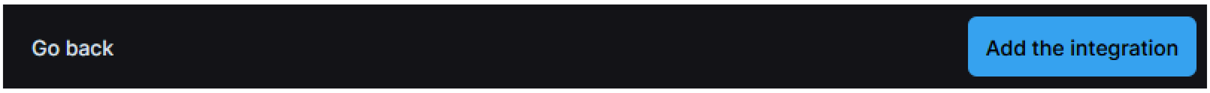
If you then switch back to your Kibana instance in the browser, you should see that 1 agent has been enrolled:



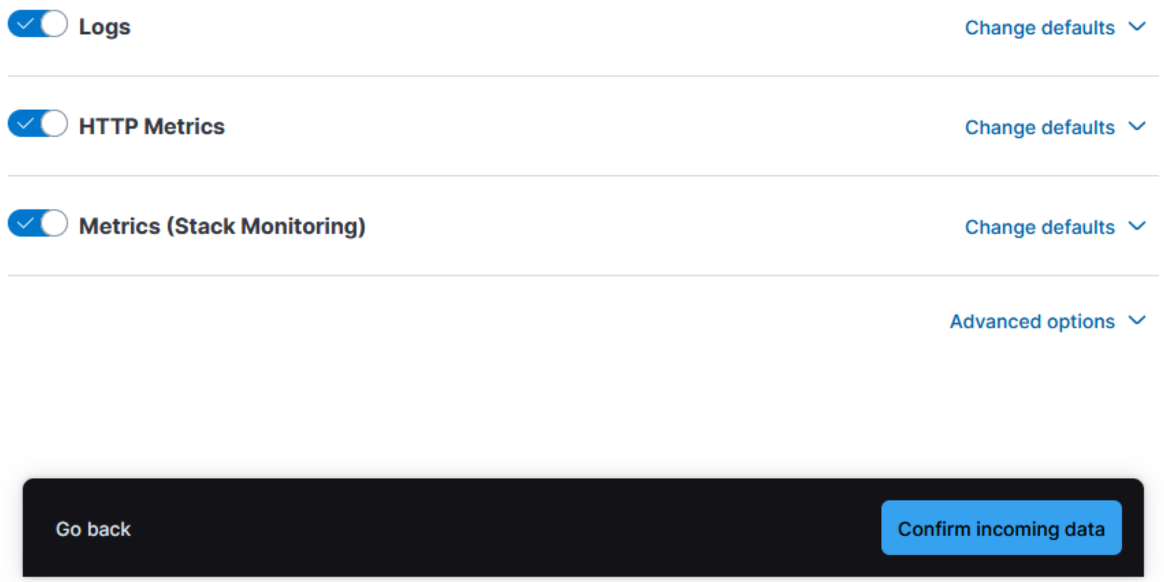
Agent enrollment confirmed

✓ 1 agent has been enrolled.

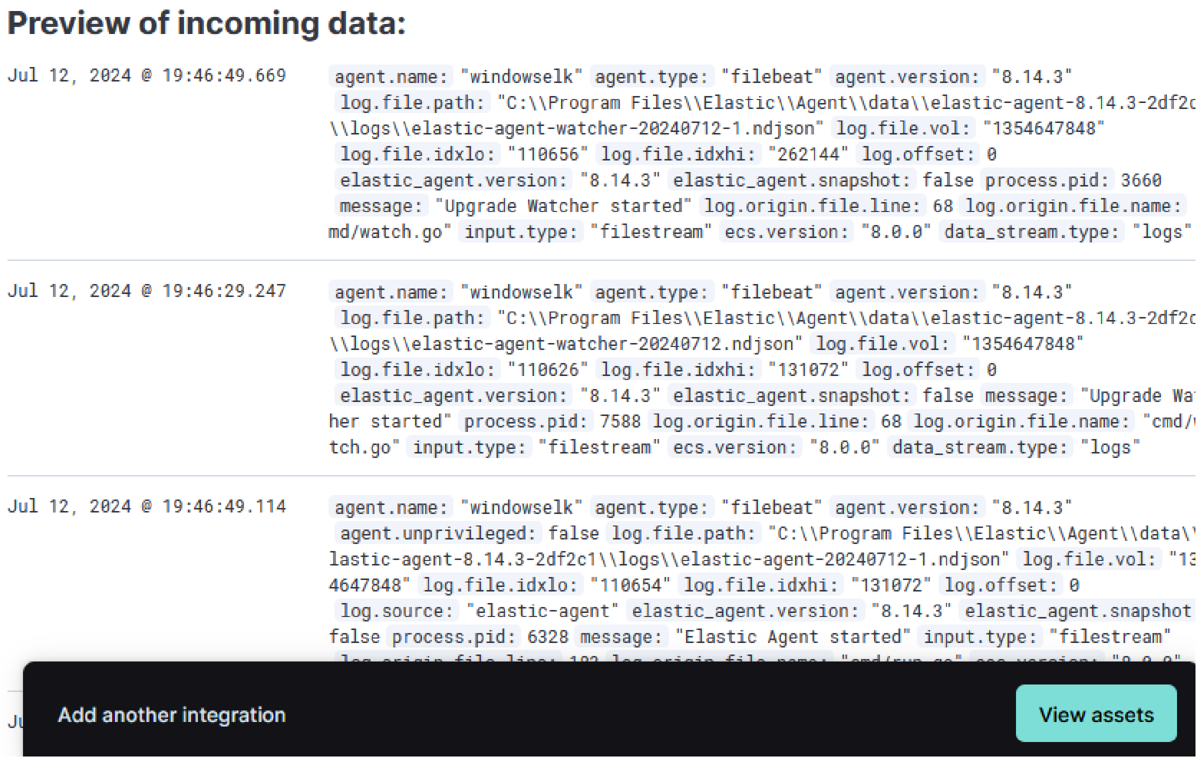
Then click 'Add to integration':



On the next page leave everything default and click 'Confirm Incoming Data':



Then click the view assets button:

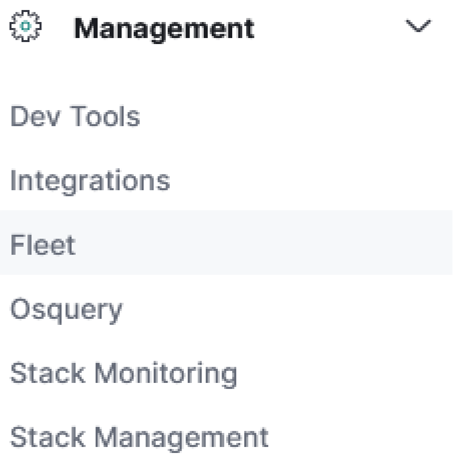


Preview of incoming data:

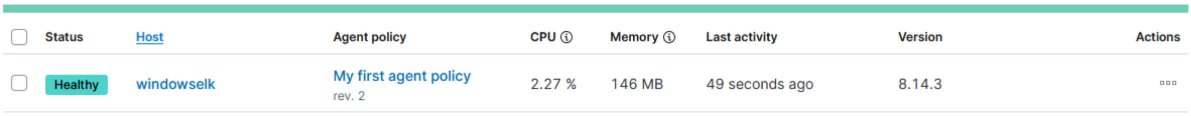
```
Jul 12, 2024 @ 19:46:49.669   agent.name: "windowselk" agent.type: "filebeat" agent.version: "8.14.3"
                              log.file.path: "C:\\Program Files\\Elastic\\Agent\\data\\elastic-agent-8.14.3-2df2c
                              \\logs\\elastic-agent-watcher-20240712-1.ndjson" log.file.vol: "1354647848"
                              log.file.idxlo: "110656" log.file.idxhi: "262144" log.offset: 0
                              elastic_agent.version: "8.14.3" elastic_agent.snapshot: false process.pid: 3660
                              message: "Upgrade Watcher started" log.origin.file.line: 68 log.origin.file.name:
                              md/watch.go" input.type: "filestream" ecs.version: "8.0.0" data_stream.type: "logs"

Jul 12, 2024 @ 19:46:29.247   agent.name: "windowselk" agent.type: "filebeat" agent.version: "8.14.3"
                              log.file.path: "C:\\Program Files\\Elastic\\Agent\\data\\elastic-agent-8.14.3-2df2c
                              \\logs\\elastic-agent-watcher-20240712.ndjson" log.file.vol: "1354647848"
                              log.file.idxlo: "110626" log.file.idxhi: "131072" log.offset: 0
                              elastic_agent.version: "8.14.3" elastic_agent.snapshot: false message: "Upgrade Wa
                              her started" process.pid: 7588 log.origin.file.line: 68 log.origin.file.name: "cmd/
                              tch.go" input.type: "filestream" ecs.version: "8.0.0" data_stream.type: "logs"

Jul 12, 2024 @ 19:46:49.114   agent.name: "windowselk" agent.type: "filebeat" agent.version: "8.14.3"
                              agent.unprivileged: false log.file.path: "C:\\Program Files\\Elastic\\Agent\\data\\
                              lastic-agent-8.14.3-2df2c1\\logs\\elastic-agent-20240712-1.ndjson" log.file.vol: "13
                              4647848" log.file.idxlo: "110654" log.file.idxhi: "131072" log.offset: 0
                              log.source: "elastic-agent" elastic_agent.version: "8.14.3" elastic_agent.snapshot
                              false process.pid: 6328 message: "Elastic Agent started" input.type: "filestream"
                              log.origin.file.line: 103 log.origin.file.name: "cmd/run.go" ecs.version: "8.0.0"
Ju
```

Check the Fleet

Once you have done everything stated above, make sure to see if the device has successfully connected. You can do this by navigating to the Fleet page:



On this page, you should see your host:

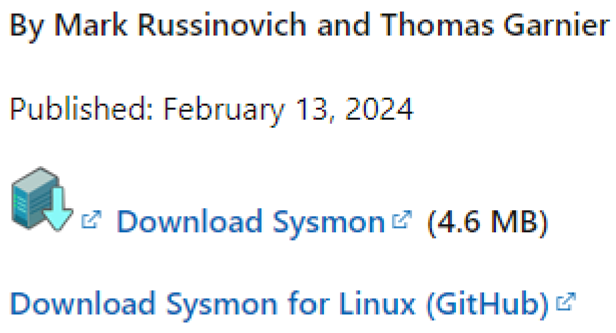


☐	Status	Host	Agent policy	CPU ⓘ	Memory ⓘ	Last activity	Version	Actions
☐	Healthy	windowselk	My first agent policy rev. 2	2.27 %	146 MB	49 seconds ago	8.14.3	···

If you can see your host, the Elastic Agent has been successfully installed and is connected to the ELK instance in the cloud. We will now cover how to configure Sysmon to submit more enriched logs to this Elastic agent, these logs will then be ingested to appear in Kibana.

Download Sysmon

Sysmon is a tool used to monitor and log events on Windows and is part of the Sysinternals package. To download Sysmon, navigate to here and download the zip file:



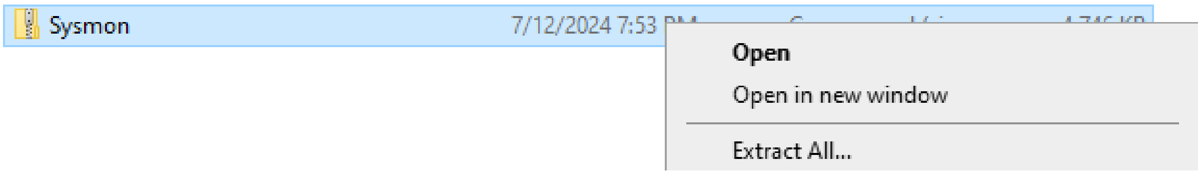
By Mark Russinovich and Thomas Garnier

Published: February 13, 2024

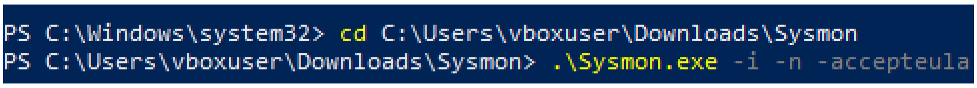
Download Sysmon (4.6 MB)

Download Sysmon for Linux (GitHub)

You then need to Extract the file like as follows:

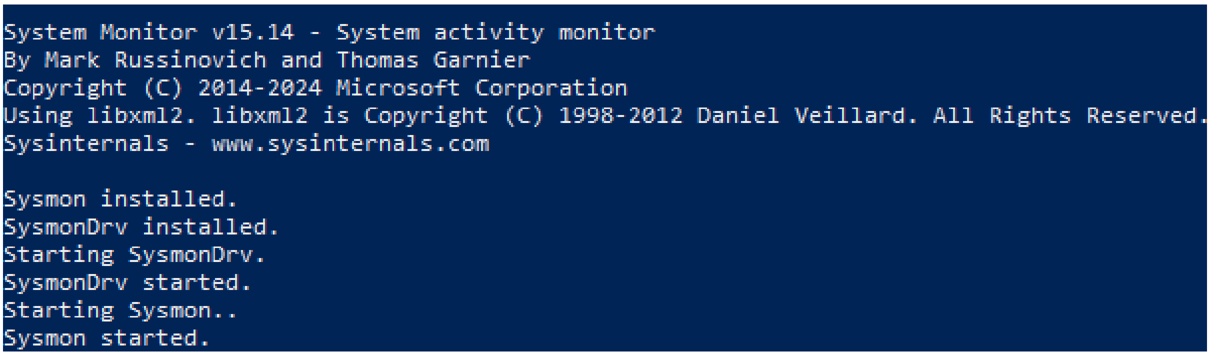


Open PowerShell as admin and navigate to the location where you installed Sysmon:



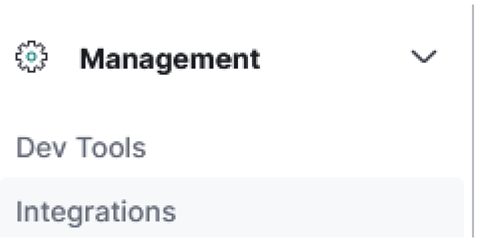
```
PS C:\Windows\system32> cd C:\Users\vboxuser\Downloads\Sysmon
PS C:\Users\vboxuser\Downloads\Sysmon> .\Sysmon.exe -i -n -accepteula
```

The second line simply installs Sysmon and accepts the user agreement, you should then be presented with the following which indicates that Sysmon has successfully installed:

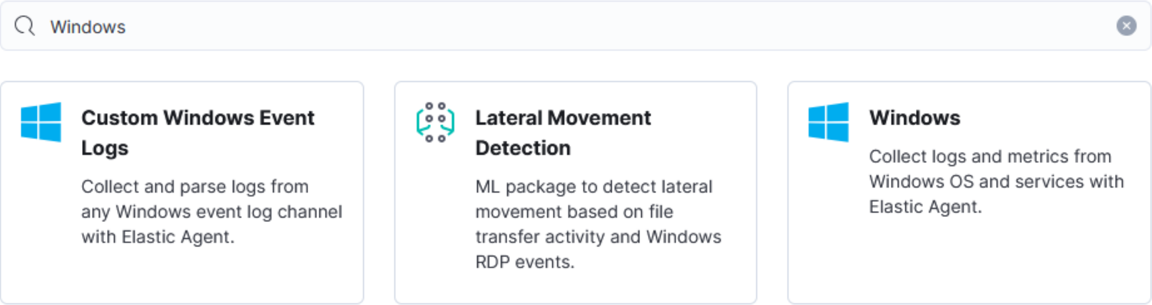


```
System Monitor v15.14 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

Navigate back to Elastic and go to Integrations which can be seen in the navigation menu:



We want to install the Windows integration; you can do so by searching for Windows:



Custom Windows Event Logs

Collect and parse logs from any Windows event log channel with Elastic Agent.

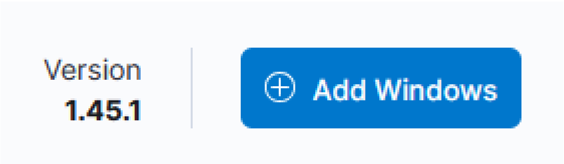
Lateral Movement Detection

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

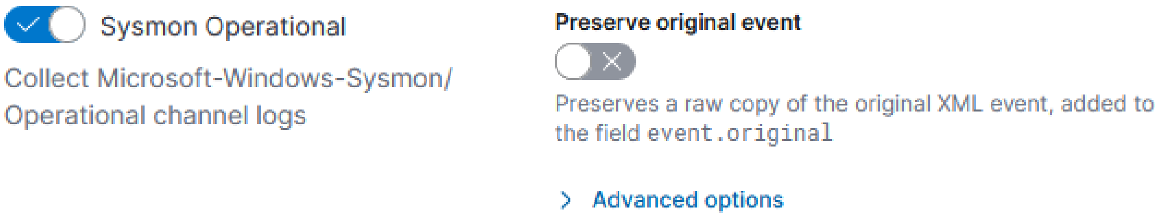
Windows

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

Select the third option (Windows) and then click the ‘Add Windows’ button on the following screen:



By default the Sysmon logs channel should be active, if it is not, you can activate it by checking the box under the “Collect events from the following Windows event log channels”:



● Sysmon Operational

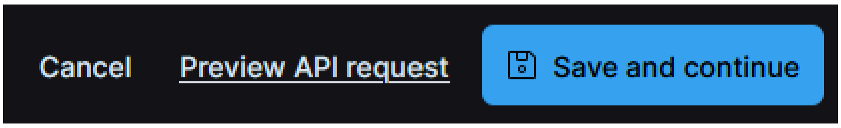
Collect Microsoft-Windows-Sysmon/Operational channel logs

Preserve original event

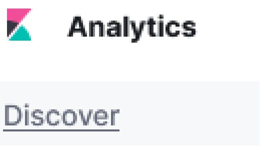
○ ✕

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

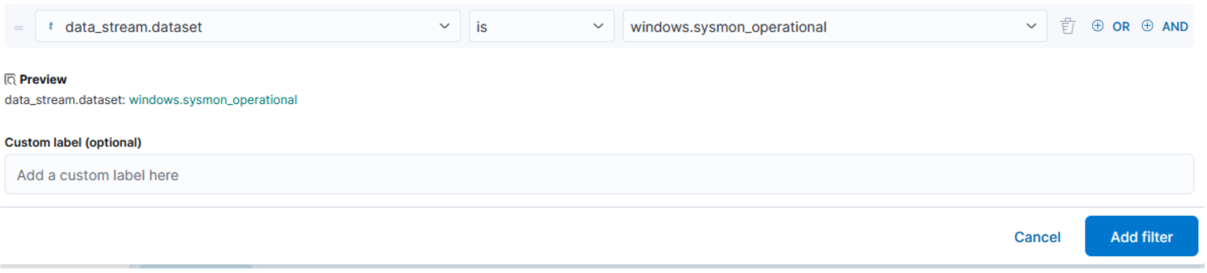
Then just make sure you have the right agent policy selected (check what agent policy the machine is assigned to) and save the integration by clicking ‘Save and continue’:



Now mess around in your machine that has the agent installed to generate some logs. After you have created log activity, navigate to the Discovery tab:



Let’s now look at the Sysmon logs, we can do this by searching the data_stream.dataset field for windows.sysmon_operational data. Then simply click the add filter button:



data_stream.dataset | is | windows.sysmon_operational

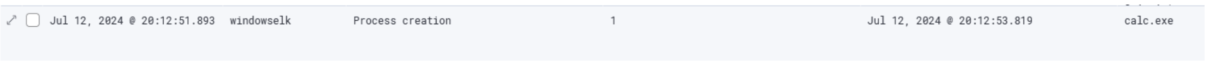
Preview

data_stream.dataset: windows.sysmon_operational

Custom label (optional)

Add a custom label here

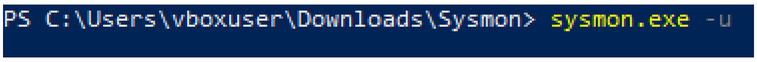
Just to show that it is working, I executed calc.exe in the cmd of the Windows 10 machine where the Elastic agent is installed. If you filter for the agent.name, event.action, event.code, event.created, and process.command_line fields, you can see the log for process creation in a neat format:



```
□ Jul 12, 2024 @ 20:12:51.893   windowselk   Process creation   1   Jul 12, 2024 @ 20:12:53.819   calc.exe
```

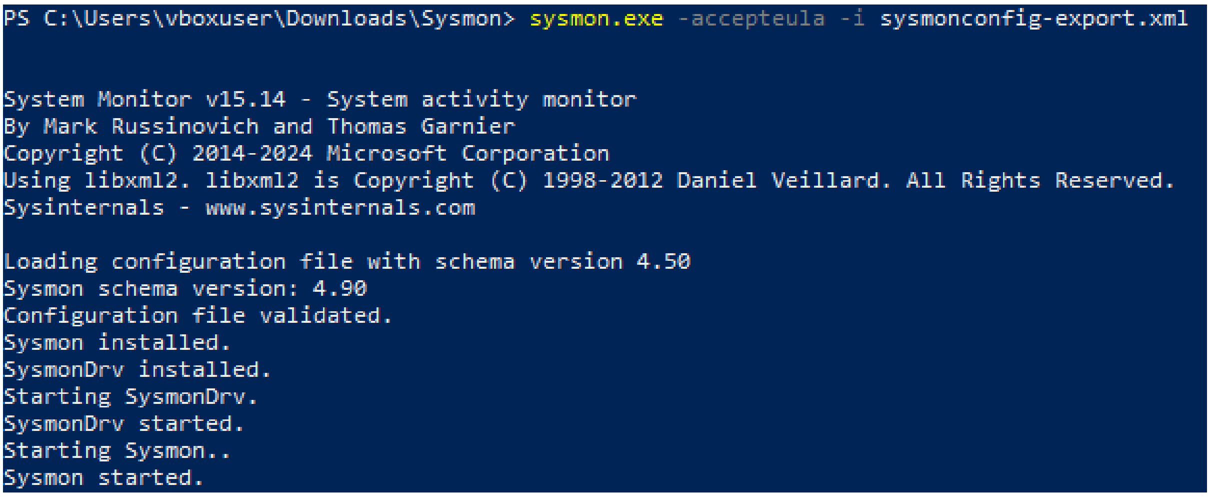
Improving Sysmon logs via custom config file

Please note that many of the following steps are from this video. To start, I am going to install a more high-quality Sysmon configuration file that functions as a good starting point for system change monitoring. You can access the configuration file here. To install, simply start a PowerShell terminal as administrator and enter the following commands:



```
PS C:\Users\vboxuser\Downloads\Sysmon> sysmon.exe -u
```

The first command uninstalls Sysmon. We then need to install Sysmon with the new config file by entering:



```
PS C:\Users\vboxuser\Downloads\Sysmon> sysmon.exe -accepteula -i sysmonconfig-export.xml


System Monitor v15.14 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```

You can also just simply update the existing configuration by entering sysmon.exe -c <config_file>.

Wrapping up

Setting up the ELK stack in the cloud may seem daunting (did to me), but with the right resources and step-by-step guidance provided by my notes along with the other resources I have referenced makes it a manageable and fun activity. This project provided a comprehensive introduction to deploying a basic ELK stack using Elastic Cloud. Through performing this project, I was able to successfully install and configure the Elastic Agent, and integrated Sysmon for enhanced log monitoring on a Windows machine.

This exercise not only broadened my understanding of log ingestion, storage, and visualisation but also highlighted the practical applications of the ELK stack in real-world scenarios (for e.g., as a SIEM too).