

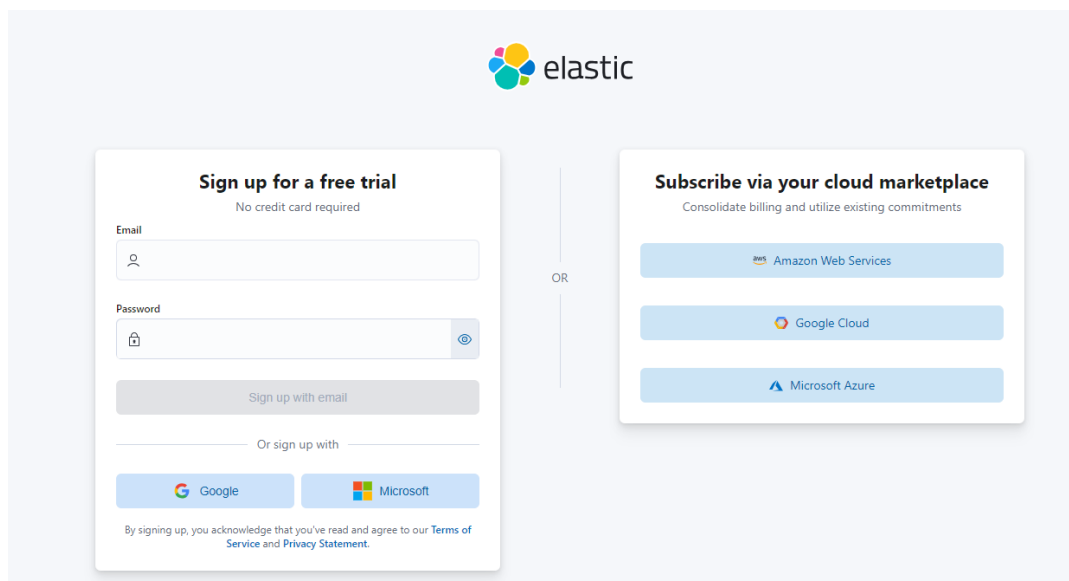
## Elastic Stack Security and Event Management (SIEM)

Before setting up a **ELK**, a little introduction about ELK. ELK is an acronym used to describe a stack that comprises three popular projects:

1. ElasticSearch – distributed search and analytics engine built on Apache Lucene.
1. Logstash – open-source data ingestion tool that allows collection of data from various sources, transform this data and then sends it to the destination.
2. Kibana.- data visualization and exploration tool used for log and time-series analytics, application monitoring, and operational intelligence use cases.

### Step 1. Setting up account at Elastic Cloud

The great thing about ElasticSearch is that it's free, so for account setup just go to the: <https://cloud.elastic.co/home>. So this display will be shown, like in the picture 1.



**Picture 1.** ELK sign in and login console

The next step is providing some general info before completing setting up the whole account. as it can be seen in picture 2.

**Welcome to Elastic**

Provide the information below for the best Elastic experience.

Full name \*

Dora Klobučar

Company \*

When it comes to Elastic, I'm... \*

New Experienced An expert

Which of the following are you primarily interested in? \*

☐ Search - Building search experiences in applications, sites or other

☐ Observability - Logs, metrics, traces, and synthetics

☒ Security - Analytics (logs/events), SIEM, endpoint protection, or cloud security

☐ Something else

Right now, I'd like to... \*

☐ Evaluate Elastic for my project or use case

☐ Migrate an existing Elasticsearch environment

☐ Get pricing information

☐ Learn more about Elastic

☒ Do something else

Next

**Picture 2.** Setting up an account

## Step 2. Creating an ELK instance


The next step is creating deployment. Name of my deployment is Siem, as it can be seen in the picture 3.

**Create your first deployment**

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

**Name**

SIEM

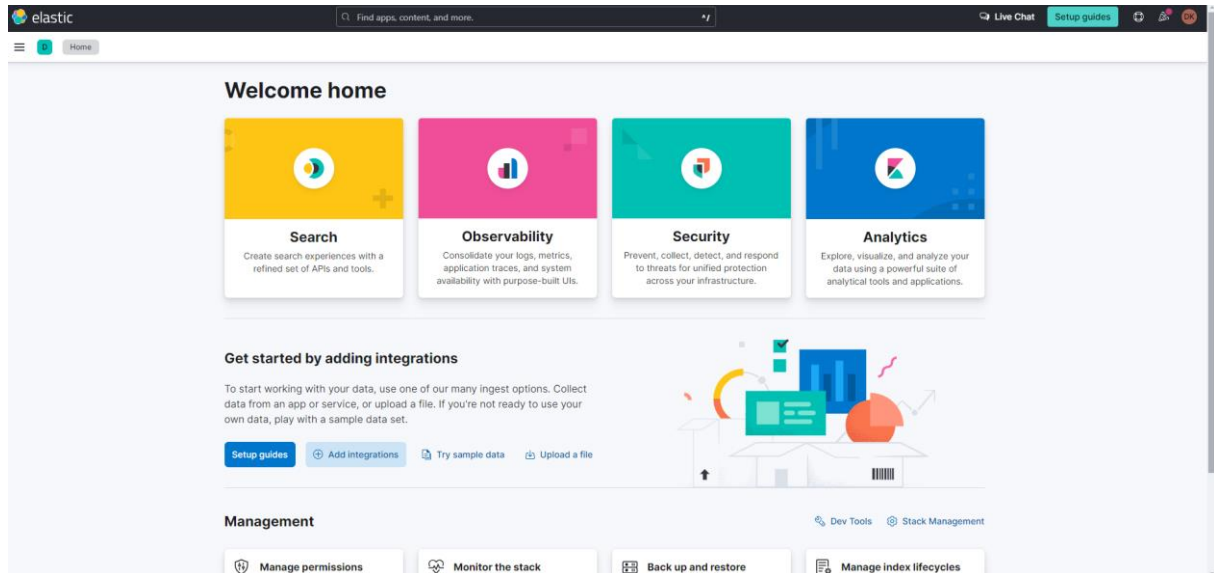
 GCP Iowa (us-central1) [Edit settings](#)

Storage optimized, 8.12.0

Create deployment

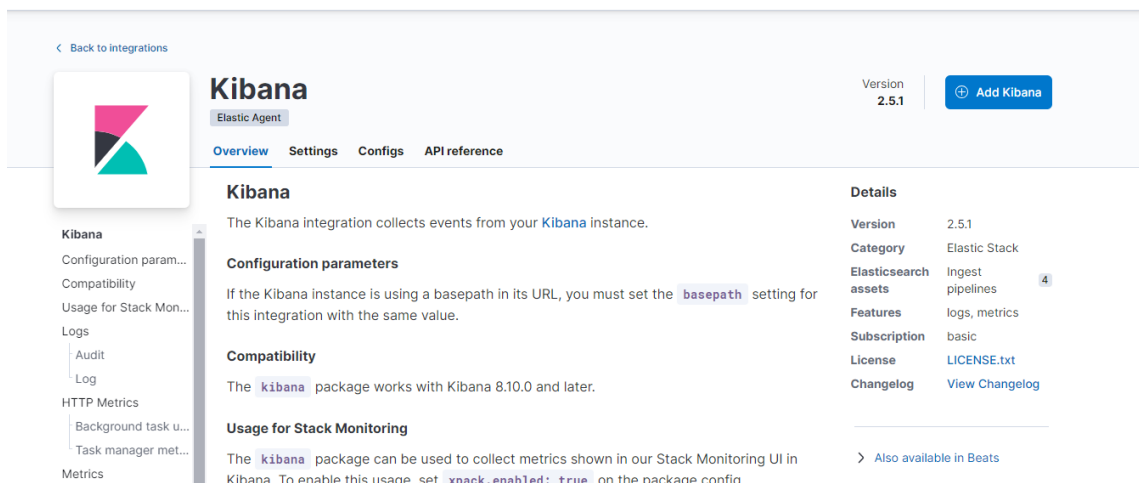
**Picture 3.** Creating deployment

After setting up an account, the necessary step is to log in to the Elastic Cloud console at <https://cloud.elastic.co>. The next step is to click on free trial and click on create deployment and choose Elasticsearch as deployment type. It's necessary to choose region and deployment size, which can be regulated. After login, the main dashboard will be displayed, like in picture 4.



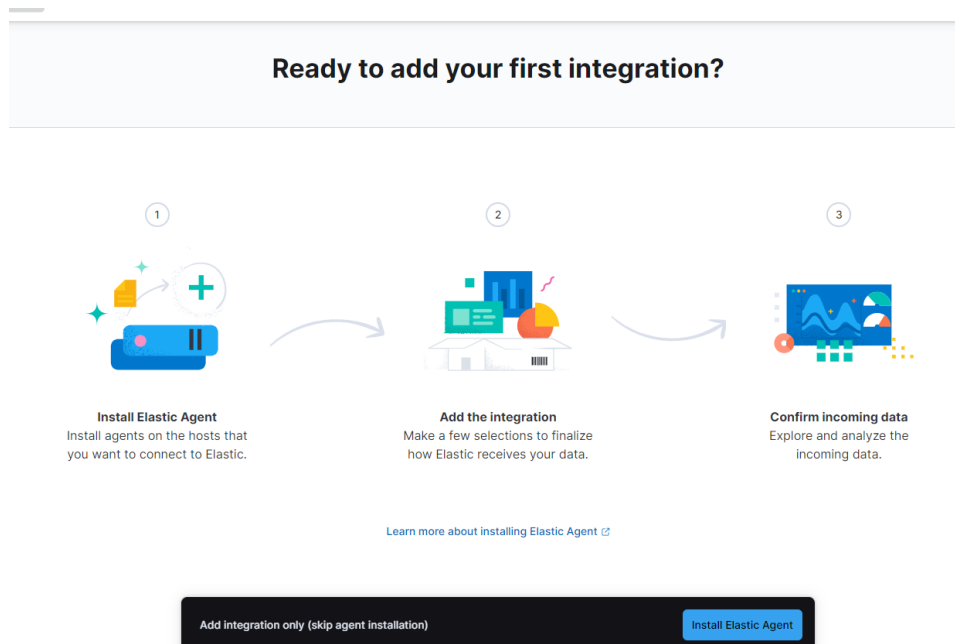
**Picture 4.** ELK main dashboard

Then at the top search bar, we should search for Kibana. Kibana is a user interface that lets you visualize your Elasticsearch data and navigate the Elastic Stack. After we find it, we should click “Add Kibana” like in picture 5.



**Picture 5.** Adding Kibana

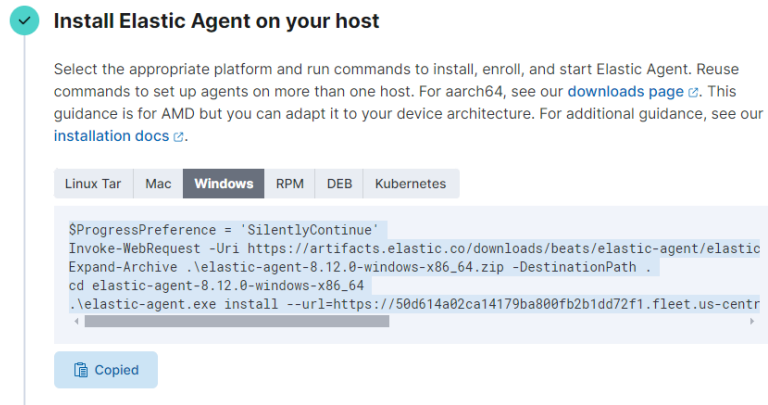
We will be then redirected to page for installing Elastic Agent. Next step is to click on “Install Elastic Agent“. Like in the picture 6.



**Picture 6.** Adding integrations

The next steps are to configure and enroll the Elastic Agent in Fleet to automatically deploy updates and centrally manage agents. An agent is a software program that is installed on a device, such as a server or endpoint, to collect and send data to a centralized system for analysis and monitoring. In the context of Elastic SIEM, an agent is used to collect and forward security-related events from your endpoints to your Elastic SIEM instance. As an alternative to Fleet, advanced users can run the agent in standalone mode. We can choose different operating systems. In this example we are using Windows.

So we select Windows, then “Copy to Clipboard “. It's recommended to copy this command in a safe place, so it doesn't get lost. I saved it in a file called agent\_install.txt. I will use this command later. Described can be seen in picture 7.



**Picture 7.** Installing agent on your host

This line of code should be deleted:

```
.\elastic-agent.exe install --url=https://50d614a02ca14179ba800fb2b1dd72f1.fleet.us-  
central1.gcp.cloud.es.io:443 --enrollment-  
token=QV9mblk0MEJVLURiWjVfTV9QSzY6NnFaTkctM3lTUUs1WkRYTndtZWJMUQ=  
=
```

After deleting, we have this code:

```
$ProgressPreference = 'SilentlyContinue'  
Invoke-WebRequest -Uri  
https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-  
8.11.0-windows-x86_64.zip  
-OutFile elastic-agent-8.11.0-windows-x86_64.zip  
Expand-Archive .\elastic-agent-8.11.0-windows-x86_64.zip -DestinationPath
```

These steps were necessary for downloading the agent. The agent should be downloaded and adjusted to everyone's system. It's recommended to use installers (TAR/ZIP) over system packages (RPM/DEB) because they provide the ability to upgrade agents within Fleet. When you download the file it should look like this in the picture 8.

| Name                         | Date modified   | Type                | Size      |
|------------------------------|-----------------|---------------------|-----------|
| data                         | 1.2.2024. 10:44 | File folder         |           |
| .build_hash.txt              | 1.2.2024. 10:44 | Tekstni dokument    | 1 KB      |
| .elastic-agent.active.commit | 1.2.2024. 10:44 | COMMIT File         | 1 KB      |
| elastic-agent.exe            | 1.2.2024. 10:44 | Application         | 50.341 KB |
| elastic-agent.reference.yml  | 1.2.2024. 10:44 | Yaml Source File    | 12 KB     |
| elastic-agent.yml            | 1.2.2024. 10:44 | Yaml Source File    | 11 KB     |
| LICENSE.txt                  | 1.2.2024. 10:44 | Tekstni dokument    | 14 KB     |
| NOTICE.txt                   | 1.2.2024. 10:44 | Tekstni dokument    | 1.023 KB  |
| package.version              | 1.2.2024. 10:44 | VERSION File        | 1 KB      |
| README.md                    | 1.2.2024. 10:44 | Markdown Source ... | 1 KB      |

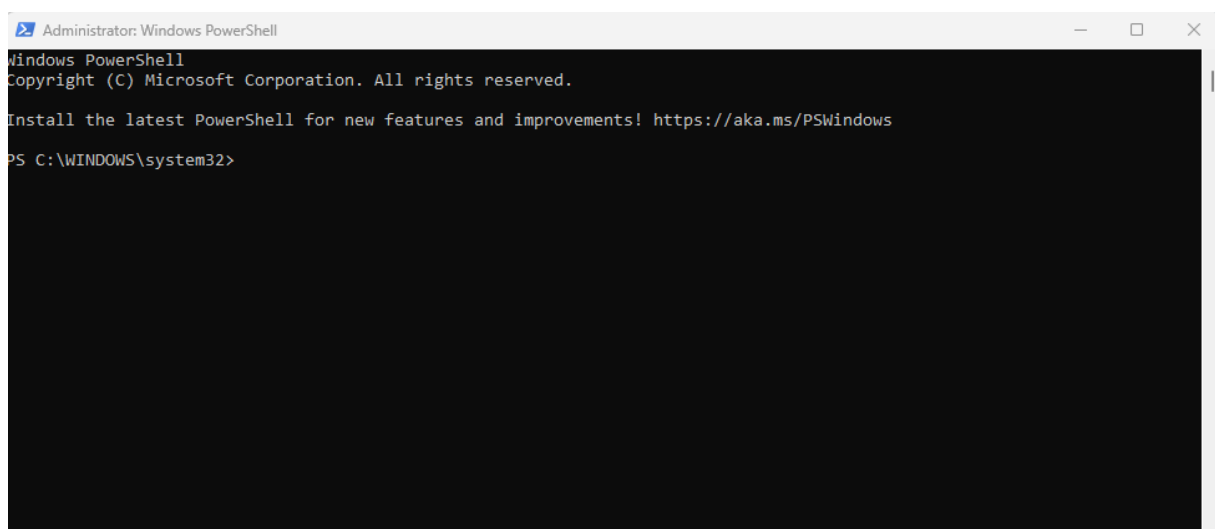
**Picture 8.** Downloading exe file

Extract/Unzip the downloaded file. Code should be in this format:

```
cd elastic-agent-8.11.0-windows-x86_64 .\elastic-agent.exe install -  
url=hxxps://xyz
```

### Step 3. Downloading the Elastic Agent

Press the windows button and run Powershell as administrator. We can see it in the picture 9.



**Picture 9.** Running Powershell as administrator

Once the Powershell opens, locate it to the directory where the file was extracted and copy what you kept in the file and paste it to install the elastic agent.

In my case it looks like this as shown in the picture 10.

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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> cd C:\Users\... \Documents\elastic-agent-8.12.0-windows-x86_64
PS C:\Users\... \Documents\elastic-agent-8.12.0-windows-x86_64>
```

**Picture 10.** Positioning to the installation file

Powershell should show this output (picture 11):

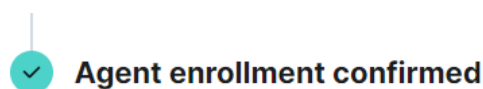
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> cd C:\Users\dklobucar\Documents\elastic-agent-8.12.0-windows-x86_64
PS C:\Users\... \Documents\elastic-agent-8.12.0-windows-x86_64> $ProgressPreference = 'SilentlyContinue'
PS C:\Users\... \Documents\elastic-agent-8.12.0-windows-x86_64> Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.0-windows-x86_64.zip -Outfile elastic-agent-8.12.0-windows-x86_64.zip
PS C:\Users\... \Documents\elastic-agent-8.12.0-windows-x86_64> Expand-Archive .\elastic-agent-8.12.0-windows-x86_64.zip -DestinationPath .
PS C:\Users\... \Documents\elastic-agent-8.12.0-windows-x86_64> .\elastic-agent.exe install --url=https://58d614a02ca14179ba080fb2b1dd72f1.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=...
Elastic Agent will be installed at C:\Program Files\Elastic\Elastic Agent and will run as a service. Do you want to continue? [Y/n]y
[+] Service Started [1m2s] Elastic Agent successfully installed, starting enrollment.
[+] Waiting for enroll... [1m2s] ["log.level":"info","@timestamp":"2024-02-01T11:45:05.770+0100","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":496},"message":"Starting enrollment to URL: https://58d614a02ca14179ba080fb2b1dd72f1.fleet.us-central1.gcp.cloud.es.io:443/", "ecs.version":"1.6.0"}]
[+] Waiting for enroll... [1m42s] ["log.level":"info","@timestamp":"2024-02-01T11:45:35.573+0100","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":461},"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"}]
[+] Waiting for enroll... [1m42s] ["log.level":"info","@timestamp":"2024-02-01T11:45:35.600+0100","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":265},"message":"Successfully triggered restart on running Elastic Agent.", "ecs.version":"1.6.0"}]
Successfully enrolled the Elastic Agent.
[+] Done [1m42s]
Elastic Agent has been successfully installed.
PS C:\Users\dklobucar\Documents\elastic-agent-8.12.0-windows-x86_64>
```

**Picture 11.** Display of finished installment

Make sure you type y and when you go back to your browser you can see the message saying “ 1 agent has been displayed“ (picture 12)

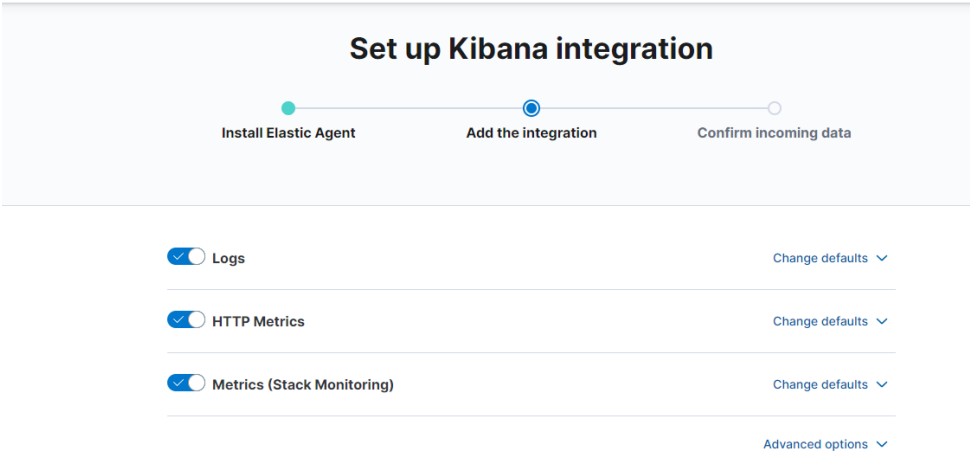


**Agent enrollment confirmed**

✓ 1 agent has been enrolled.

**Picture 12.** Display of agent enrollment

Then click “Add to Integration“. On the next page leave everything default and click “. As it can be seen in picture 13.



Picture 13. Setting up Kibana integration

Preview of incoming data:



Picture 14. Preview of incoming dana

To check wheter installation was successful, we should select Fleet option in management section.

Showing 2 agents [Clear filters](#) ● Healthy 2 ● Unhealthy 0 ● Updating 0 ● Offline 0

| <input type="checkbox"/>            | Status  | Host          | Agent policy                           | CPU ①  | Memory ① | Last activity  | Version | Actions |
|-------------------------------------|---------|---------------|--|--------|----------|----------------|---------|---------|
| <input type="checkbox"/>            | Healthy | tss-dklobucar | My first agent policy<br>rev. 2        | 0.29 % | 132 MB   | 29 seconds ago | 8.12.0  | ...     |
| <input checked="" type="checkbox"/> | Healthy | 64d37222a8b5  | Elastic Cloud agent policy ②<br>rev. 5 | N/A ①  | N/A ①    | 18 seconds ago | 8.12.0  | ...     |

Rows per page: 20 < 1 >

Picture 15. Checking installation

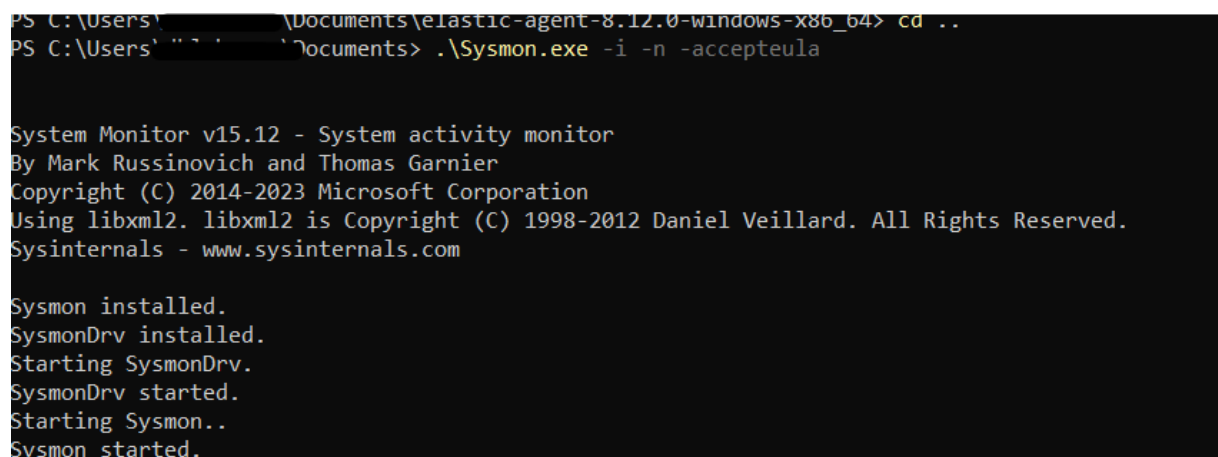


We can see that our Elastic Agent is installed and configured to be connected to our ELK instance in the cloud.

#### Step 4. Sysmon download

Keeping in mind that we can't only rely on Windows logs, we should also download additional monitoring tool. Sysmon is one of the most used add-ons for Windows logging. Sysmon can detect malicious activity by tracking code behaviour and network traffic, as well as create detections based on malicious activity.

Follow this link for download [Download Sysmon](#). Scroll down and find Download Sysmon and then extract the document. Then go to the Powershell and run it as administrator. Like in the picture 16. We should reposition to the directory where Sysmon was extracted and then install and start Sysmon service. Output is shown in picture 16.



```
PS C:\Users\... \Documents\elastic-agent-8.12.0-windows-x86_64> cd ..
PS C:\Users\... \Documents> .\Sysmon.exe -i -n -accepteula

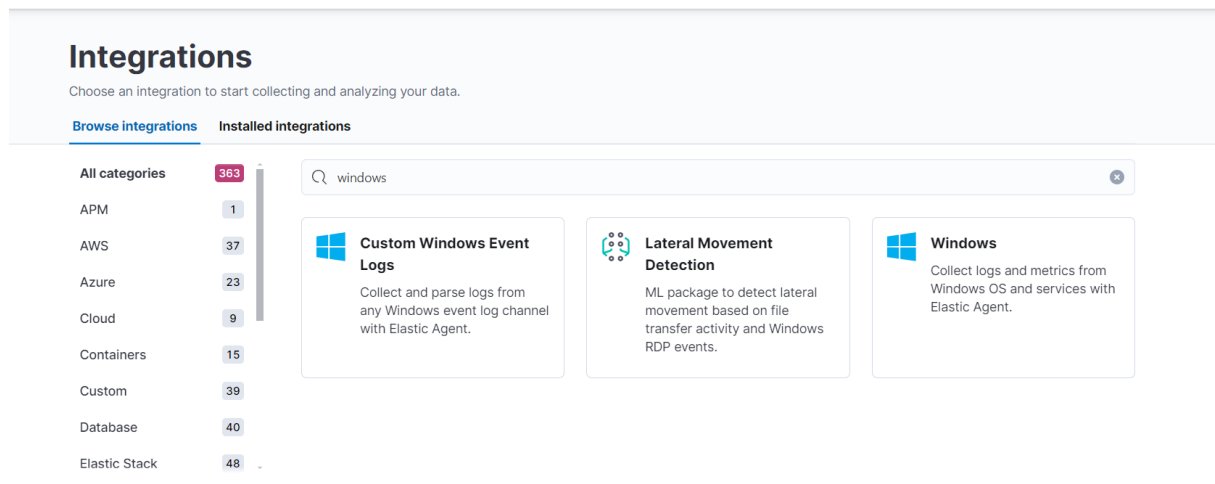
System Monitor v15.12 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

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

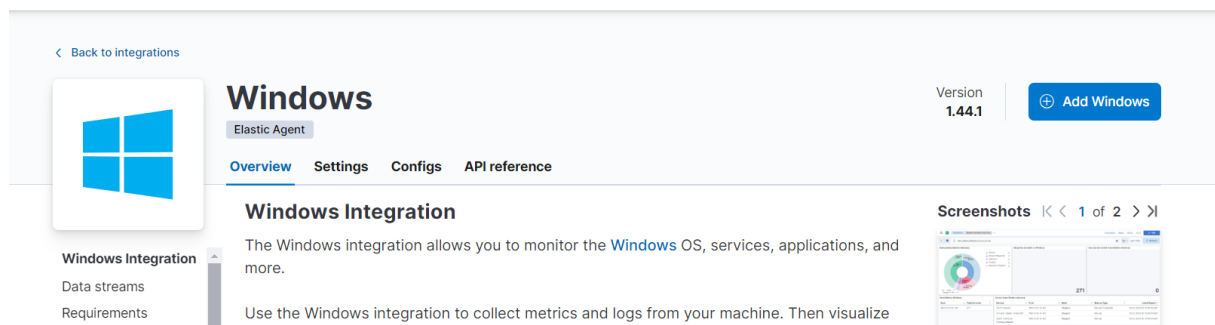
**Picture 16.** Startin Sysmon service

Next step is to configure our Elastic agent to gather these logs. So should go back to Elastic Cloud console.

Navigate to the Integrations section and add Windows.

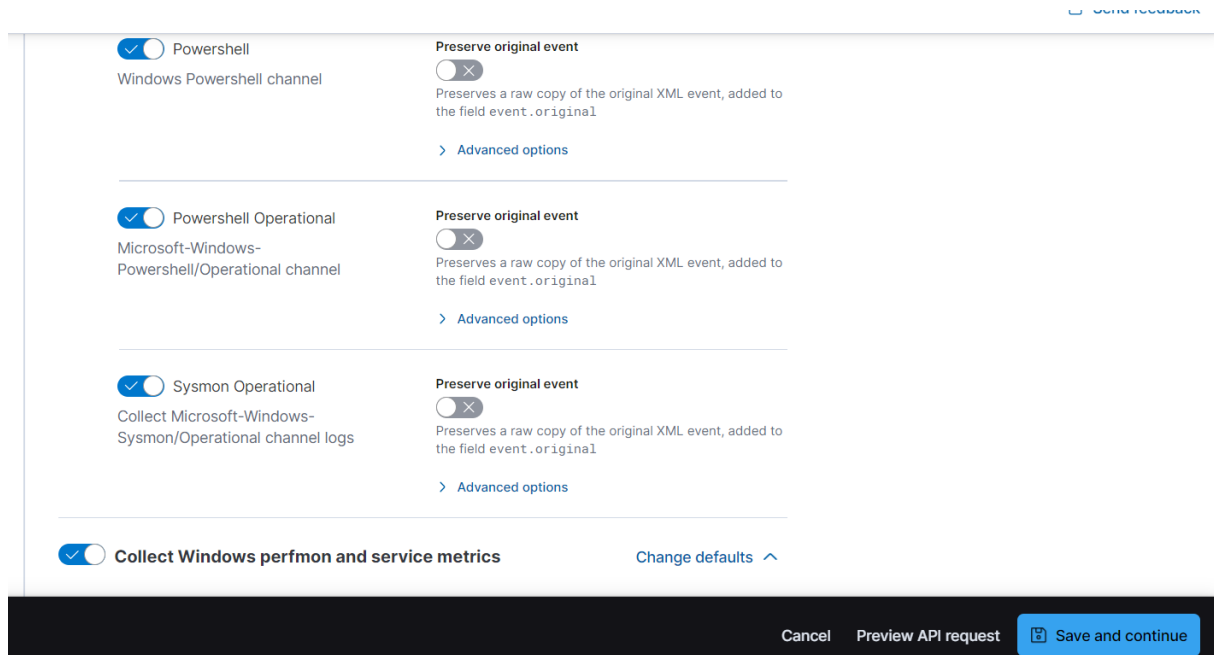


**Picture 17.** Adding Windows integration



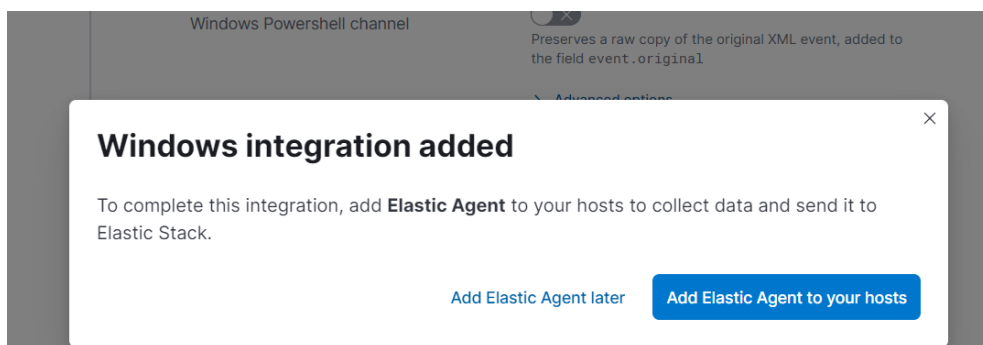
**Picture 18.** Adding Windows integration

Then check whether Sysmon is operation, by default, it should be. Go to the “Collect logs from the following Windows Event log channels“ section of the “Add Integration“ page.



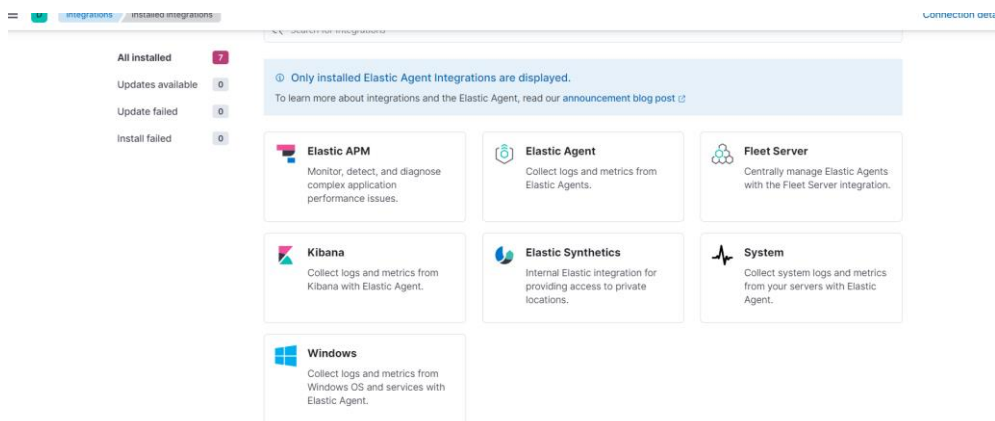
**Picture 19.** Checking Sysmon enabelment

After checking, click save and continue. When prompted click “Add elastic agent to your hosts“.



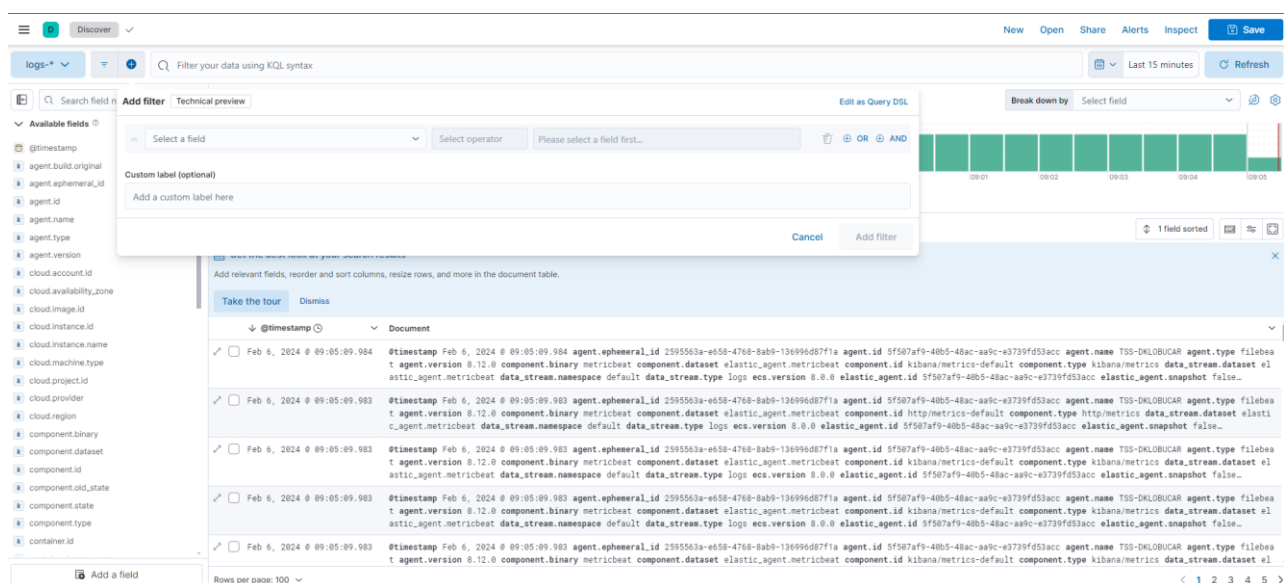
**Picture 20.** Adding Elastic Agent to your hosts

In installed integrations tabs we can see that Endpoint Security and System are automatically installed. We can see installed applications in picture 21.



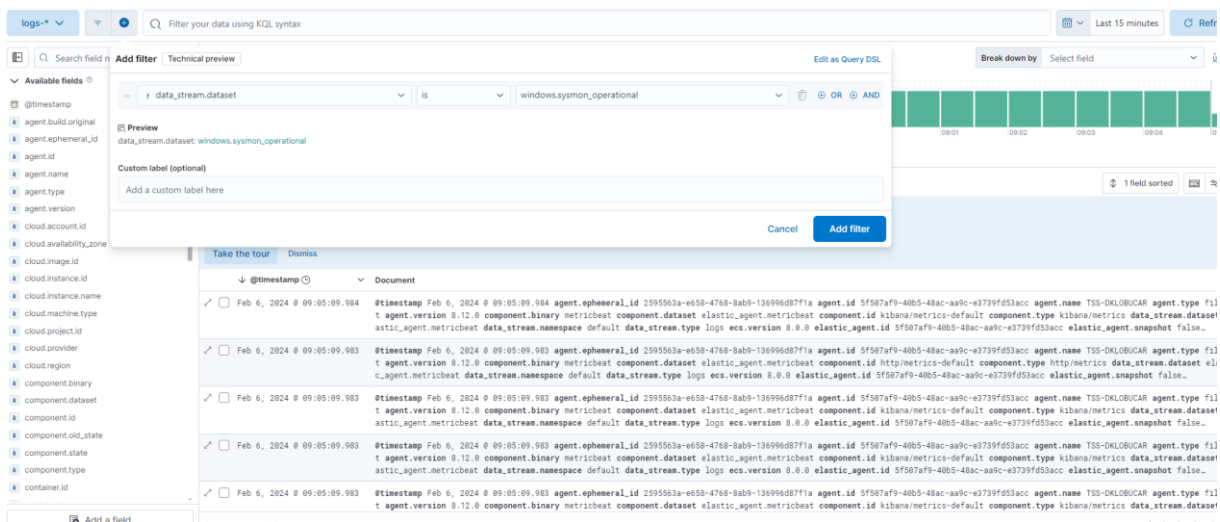
**Picture 21.** Display of installed integrations

After creating some log activity, navigate to “Discover” by accessing hamburger menu on the top left.



**Picture 22.** Setting a filter on your data to limit your result to sysmon dana

Now when ELK is configured, go play around and create some logs; browse on the Internet, create directories, delete them, etc. After creating some logs navigate to Discovery, and set a filter on your data to limit your result to Sysmon data. This can be done by searching `data_stream.dataset` field for `windows.sysmon_operational.data`. Then click “Add filter“. Your filter should be seen then.



**Picture 23.** Example of setting filter on data to limit results to Sysmon data

If you have result and not an error, your Sysmon data is being sent and collected to Elastic. Example can be seen on picture 24.



**Picture 24.** Display of collected data

After successful implementation you will be able to get all logs from your device to elastic cloud and analyse generated logs.

More detailed report can be seen in this link

[https://github.com/strandjs/IntroLabs/blob/master/IntroClassFiles/Tools/IntroClass/md/system\\_logs.md](https://github.com/strandjs/IntroLabs/blob/master/IntroClassFiles/Tools/IntroClass/md/system_logs.md) .