Sahil Borse - Sysmon Logs to Elastic-Search-ELK

Pushing Sysmon Logs to Elastic search and visualize them in Kibana

Monday, October 06, 2025 5:58 AM

Installing Elastic Search on Debian:
Link :
https://www.elastic.co/docs/deploy-manage/deploy/self-managed/install-elasticsearch-with-debian-package

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

Save the repository definition to /etc/apt/sources.list.d/elastic-9.x.list:
Command:

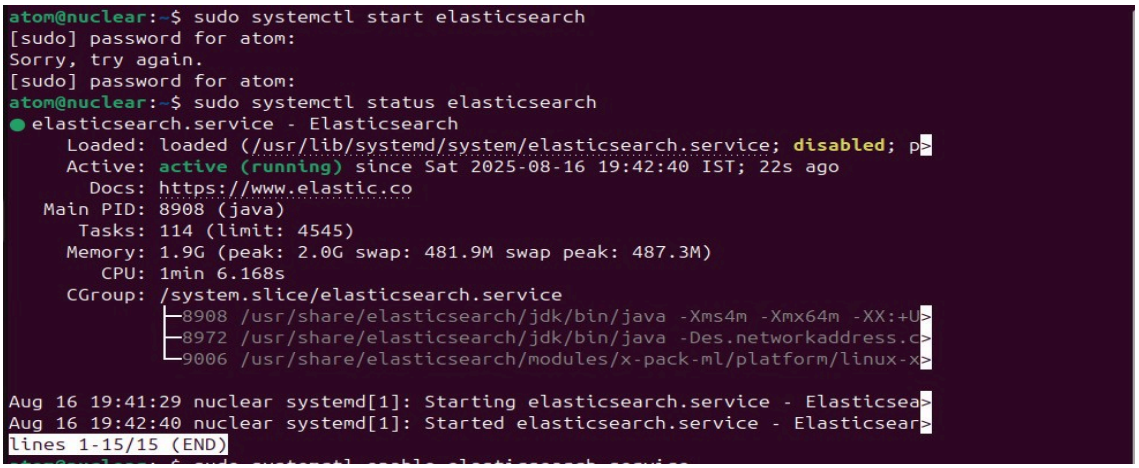
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/9.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-9.x.list

Elasticsearch Debian package intall:
Command:

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

Starting and Enabling Elastic search service:
Command:

sudo systemctl start elasticsearch
sudo systemctl enable elasticsearch.service



```
atom@nuclear:~$ sudo systemctl enable elasticsearch.service
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /usr/lib/syst
emd/system/elasticsearch.service.
```

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

```
atom@nuclear:~$ curl -X GET -k "https://elastic:YfuLpmsCVmIKOPsIRdFm@localhost:9200"
{
  "name" : "nuclear",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "CwKahkLTSPiFPnwQAAxpHw",
  "version" : {
    "number" : "9.1.2",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "ca1a70216fbdefbef3c65b1dff04903ea5964ef5",
    "build_date" : "2025-08-11T15:04:41.449624592Z",
    "build_snapshot" : false,
    "lucene_version" : "10.2.2",
    "minimum_wire_compatibility_version" : "8.19.0",
    "minimum_index_compatibility_version" : "8.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Installing Kibana:
Command:
sudo apt install kibana

```
atom@nuclear:~$ 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 4 not upgraded.
Need to get 362 MB of archives.
After this operation, 1,122 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/9.x/apt stable/main amd64 kibana amd64 9.1.2 [362 MB]
Fetched 362 MB in 2min 16s (2,657 kB/s)
Selecting previously unselected package kibana.
(Reading database ... 153751 files and directories currently installed.)
Preparing to unpack .../kibana_9.1.2_amd64.deb ...
Unpacking kibana (9.1.2) ...
Setting up kibana (9.1.2) ...
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

```
atom@nuclear:~$ sudo apt install logstash
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 4 not upgraded.
Need to get 428 MB of archives.
After this operation, 706 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/9.x/apt stable/main amd64 logstash amd64 1:9.1.2-1 [4
28 MB]
Fetched 428 MB in 1min 53s (3,777 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 265619 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a9.1.2-1_amd64.deb ...
Unpacking logstash (1:9.1.2-1) ...
```

```
Setting up logstash (1:9.1.2-1) ...
```

sudo systemctl start logstash.service
sudo systemctl enable logstash.service

```
atom@nuclear:~$ sudo systemctl start logstash.service
atom@nuclear:~$ sudo systemctl enable logstash.service
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /usr/lib/systemd/system/logstash.service.
```

Creating Enrollment tickets from elastic for kibana:
Command:
/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
(copy the generated token)

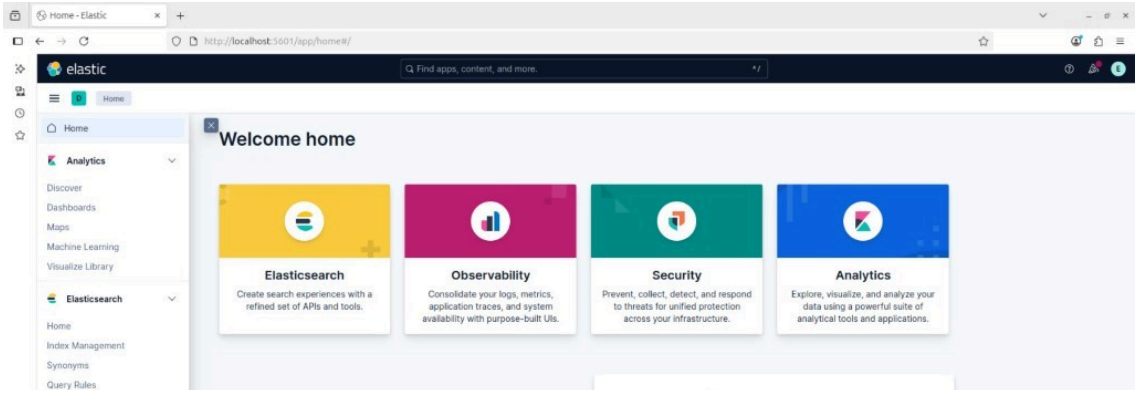
Setup of kibana from previously generated enrollment ticket:
Command:
/usr/share/kibana/bin/kibana-setup
<paste the token>

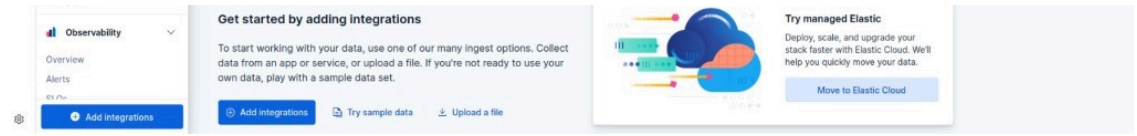
```
root@nuclear:/home/atom# /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiOlsiMTkyLjE2OC41OS4xMjk6OTIwMCJdLCJmZ3IiOiJjZWE5ZTQwZWQ3NjAyYjBiYjg0ZGJmODhhMGY2NjZhYWRjNzM1ZmRmNzg0NmQzODc2ZDZmNTgzOTNjNGI2OWY5Iiwia2V5IjoidmhaYXM1Z0I1eU84SVg4ZEF6NzU6NnlqTUJvSnkwa0FkbzF4WVQ2Z21FZyJ9
root@nuclear:/home/atom# /usr/share/kibana/bin/kibana-setup
Native global console methods have been overridden in production environment.
? Enter enrollment token: eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiOlsiMTkyLjE2OC41OS4xMjk6OTIwMCJdLCJmZ3IiOiJjZWE5ZTQwZWQ3NjAyYjBiYjg0ZGJmODhhMGY2NjZhYWRjNzM1ZmRmNzg0NmQzODc2ZDZmNTgzOTNjNGI2OWY5Iiwia2V5IjoidmhaYXM1Z0I1eU84SVg4ZEF6NzU6NnlqTUJvSnkwa0FkbzF4WVQ2Z21FZyJ9

✔ 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

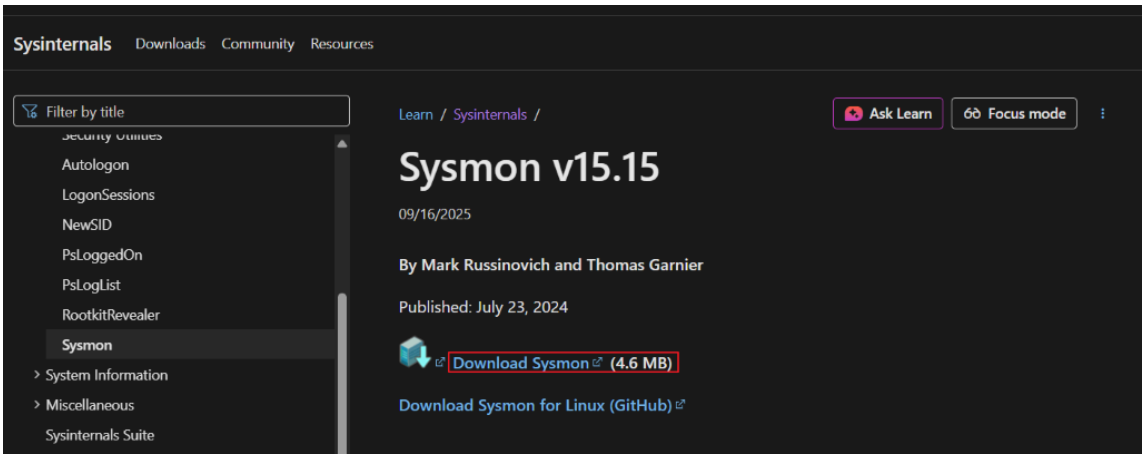
```
root@nuclear:/home/atom# sudo systemctl start kibana.service
root@nuclear:/home/atom# sudo systemctl enable kibana.service
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /usr/lib/systemd/system/kibana.service.
```

Accessing Kibana:
http://localhost:5601

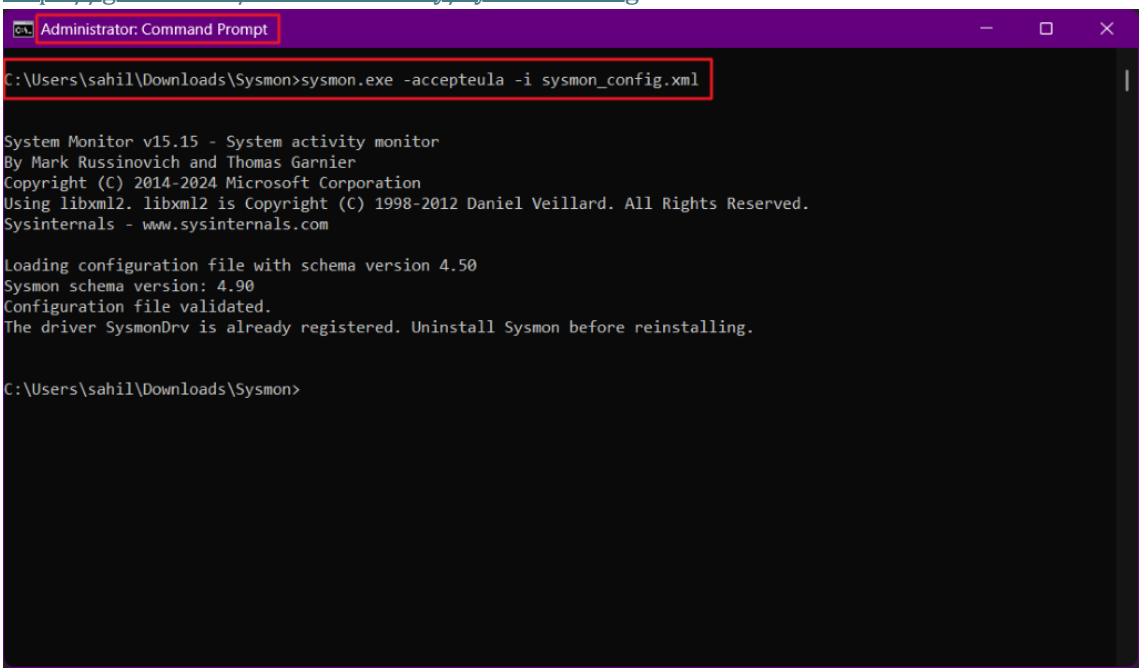




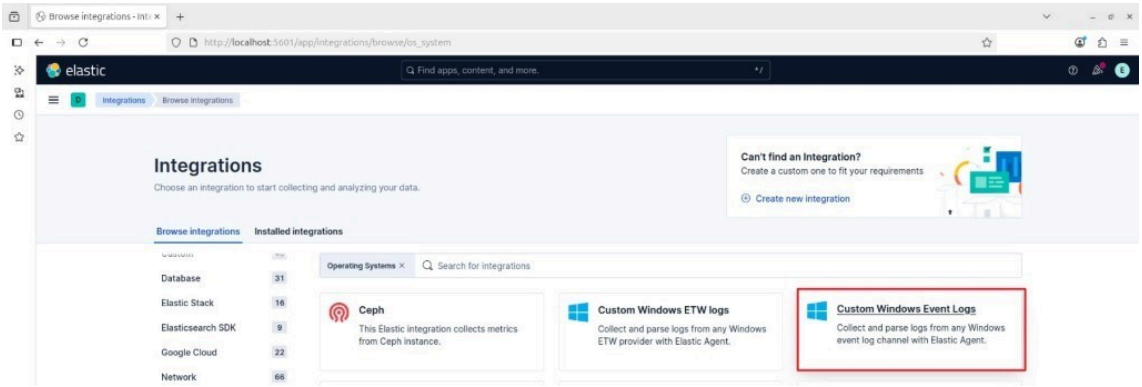
Download Sysmon on Windows:
https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon



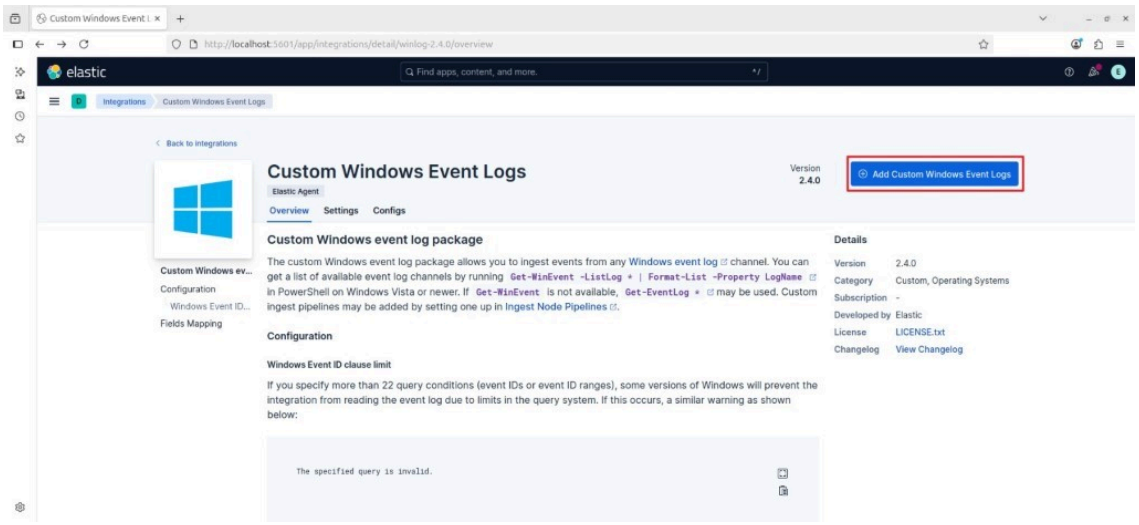
Downloading Sysmon configuration '.xml' file from GitHub:
https://github.com/SwiftOnSecurity/sysmon-config

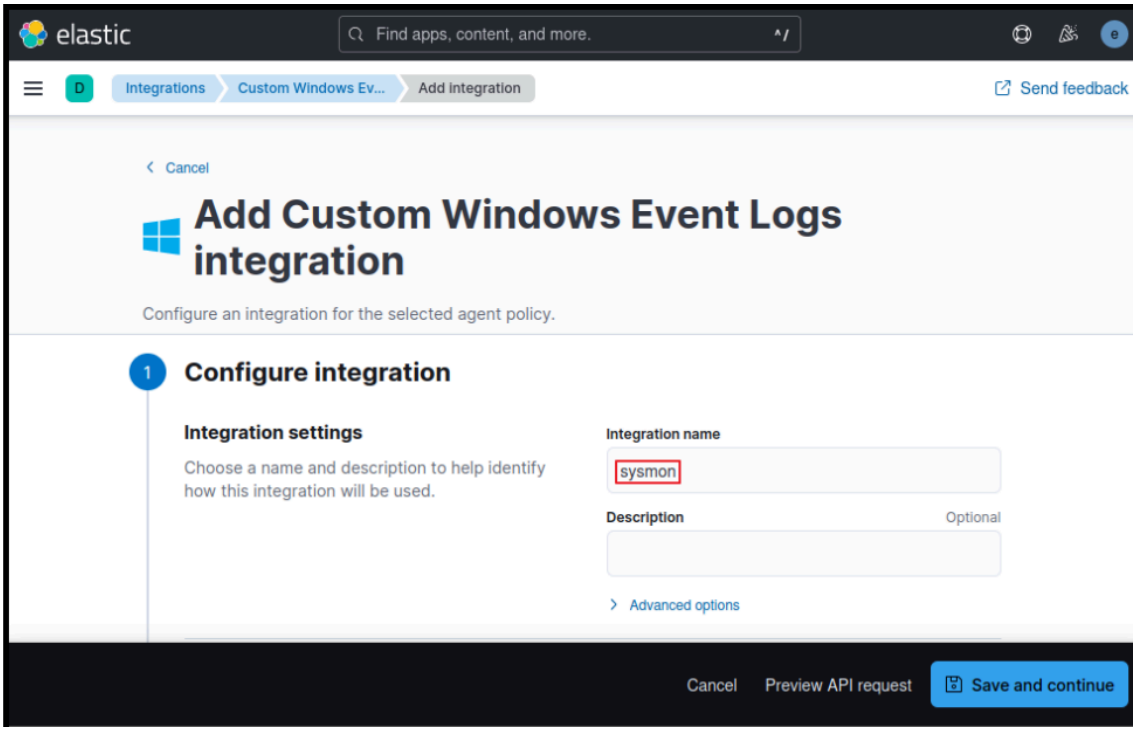


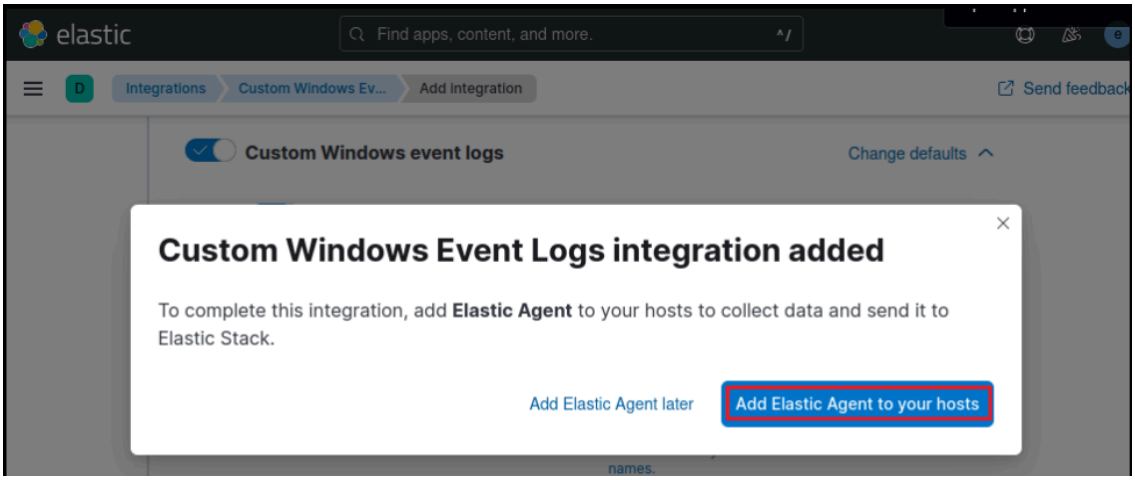
On kibana, navigating to integrations and installing Windows Custom Logs:

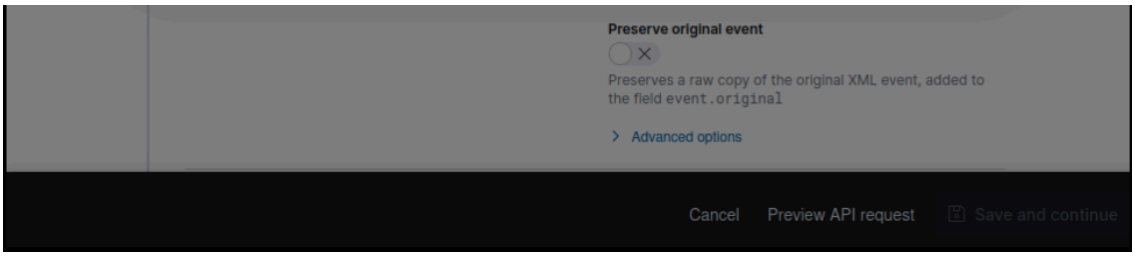


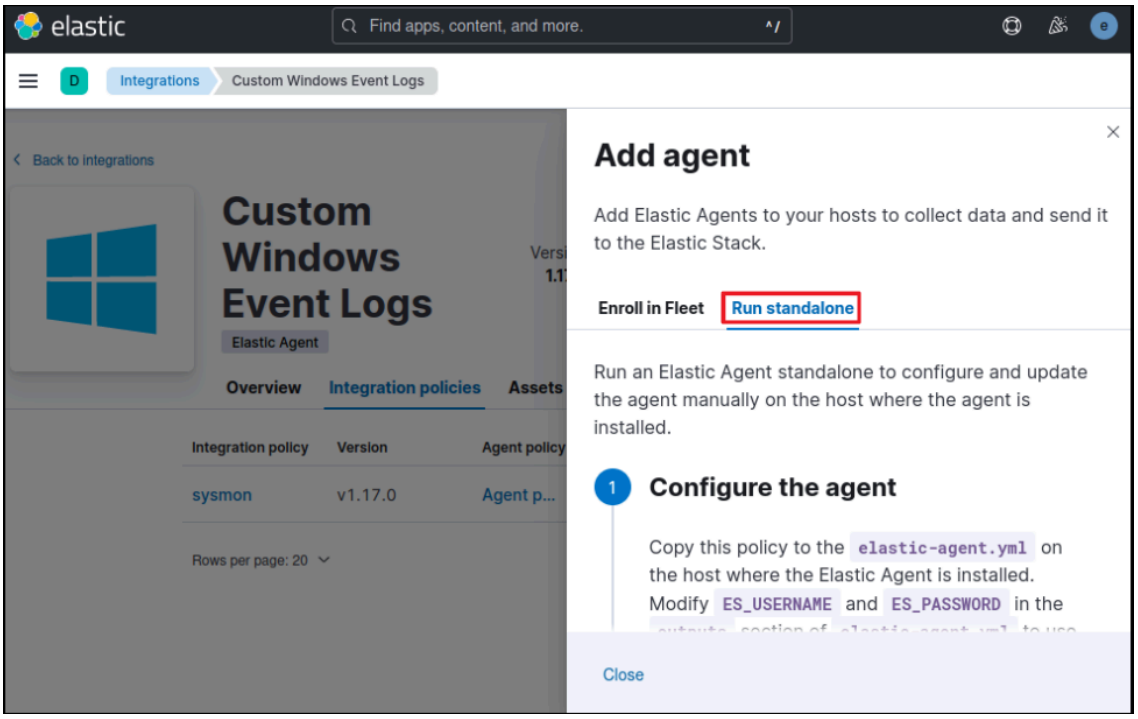

Observability 144
Operating Systems 7
Productivity 2
Elasticsearch 1
Security 234
Sysmon for Linux
Collect Sysmon Linux logs with Elastic Agent.
System
Collect system logs and metrics from your servers with Elastic Agent.
System Audit
Collect various logs & metrics from System Audit modules with Elastic Agent.
Windows
Collect logs and metrics from Windows OS and services with Elastic Agent.

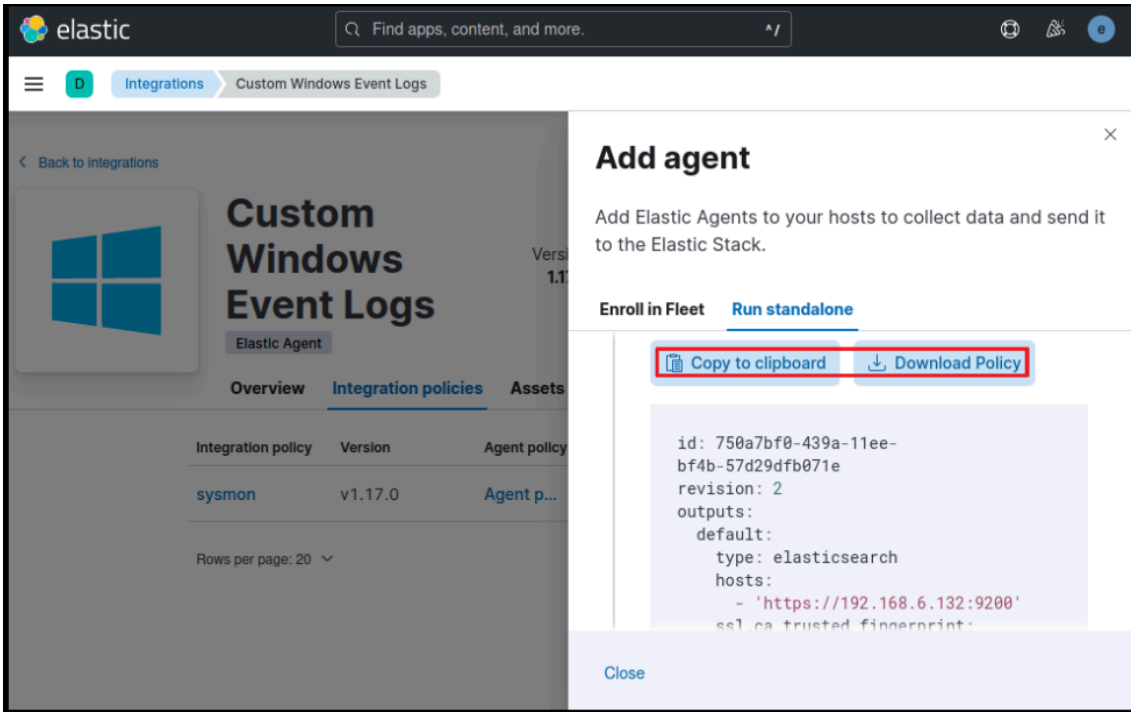

elastic
Integrations
Custom Windows Event Logs
Back to integrations
Custom Windows Event Logs
Elastic Agent
Overview
Settings
Configs
Version 2.4.0
Add Custom Windows Event Logs
Custom Windows event log package
The custom Windows event log package allows you to ingest events from any Windows event log 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
Windows Event ID clause limit
If you specify more than 22 query conditions (event IDs or event ID ranges), some versions of Windows will prevent the integration from reading the event log due to limits in the query system. If this occurs, a similar warning as shown below:
The specified query is invalid.
Details
Version 2.4.0
Category Custom, Operating Systems
Subscription -
Developed by Elastic
License LICENSE.txt
Changelog View Changelog
Custom Windows ev...
Configuration
Windows Event ID...
Fields Mapping


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
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.

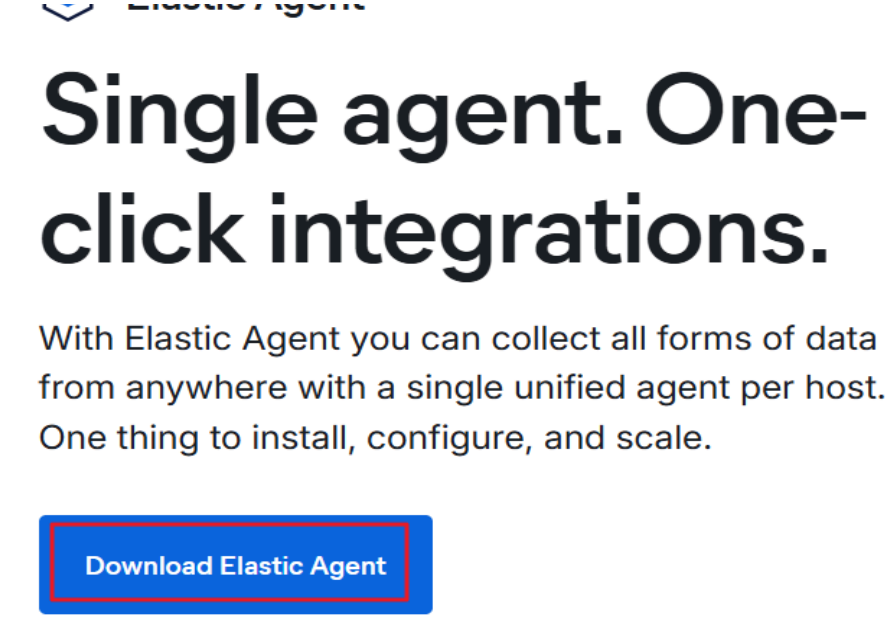






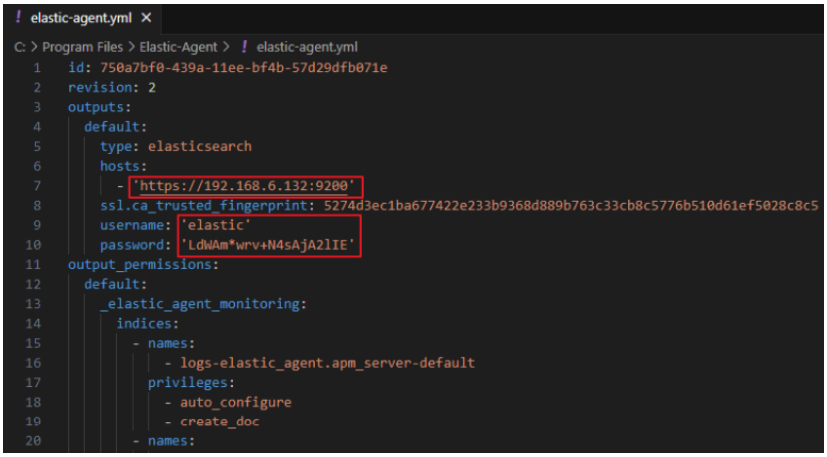
Downloading Elastic Agent on host machine:
https://www.elastic.co/elastic-agent

Elastic Agent

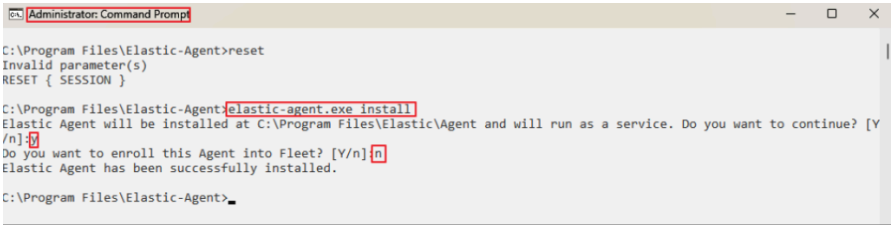


Configuring elastic-agent.yml file:

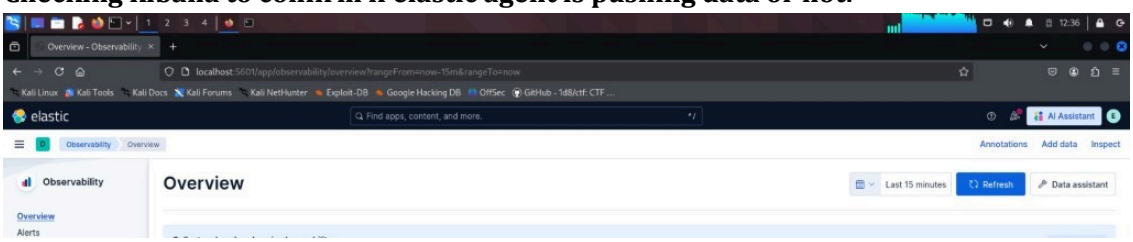
Enter the password used to log into kibana.

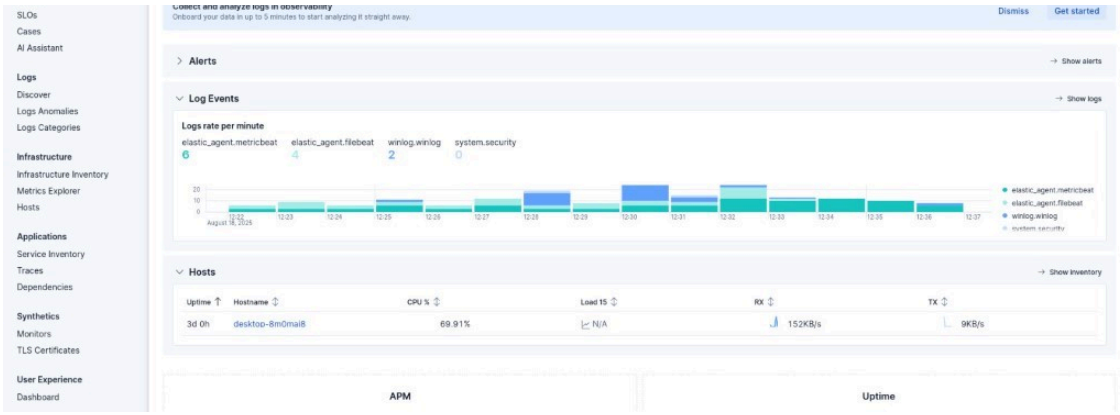


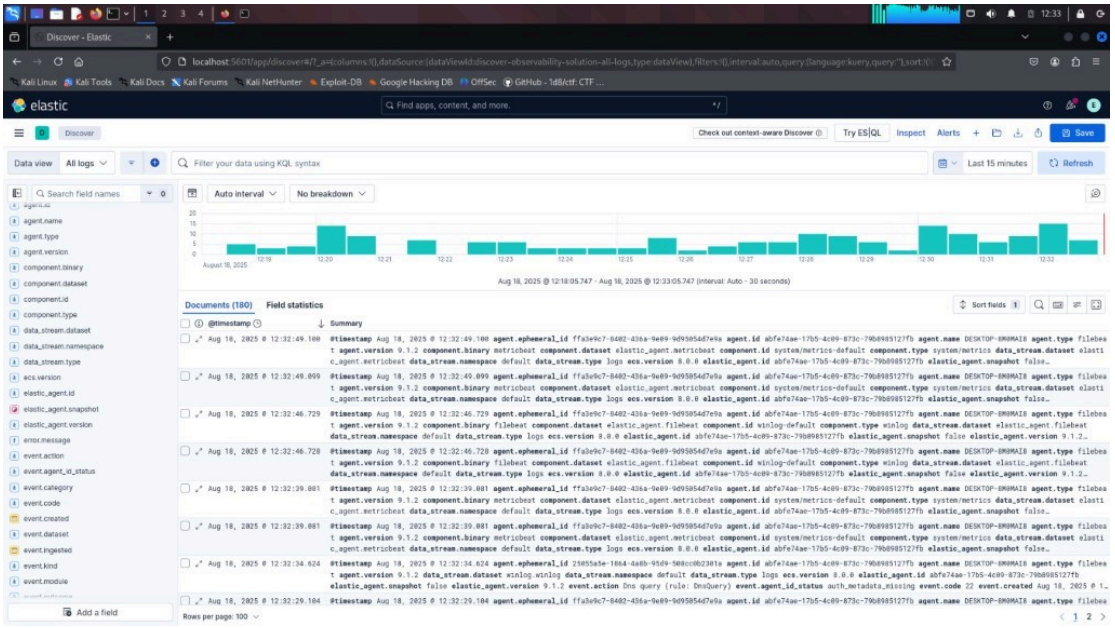
Installing configured elastic agent as service:
Command:
elastic-agent.exe install



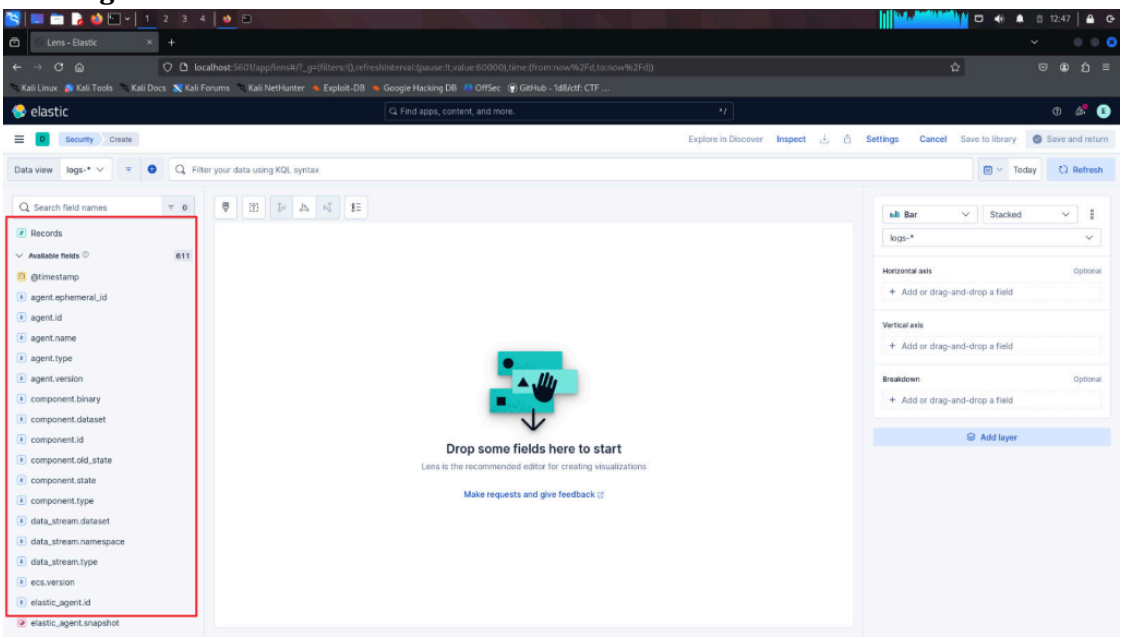
Checking kibana to confirm if elastic agent is pushing data or not:



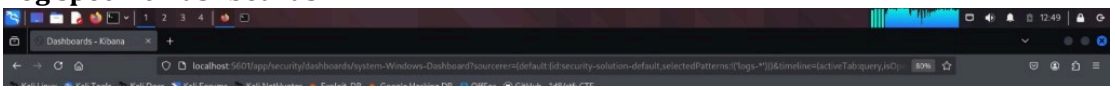


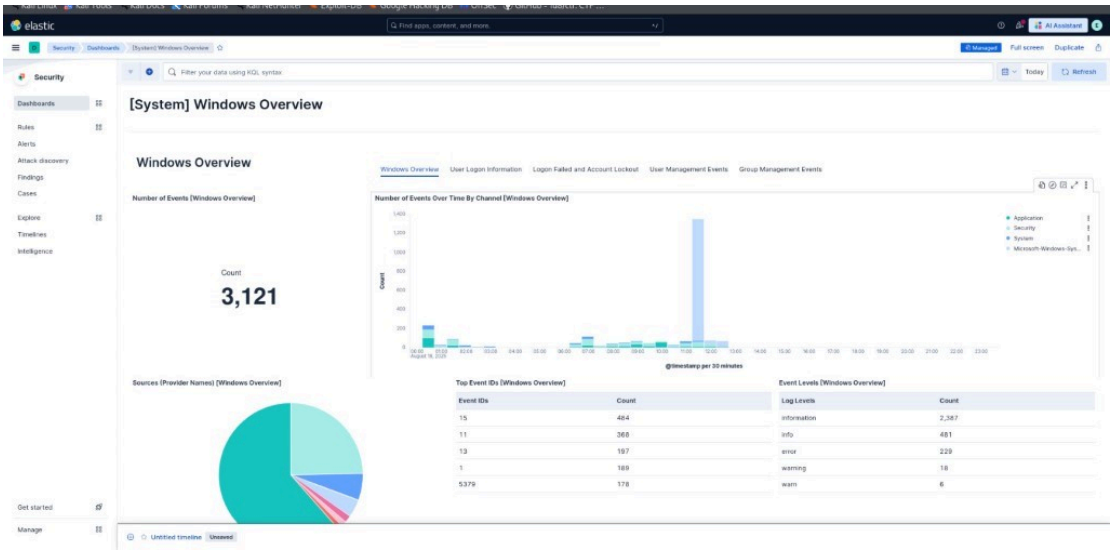


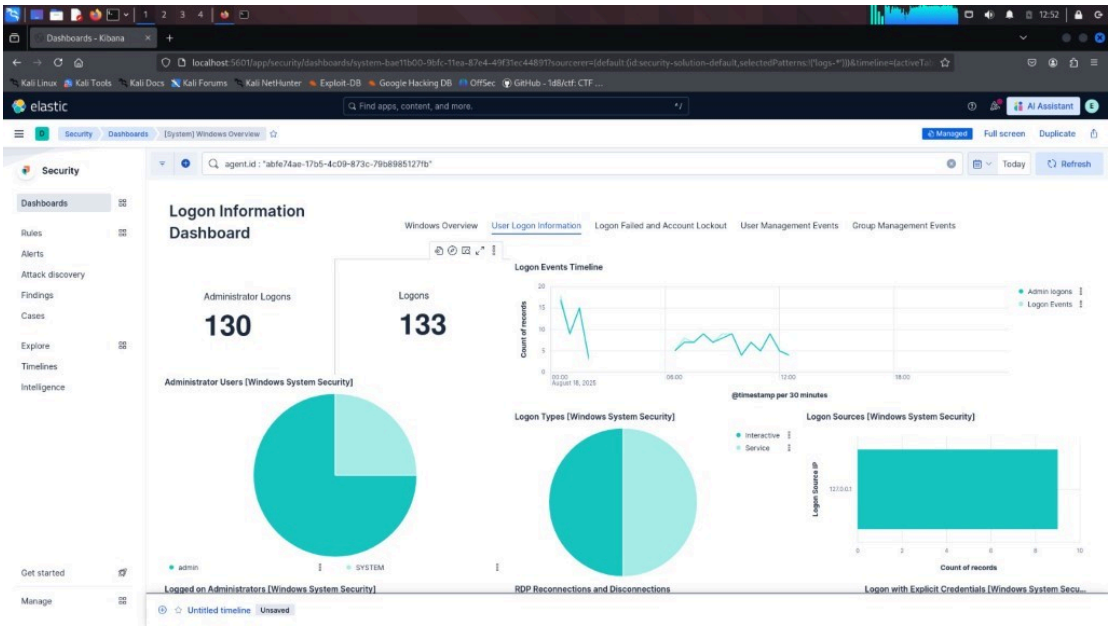
Creating custom Dashboards:



Log specific Dashboards:




elastic
Security
[System] Windows Overview
Windows Overview
Windows Overview
User Logon Information
Logon Failed and Account Lockout
User Management Events
Group Management Events
Number of Events [Windows Overview]
Count
3,121
Number of Events Over Time By Channel [Windows Overview]
@timestamp per 30 minutes
Sources (Provider Names) [Windows Overview]
Top Event IDs [Windows Overview]
Event IDs
Count
15
484
11
368
13
197
1
189
5379
178
Event Levels [Windows Overview]
Log Levels
Count
information
2,387
info
481
error
229
warning
18
warn
6


Dashboards - Kibana
elastic
Security
Dashboards
Logon Information Dashboard
Windows Overview
User Logon Information
Logon Failed and Account Lockout
User Management Events
Group Management Events
Administrator Logons
130
Logons
133
Logon Events Timeline
@timestamp per 30 minutes
Administrator Users [Windows System Security]
Logon Types [Windows System Security]
Logon Sources [Windows System Security]
Count of records
Logged on Administrators [Windows System Security]
RDP Reconnections and Disconnections
Logon with Explicit Credentials [Windows System Secu...
Untitled timeline
Unsaved