ELK SETUP

ELK Stack Setup Documentation

The ELK Stack (Elasticsearch, Logstash, and Kibana) is a powerful open-source platform for data ingestion, search, and visualization. This documentation outlines the essential steps to set up and configure your own ELK Stack environment.

Prerequisites:

- Basic understanding of Linux and Bash scripting
- CMD
- Download and extract Elasticsearch, Logstash, and Kibana distributions

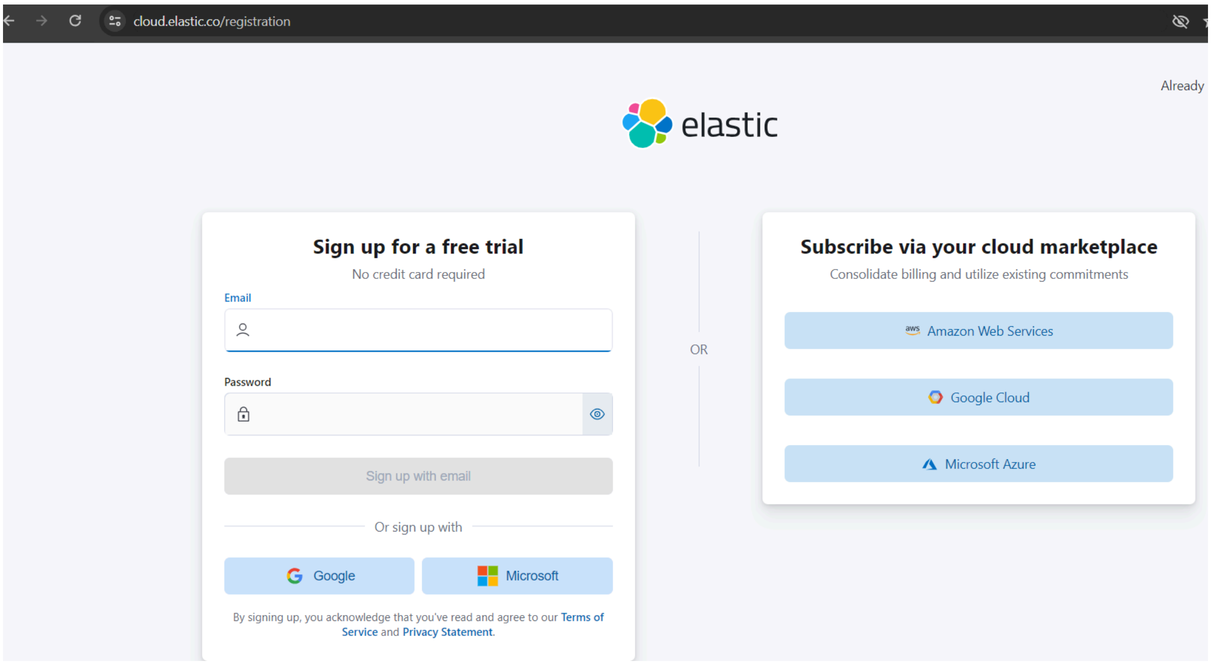
1. Elasticsearch Setup:

To learn ELK, we don't need several servers or to spend large sums of money. We can get into the driver's seat and experiment with ELK by using the Elastic Cloud 14-day trial. The trial does not require a credit card to get started. You only need an email and a password.

Set up an account.

Start your free Elastic Cloud Trial

This link is for the trial sign up page. Start a trial by signing up



cloud.elastic.co/registration

Sign up for a free trial

No credit card required

Subscribe via your cloud marketplace

Consolidate billing and utilize existing commitments

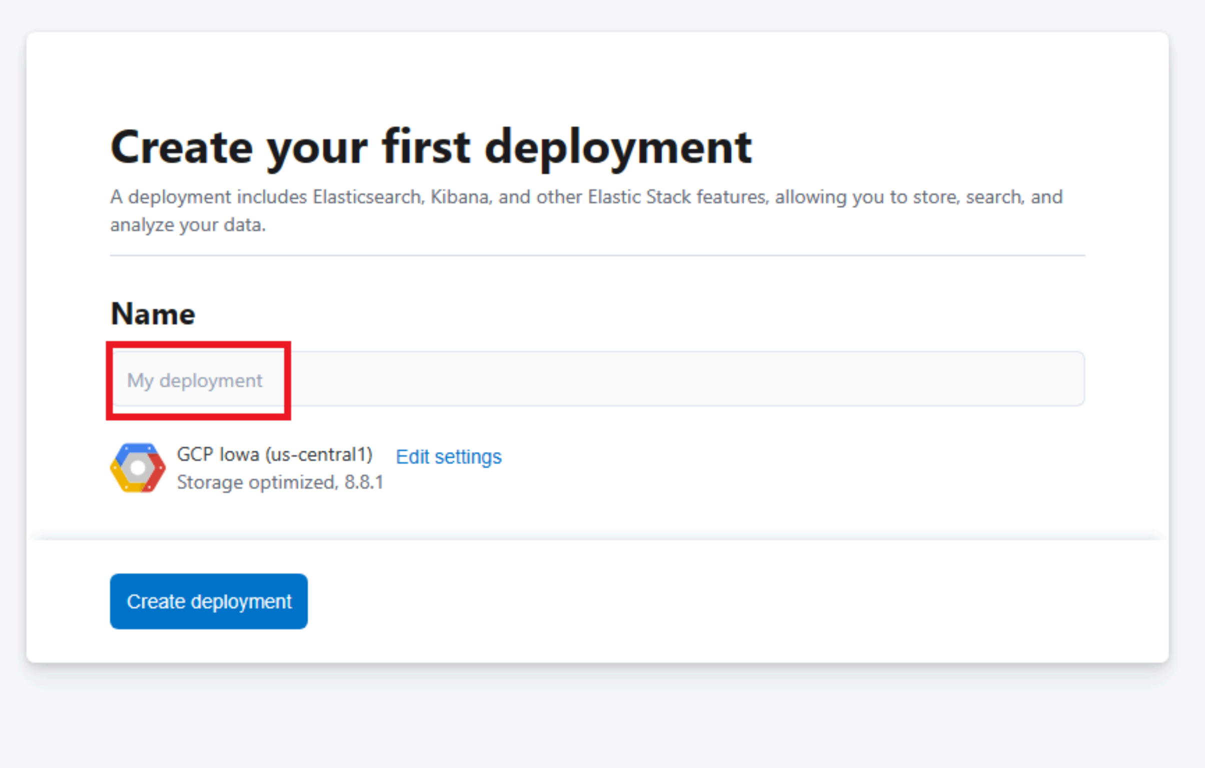
By signing up, you acknowledge that you've read and agree to our Terms of Service and Privacy Statement.

After logging in, You can set up the account and your ready to explore more into it.

Fill out the proper filed with the correct information pictured below and select the check boxes with red dots.

Start an ELK instance

After filling the details, go to next step. For my instance I will be calling it "security-development. Make sure to enter the name of your deployment 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.

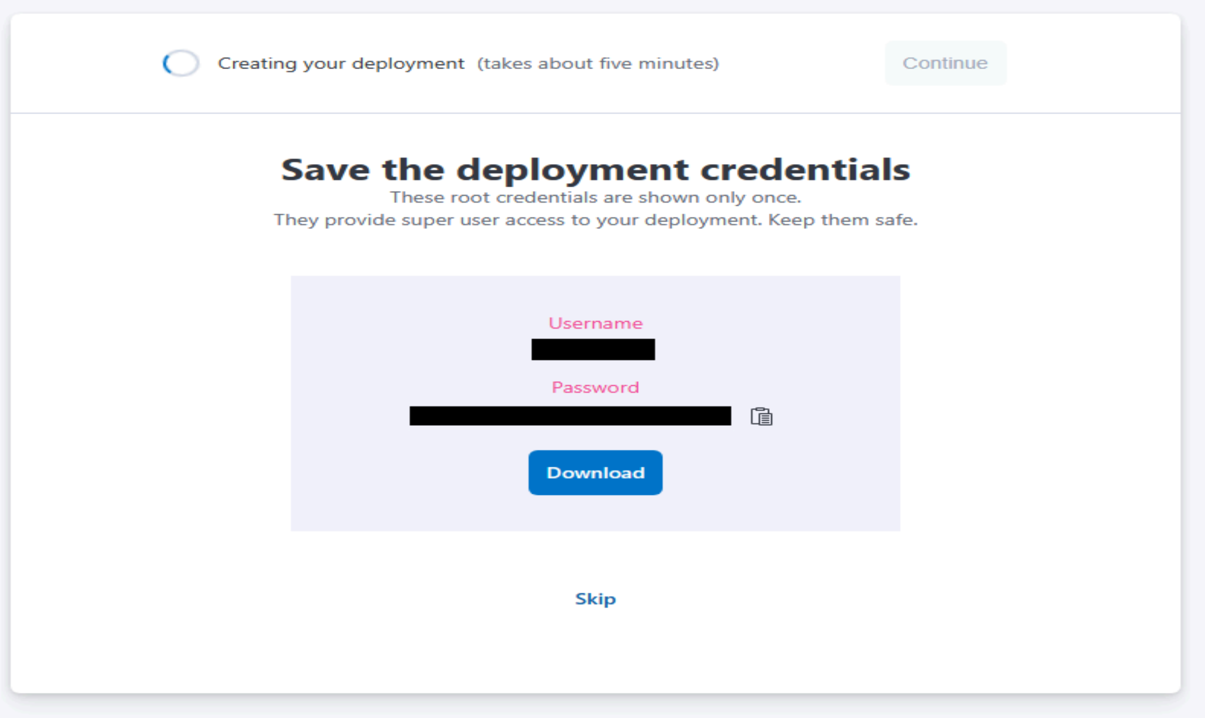
Name

My deployment

GCP Iowa (us-central1) Storage optimized, 8.8.1

Next we will see this page.

Elastic will present the credentials for this ELK stack. There is the option to download a CSV of the credentials. However you decide to hold onto these credentials, don't lose them.



Creating your deployment (takes about five minutes)

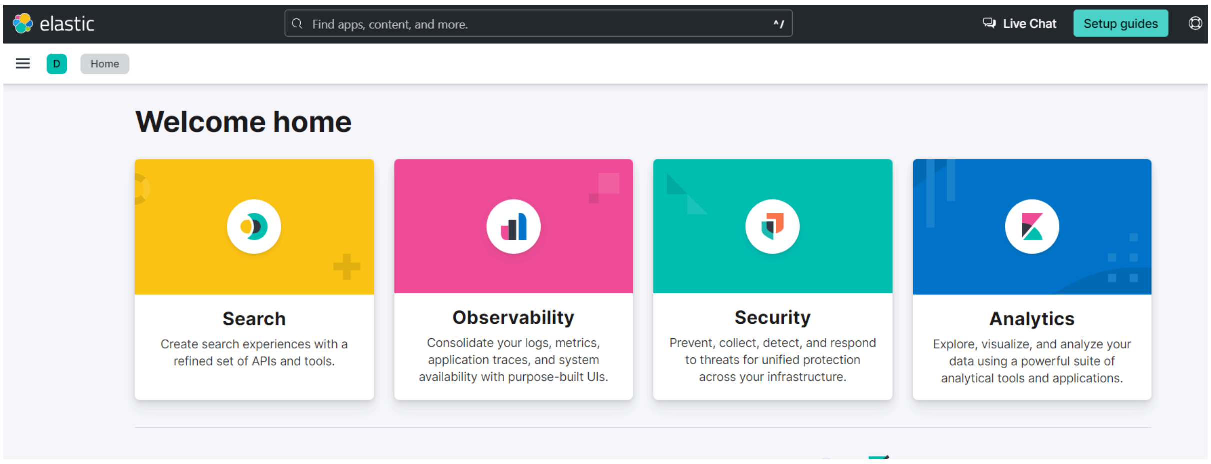
Save the deployment credentials

These root credentials are shown only once.
They provide super user access to your deployment. Keep them safe.

Username
[redacted]

Password
[redacted]

Then we will need to wait for the continue button to turn blue, once that's done click continue



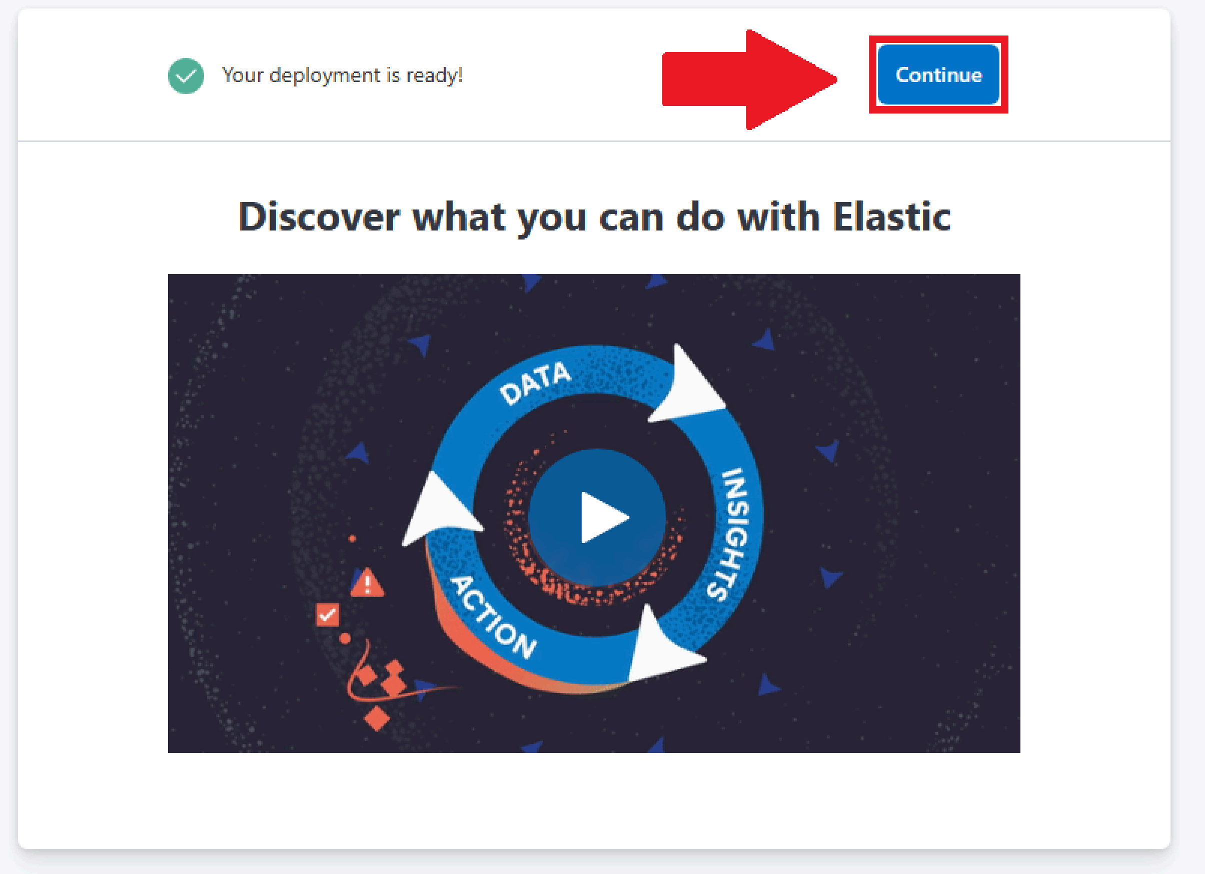
Welcome home

Search
Create search experiences with a refined set of APIs and tools.

Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

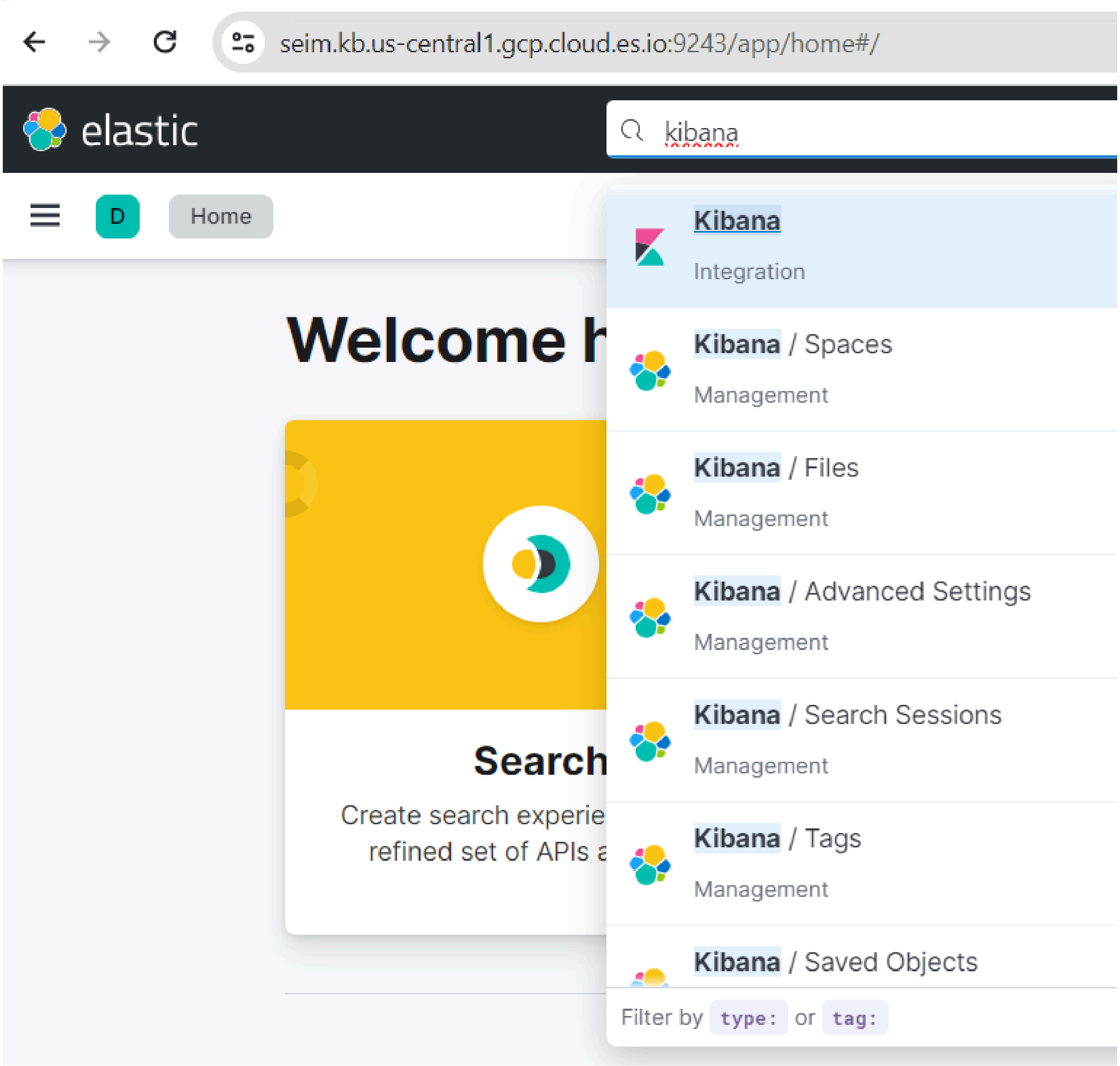
Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.



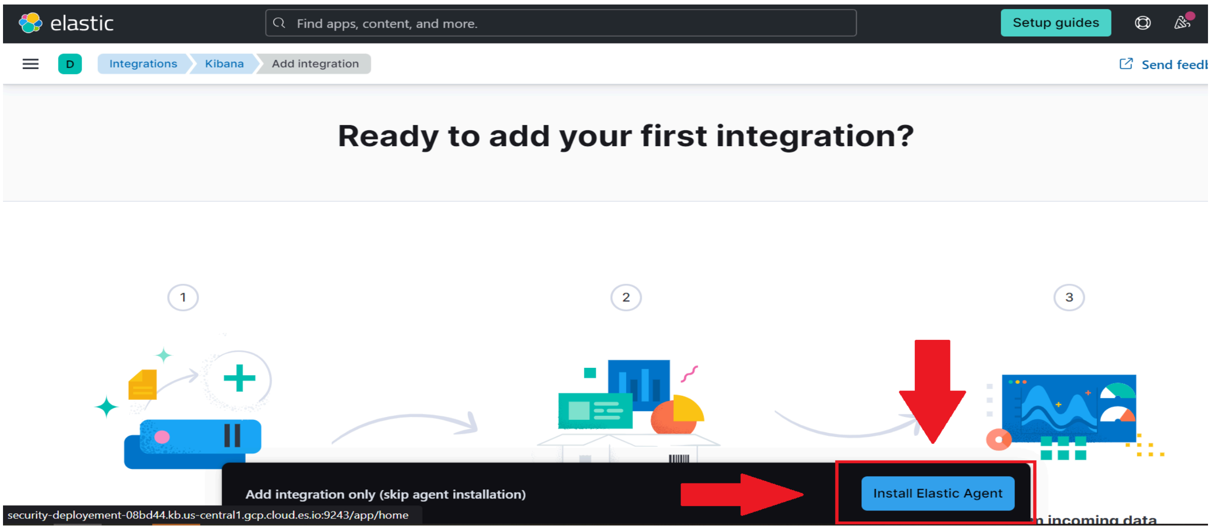
Your deployment is ready!

Discover what you can do with Elastic

We will be greeted with menu of options, we want to skip that menu.For kibana we have to do the installation. at the top of the page we want to click search and type "kibana" and hit enter.

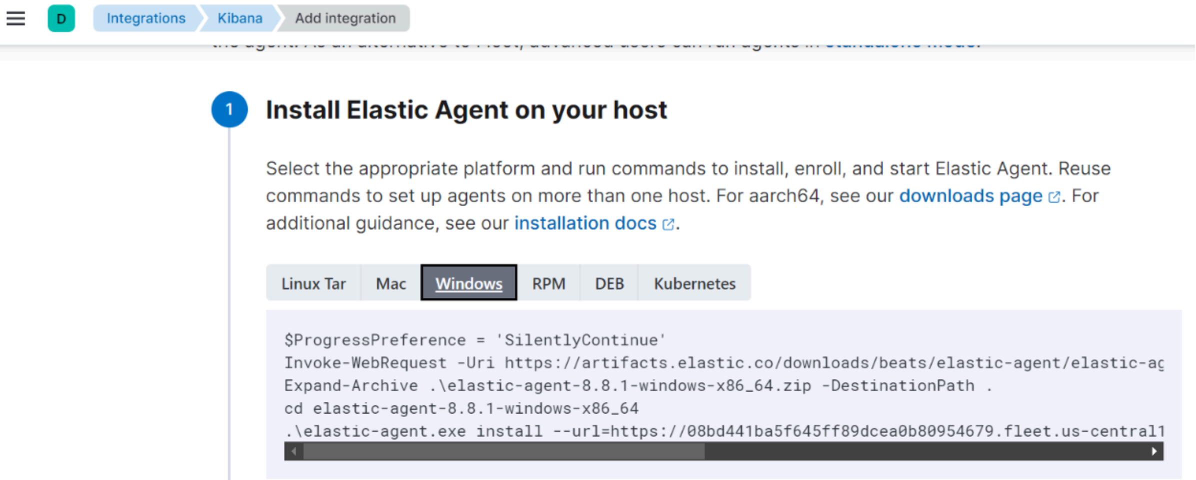

seim.kb.us-central1.gcp.cloud.es.io:9243/app/home#/

Once the next page load we want to add kibana. Select "Add Kibana" and add integration the kibana integration.


Ready to add your first integration?

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

Next you have to copy the code in the clipboard to securely connect it to logs.



the agent. As an alternative to Fleet, advanced users can run agents in standalone mode.

1 **Install Elastic Agent on your host**

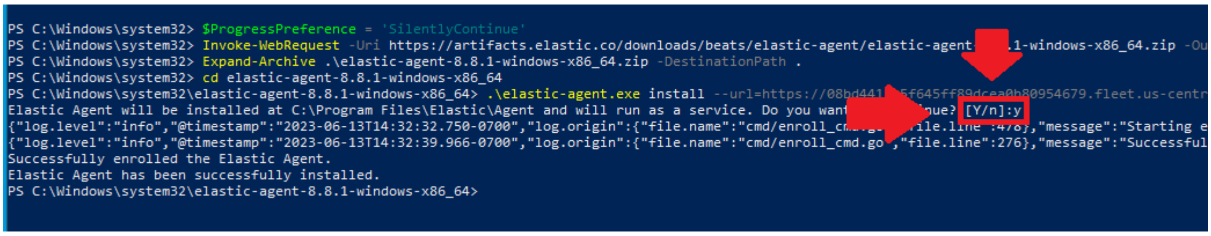
Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our downloads page. For additional guidance, see our installation docs.

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-ag
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 the scrip tand save it to some place better where you can see it. 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.

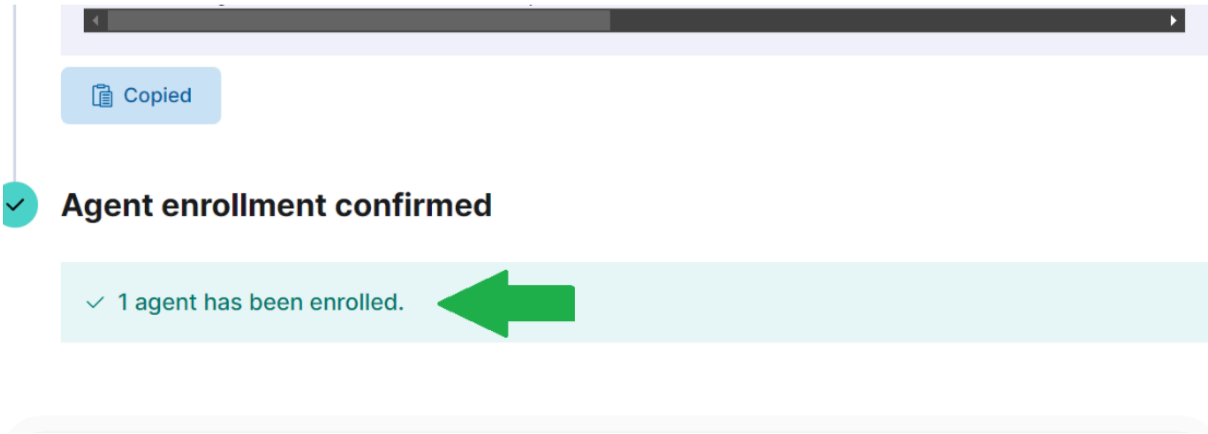
2. Download the Elastic Agent.

Now go to powershell and run it as an administrator. As the powershell opens , paste the text that you kept . paste it into the powershell and hit enter.



```
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 -Ou
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-8.8.1-windows-x86_64> .\elastic-agent.exe install --url=https://08bd441ba5f645ff89dcea0b80954679.fleet.us-centr
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":"2023-06-13T14:32:32.750-0700","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":478},"message":"Starting e
{"log.level":"info","@timestamp":"2023-06-13T14:32:39.966-0700","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":276},"message":"Successful
Successfully enrolled the Elastic Agent.
Elastic Agent has been successfully installed.
PS C:\Windows\system32\elastic-agent-8.8.1-windows-x86_64>
```

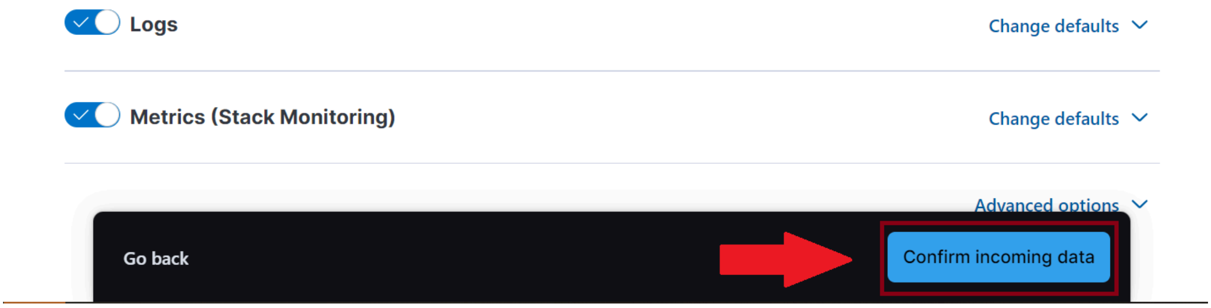
Make sure you type y and hit enter when prompted by powershell.
Now go back to the browser and you should see "1 Agent has been enrolled" successfully.



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".

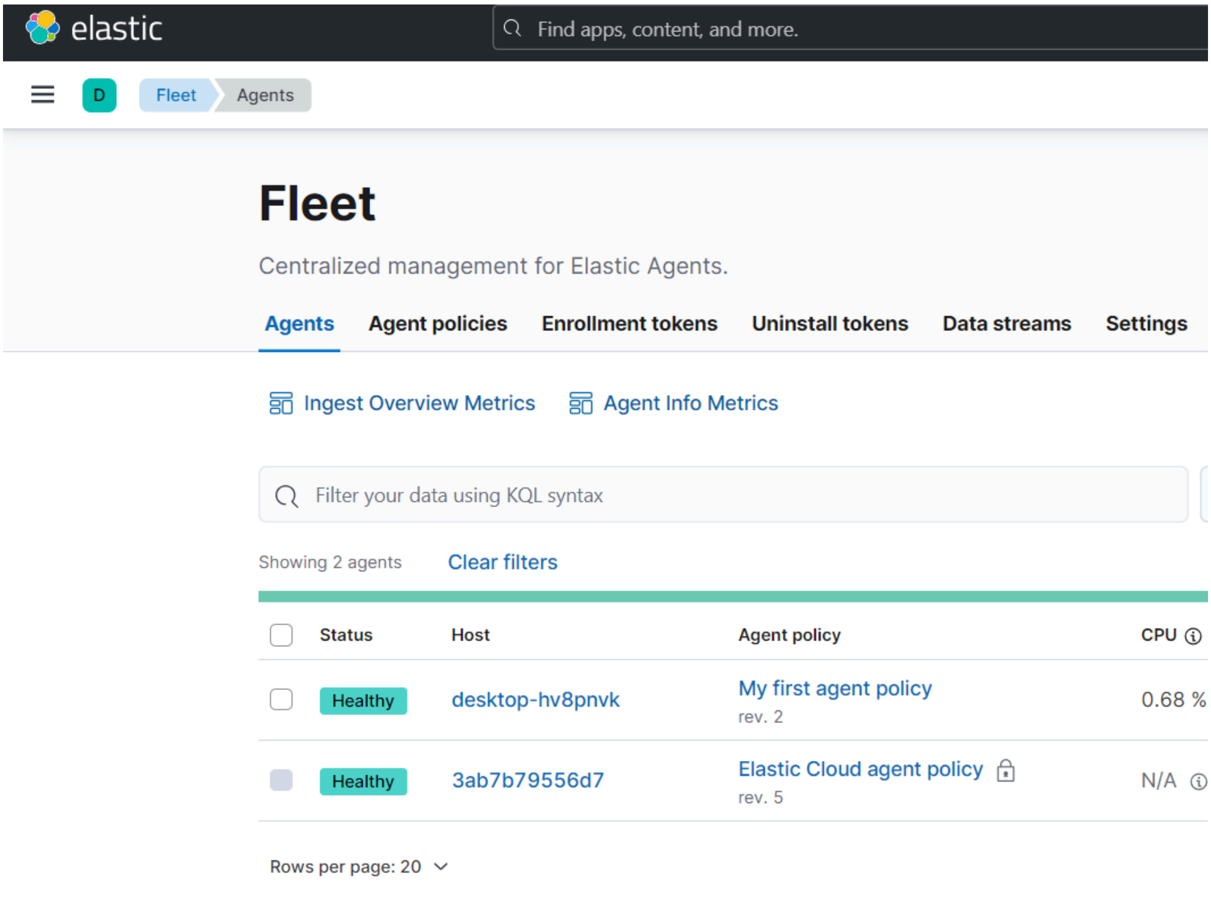


☑ Logs

☑ Metrics (Stack Monitoring)

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

Verify the Fleet Status.Once this step is completed, we should establish a connection and be prepared for the next phase. Before proceeding, ensure that the device has successfully established a connection.
For Fleet navigate to the top-left corner of the window, click the hamburger icon, and scroll down almost to the bottom. Look for the 'Fleet' option and select it.



Fleet

Centralized management for Elastic Agents.

Showing 2 agents

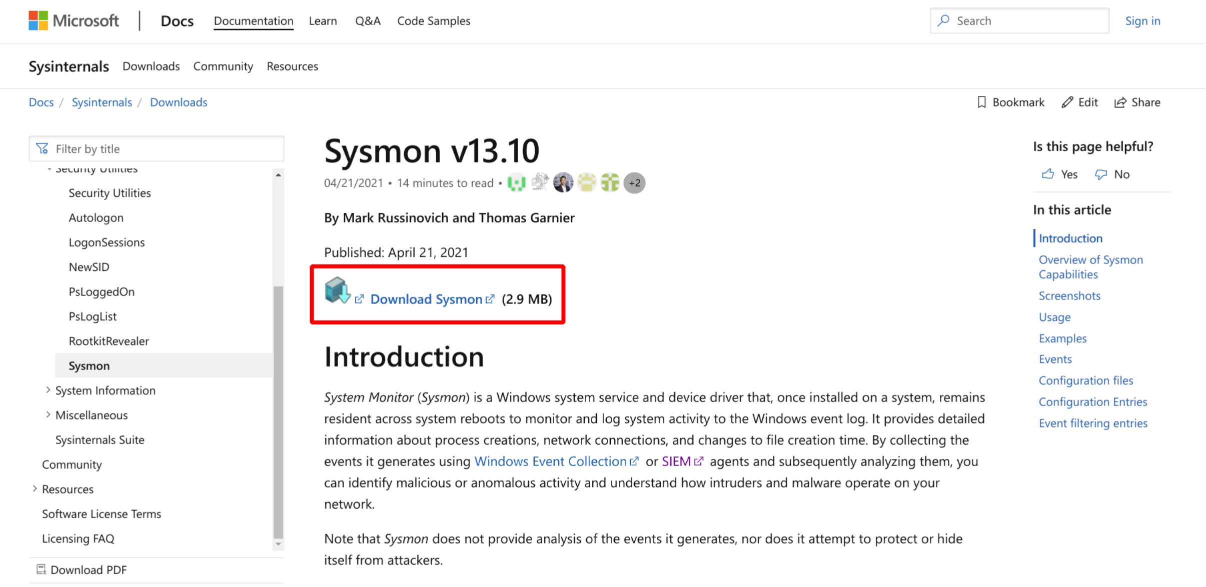
Status	Host	Agent policy	CPU
Healthy	desktop-hv8pnvk	My first agent policy rev. 2	0.68 %
Healthy	3ab7b79556d7	Elastic Cloud agent policy rev. 5	N/A

The Elastic Agent has been installed and configured to connect to our ELK instance in the cloud. In the upcoming section (part three), we will guide you on configuring Sysmon to send logs to this Elastic Agent. The Elastic Agent will then ingest these logs, making them visible in Kibana.

3. Download Sysmon

[Download Sysmon]

Find the "Download Sysmon" link.



Sysmon v13.10

04/21/2021 • 14 minutes to read • +2

By Mark Russinovich and Thomas Garnier

Published: April 21, 2021

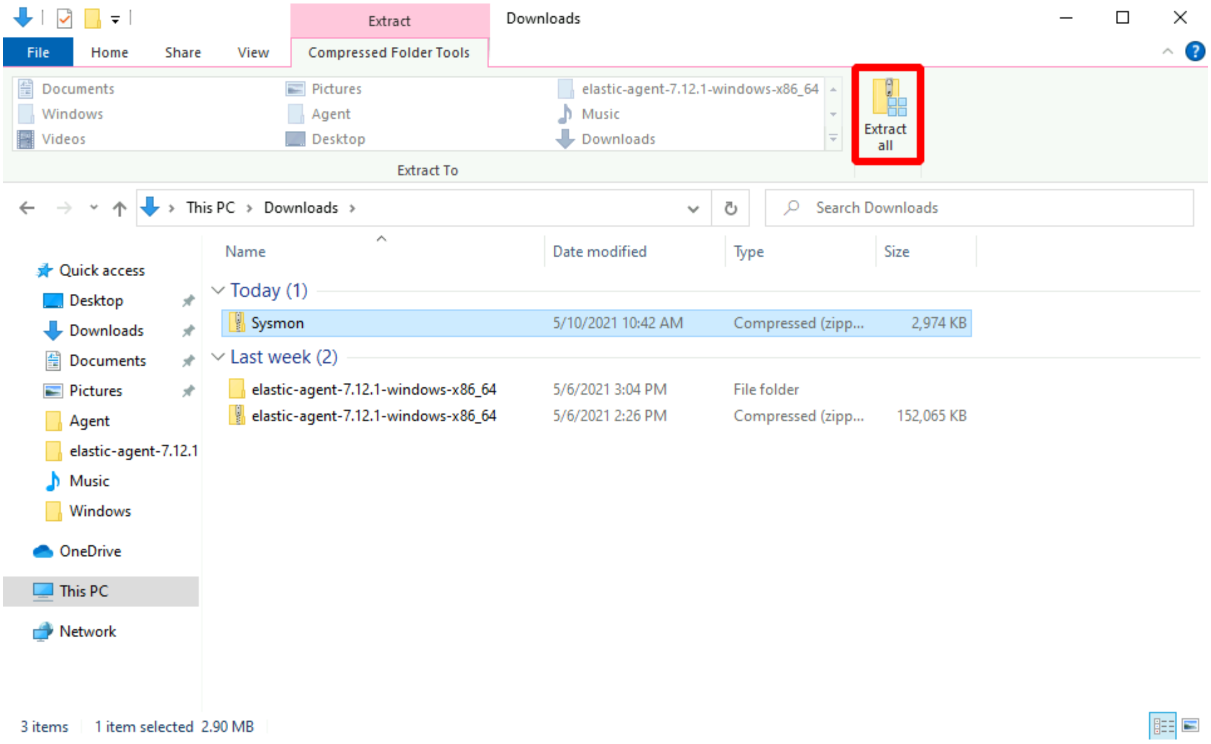
Download Sysmon (2.9 MB)

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.

Perform "Extract All" on the Sysmon Folder. Ensure the Sysmon folder is selected -- It will be highlighted blue.



Name	Date modified	Type	Size
Today (1)			
Sysmon	5/10/2021 10:42 AM	Compressed (zipp...	2,974 KB
Last week (2)			
elastic-agent-7.12.1-windows-x86_64	5/6/2021 3:04 PM	File folder	
elastic-agent-7.12.1-windows-x86_64	5/6/2021 2:26 PM	Compressed (zipp...	152,065 KB

"Extract" to the Downloads folder. Windows should auto-populate the Downloads path.

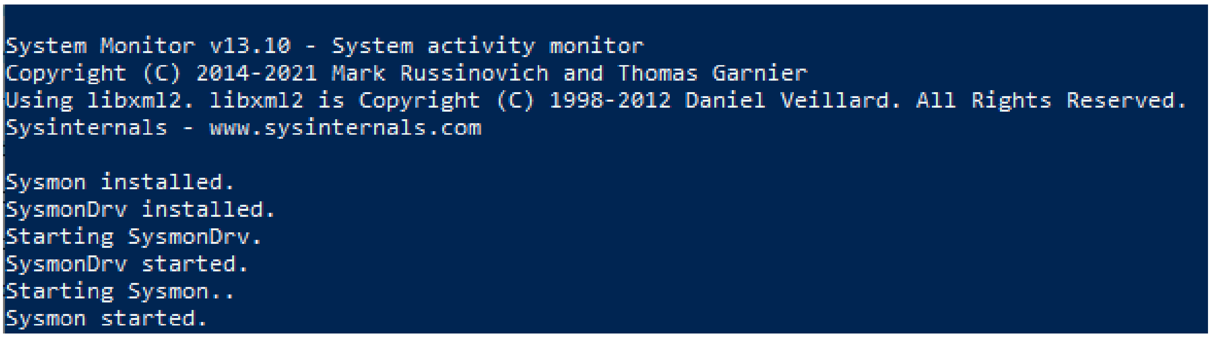
In your PowerShell window, enter the following command. You will need to substitute [USER] for the user you are using on your local system.

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

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

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

Your following output should look similar to this.



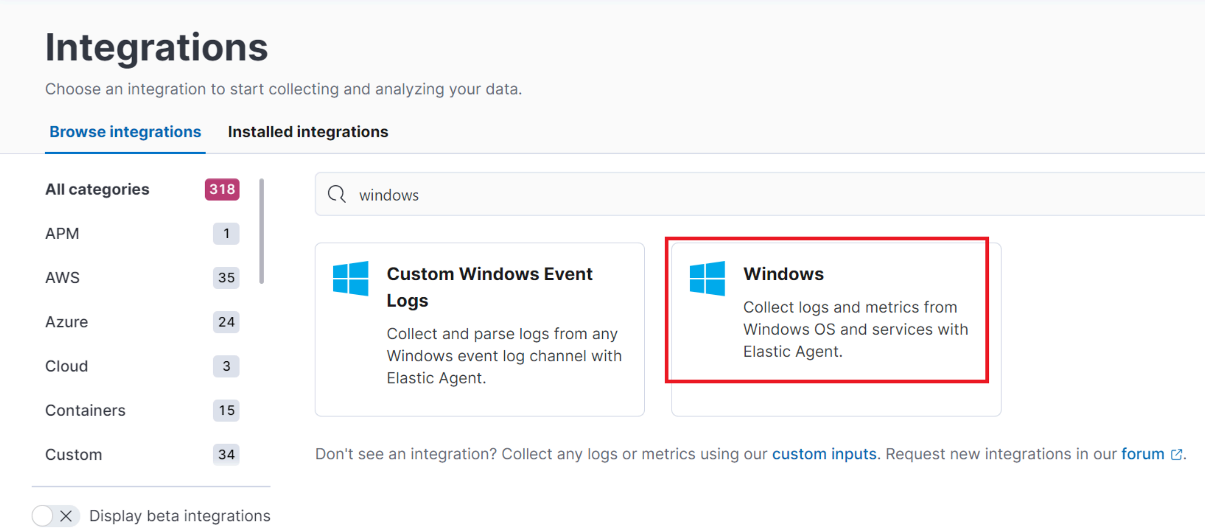
```
System Monitor v13.10 - System activity monitor
Copyright (C) 2014-2021 Mark Russinovich and Thomas Garnier
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

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

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 the Windows option with the red square pictured below.



Integrations

Choose an integration to start collecting and analyzing your data.

All categories	318
APM	1
AWS	35
Azure	24
Cloud	3
Containers	15
Custom	34

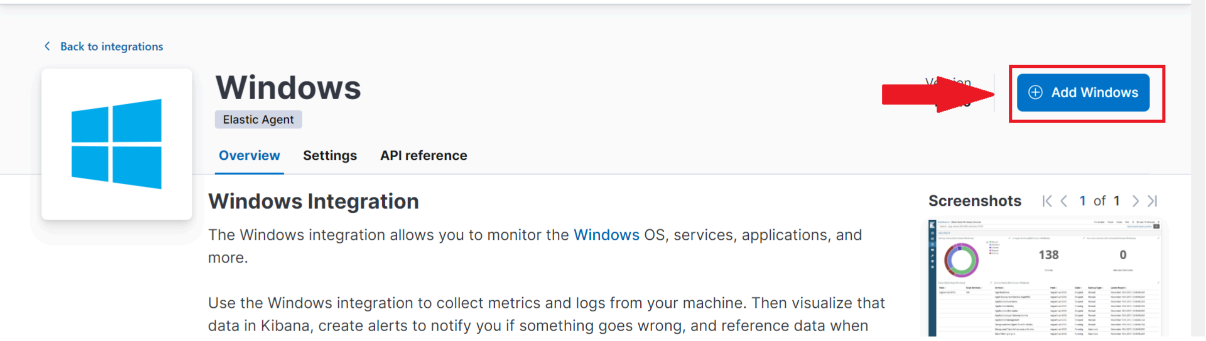
windows

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

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

Don't see an integration? Collect any logs or metrics using our custom inputs. Request new integrations in our forum.

Add this integration.



Windows

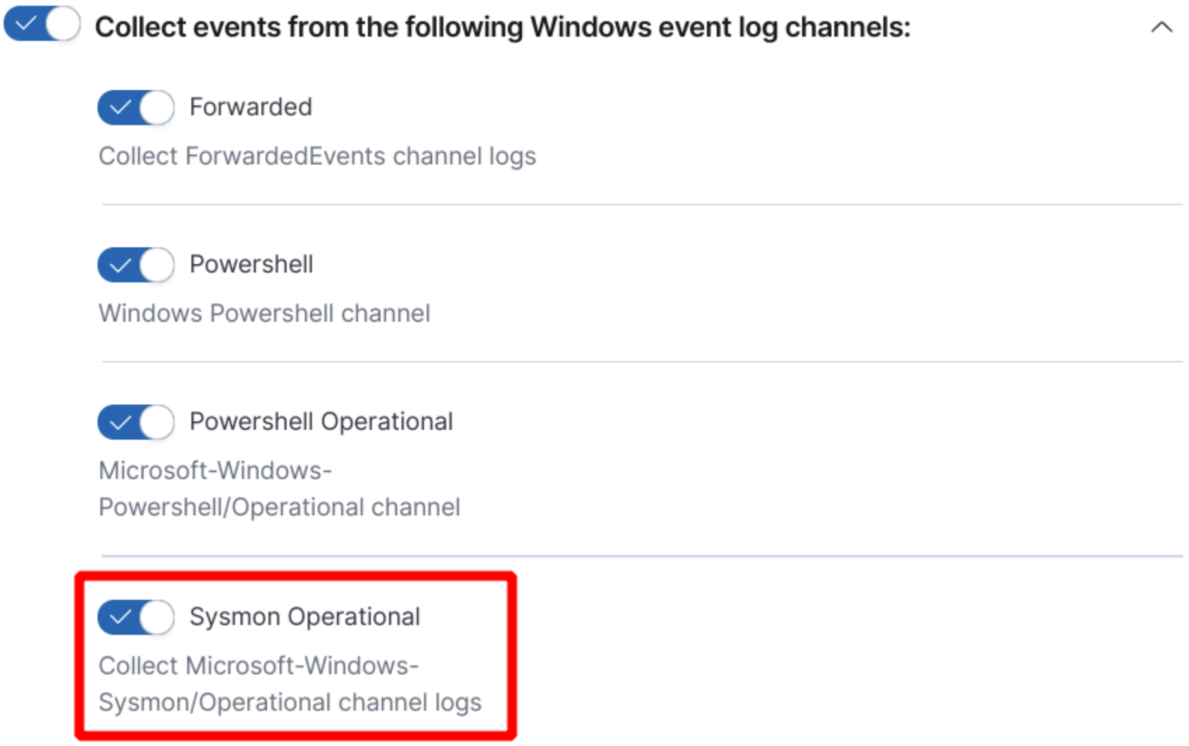
Elastic Agent

Windows Integration

The Windows integration allows you to monitor the Windows OS, services, applications, and more.

Use the Windows integration to collect metrics and logs from your machine. Then visualize that data in Kibana, create alerts to notify you if something goes wrong, and reference data when

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

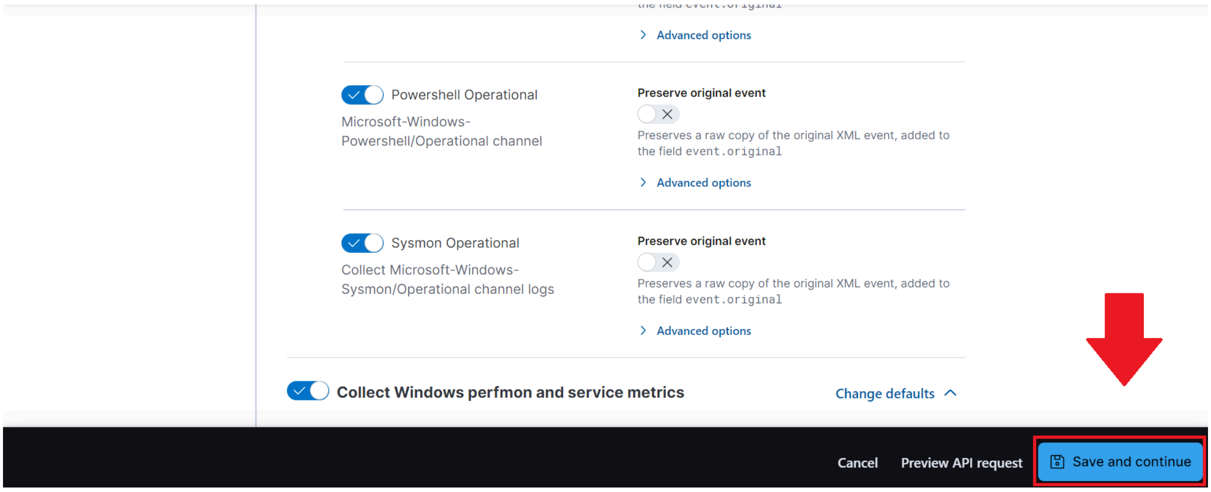
✓ Powershell Operational

Microsoft-Windows-Powershell/Operational channel

✓ Sysmon Operational

Collect Microsoft-Windows-Sysmon/Operational channel logs

Save the Integration.



Advanced options

Powershell Operational

Microsoft-Windows-Powershell/Operational channel

Preserve original event

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

Advanced options

Sysmon Operational

Collect Microsoft-Windows-Sysmon/Operational channel logs

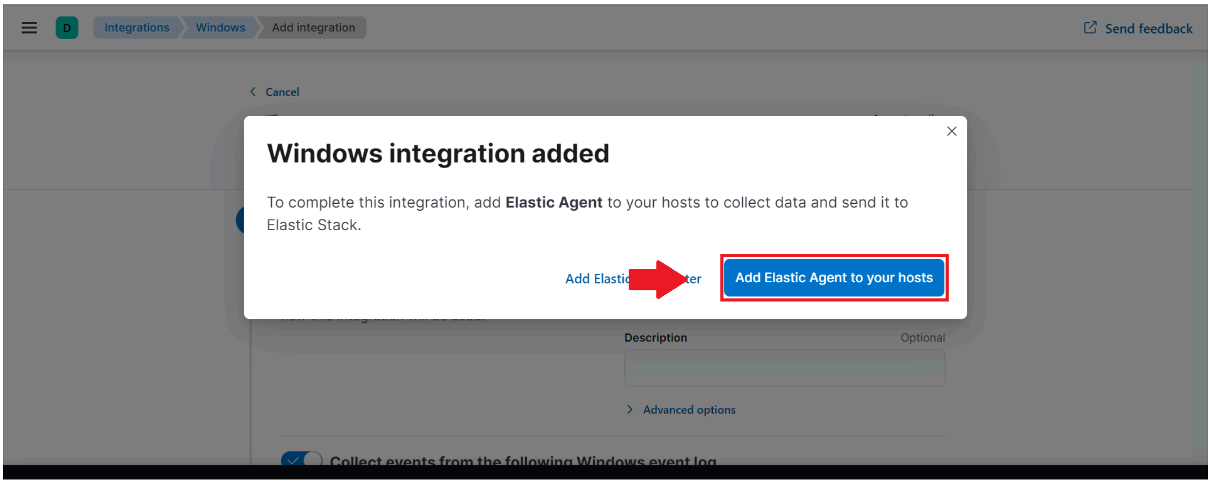
Preserve original event

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

Advanced options

Collect Windows perfmon and service metrics

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

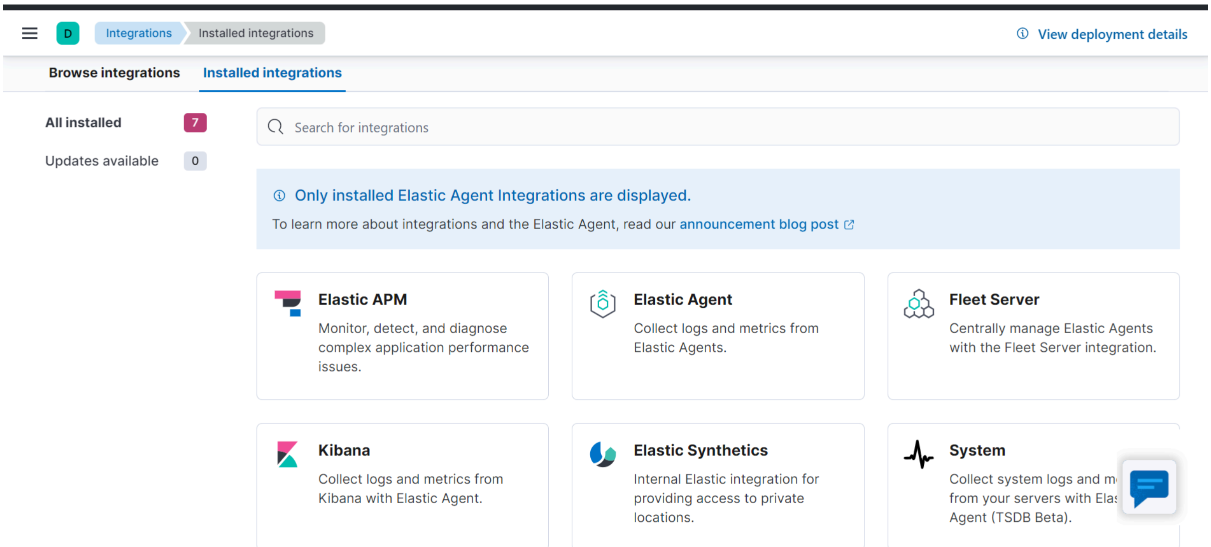


Windows integration added

To complete this integration, add **Elastic Agent** to your hosts to collect data and send it to Elastic Stack.

Add Elastic Agent later
Add Elastic Agent to your hosts
Description
Optional
Advanced options
Collect events from the following Windows event log

In the Integrations menu, find the "Installed integrations" tab.



Only installed Elastic Agent Integrations are displayed.

To learn more about integrations and the Elastic Agent, read our announcement blog post

Elastic APM
Monitor, detect, and diagnose complex application performance issues.

Elastic Agent
Collect logs and metrics from Elastic Agents.

Fleet Server
Centrally manage Elastic Agents with the Fleet Server integration.

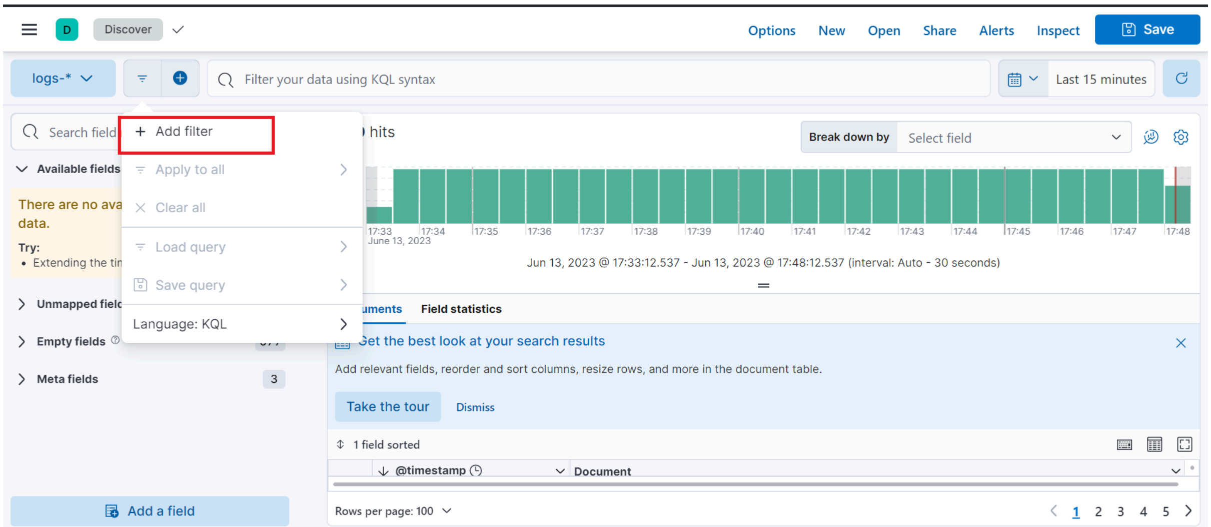
Kibana
Collect logs and metrics from Kibana with Elastic Agent.

Elastic Synthetics
Internal Elastic integration for providing access to private locations.

System
Collect system logs and m from your servers with Elas Agent (TSDB Beta).

At this point, play around on the computer that has Elastic Agent installed. Move files around, create files, start programs, make a few Google searches. This will generate some logs to ensure that we have Sysmon logs reaching our cloud.

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



There are no ava data.

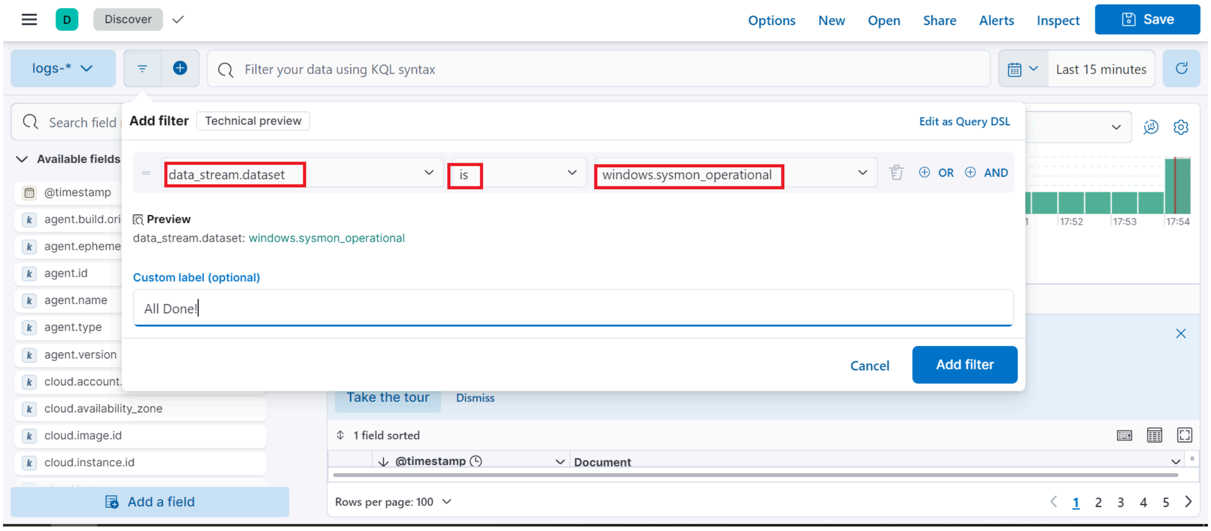
Try:
- Extending the tin

Jun 13, 2023 @ 17:33:12.537 - Jun 13, 2023 @ 17:48:12.537 (interval: Auto - 30 seconds)

Set the best look at your search results

Add relevant fields, reorder and sort columns, resize rows, and more in the document table.

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.

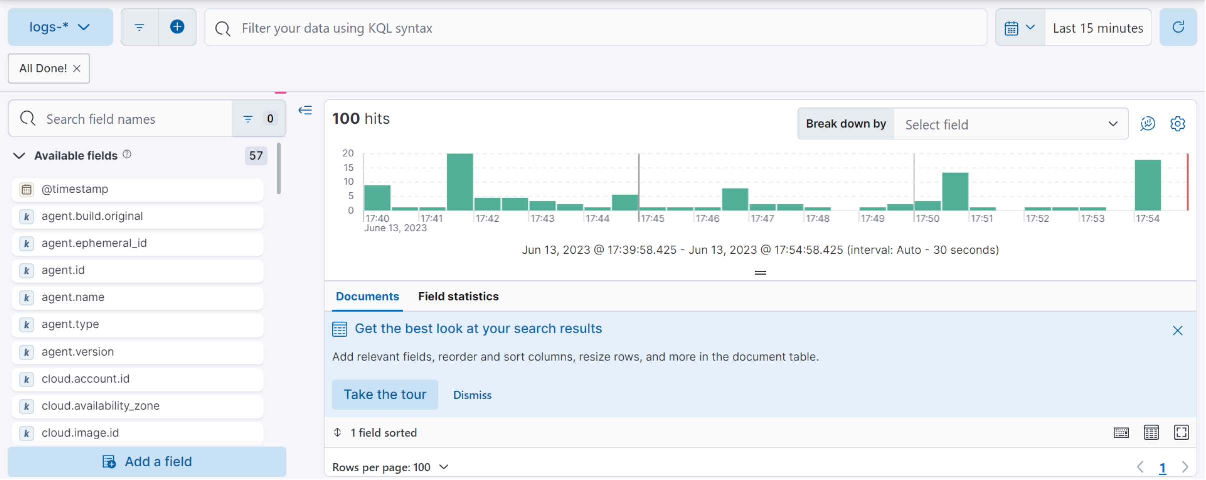


data_stream.dataset is windows.sysmon_operational

Preview
data_stream.dataset: windows.sysmon_operational

Custom label (optional)
All Done!

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



100 hits

Jun 13, 2023 @ 17:39:58.425 - Jun 13, 2023 @ 17:54:58.425 (interval: Auto - 30 seconds)

Get the best look at your search results

Add relevant fields, reorder and sort columns, resize rows, and more in the document table.

After completing this labs you'll be able to get all logs from your device to elastic cloud and you can analyse the logs generated.

For more detailed report you can go John strands github .