Kailash Parshad - Sysmon-Logs-To-Elastic-Search-ELK

- *Pushing Sysmon Log to Elastic search and visualize them in Kibana.*

GitHub: - https://github.com/at0m-b0mb

LinkedIn: - https://www.linkedin.com/in/kailash-parshad/

Installing Elastic Search on Debian: -

Link: -
https://www.elastic.co/guide/en/elasticsearch/reference/current/deb.html

Download and install the public signing key:

Command: -

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch |
sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-
keyring.gpg
```

Installing from the APT repository

Command: -

```
sudo apt-get install apt-transport-https
```

```
┌──(root㉿b0mb)-[/home/at0m]
└─# sudo apt-get install apt-transport-https -y
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
  apt apt-utils libapt-pkg6.0
Suggested packages:
  apt-doc aptitude | synaptic | wajig
The following NEW packages will be installed:
  apt-transport-https
The following packages will be upgraded:
  apt apt-utils libapt-pkg6.0
3 upgraded, 1 newly installed, 0 to remove and 835 not upgraded.
Need to get 2,615 kB of archives.
After this operation, 74.8 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 libapt-pkg6.0 amd64 2
.6.1 [907 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 apt amd64 2.6.1 [1,37
3 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 apt-utils amd64 2.6.1
 [309 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 apt-transport-https a
ll 2.6.1 [25.2 kB]
```

Save the repository definition to /etc/apt/sources.list.d/elastic-8.x.list

Command: -

```
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list
```

```
┌──(root㉿b0mb)-[/home/at0m]
└─# echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https
://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sou
rces.list.d/elastic-8.x.list
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifac
ts.elastic.co/packages/8.x/apt stable main
```

Elasticsearch Debian package install

Command: -

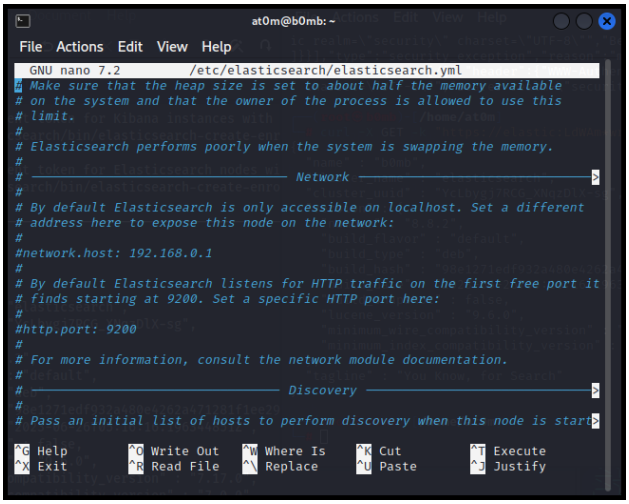
```
sudo apt-get update && sudo apt-get install elasticsearch
```

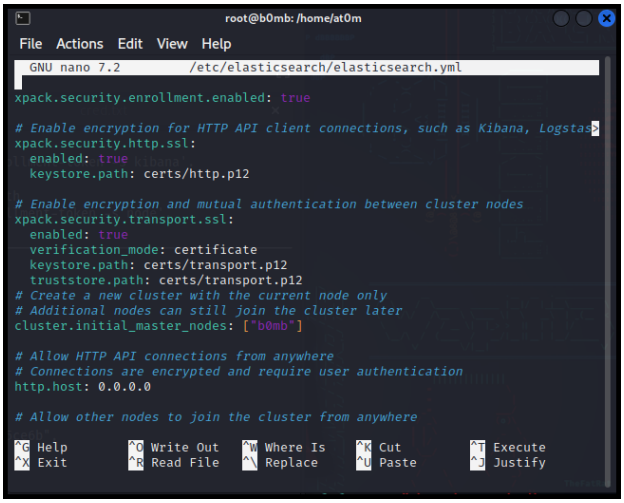
```
┌──(root㉿b0mb)-[/home/at0m]
└─# sudo apt-get update && sudo apt-get install elasticsearch
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable InRelease [10.4 kB
]
Get:2 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Package
s [55.3 kB]
Get:4 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Content
s (deb) [1,697 kB]
Hit:3 http://kali.download/kali kali-rolling InRelease
Fetched 1,763 kB in 1s (1,254 kB/s)
Reading package lists ... Done
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 835 not upgraded.
Need to get 597 MB of archives.
After this operation, 1,236 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elastic
search amd64 8.8.2 [597 MB]
Fetched 597 MB in 3min 33s (2,800 kB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 392697 files and directories currently installed.)
Preparing to unpack .../elasticsearch_8.8.2_amd64.deb ...
Creating elasticsearch group ... OK
Creating elasticsearch user ... OK
```

Editing elasticsearch.yml file

Command: -

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```





Starting and Enabling Elastic Search Service

Command: -

```
sudo systemctl start elasticsearch
```

```
sudo systemctl enable elasticsearch.service
```

```
┌──(root㉿b0mb)-[/home/at0m]
└─# sudo systemctl start elasticsearch

┌──(root㉿b0mb)-[/home/at0m]
└─# curl -X GET "localhost:9200"
curl: (52) Empty reply from server

┌──(root㉿b0mb)-[/home/at0m]
└─# sudo systemctl enable elasticsearch.service
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.ser
vice → /lib/systemd/system/elasticsearch.service.
```

Starting and Enabling Elastic Search Service

Command: -

```
curl -X GET -k "https://elastic:<your_password>@localhost:9200"
```

```
┌──(root㉿b0mb)-[/home/at0m]
└─# curl -X GET -k "https://elastic:LdWAm*wrv+N4sAjA2lIE@localhost:9200"
{
  "name" : "b0mb",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "YcLbygj7RCG_XNqzDlX-sg",
  "version" : {
    "number" : "8.8.2",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "98e1271edf932a480e4262a471281f1ee295ce6b",
    "build_date" : "2023-06-26T05:16:16.196344851Z",
    "build_snapshot" : false,
    "lucene_version" : "9.6.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Installing Kibana: -

Command: -

```
sudo apt install kibana
```

```
┌──(root㉿b0mb)-[/home/at0m]
└─# sudo apt install kibana
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  kibana
0 upgraded, 1 newly installed, 0 to remove and 835 not upgraded.
Need to get 281 MB of archives.
After this operation, 750 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 kibana
amd64 8.8.2 [281 MB]
Fetched 281 MB in 1min 34s (2,984 kB/s)
Selecting previously unselected package kibana.
(Reading database ... 393995 files and directories currently installed.)
Preparing to unpack .../kibana_8.8.2_amd64.deb ...
Unpacking kibana (8.8.2) ...
Setting up kibana (8.8.2) ...
Creating kibana group ... OK
Creating kibana user ... OK
Created Kibana keystore in /etc/kibana/kibana.keystore
```

Starting and Enabling Logstash Service

Command: -

```
sudo apt-get install logstash
```

```
┌──(root㉿b0mb)-[/home/at0m]
└─# sudo apt install logstash
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontend. It is
 held by process 27996 (apt-get)
Reading package lists ... 0%
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 835 not upgraded.
Need to get 346 MB of archives.
After this operation, 602 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 logstas
h amd64 1:8.8.2-1 [346 MB]
Fetched 346 MB in 4min 1s (1,436 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 467866 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a8.8.2-1_amd64.deb ...
Unpacking logstash (1:8.8.2-1) ...
Setting up logstash (1:8.8.2-1) ...
```

Starting and Enabling Logstash Service

Command: -

```
sudo systemctl start logstash.service
```

```
sudo systemctl enable logstash.service
```

```
┌──(root㉿b0mb)-[/home/at0m]
└─# sudo systemctl start logstash

┌──(root㉿b0mb)-[/home/at0m]
└─# sudo systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service
→ /lib/systemd/system/logstash.service.
```

Creating Enrolment Tickets from Elastic for Kibana: -

Command: -

```
/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token
-s kibana
```

```
┌──(root㉿b0mb)-[/home/at0m]
└─# /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kib
ana
eyJ2ZXIiOiI4LjguMiIsImFkciI6WyIxOTIuMTY4LjYuMTMyOjkyMDAiXSwiZmdyIjoiNTI3NGQzZ
WMxYmE2Nzc0MjJlMjMzYjkzNjhkODg5Yjc2M2MzM2NiOGM1Nzc2YjUxMGQ2MWVmNTAyOGM4YzVlMi
IsImtleSI6Ii1LSkdSb2tCa3BpTDZHcU9id0l3OlQ1a3d5ZEtGUS02TVJyR3B6djZ3aHcifQ==
```

Doing setup of Kibana from the previously generated Enrolment Ticket: -

Command: -

```
/usr/share/kibana/bin/kibana-setup
```

```
<After this Enter the Previous Generated Ticket in the previous
command>
```

```
┌──(root㉿b0mb)-[/home/at0m]
└─# /usr/share/kibana/bin/kibana-setup
? Enter enrollment token: eyJ2ZXIiOiI4LjguMiIsImFkciI6WyIxOTIuMTY4LjYuMTMyOjk
yMDAiXSwiZmdyIjoiNTI3NGQzZWMxYmE2Nzc0MjJlMjMzYjkzNjhkODg5Yjc2M2MzM2NiOGM1Nzc2
YjUxMGQ2MWVmNTAyOGM4YzVlMiIsImtleSI6Ii1xSkhSb2tCa3BpTDZHcU9DUUxxOlExNlRxUENIU
1hTU1pEc014YjlVNEEifQ==

✓ Kibana configured successfully.

To start Kibana run:
  bin/kibana
```

Starting and Enabling Kibana Service

Command: -

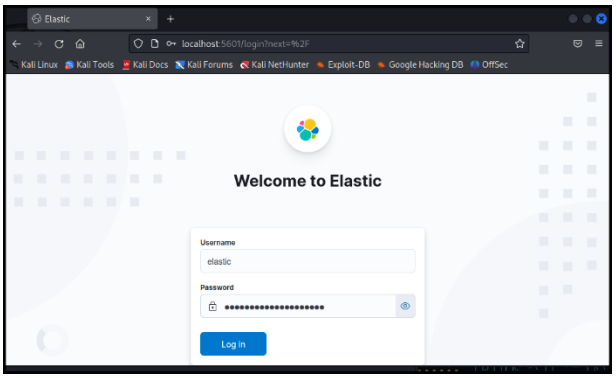
```
sudo systemctl start kibana.service
```

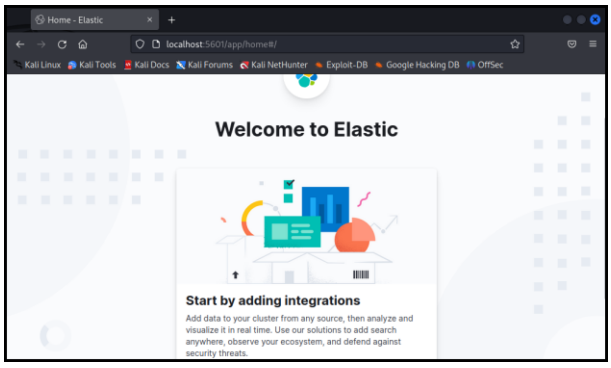
```
sudo systemctl enable kibana.service
```

```
┌──(root㉿b0mb)-[/home/at0m]
└─# sudo systemctl start kibana

┌──(root㉿b0mb)-[/home/at0m]
└─# sudo systemctl enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service →
/lib/systemd/system/kibana.service.
```

Checking if we can Access Kibana on: -

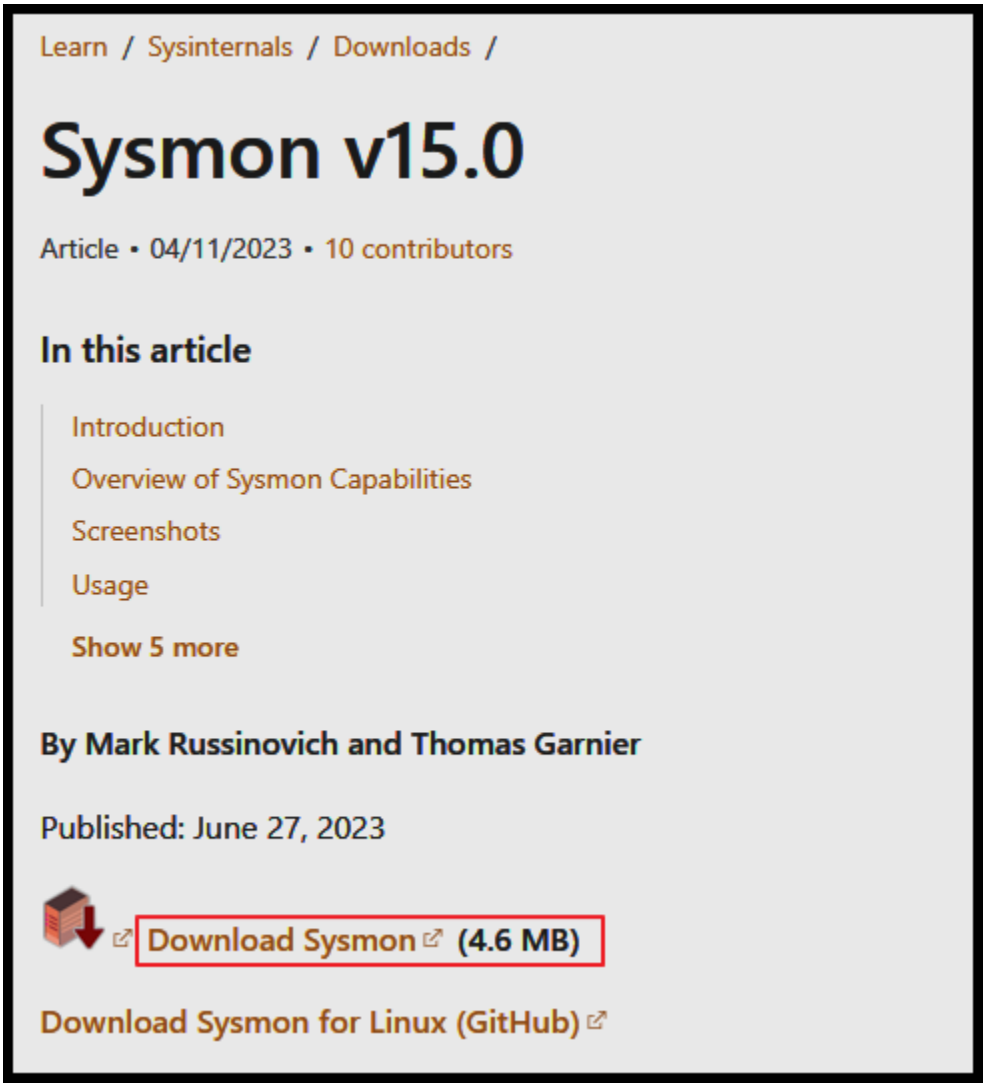
http://localhost:5601





Download Sysmon on Windows: -

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon



Downloading Sysmon configuration ".xml" file from GitHub: -

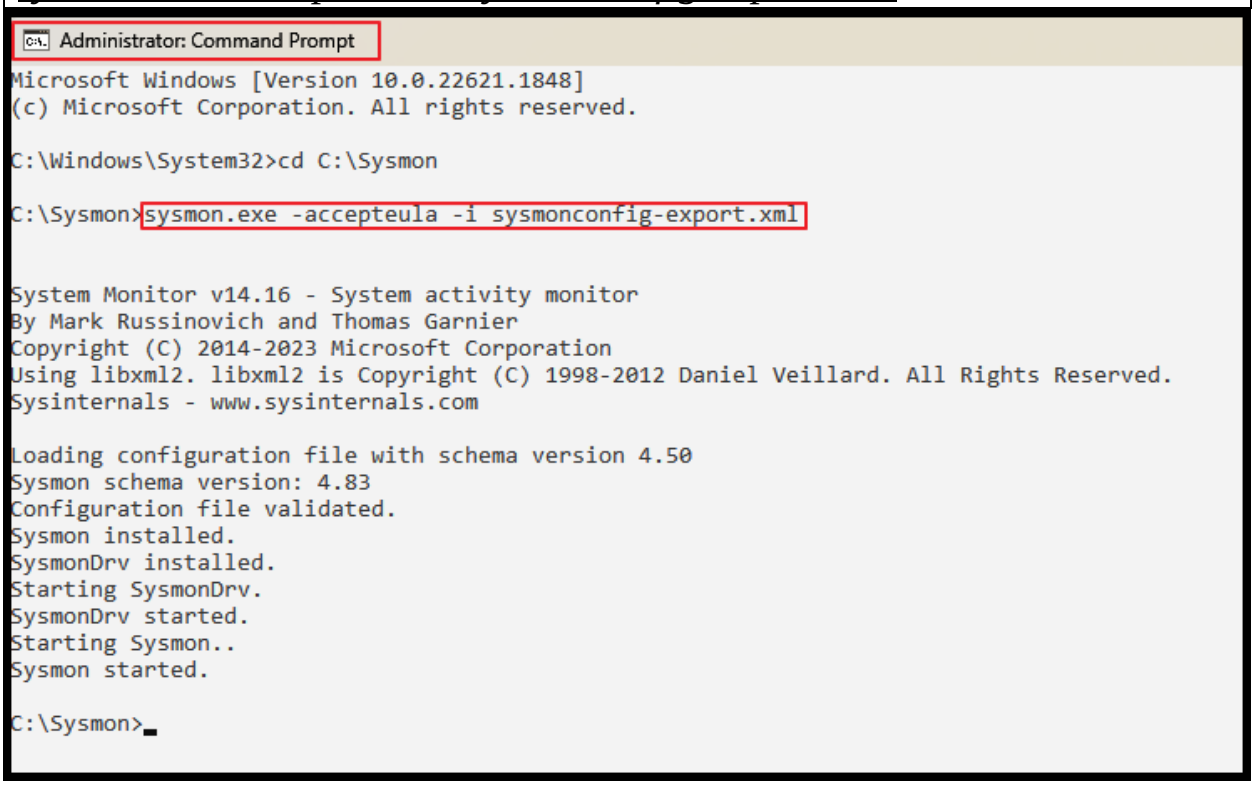
https://github.com/SwiftOnSecurity/sysmon-config

or

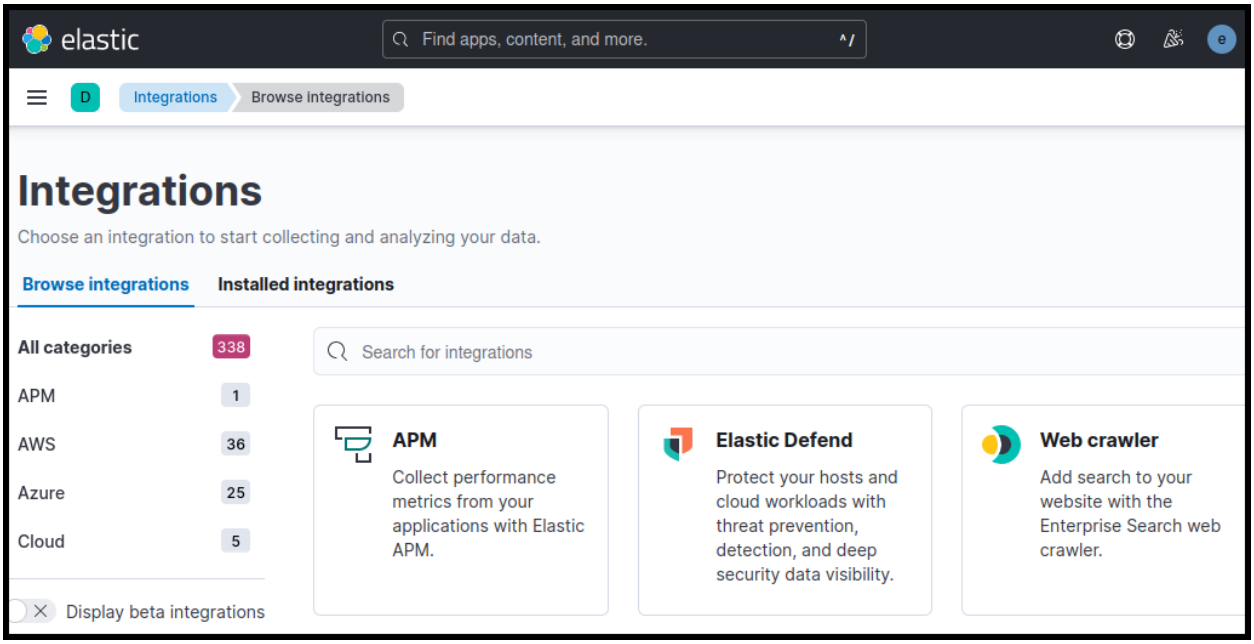
GitHub - SwiftOnSecurity/sysmon-config: Sysmon configuration file template with default high-quality event tracing

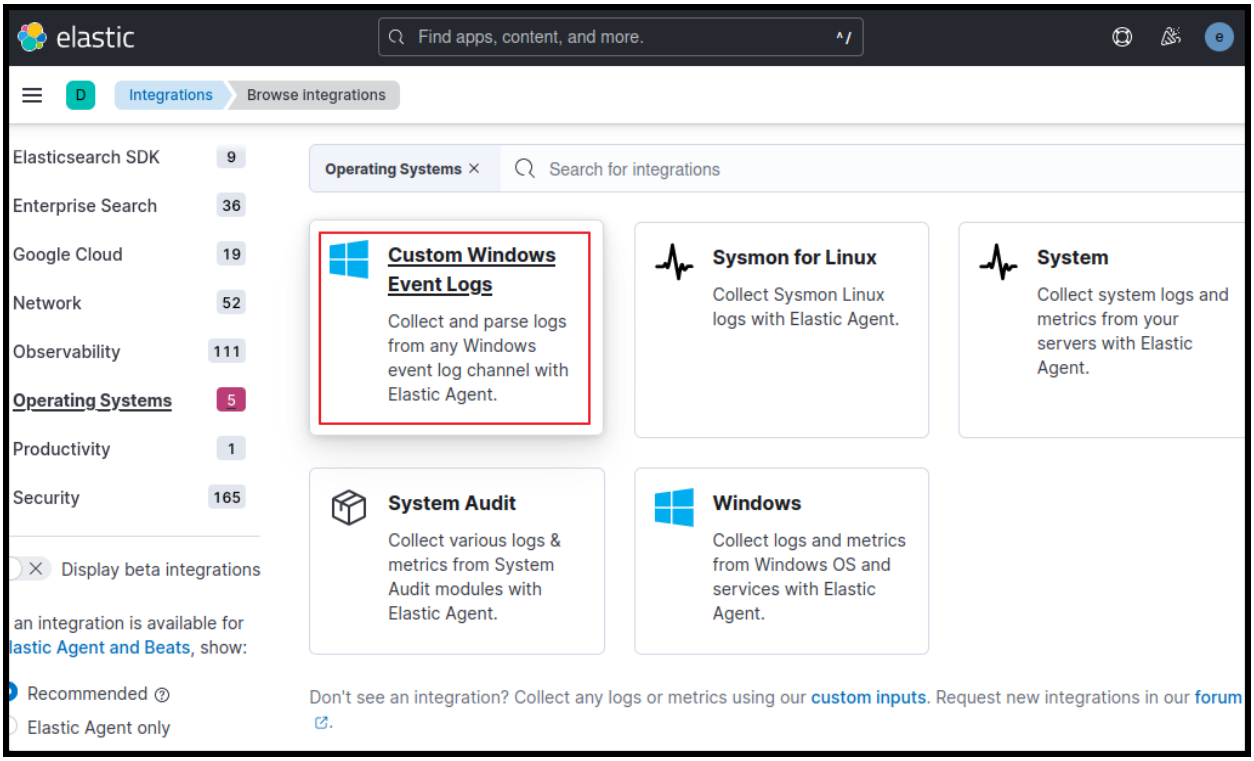
Code: -

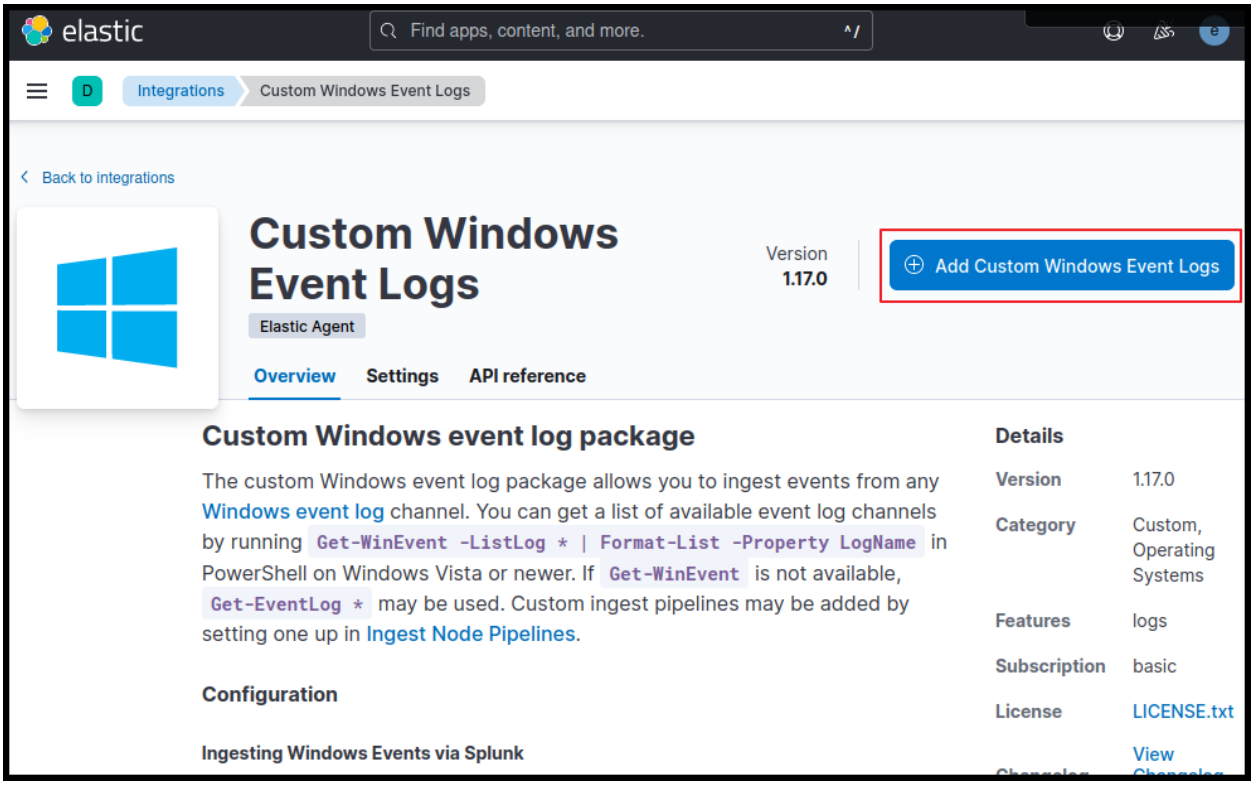
sysmon.exe -accepteula -i sysmonconfig-export.xml

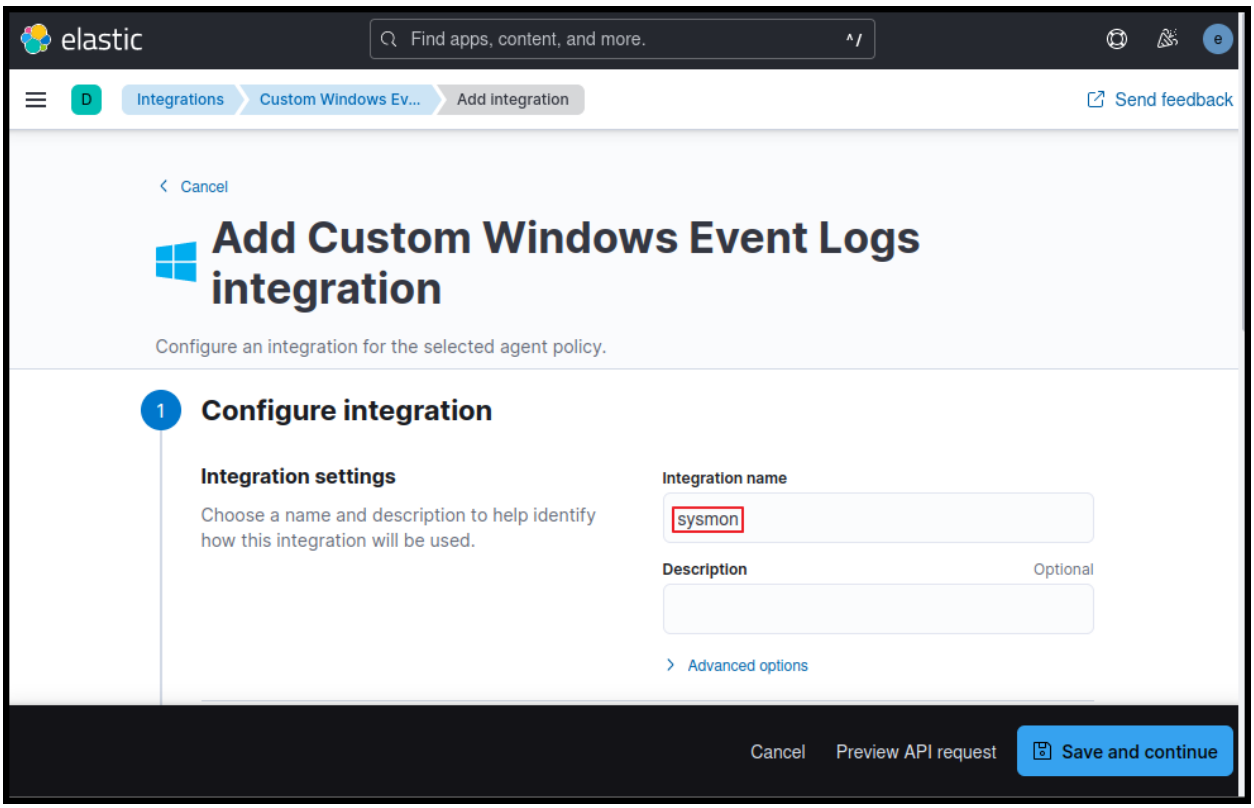


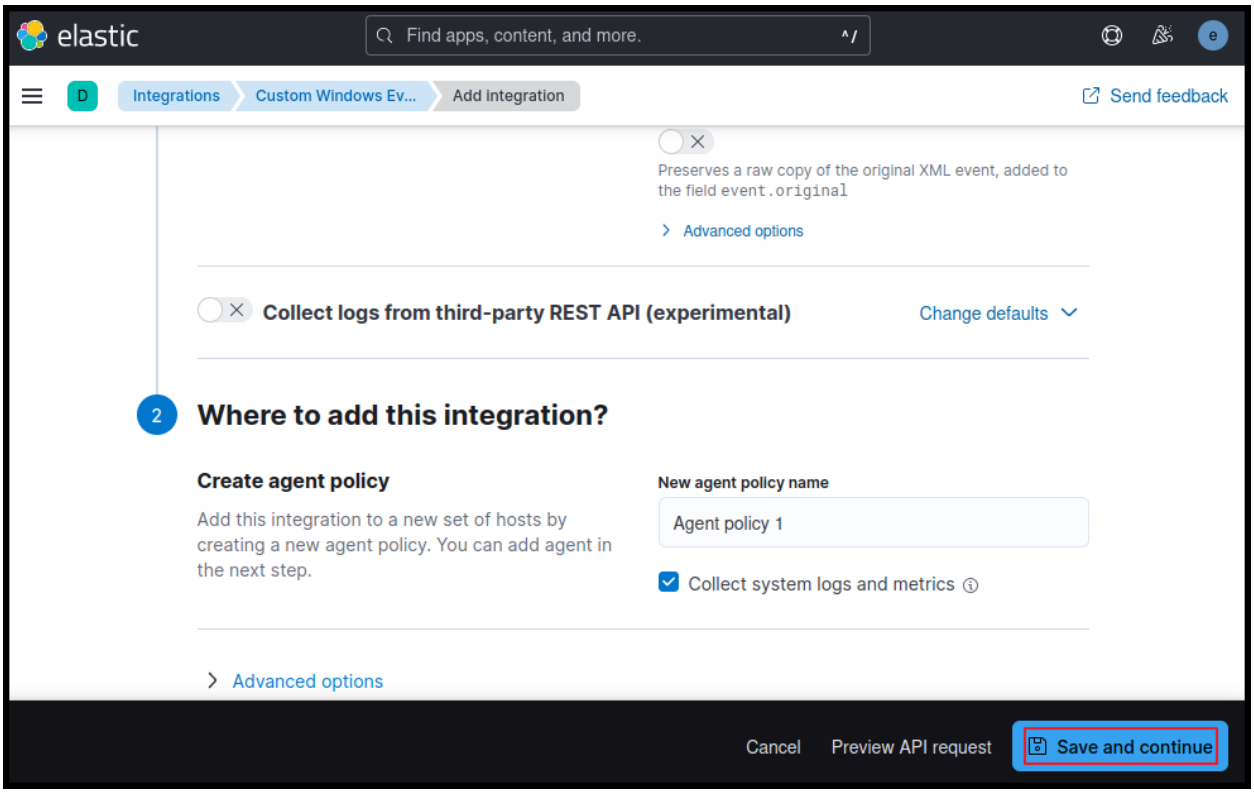
Going to the Integrations and installing Windows Custom Logs: -

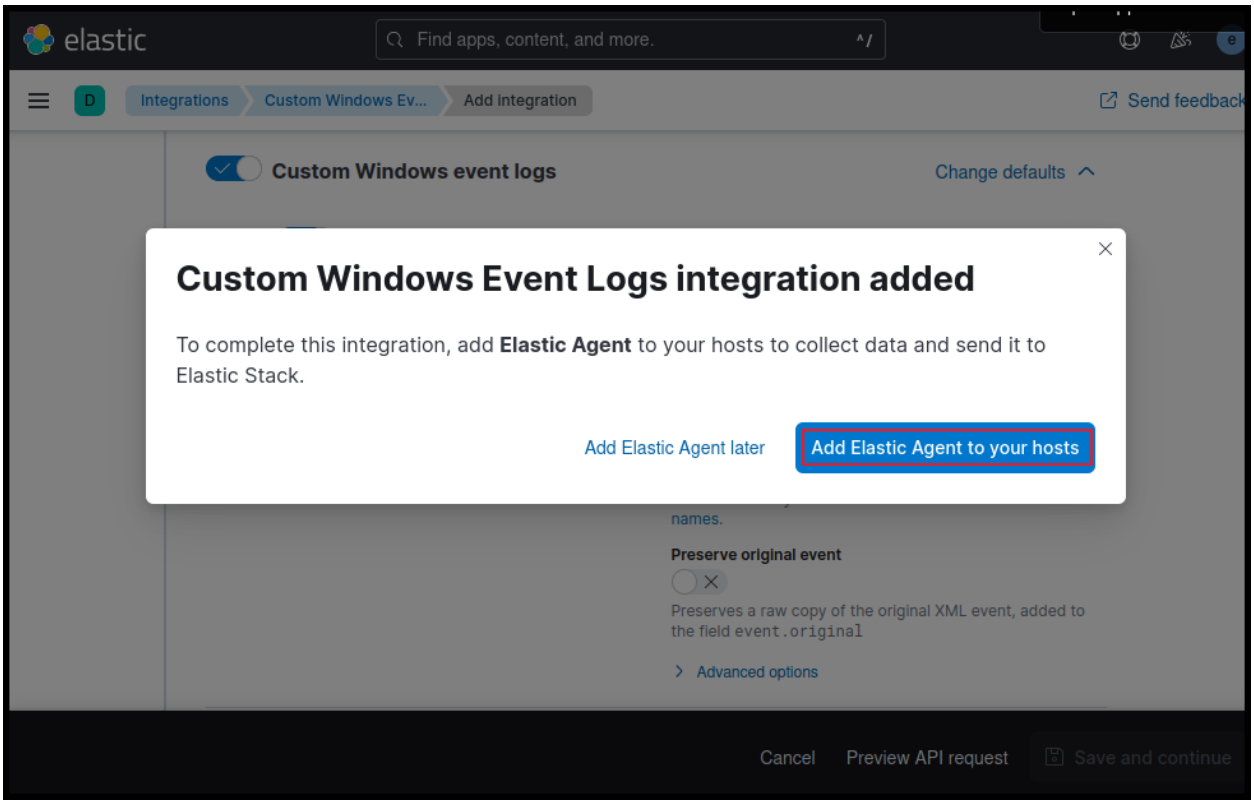


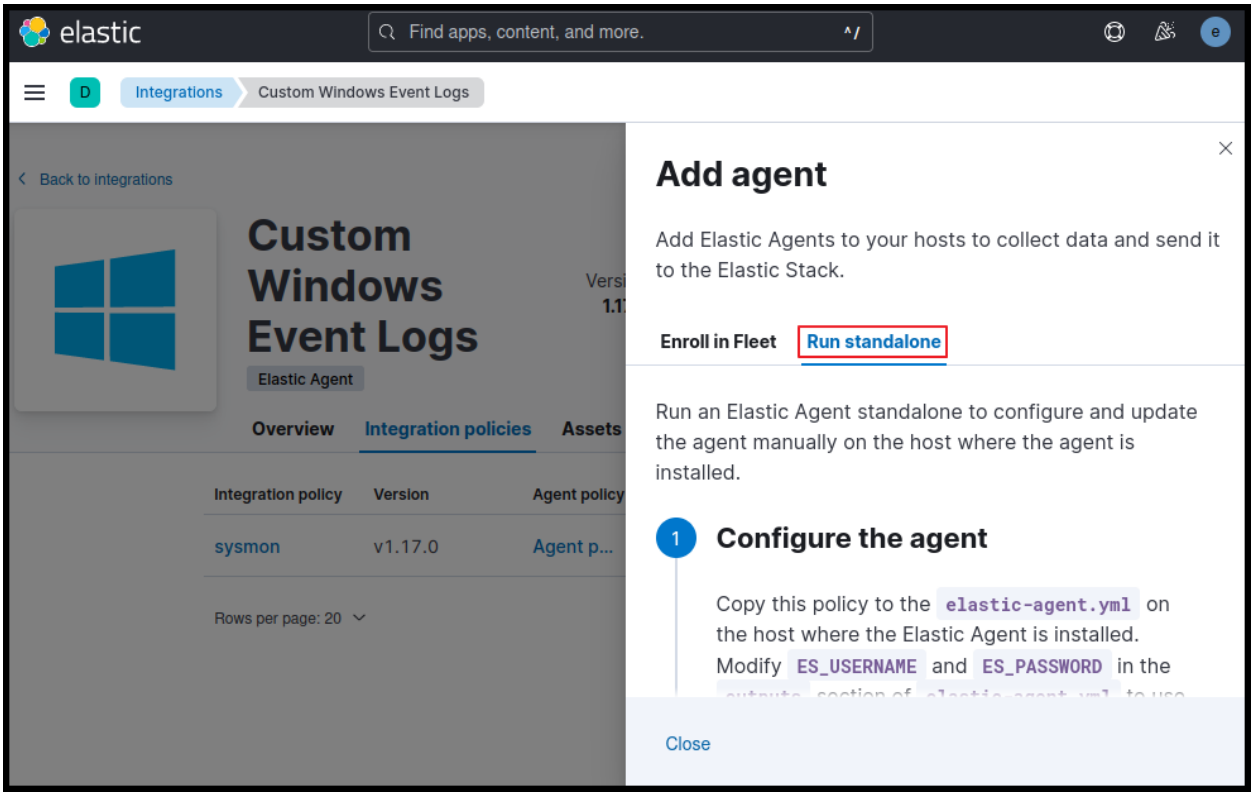

elastic
Find apps, content, and more.
Integrations
Browse integrations
Elasticsearch SDK 9
Enterprise Search 36
Google Cloud 19
Network 52
Observability 111
Operating Systems 5
Productivity 1
Security 165
Display beta integrations
an integration is available for
lastic Agent and Beats, show:
Recommended
Elastic Agent only
Operating Systems
Search for integrations
Custom Windows Event Logs
Collect and parse logs from any Windows event log channel with Elastic Agent.
Sysmon for Linux
Collect Sysmon Linux logs with Elastic Agent.
System
Collect system logs and metrics from your servers with Elastic Agent.
System Audit
Collect various logs & metrics from System Audit modules 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

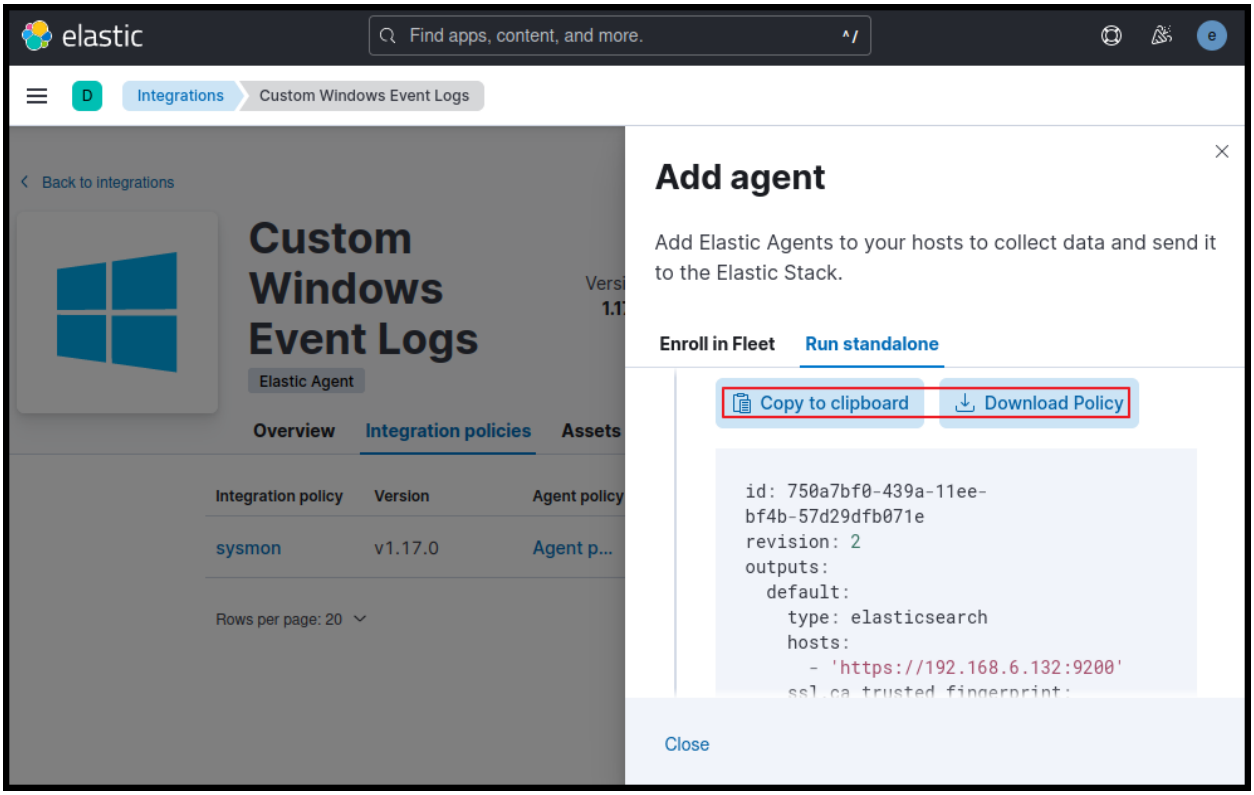

elastic
Find apps, content, and more.
Integrations
Custom Windows Event Logs
Back to integrations
Custom Windows Event Logs
Elastic Agent
Version
1.17.0
Add Custom Windows Event Logs
Overview
Settings
API reference
Custom Windows event log package
The custom Windows event log package allows you to ingest events from any Windows event log channel. You can get a list of available event log channels by running Get-WinEvent -ListLog * | Format-List -Property LogName in PowerShell on Windows Vista or newer. If Get-WinEvent is not available, Get-EventLog * may be used. Custom ingest pipelines may be added by setting one up in Ingest Node Pipelines.
Configuration
Ingesting Windows Events via Splunk
Details
Version 1.17.0
Category Custom, Operating Systems
Features logs
Subscription basic
License LICENSE.txt
View


elastic
Find apps, content, and more.
Integrations
Custom Windows Ev...
Add integration
Send feedback
Cancel
Add Custom Windows Event Logs integration
Configure an integration for the selected agent policy.
1
Configure integration
Integration settings
Choose a name and description to help identify how this integration will be used.
Integration name
sysmon
Description
Optional
Advanced options
Cancel
Preview API request
Save and continue


elastic
Find apps, content, and more.
Integrations
Custom Windows Ev...
Add integration
Send feedback
Preserves a raw copy of the original XML event, added to the field event.original
Advanced options
Collect logs from third-party REST API (experimental)
Change defaults
2
Where to add this integration?
Create agent policy
Add this integration to a new set of hosts by creating a new agent policy. You can add agent in the next step.
New agent policy name
Agent policy 1
Collect system logs and metrics
Advanced options
Cancel
Preview API request
Save and continue

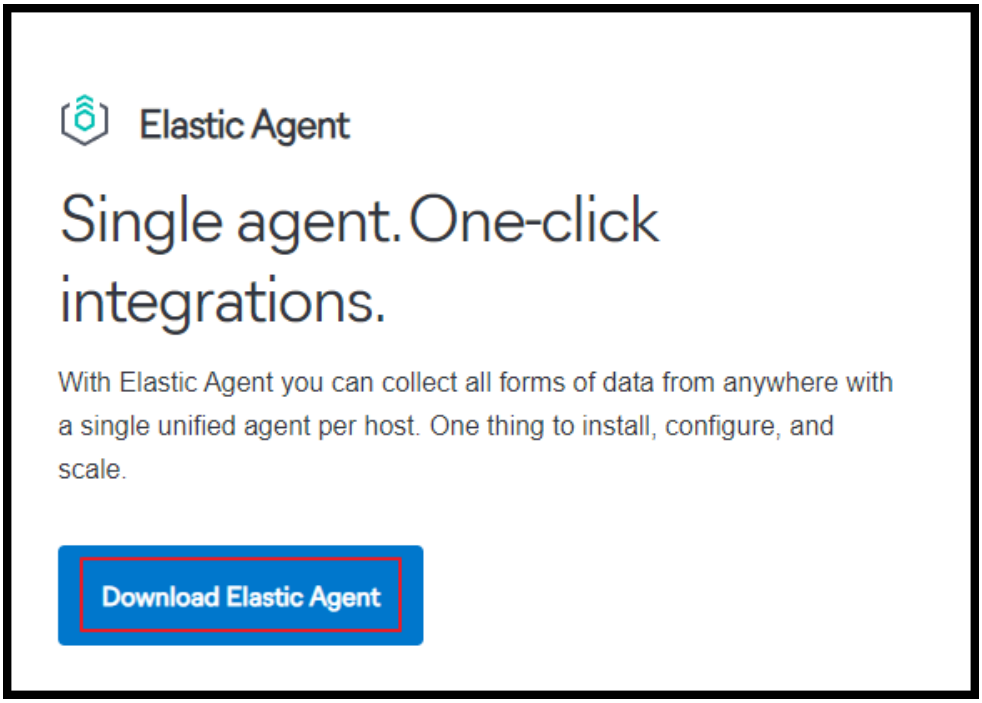

elastic
Find apps, content, and more.
Integrations
Custom Windows Ev...
Add integration
Send feedback
Custom Windows event logs
Change defaults
Custom Windows Event Logs integration added
To complete this integration, add Elastic Agent to your hosts to collect data and send it to Elastic Stack.
Add Elastic Agent later
Add Elastic Agent to your hosts
names.
Preserve original event
Preserves a raw copy of the original XML event, added to the field event.original
Advanced options
Cancel
Preview API request
Save and continue


elastic
Find apps, content, and more.
Integrations
Custom Windows Event Logs
Back to integrations
Custom Windows Event Logs
Elastic Agent
Overview
Integration policies
Assets
Integration policy
Version
Agent policy
sysmon
v1.17.0
Agent p...
Rows per page: 20
Add agent
Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.
Enroll in Fleet
Run standalone
Run an Elastic Agent standalone to configure and update the agent manually on the host where the agent is installed.
1
Configure the agent
Copy this policy to the elastic-agent.yml on the host where the Elastic Agent is installed. Modify ES_USERNAME and ES_PASSWORD in the
Close



Downloading Elastic Agent: -

https://www.elastic.co/elastic-agent



Configuring Elastic Agent "elastic-agent.yml" file: -

elastic-agent.yml

C: > Program Files > Elastic-Agent > elastic-agent.yml

```yaml
id: 750a7bf0-439a-11ee-bf4b-57d29dfb071e
revision: 2
outputs:
  default:
    type: elasticsearch
    hosts:
      - 'https://192.168.6.132:9200'
    ssl.ca_trusted_fingerprint: 5274d3ec1ba677422e233b9368d889b763c33cb8c5776b510d61ef5028c8c5
    username: 'elastic'
    password: 'LdWAm*wrv+N4sAjA2lIE'
output_permissions:
  default:
    _elastic_agent_monitoring:
      indices:
        - names:
            - logs-elastic_agent.apm_server-default
          privileges:
            - auto_configure
            - create_doc
        - names:
            - metrics-elastic_agent.apm_server-default
          privileges:
            - auto_configure
            - create_doc
        - names:
            - logs-elastic_agent.auditbeat-default
          privileges:
            - auto_configure
            - create_doc
        - names:
            - metrics-elastic_agent.auditbeat-default
          privileges:
```

Installing configured Elastic-agent as an service: -

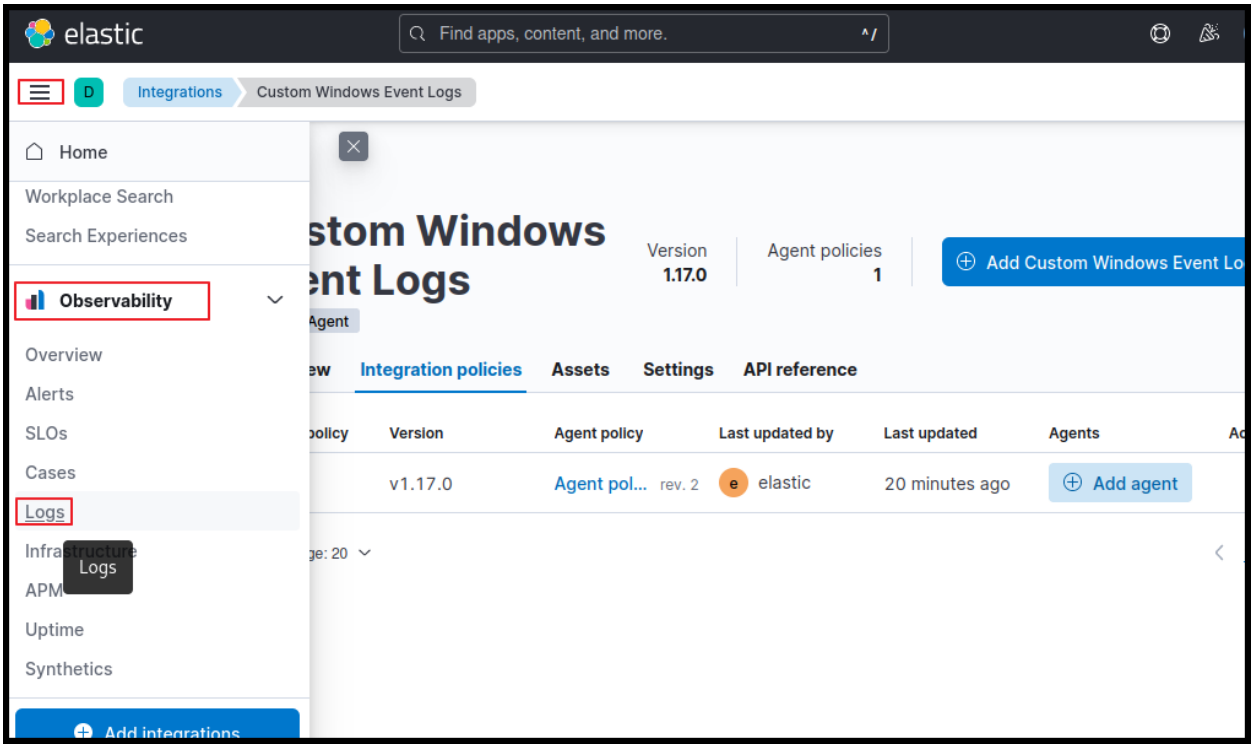
Command: -

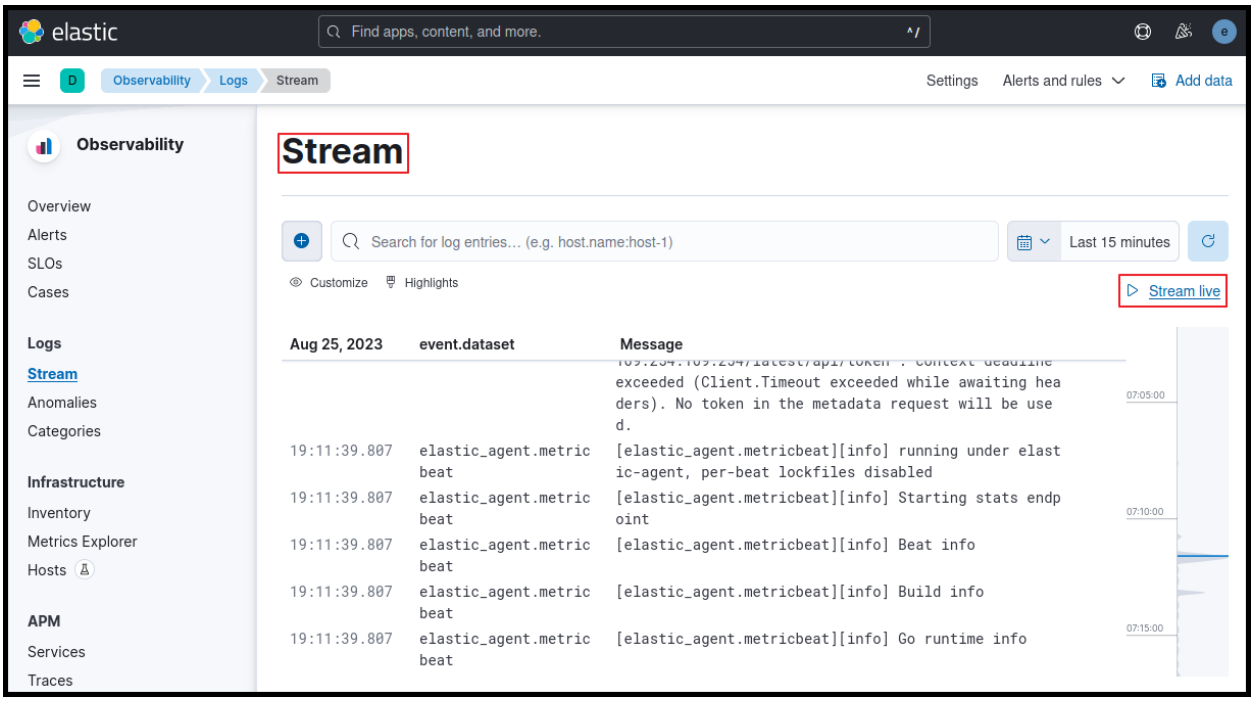
```
elastic-agent.exe install
```

Administrator: Command Prompt

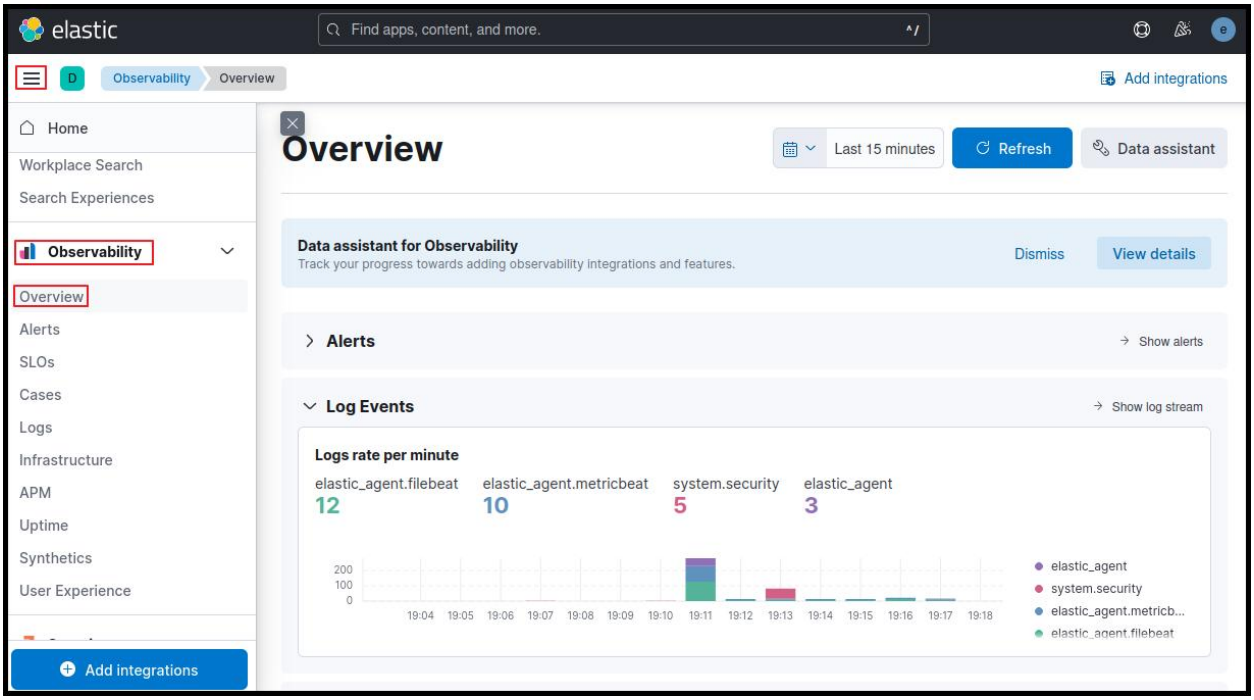
```
C:\Program Files\Elastic-Agent>reset
Invalid parameter(s)
RESET { SESSION }

C:\Program Files\Elastic-Agent>elastic-agent.exe install
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
Do you want to enroll this Agent into Fleet? [Y/n]:n
Elastic Agent has been successfully installed.

C:\Program Files\Elastic-Agent>
```

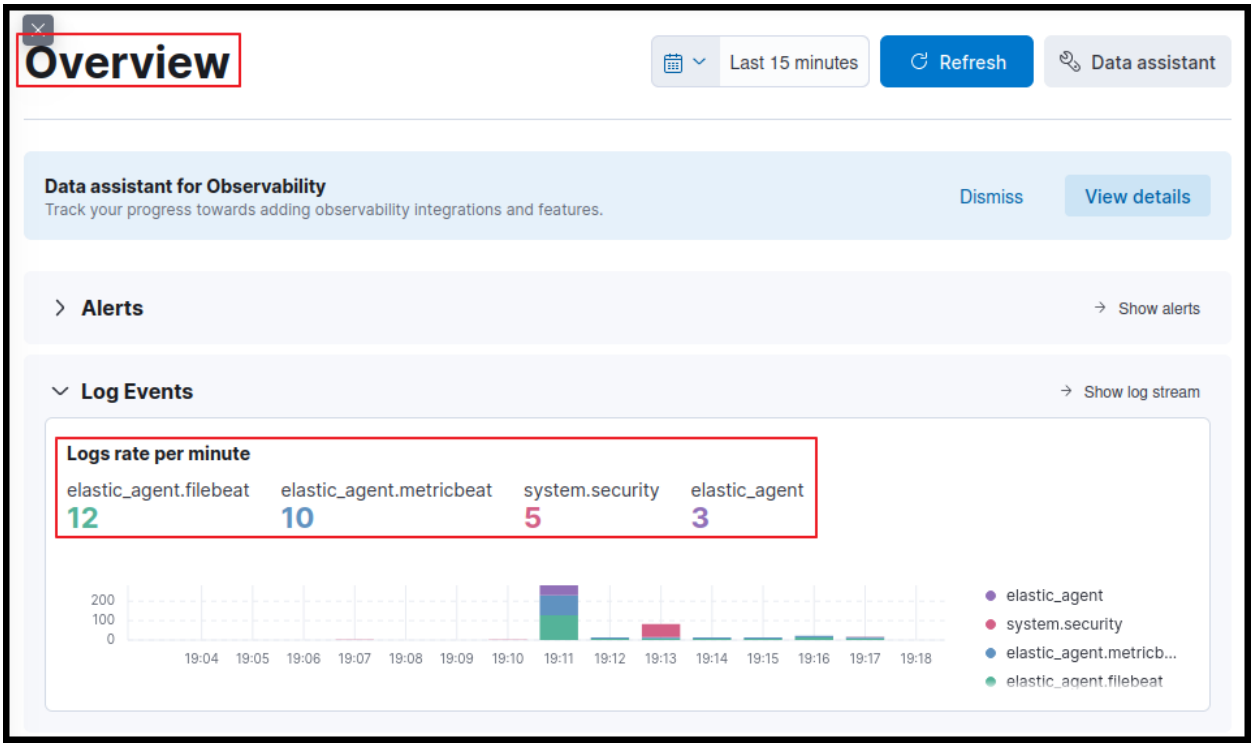
Checking Logs Streams if elastic-agent is pushing data or not: -



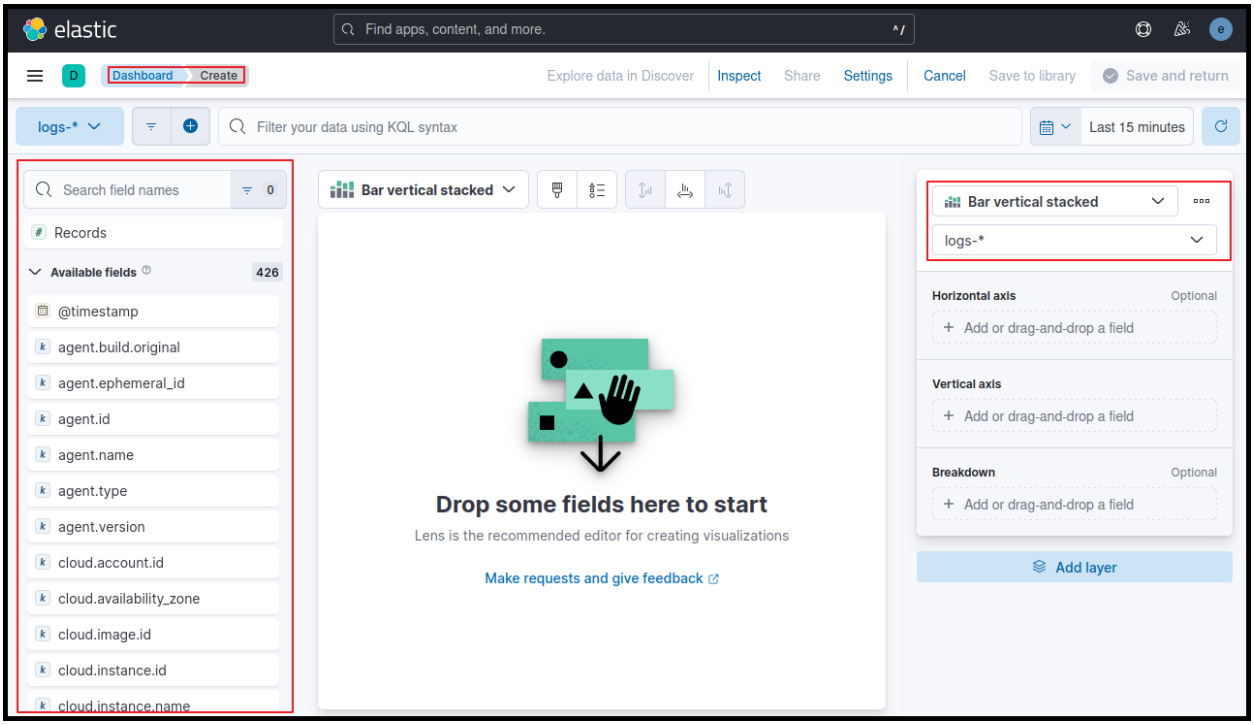


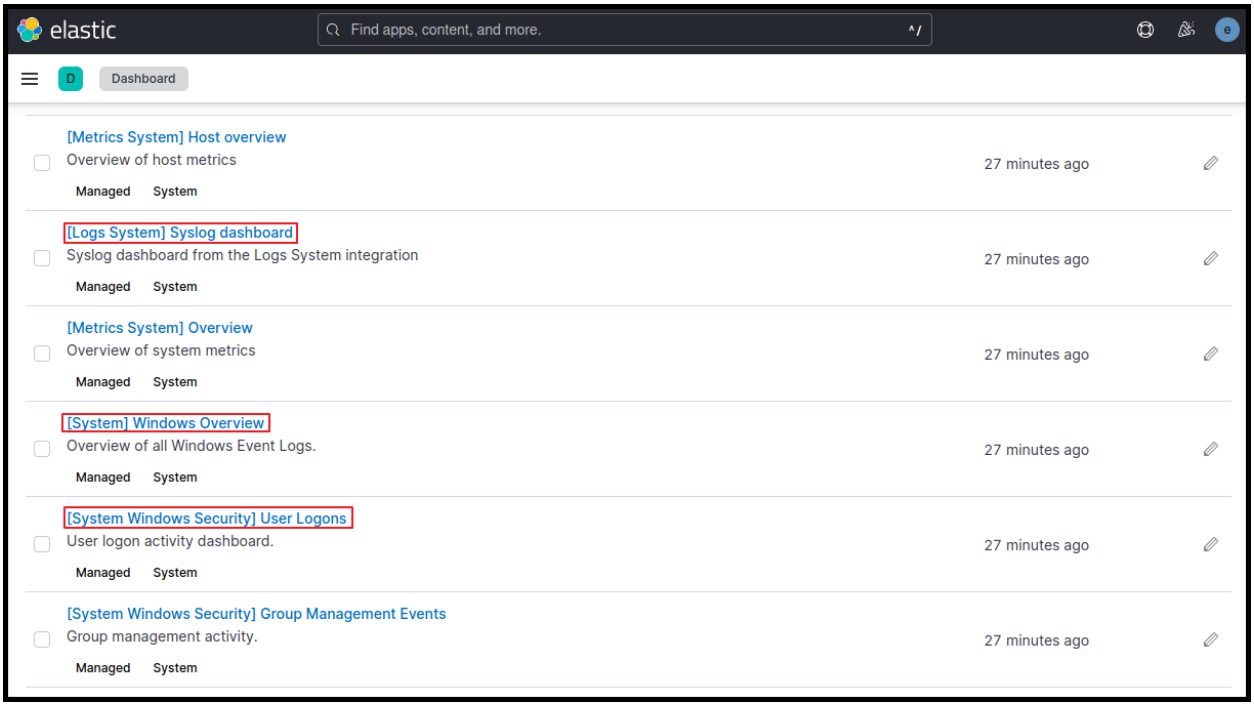
Checking Overviews to see all the logs in a General Dashboard: -

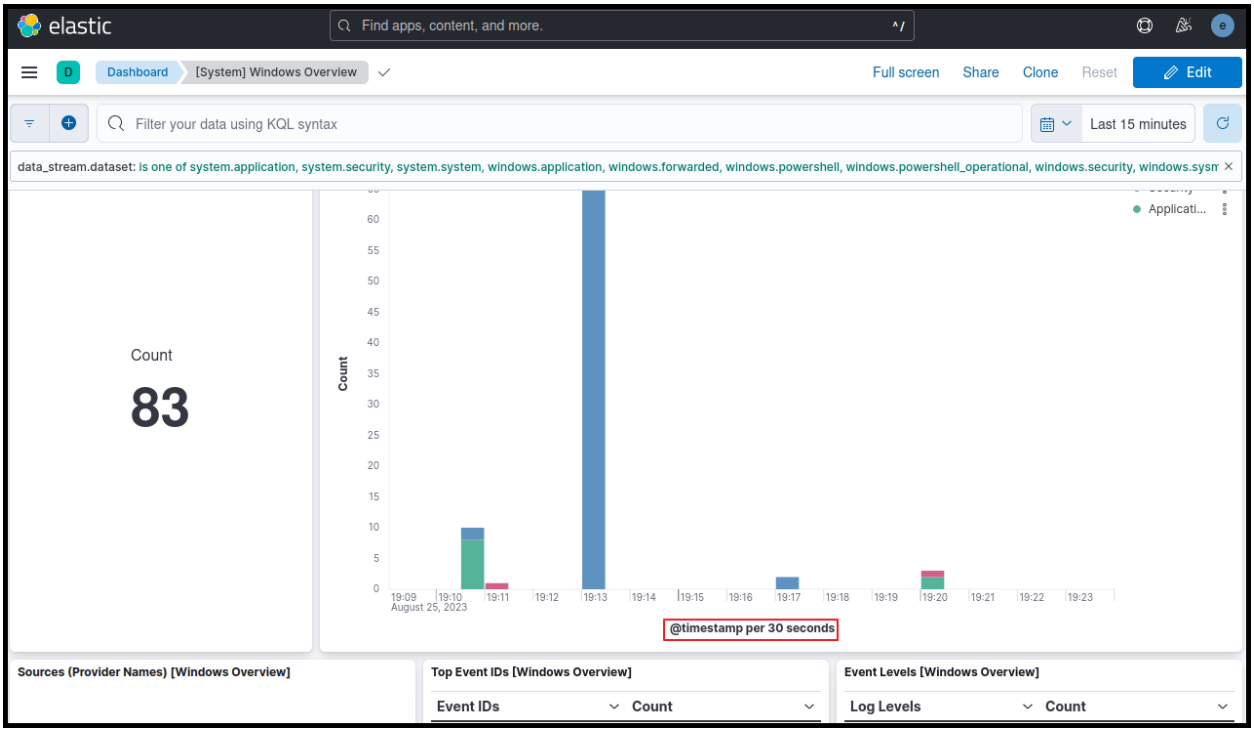


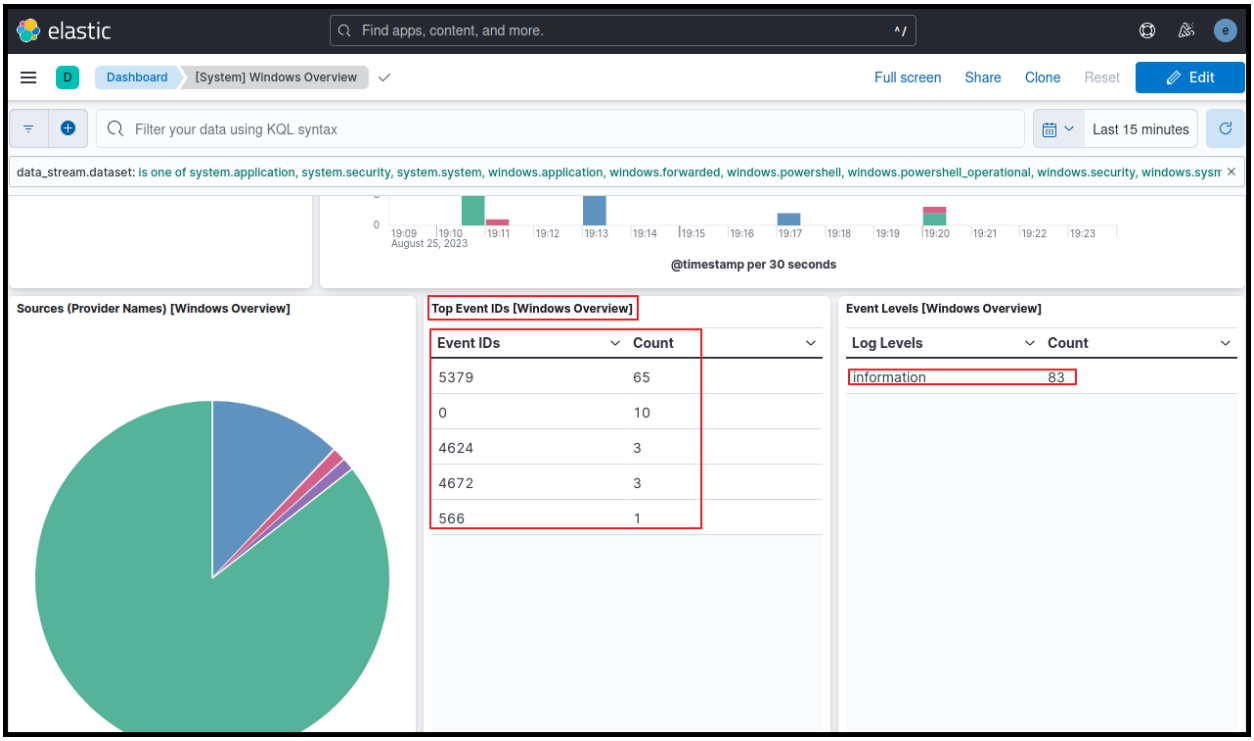


Creating our own custom Dashboards: -






elastic
Find apps, content, and more.
Dashboard
[System] Windows Overview
Full screen
Share
Clone
Reset
Edit
Filter your data using KQL syntax
Last 15 minutes
data_stream.dataset: is one of system.application, system.security, system.system, windows.application, windows.forwarded, windows.powershell, windows.powershell_operational, windows.security, windows.sysm
Count
83
Count
@timestamp per 30 seconds
Sources (Provider Names) [Windows Overview]
Top Event IDs [Windows Overview]
Event IDs
Count
Event Levels [Windows Overview]
Log Levels
Count


elastic
Find apps, content, and more.
Dashboard
[System] Windows Overview
Full screen
Share
Clone
Reset
Edit
Filter your data using KQL syntax
Last 15 minutes
data_stream.dataset: is one of system.application, system.security, system.system, windows.application, windows.forwarded, windows.powershell, windows.powershell_operational, windows.security, windows.sysm
@timestamp per 30 seconds
Sources (Provider Names) [Windows Overview]
Top Event IDs [Windows Overview]
Event IDs
Count
5379
65
0
10
4624
3
4672
3
566
1
Event Levels [Windows Overview]
Log Levels
Count
information
83

Running KQL Queries to filter Data: -