OBJECTIVE IS TO SETUP LOGGING ON ELASTIC.

ASSIGNMENT TASK FOR SOC

Presented By
Anveeksh Mahesh Rao

Table of Contents

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?
  Now create a account using yo ur google account
- redirectTo=%2Fhome
- Now fill the details clearly

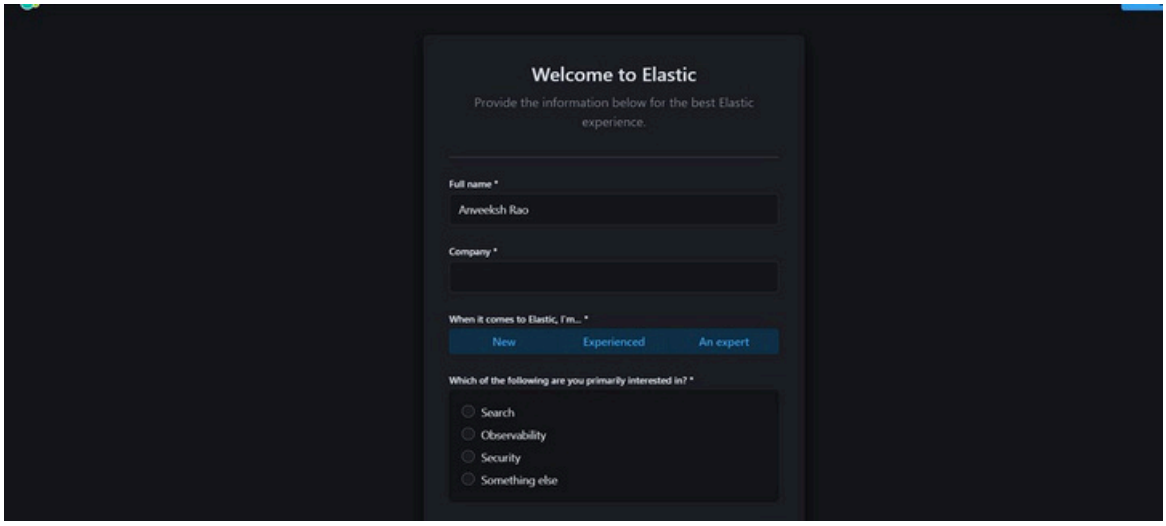


Fig 1

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

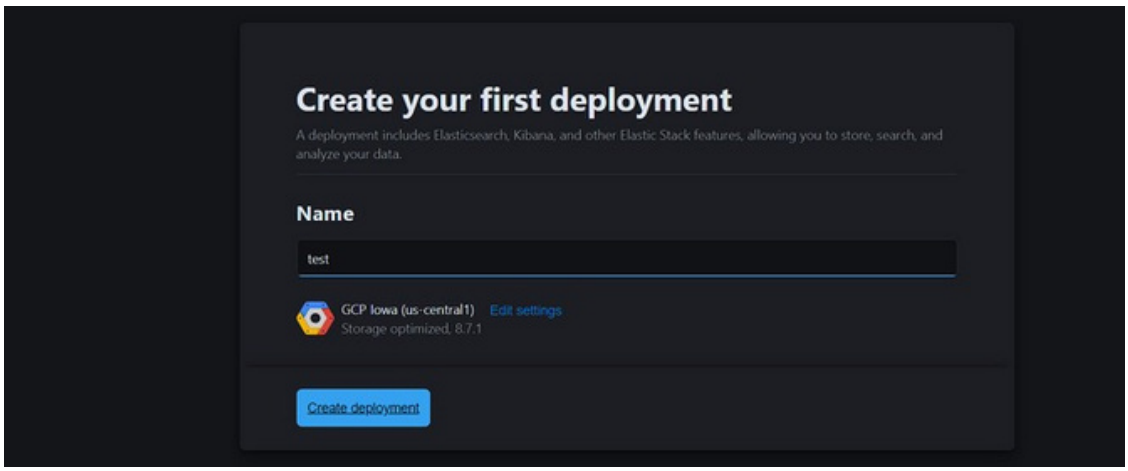
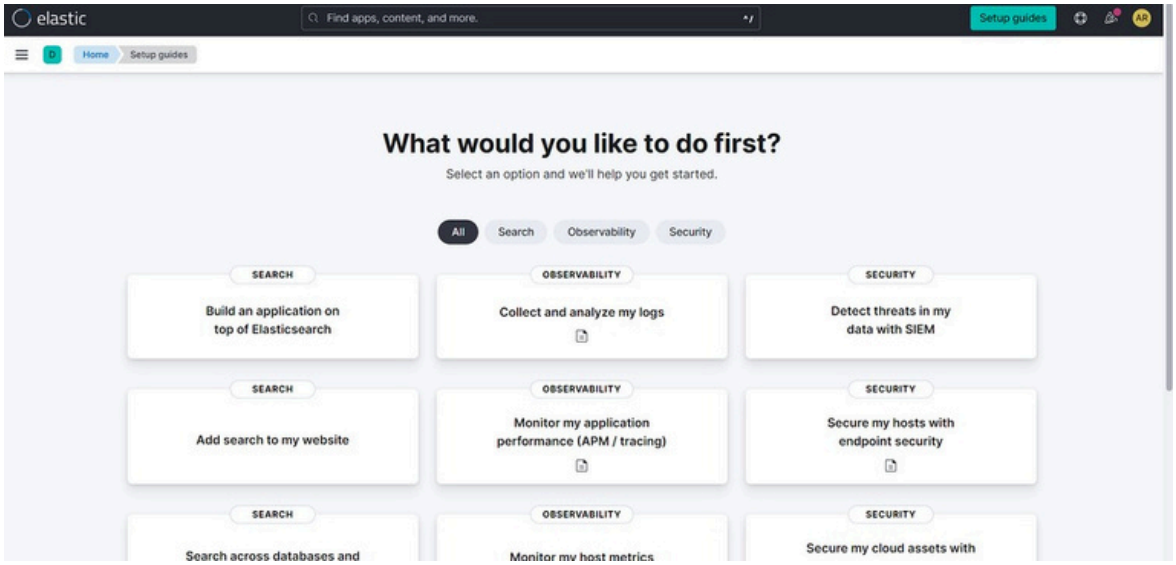
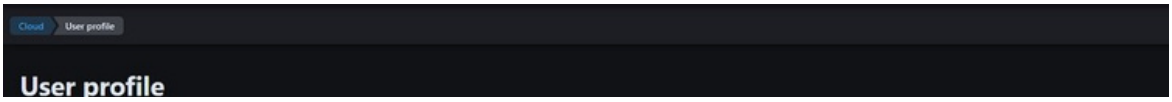


Fig 2

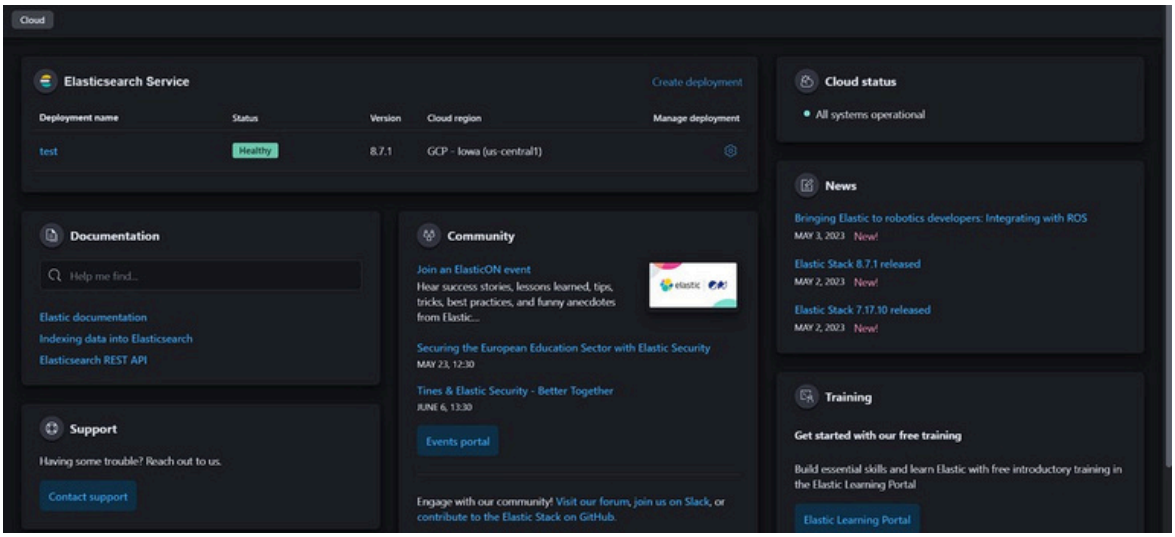
SET UP YOUR PROFILE



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

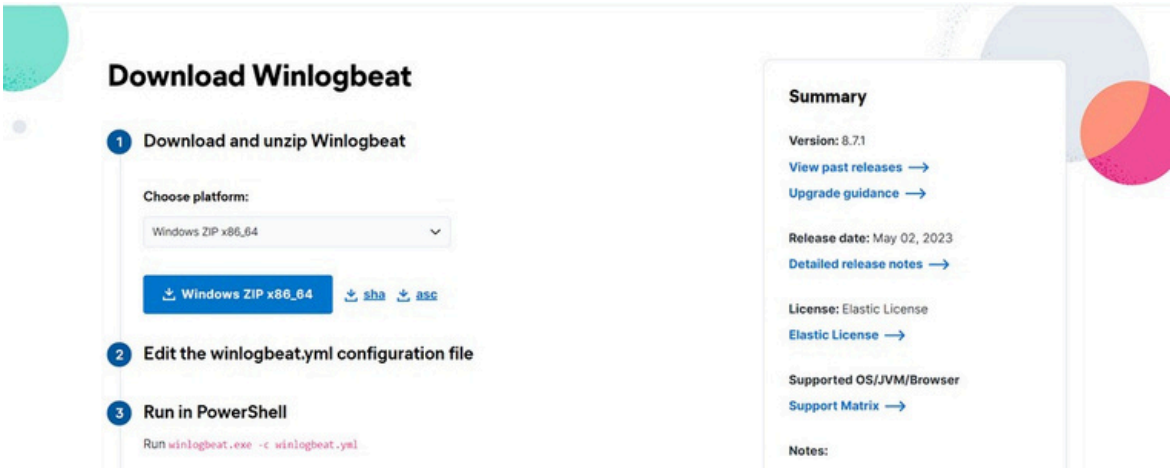


- Now click on Cloud now you can see below type of interface and click on ⚙ button on Elasticsearch Service

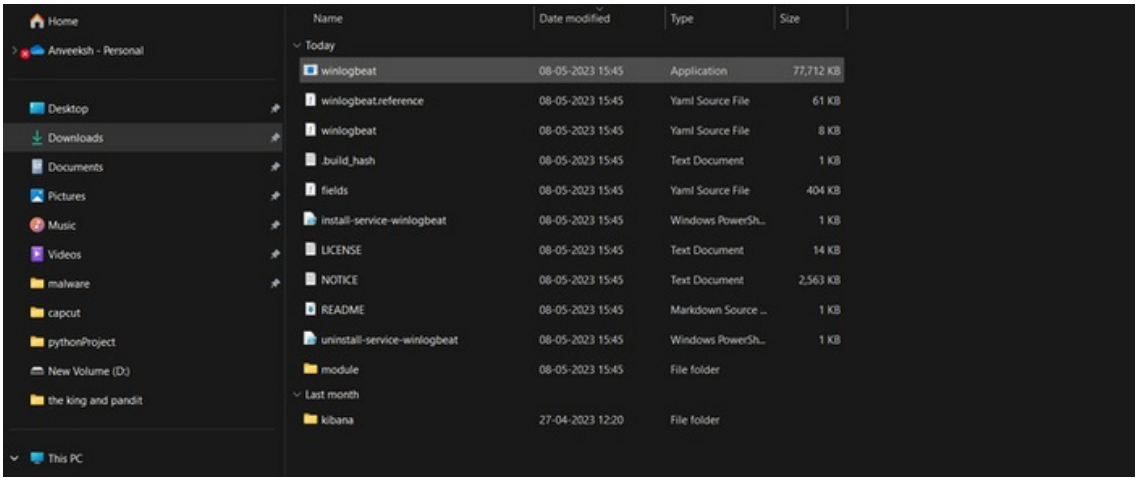


INSTALLING WINLOGBEAT & CONFIGERING

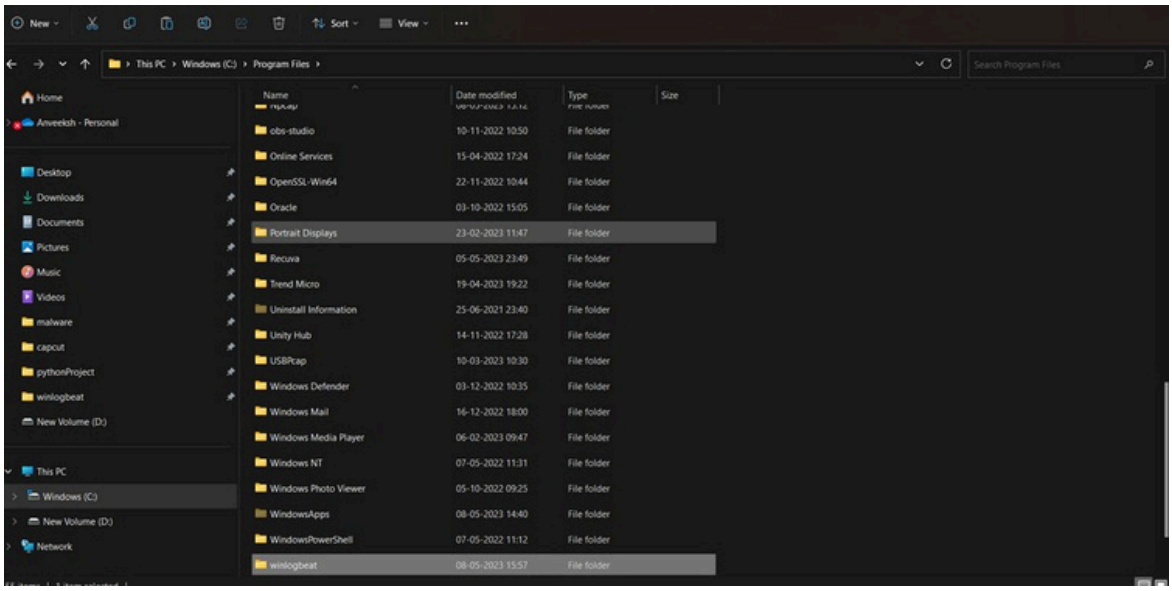
- Now go to new tab and install winlogbeat



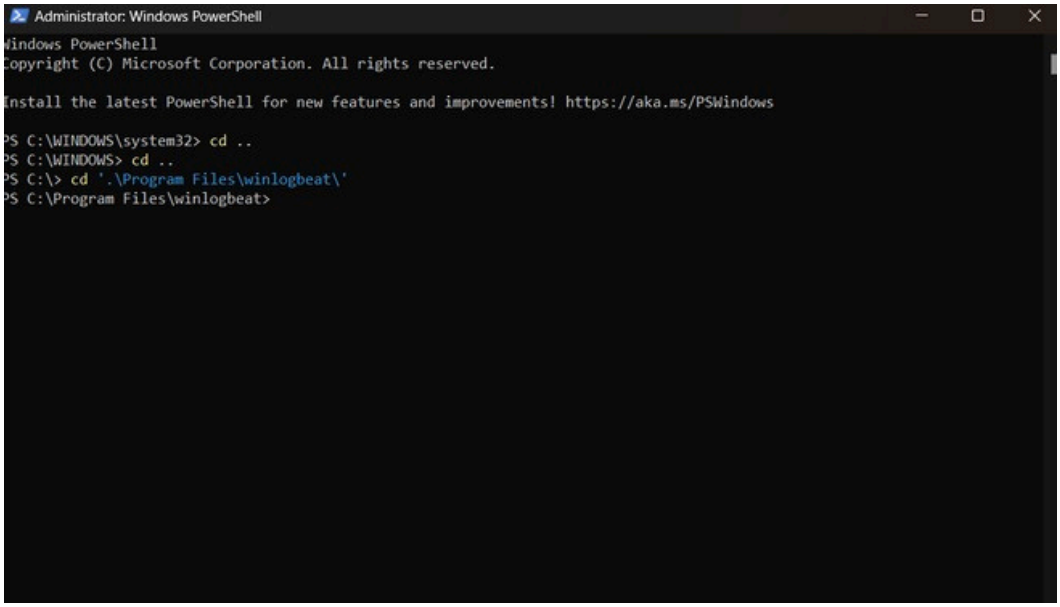
- Once installed extract it and then modify it
- Now modify the Winlogbeat yml file with your elastic configeration



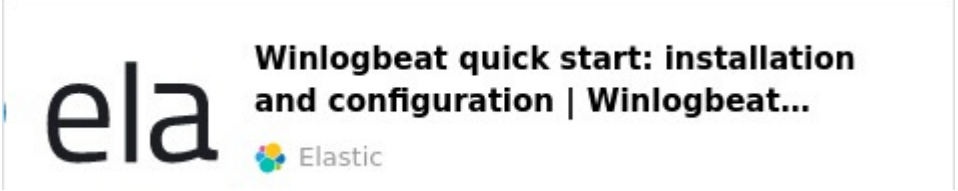
- Before that copy the winlogbeat file to c drive in program file



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

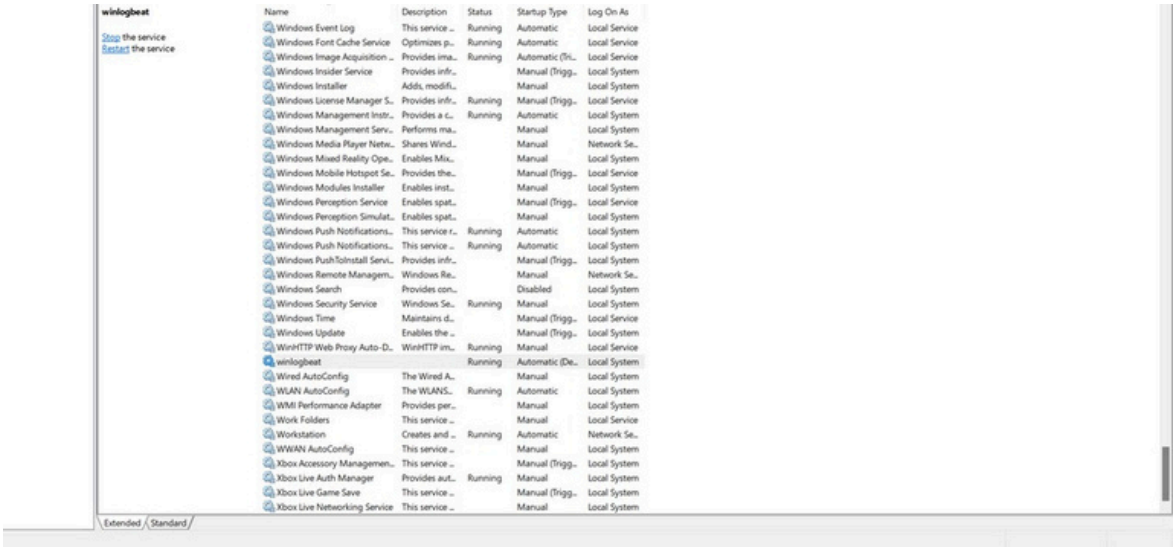


- Now use the guide and start doing configeration
- link is below

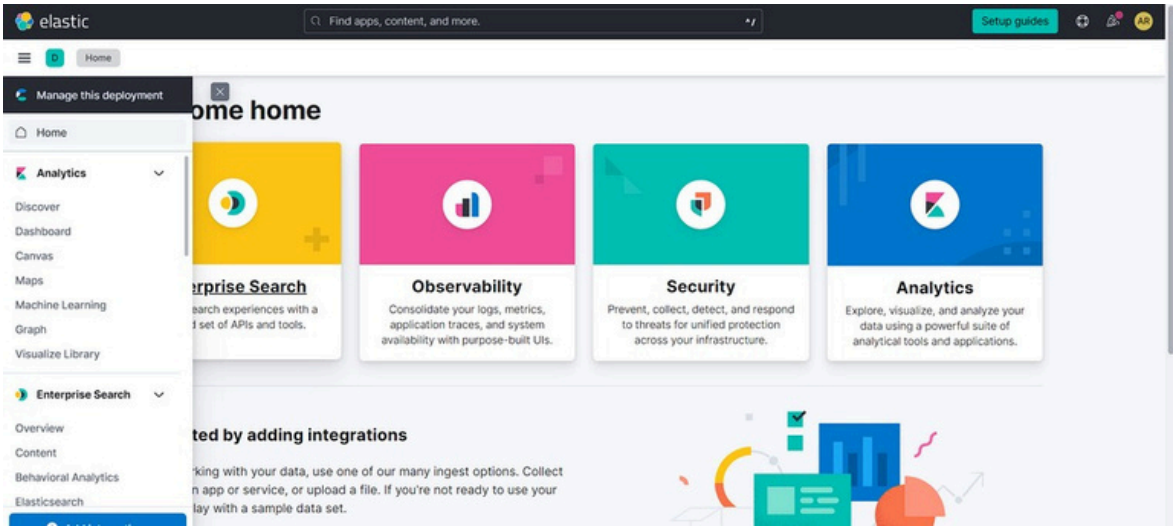


- once all setup is done in Command format type **service.msc**

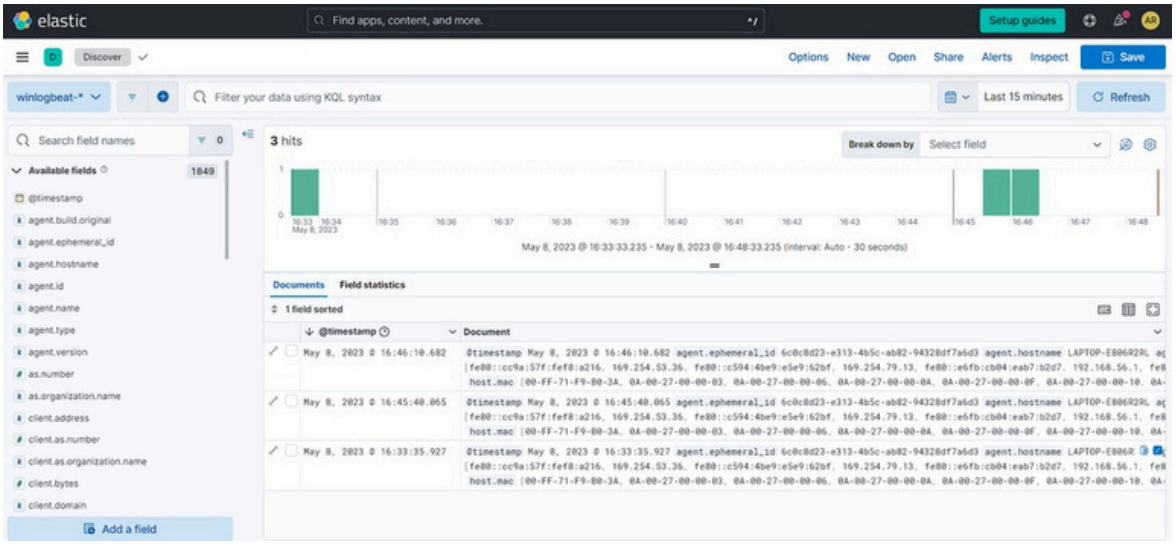
- The below type of interface will open , later search for winlogbeat and start it



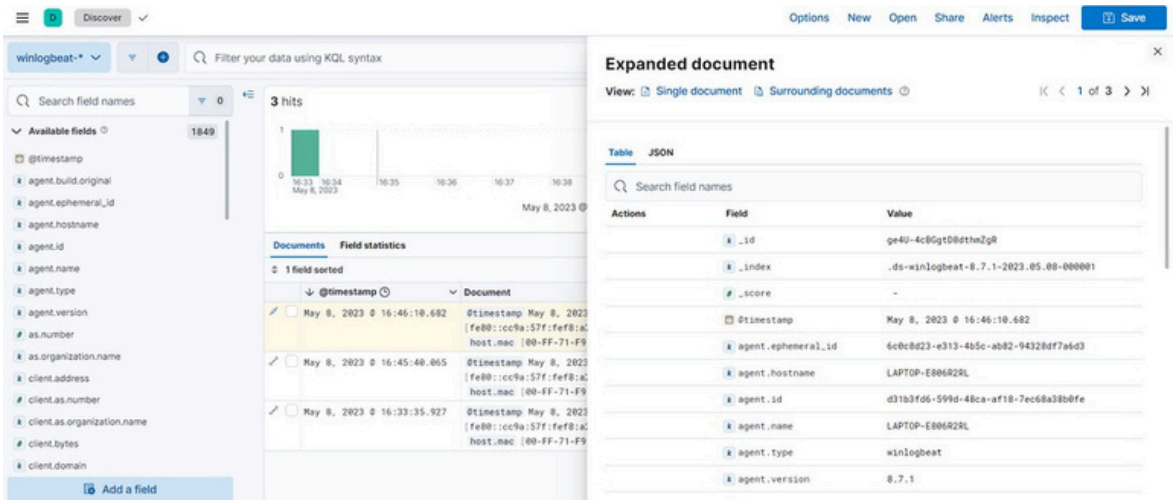
- Now go to chrome where cloud.elastic.co was opened



Now click on discover and now navigate to winlogbeat an refersh it



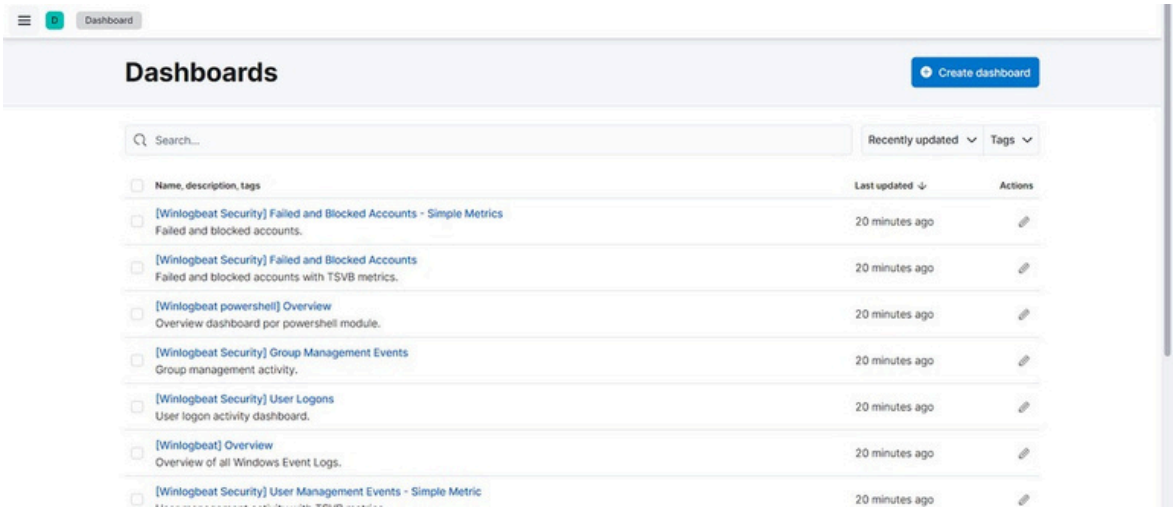
- you will see the likely view of above interface.
- now if you want to expand the logger you can just click on expand documents



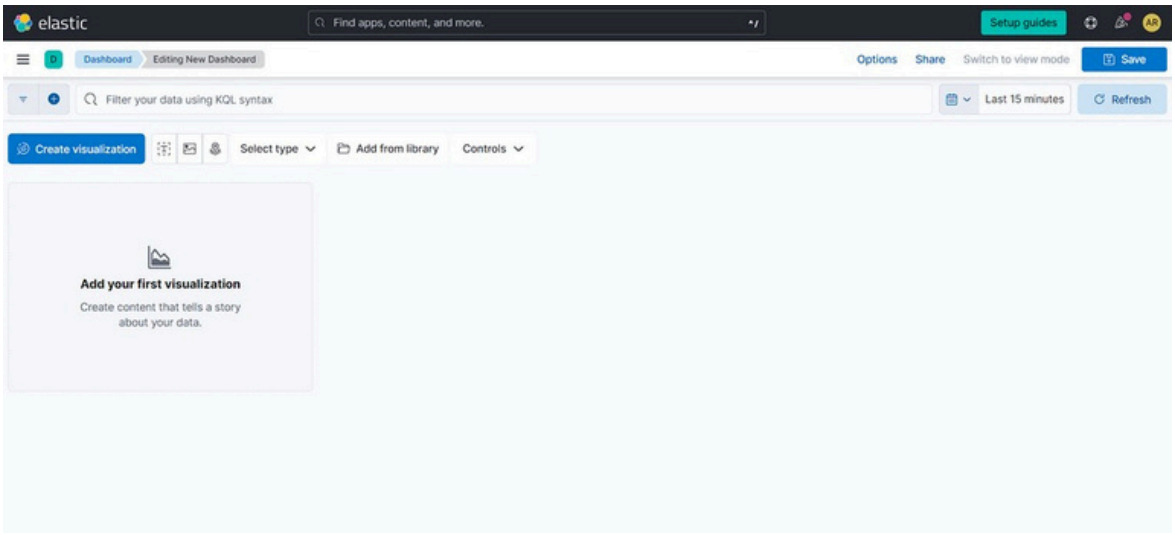
CREATE A DASHBOARD TO SUMMARIZE THE LOGS FROM THE MACHINE

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

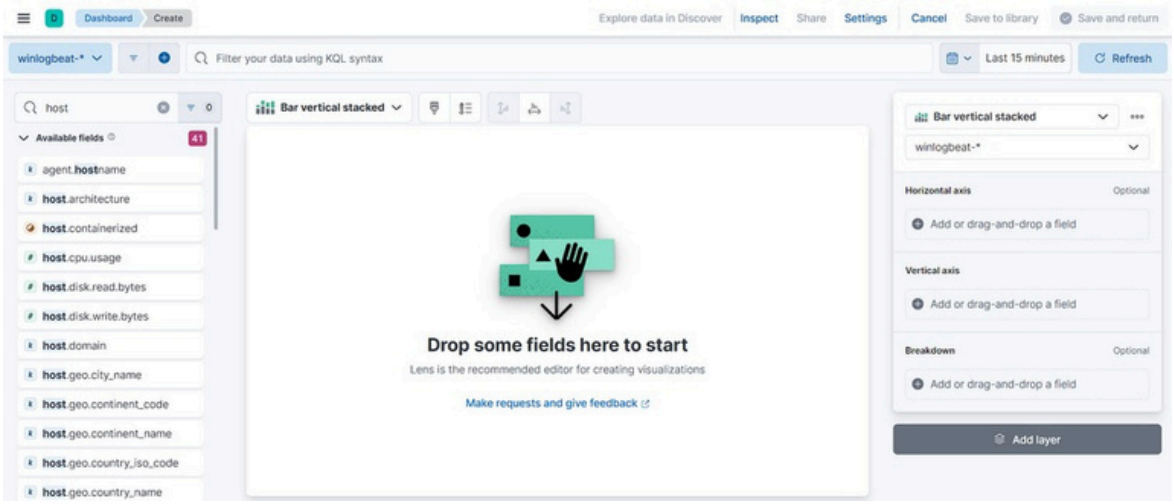
- once you click on it you will see this type of interface . Now click on Create Dashboard

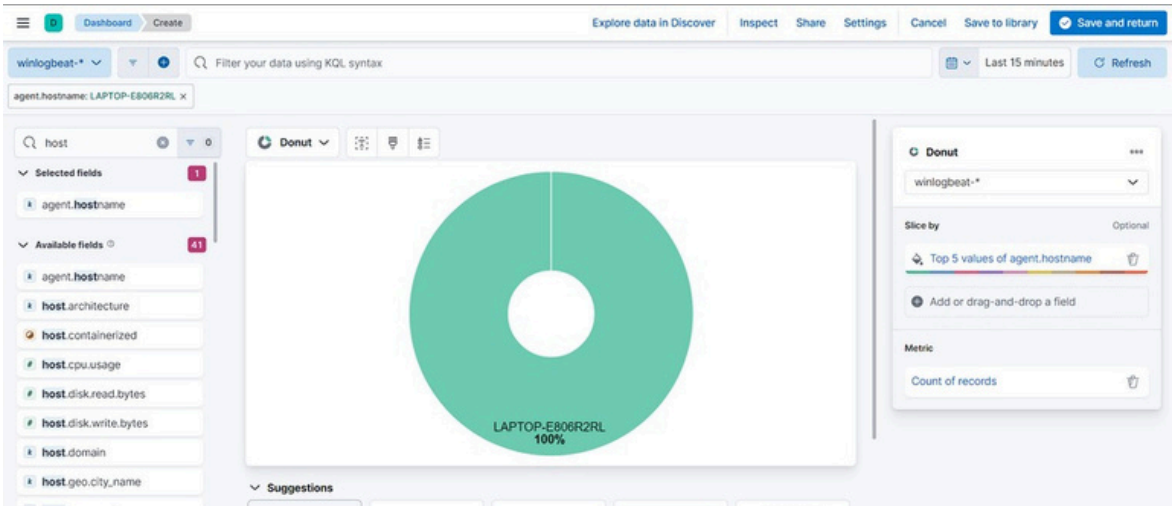


- once you clicked on the Create Dashboard now click on create vizulaization

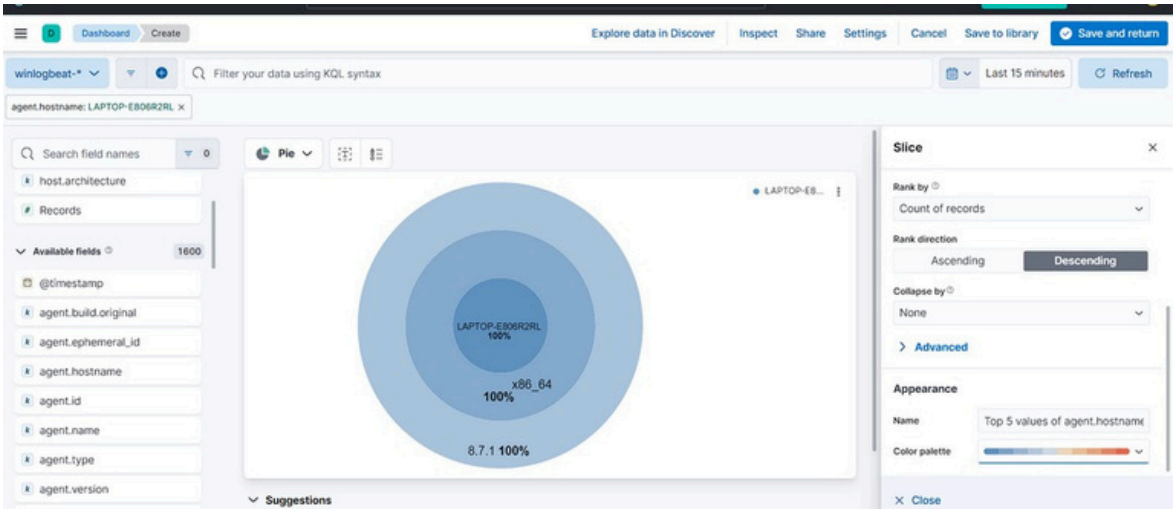


- Now you can filter what you want to know example i want to know about agent.hostname i will search there and drag it to Drop some feilds here to start

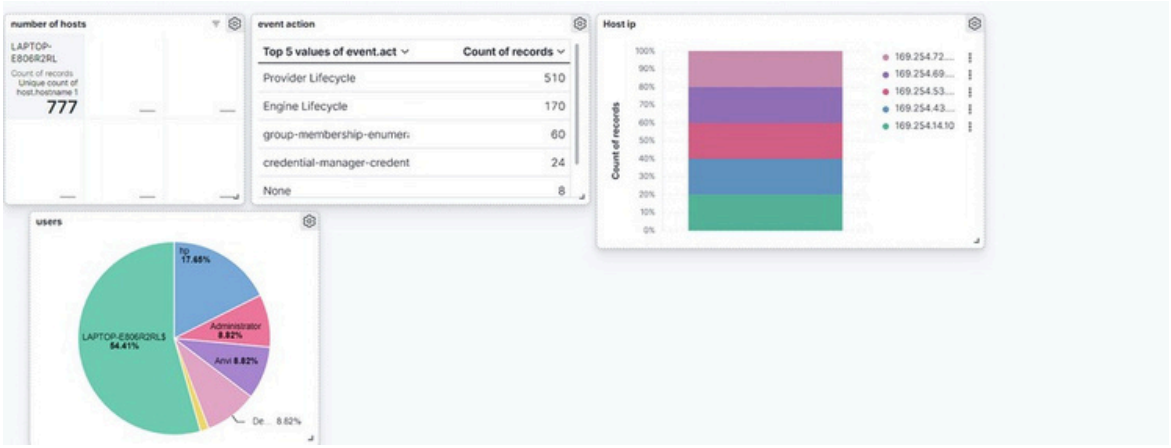




- Now let me drag more feilds



- 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,combiningElasticwith 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.