

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
```

```
(root@b0mb)-[/home/at0m]  
# 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
11 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 Packages [55.3 kB]
Get:4 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Contents (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 elasticsearch 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
```

```

GNU nano 7.2 /etc/elasticsearch/elasticsearch.yml
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ----- Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
#network.host: 192.168.0.1
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node starts

```

```

root@b0mb: /home/at0m
GNU nano 7.2 /etc/elasticsearch/elasticsearch.yml
xpack.security.enrollment.enabled: true
# Enable encryption for HTTP API client connections, such as Kibana, Logstash
xpack.security.http.ssl:
  enabled: true
  keystore.path: certs/http.p12
# Enable encryption and mutual authentication between cluster nodes
xpack.security.transport.ssl:
  enabled: true
  verification_mode: certificate
  keystore.path: certs/transport.p12
  truststore.path: certs/transport.p12
# Create a new cluster with the current node only
# Additional nodes can still join the cluster later
cluster.initial_master_nodes: ["b0mb"]
# Allow HTTP API connections from anywhere
# Connections are encrypted and require user authentication
http.host: 0.0.0.0
# Allow other nodes to join the cluster from anywhere

```

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.service → /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-frontent. It is
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontent. 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
eyJ2ZXIiOiI4LjguMiIsImFkciI6WyIxOTIuMTY4LjYuMTMyOjkyMDAiXSwiZmdyIjoIiNTI3NGQzZWMxYmE2Nzc0MjJlMjYjkzNjhkODg5Yjc2M2MzM2NiOGM1Nzc2YjUxMGQ2MWVmNTAyOGM4YzVlMiIsImtleSI6Ii1LSkdSb2tCa3BpTDZHCu9id0l30lQ1a3d5ZEtGUS02TVJyR3B6djZ3aHcifQ=
```

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: eyJ2ZXIiOiI4LjguMiIsImFkciI6WyIxOTIuMTY4LjYuMTMyOjkyMDAiXSwiZmdyIjoIOTI3NGQzZWxYmE2Nzc0MjJlMjZyYjZkZnJhKODg5Yjc2M2MzM2NiOGM1Nzc2YjUxMGQzMWVmNTAyOGM4YzVlMiIsImtleSI6Ii1xSkhSb2tCa3BpTDZhcU9DUUxxOlExNlRxUENIU1hTU1pEc014YjVNEEifQ==
configure this with
✓ Kibana configured successfully.
To start Kibana run:
bin/kibana
```

Starting and Enabling Kibana Service

Command: -

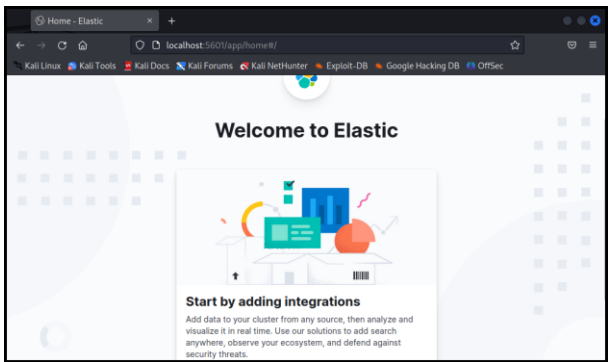
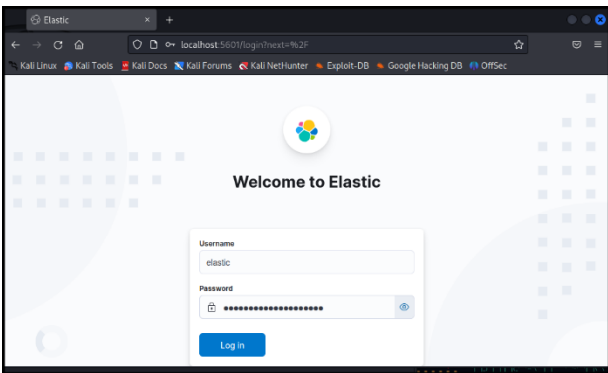
```
sudo systemctl start kibana.service
sudo systemctl enable kibana.service
```

```
(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>



The screenshot shows the top section of a web article for Sysmon v15.0. At the top, there is a breadcrumb trail: "Learn / Sysinternals / Downloads /". Below this is the title "Sysmon v15.0" in a large, bold font. Under the title, it says "Article • 04/11/2023 • 10 contributors". A section titled "In this article" lists several links: "Introduction", "Overview of Sysmon Capabilities", "Screenshots", "Usage", and "Show 5 more". Below this list, it says "By Mark Russinovich and Thomas Garnier". Further down, it says "Published: June 27, 2023". At the bottom of the section, there is a download button with a red box around it that says "Download Sysmon (4.6 MB)". Below the button, there is a link that says "Download Sysmon for Linux (GitHub)".

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](https://github.com/SwiftOnSecurity/sysmon-config)

Code: -

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

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22621.1848]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Sysmon

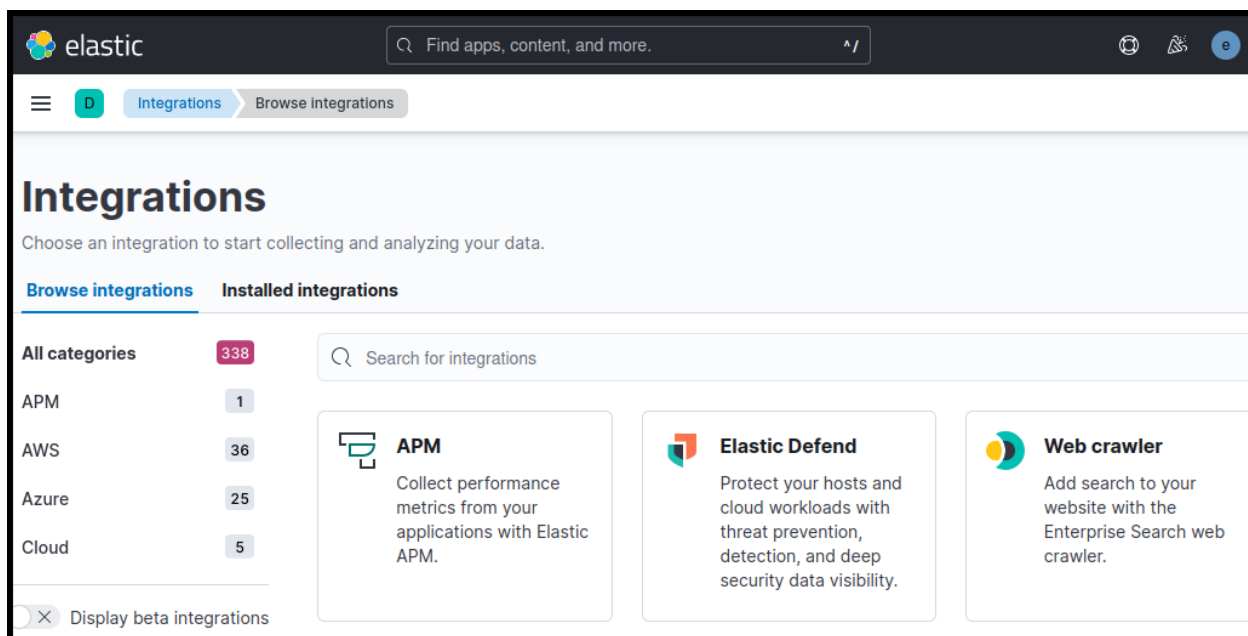
C:\Sysmon>sysmon.exe -accepteula -i sysmonconfig-export.xml

System Monitor v14.16 - 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

Loading configuration file with schema version 4.50
Sysmon schema version: 4.83
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.

C:\Sysmon>
```

Going to the Integrations and installing Windows Custom Logs: -



elastic

Find apps, content, and more.

Integrations

Browse Integrations

Elasticsearch SDK9

Enterprise Search36

Google Cloud19

Network52

Observability111

Operating Systems5

Productivity1

Security165

Operating Systems x

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.

Display beta integrations

an integration is available for Elastic Agent and Beats, show:

Recommended

Elastic Agent only

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
Channels	View Channels




Find apps, content, and more.



IntegrationsCustom 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

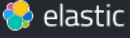
sysmon

DescriptionOptional




[Advanced options](#)

CancelPreview API request

Save and continue



Find apps, content, and more.



IntegrationsCustom 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

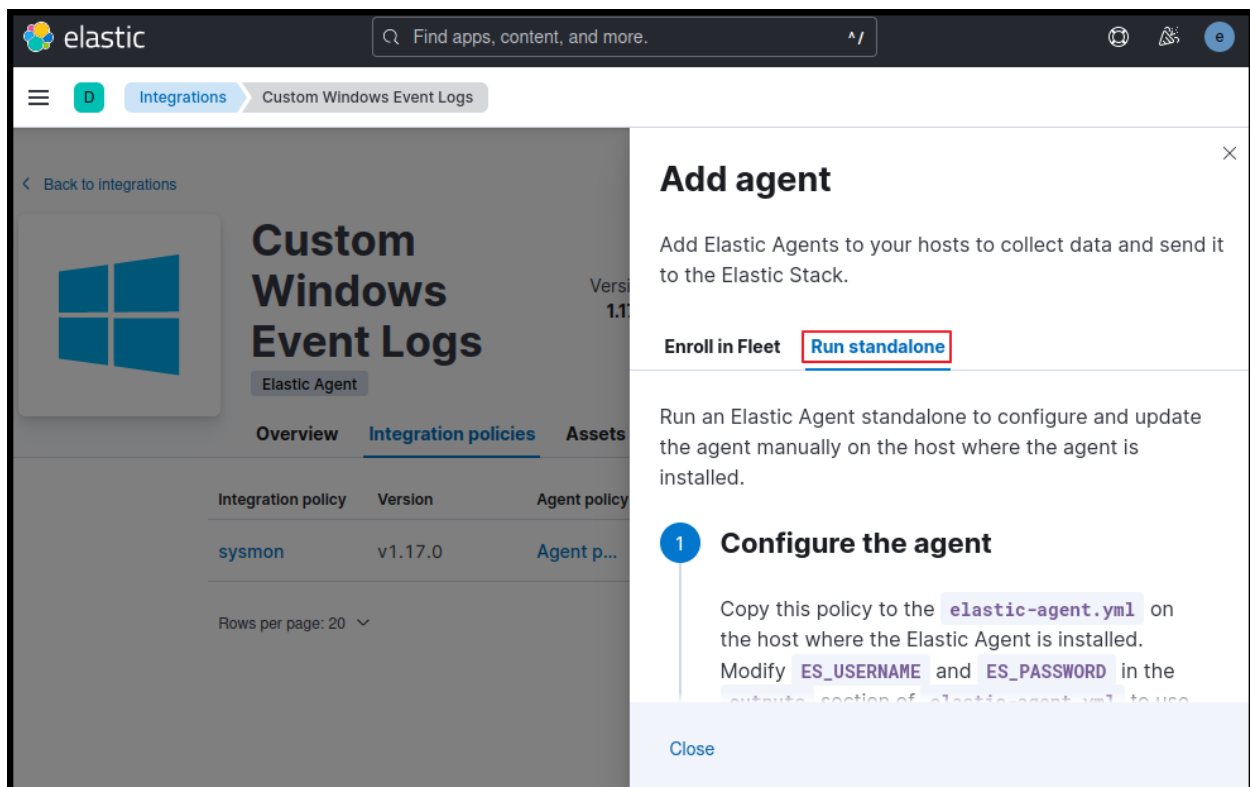
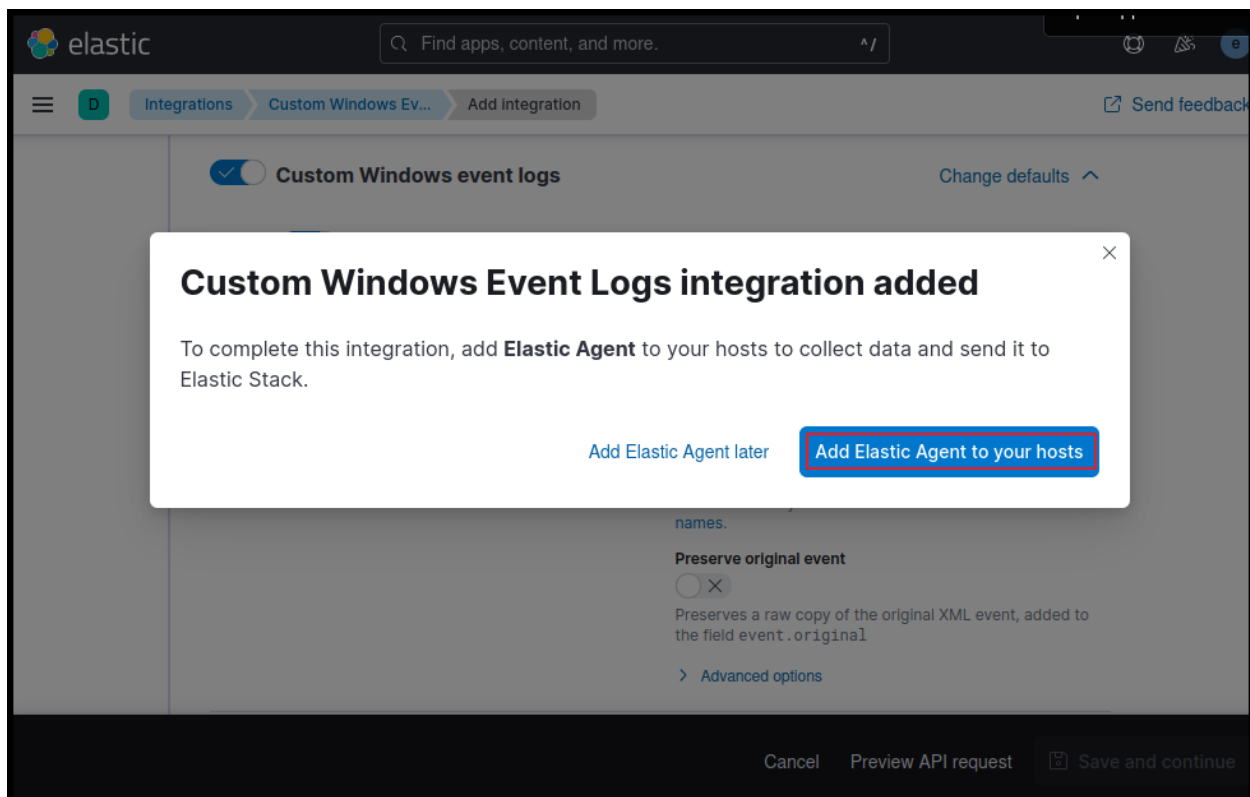
Agent policy 1

☒ Collect system logs and metrics ⓘ

[Advanced options](#)

CancelPreview API request

Save and continue



The screenshot shows the Elastic UI interface. On the left, a sidebar displays 'Custom Windows Event Logs' under 'Integrations'. The main panel shows the 'Add agent' modal. The modal has a title 'Add agent' and a description: 'Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.' Below the description, there are two tabs: 'Enroll in Fleet' and 'Run standalone'. The 'Run standalone' tab is selected. Under this tab, there are two buttons: 'Copy to clipboard' and 'Download Policy'. Below these buttons, a code block displays the following configuration:

```
id: 750a7bf0-439a-11ee-  
bf4b-57d29dfb071e  
revision: 2  
outputs:  
  default:  
    type: elasticsearch  
    hosts:  
      - 'https://192.168.6.132:9200'  
ssl.ca.trusted.fingerprint:
```

At the bottom of the modal, there is a 'Close' button.

Downloading Elastic Agent: -

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

The banner features the Elastic Agent logo at the top left. Below the logo, the text reads 'Single agent. One-click integrations.' followed by a paragraph: 'With Elastic Agent you can collect all forms of data from anywhere with a single unified agent per host. One thing to install, configure, and scale.' At the bottom, there is a blue button with the text 'Download Elastic Agent'.

Configuring Elastic Agent “elastic-agent.yml” file: -

```
! elastic-agent.yml X
C: > Program Files > Elastic-Agent > ! elastic-agent.yml
1 id: 750a7bf0-439a-11ee-bf4b-57d29dfb071e
2 revision: 2
3 outputs:
4   default:
5     type: elasticsearch
6     hosts:
7       - 'https://192.168.6.132:9200'
8     ssl.ca_trusted_fingerprint: 5274d3ec1ba677422e233b9368d889b763c33cb8c5776b510d61ef5028c8c5
9     username: 'elastic'
10    password: 'LdWAm*wrV+N4sAjA2lIE'
11  output_permissions:
12    default:
13      _elastic_agent_monitoring:
14        indices:
15          - names:
16              - logs-elastic_agent.apm_server-default
17            privileges:
18              - auto_configure
19              - create_doc
20          - names:
21              - metrics-elastic_agent.apm_server-default
22            privileges:
23              - auto_configure
24              - create_doc
25          - names:
26              - logs-elastic_agent.auditbeat-default
27            privileges:
28              - auto_configure
29              - create_doc
30          - names:
31              - metrics-elastic_agent.auditbeat-default
32            privileges:
33              - auto_configure
```

Installing configured Elastic-agent as an service: -

Command: -

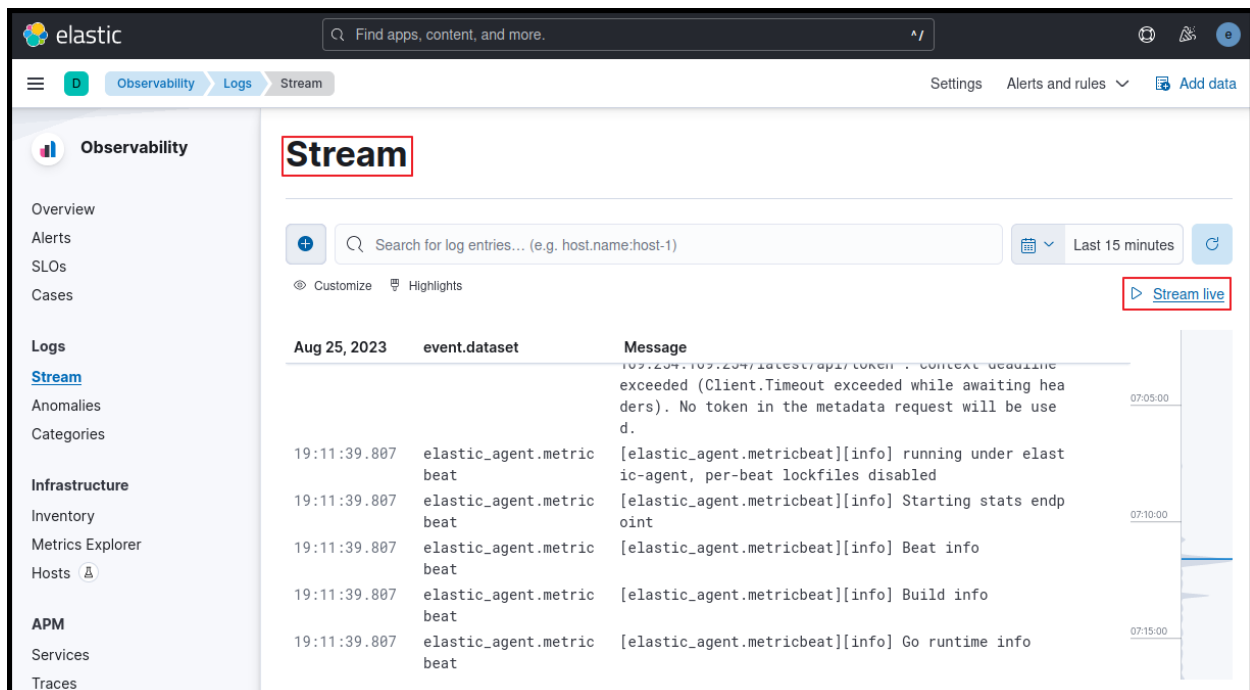
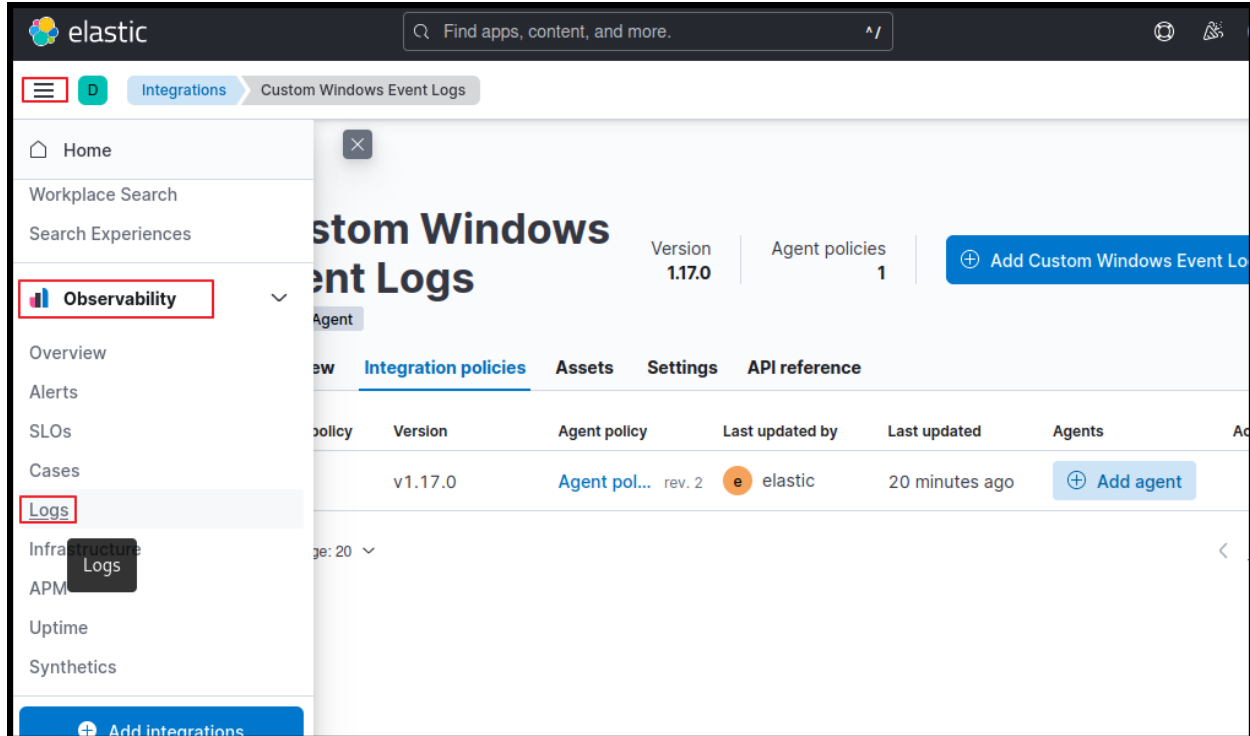
```
elastic-agent.exe install

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

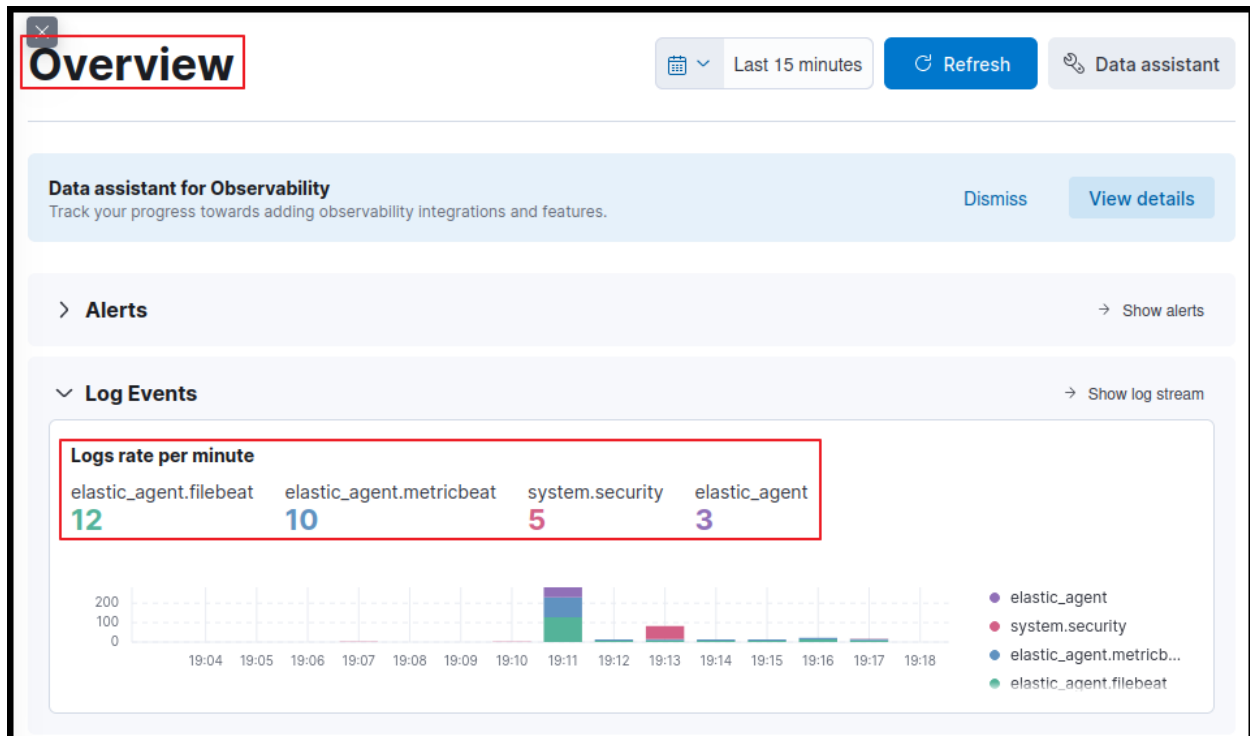
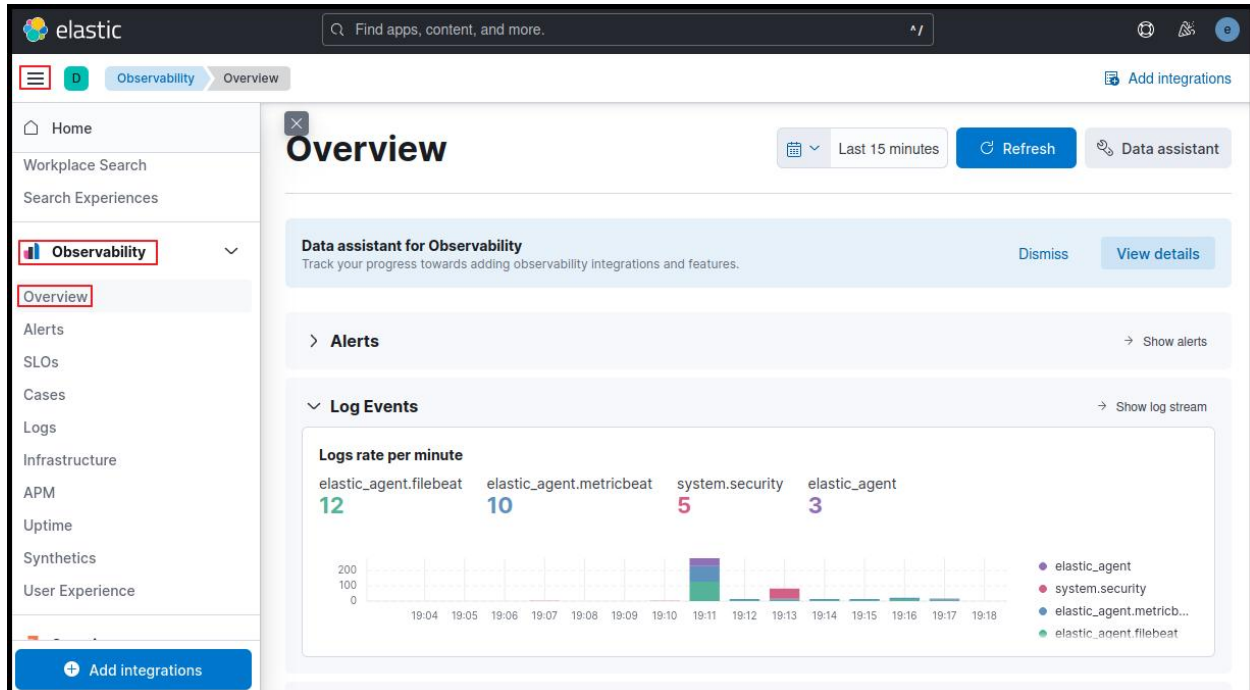
C:\Program Files\Elastic-Agent>elastic-agent.exe install
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]: Y
Do you want to enroll this Agent into Fleet? [Y/n]: n
Elastic Agent has been successfully installed.

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: -

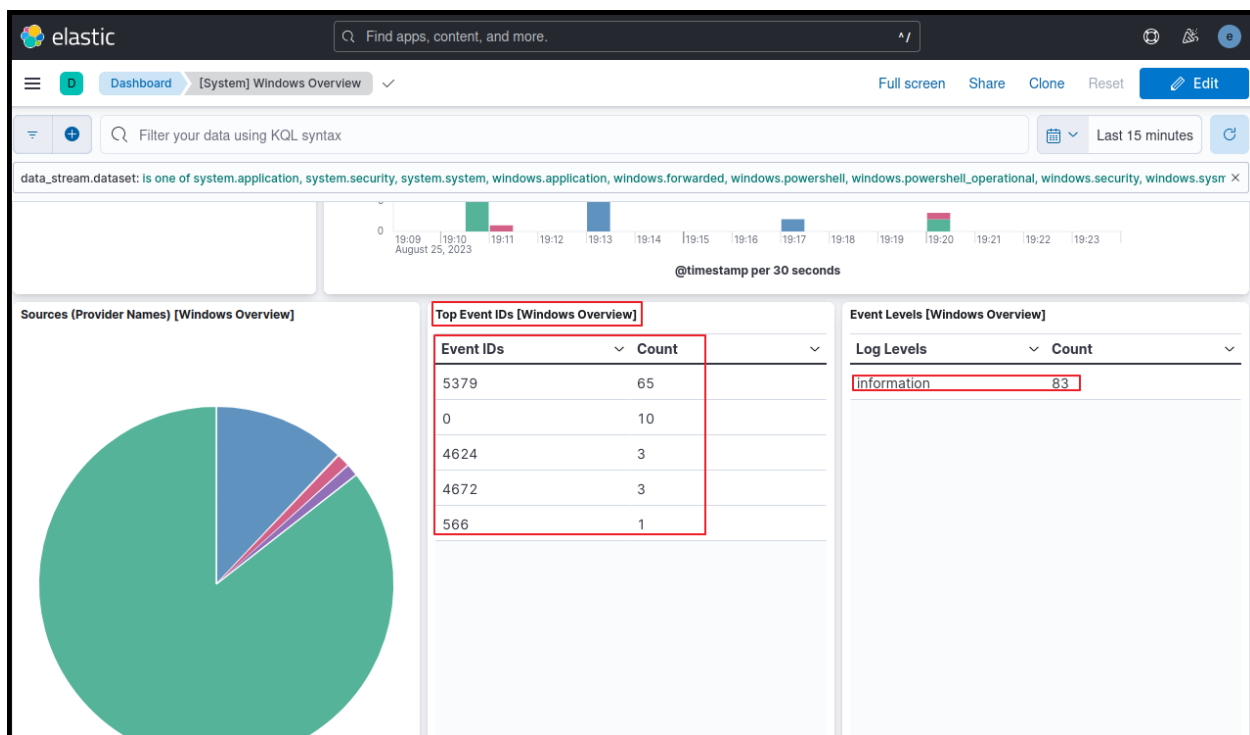
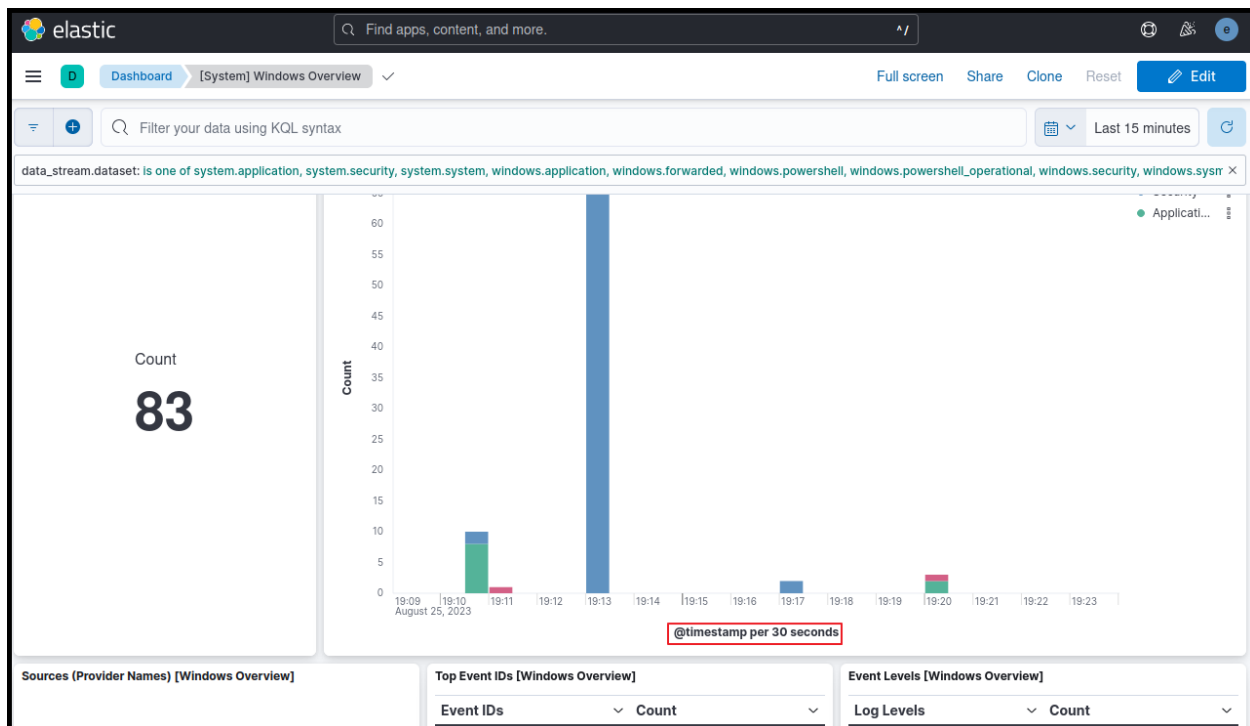


Creating our own custom Dashboards: -

This screenshot shows the Elastic dashboard creation interface. The top navigation bar includes the Elastic logo, a search bar, and a 'Create' button. Below the navigation bar, there's a 'logs-*' dropdown and a search bar for KQL syntax. The main area is divided into three sections: a left sidebar with 'Available fields' (426), a central visualization area with a 'Drop some fields here to start' message, and a right sidebar with configuration options for the 'Bar vertical stacked' chart. The 'Available fields' list includes fields like @timestamp, agent.build.original, agent.ephemeral_id, agent.id, agent.name, agent.type, agent.version, cloud.account.id, cloud.availability_zone, cloud.image.id, cloud.instance.id, and cloud.instance.name. The right sidebar has sections for 'Horizontal axis', 'Vertical axis', and 'Breakdown', each with an 'Add or drag-and-drop a field' button. The 'Add layer' button is at the bottom of the right sidebar.

This screenshot shows the Elastic dashboard list. The top navigation bar includes the Elastic logo, a search bar, and a 'Dashboard' button. Below the navigation bar, there's a list of dashboards. The list includes:

- [Metrics System] Host overview**
 - Overview of host metrics (27 minutes ago)
 - Managed System
- [Logs System] Syslog dashboard**
 - Syslog dashboard from the Logs System integration (27 minutes ago)
 - Managed System
- [Metrics System] Overview**
 - Overview of system metrics (27 minutes ago)
 - Managed System
- [System] Windows Overview**
 - Overview of all Windows Event Logs. (27 minutes ago)
 - Managed System
- [System Windows Security] User Logons**
 - User logon activity dashboard. (27 minutes ago)
 - Managed System
- [System Windows Security] Group Management Events**
 - Group management activity. (27 minutes ago)
 - Managed System



Running KQL Queries to filter Data: -

