

OBJECTIVE IS TO SETUP LOGGING ON ELASTIC.

ASSIGNMENT TASK FOR SOC

Presented By
Anveeksh Mahesh Rao

Table of Contents

01

Elastic. & WinLogBeat

02

Installing and Configuring

03

Working on
Elastic

Elastic

Elastic NV, a business that delivers open source solutions for search, logging, analytics, and security use cases, offers a cloud-based software as a service (SaaS) platform called Cloud.elastic.co. Users may utilise the platform to deploy and administer Elasticsearch, Kibana, Logstash, and other Elastic Stack components on the cloud. Users may select from a variety of deployment options, such as managed Elasticsearch clusters, Kibana instances, and other Elastic Stack components.

Cloud.elastic.co also provides a number of tools and features, such as automated scaling, data backups, security controls, and interaction with other services. Users may use the platform's dashboard and visualisation tools to monitor and analyse their data in real time, as well as set up alerts and notifications to get data changes.

Overall, cloud.elastic.co delivers an easy-to-use and scalable solution for organisations and enterprises that require sophisticated cloud search, logging, analytics, and security capabilities.

WinLogBeat

Elastic NV, the same business that delivers the Elastic Stack, which comprises Elasticsearch, Kibana, Logstash, and Beats, provides WinLogBeat, an open-source data shipper. WinLogBeat is a Windows-specific application that collects and forwards event log data to a centralised place for analysis, visualisation, and monitoring.

WinLogBeat may be set to gather logs from a variety of Windows operating system sources, including application logs, system logs, and security logs. The gathered logs can then be sent to a user-specified destination, such as an Elasticsearch cluster or Logstash, for additional processing and analysis.

WinLogBeat is very customizable, and users may tailor the configuration file to their unique requirements. It may be implemented as a service, making it simple to start and stop data shipping as needed. WinLogBeat is lightweight, efficient, and designed to have a minimal impact on system resources, making it appropriate for usage in production applications.

Overall, WinLogBeat is a valuable tool for organisations that require event log data from Windows systems to be collected and analysed. Users may receive significant insights into system performance, security, and other vital parameters by centralising logs.

Installing and Configuring

let's create an account in cloud.elastic.co

- First open the link [https://cloud.elastic.co/login?](https://cloud.elastic.co/login?redirectTo=%2Fhome)
Now create a account using yo ur google account
- [redirectTo=%2Fhome](https://cloud.elastic.co/login?redirectTo=%2Fhome)
- Now fill the details clearly

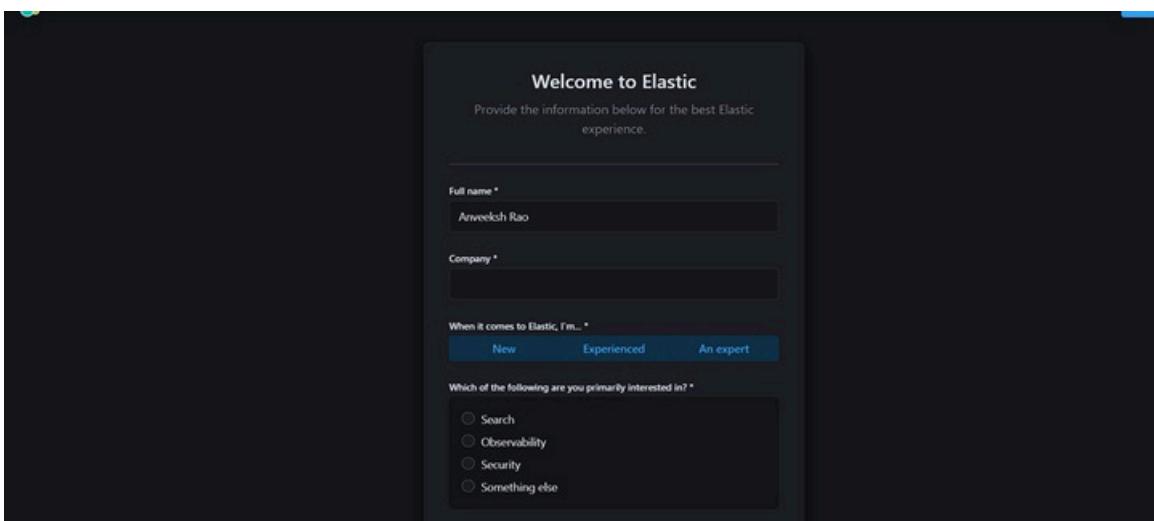


Fig 1

- Now create a first deployment ,let me give a name test and create deployment

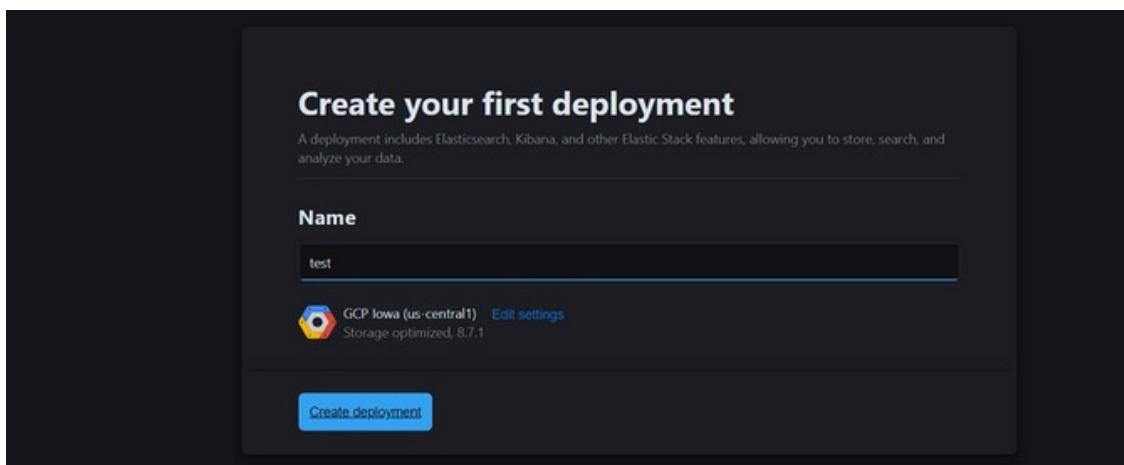
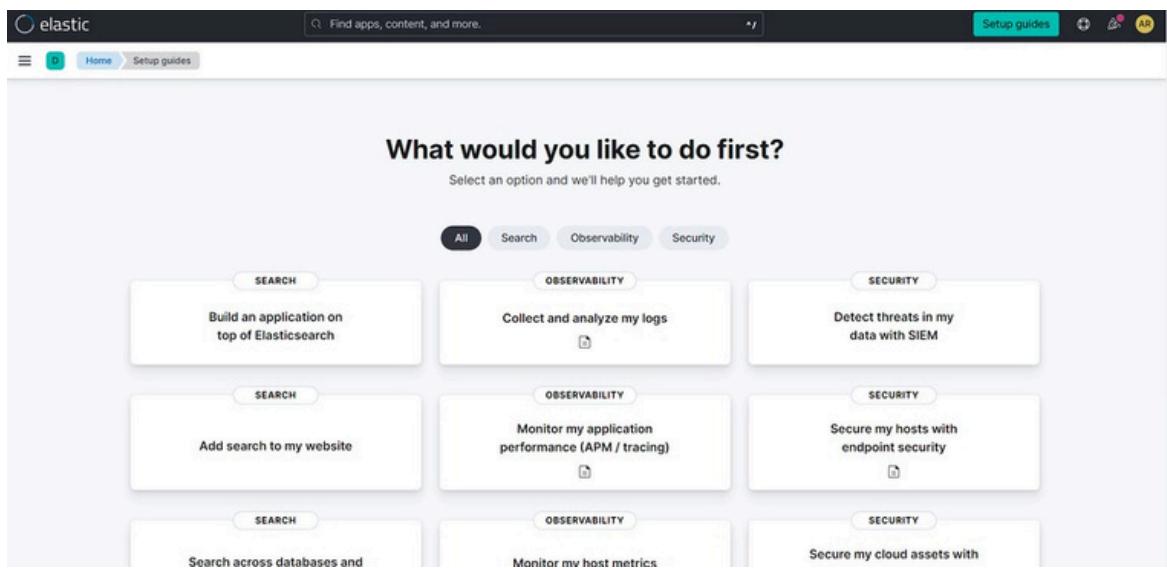


Fig 2

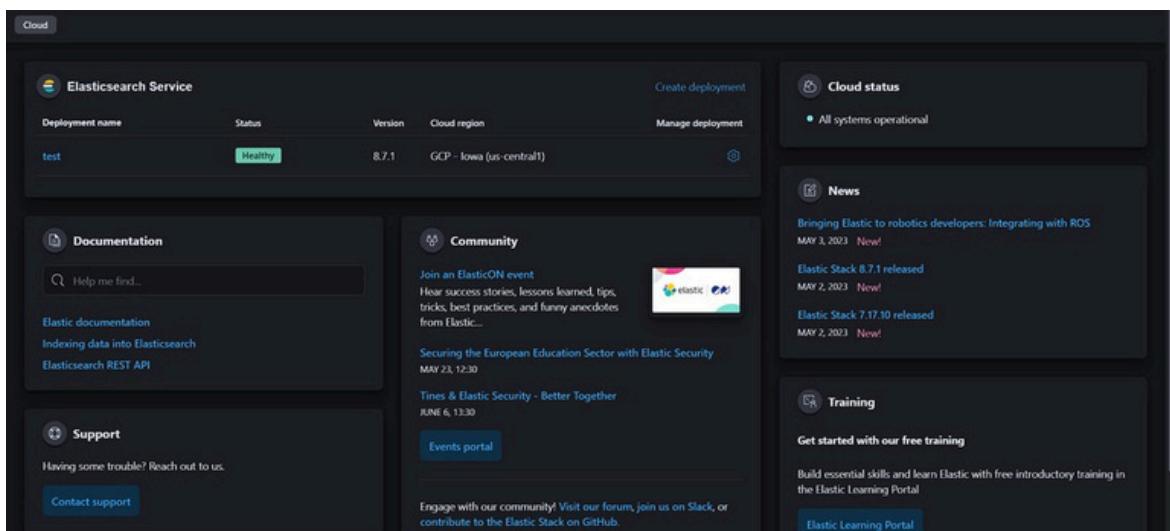
SET UP YOUR PROFILE



- you will see above interface in your system , now go to **profile** right corner of your interface, and click on **Edit Profile**



- Now click on **Cloud** now you can see below type of interface and click on button on Elasticsearch Service

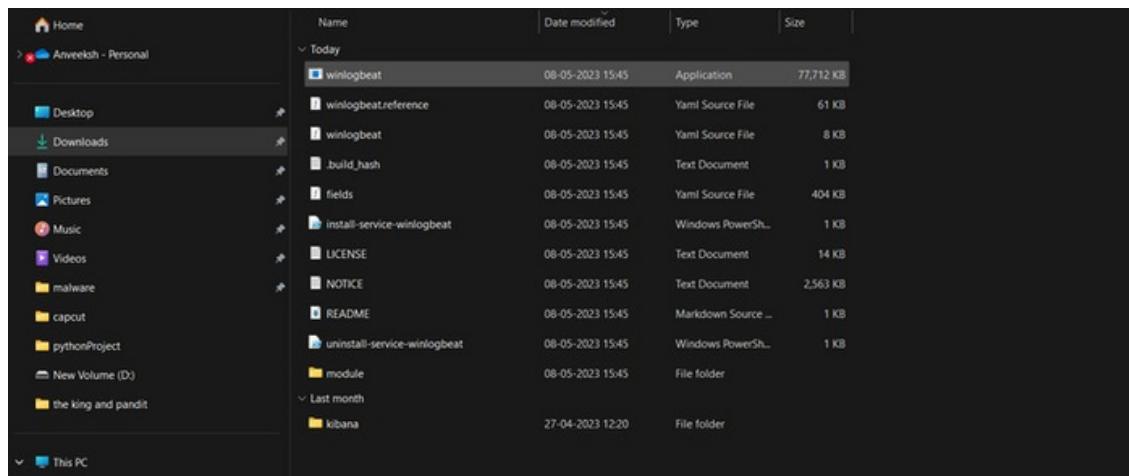


INSTALLING WINLOGBEAT & CONFIGURING

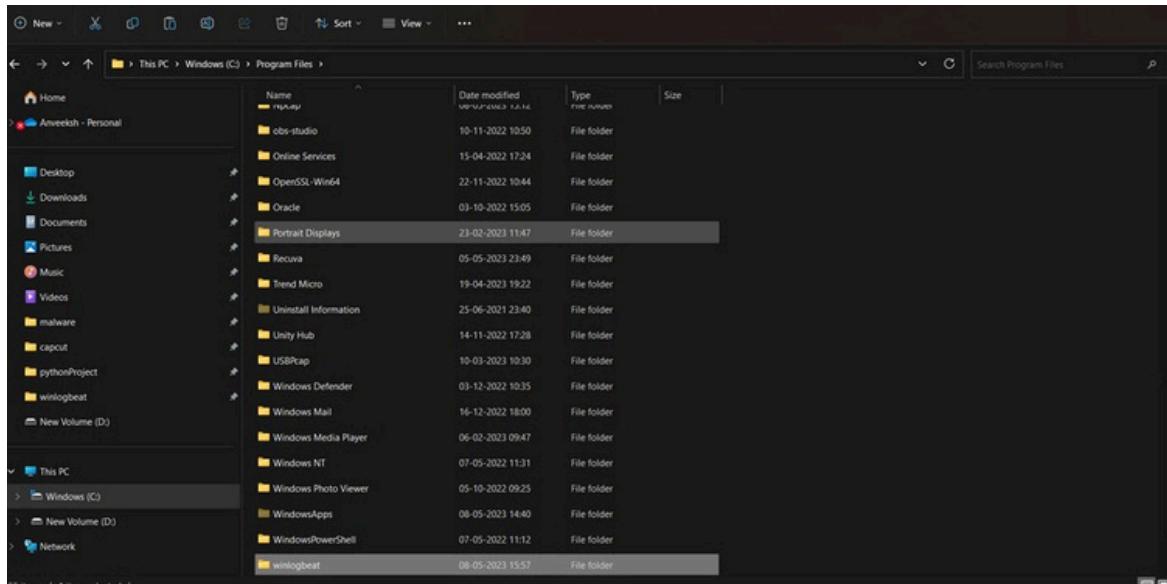
- Now go to new tab and install winlogbeat

The screenshot shows the GitHub release page for Winlogbeat version 8.7.1. It includes a summary box with version information, release date (May 02, 2023), and supported OS/JVM/Browser. Below the summary are three numbered steps: 1. Download and unzip Winlogbeat, 2. Edit the winlogbeat.yml configuration file, and 3. Run in PowerShell. Step 1 has a dropdown for 'Choose platform' set to 'Windows ZIP x86_64' and a download button for 'Windows ZIP x86_64'. Step 3 includes a command: 'Run winlogbeat.exe -c winlogbeat.yml'.

- Once installed extract it and then modify it
- Now modify the Winlogbeat yml file with your elastic configuration



- Before that copy the winlogbeat file to c drive in program file



- Now open the Powershell and verify weather file is uploaded or not

```
Administrator: Windows PowerShell
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 ..
PS C:\WINDOWS> cd ..
PS C:\> cd '\Program Files\winlogbeat\'
```

A screenshot of a Windows PowerShell window titled 'Administrator: Windows PowerShell'. The window shows a command history. The user has navigated from the system32 directory up to the root directory (C:\) and then into the 'winlogbeat' folder located in the 'Program Files' directory.

- Now use the guide and start doing configuration
- link is below

The image shows a screenshot of a web page from the Elastic website. On the left, there is a large 'ela' logo. To the right of the logo, the text 'Winlogbeat quick start: installation and configuration | Winlogbeat...' is displayed in bold black font. Below this text is the Elastic logo, which consists of a colorful hexagonal icon followed by the word 'Elastic'.

- once all setup is done in Command format type **service.msc**

- The below type of interface will open , later search for winlogbeat and start it

Service Name	Description	Status	Startup Type	Log On As
Windows Event Log	This service ...	Running	Automatic	Local Service
Windows Font Cache Service	Optimizes per...	Running	Automatic	Local Service
Windows Image Acquisition	Provides ima...	Running	Automatic (Trig...	Local Service
Windows Insider Service	Provides info...	Manual (Trigg...	Local System	
Windows Installer	Adds, modifi...	Manual	Local System	
Windows License Manager S...	Provides info...	Running	Manual (Trigg...	Local Service
Windows Management Inst...	Provides a cl...	Running	Automatic	Local System
Windows Management Servi...	Performs ma...	Manual	Local System	
Windows Media Player Netw...	Shares Wind...	Manual	Network Se...	
Windows Mixed Reality Opt...	Enables Mix...	Manual	Local System	
Windows Mobile Hotspot Se...	Provides the...	Manual (Trigg...	Local Service	
Windows Modules Installer	Enables inst...	Manual	Local System	
Windows Perception Service	Enables spat...	Manual (Trigg...	Local Service	
Windows Perception Simulator	Enables spat...	Manual	Local System	
Windows Push Notifications	This service r...	Running	Automatic	Local System
Windows Push Notifications	This service r...	Running	Automatic	Local System
Windows PushReinstall Servi...	Provides info...	Manual (Trigg...	Local System	
Windows Remote Management	Windows Re...	Manual	Network Se...	
Windows Search	Provides con...	Disabled	Local System	
Windows Security Service	Windows Se...	Running	Manual	Local System
Windows Time	Maintains da...	Manual (Trigg...	Local Service	
Windows Update	Enables the ...	Manual (Trigg...	Local System	
WinHTTP Web Proxy Auto-D...	WinHTTP im...	Running	Manual	Local Service
winlogbeat		Running	Automatic (De...	Local System
Wired AutoConfig	The Wired A...	Manual	Local System	
WLAN AutoConfig	The WLAN...	Running	Automatic	Local System
WMI Performance Adapter	Provides per...	Manual	Local System	
Work Folders	This service ...	Manual	Local Service	
Workstation	Creates and ...	Running	Automatic	Network Se...
WWAN AutoConfig	This service ...	Manual	Local System	
Xbox Accessory Management	This service ...	Manual (Trigg...	Local System	
Xbox Live Auth Manager	Provides aut...	Running	Manual	Local System
Xbox Live Game Save	This service ...	Manual (Trigg...	Local System	
Xbox Live Networking Service	This service ...	Manual	Local System	

- Now go to chrome where cloud.elastic.co was opened

The screenshot shows the Elastic Home page. At the top, there's a search bar with the placeholder "Find apps, content, and more." and a "Setup guides" button. The main navigation bar includes "Home" and "Manage this deployment". On the left, a sidebar lists "Analytics" (Discover, Dashboard, Canvas, Maps, Machine Learning, Graph, Visualize Library) and "Enterprise Search" (Overview, Content, Behavioral Analytics, Elasticsearch). The main content area features four cards: "Enterprise Search" (yellow background, plus icon), "Observability" (pink background, chart icon), "Security" (teal background, shield icon), and "Analytics" (blue background, Kibana icon). Below these cards, a section titled "Integrate with your data" discusses adding integrations and provides a link to "Learn more".

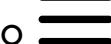
Now click on discover and now navigate to winlogbeat and refresh it

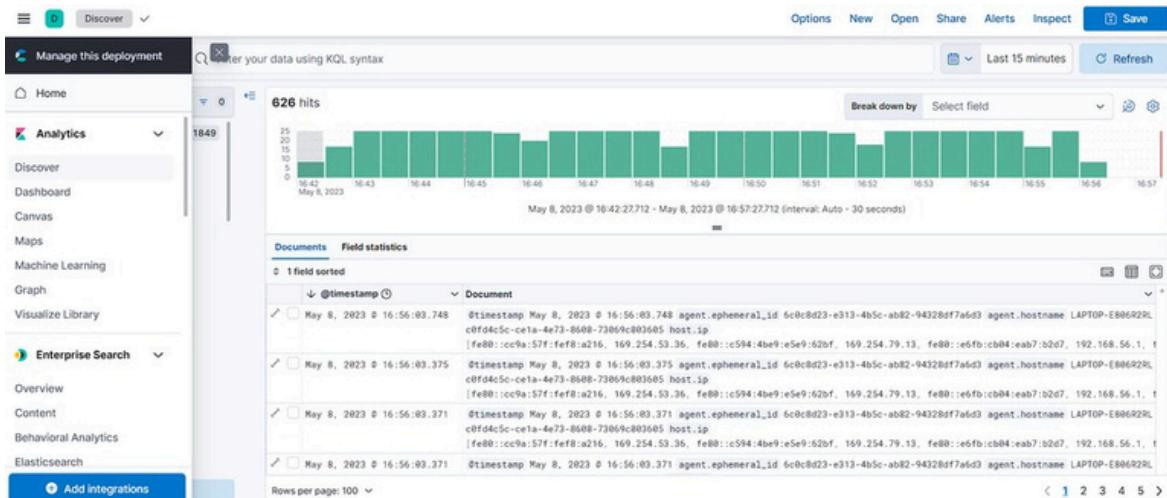
- you will see the likely view of above interface.
 - now if you want to expand the logger you can just click on expand documents

The screenshot shows the Winlogbeat dashboard in Kibana. The left sidebar displays available fields like @timestamp, agent.build.original, and agent.hostname. The main search bar contains the query "winlogbeat-*". Below it, a histogram shows 3 hits for May 8, 2023, between 16:33 and 16:38. The "Field statistics" section shows 1 field sorted by timestamp. The "Documents" table lists three log entries from May 8, 2023, at 16:46:10.682, 16:45:48.065, and 16:33:35.927. Each entry includes timestamp, host.mac, and host.ip. The right panel is titled "Expanded document" and shows the details for the first log entry in JSON format:

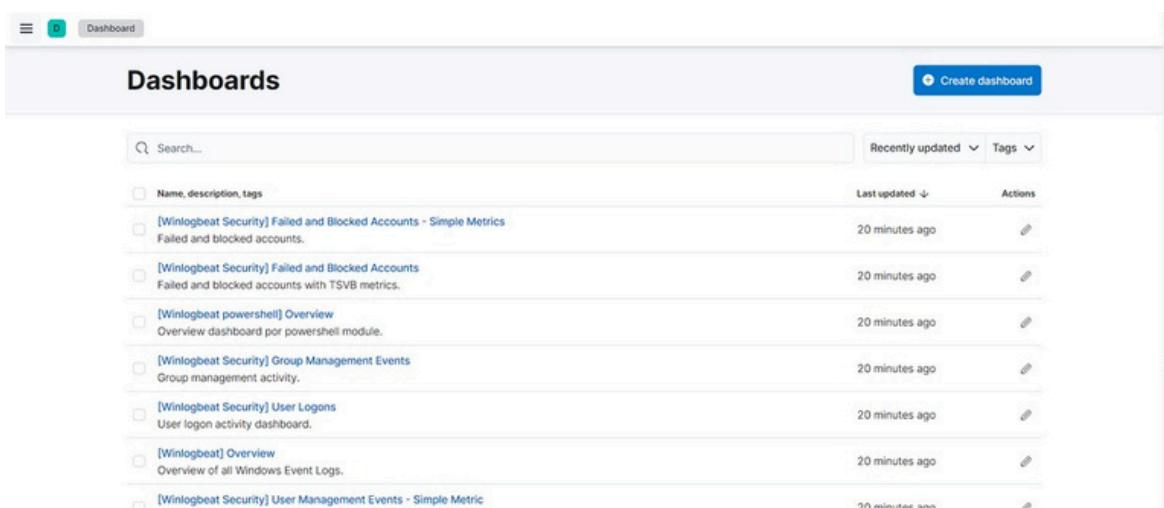
Actions	Field	Value
	_id	ge4U-4cB0gtD0dthmZgR
	_index	.ds-winlogbeat-8.7.1-2023.05.08-000001
	_score	-
	@timestamp	May 8, 2023 0:16:46:10.682
	agent.ephemeral_id	6c0cb23-e313-4b5c-ab82-94328df7a6d3
	agent.hostname	LAPTOP-E806R29L
	agent.id	d31b3fd6-599d-48ca-af18-7ec68a38b0fe
	agent.name	LAPTOP-E806R29L
	agent.type	winlogbeat
	agent.version	8.7.1

CREATE A DASHBOARD TO SUMMARIZE THE LOGS FROM THE MACHINE

- Now in this step i will showcase how to create dashboard
- so first go to  and look for Dashboard. click on it



- once you click on it you will see this type of interface . Now click on Create Dashboard



- once you clicked on the Create Dashboard now click on create visualization

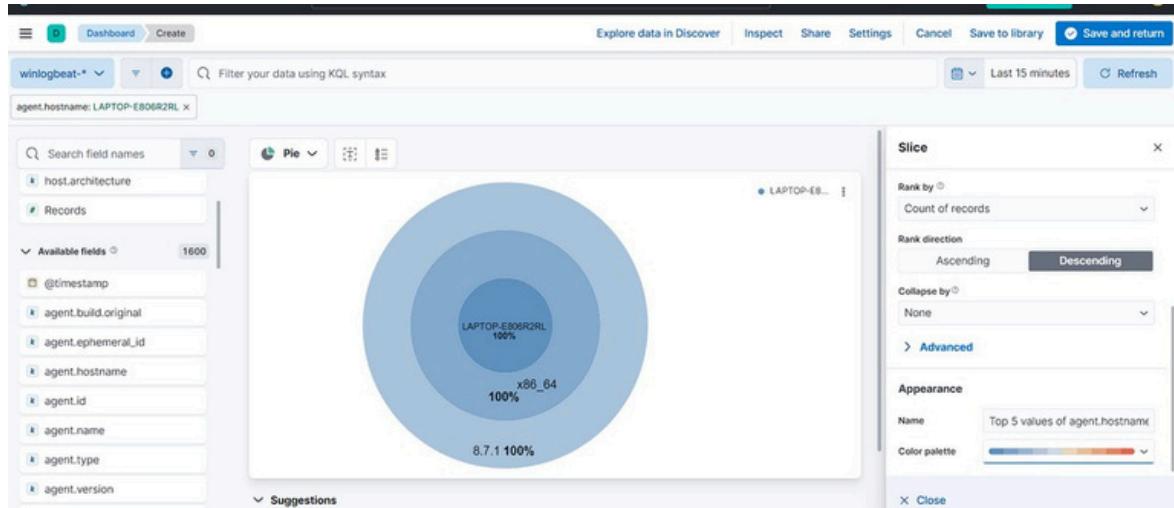
The screenshot shows the Elasticsearch interface for creating a new dashboard. At the top, there's a search bar and several navigation buttons like 'Options', 'Share', and 'Save'. Below the search bar, there's a section titled 'Create visualization' with a large button of the same name. To the right of this button are icons for 'Select type', 'Add from library', and 'Controls'. A message 'Add your first visualization' with a small chart icon is displayed, followed by the instruction 'Create content that tells a story about your data.'

- Now you can filter what you want to know example i want to know about agent.hostname i will search there and drag it to Drop some feilds here to start

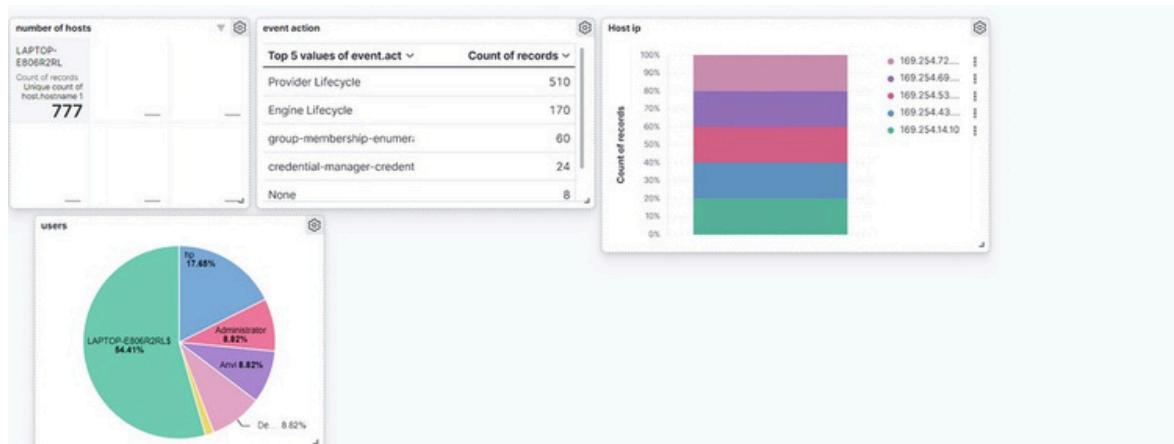
The first part of the screenshot shows the 'Bar vertical stacked' visualization configuration. On the left, a sidebar lists 'Available fields' under the 'host' category, including 'agent.hostname', 'host.architecture', 'host.containerized', etc. In the center, there's a placeholder area with a hand icon and the text 'Drop some fields here to start'. On the right, there are sections for 'Horizontal axis' and 'Vertical axis', both with 'Optional' status and 'Add or drag-and-drop a field' instructions.

The second part of the screenshot shows the resulting visualization. The sidebar now shows 'Selected fields' with 'agent.hostname' selected. The main area displays a large green donut chart where the single segment represents 100% and is labeled 'LAPTOP-E806R2RL'. The configuration panel on the right shows the 'Donut' type selected, 'winlogbeat-*' as the source, and 'Metric' set to 'Count of records'.

- Now let me drag more fields



- Now you can save not only in one view you can choose table , pie chart etc and save it and share it to the respective teams,



Conclusion

Finally, combining Elastic with Winlogbeat can give a complete solution for handling and analysing log data in a Windows context. They are both effective tools for improving system performance, monitoring security incidents, and providing useful insights into system behaviour.