مهیمن

Log Monitoring

مقدمه:

آنالیز و نظارت بر لاگ‌ها برای درک و عیب‌یابی رفتار هر برنامه‌ای بسیار مهم است. لاگ‌ها می‌توانند گزارش‌های ارزشمندی در مورد عملکرد سیستم شما ارائه دهند تا شما با بررسی آنها مشکلات را سریع، برطرف کنید. ابزارهای بسیار زیادی برای جمع آوری و آنالیز لاگ‌ها وجود دارند، ابزاری که ما میخواهیم تا شما به وسیله آن لاگ‌ها را جمع آوری و آنالیز کنید استک ELK هست.

شرح ورودی:

فایل‌هایی که در اختیار شما قرار گرفته، لاگ‌های عملکرد یک نرم افزار می‌باشد که این فایل‌ها در قالب json است. در ابتدا می‌بایست این فایل‌ها را به وسیله ابزاری جمع آوری کرده و در پردازش‌گر داده Logstash بارگذاری کنید سپس با استفاده از Logstash فرایندی طراحی کنید تا این لاگ‌ها بعد از پردازش در دیتا استور Elasticsearch ذخیره شوند.

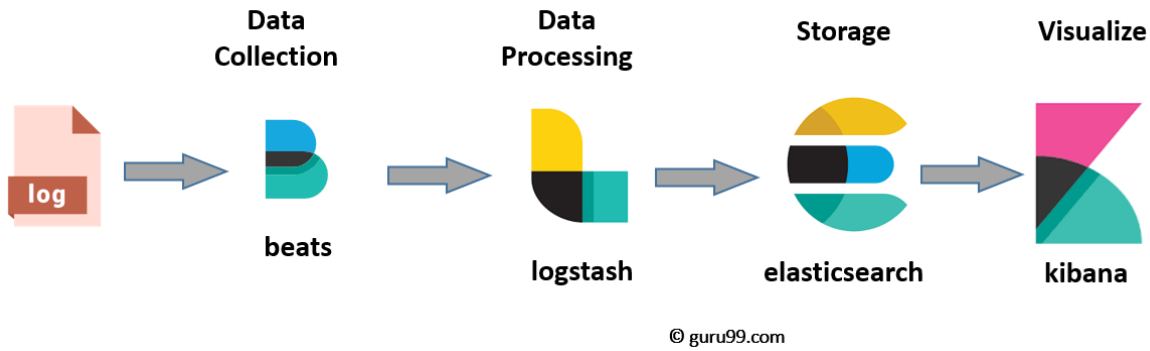
خروجی گزارش:

1-با استفاده از ابزار بصری سازی Kibana بتوانیم ایندکس مورد نظری که ساخته شده را مشاهده کنیم.

2-این فایل های json را در مسیر مشخصی بعد از پردازش، بتوانیم آرشیو کنیم. اگر مثلا این فایل‌های خام ما در مسیر / Data هستند آنها را به /Data/Archive منتقل کنیم.

نکته اگر بتوانید این لاگ‌ها را بعد از اینکه به آرشیو منتقل شدند به صورت فشرده ذخیره کنید امتیاز مثبت خواهید داشت.

راهنمای ورودی:



لاگ ها به وسیله ابزاری باید گردآوری شوند سپس با استفاده از ابزار پردازشگر داده، پردازش و فیلتر شوند و بعد از آن بتوانیم در دیتا استور Elasticsearch آن ها را ذخیره کنیم و با استفاده از ابزار بصری‌سازی Kibana ایندکس های ساخته شده را مشاهده کنیم.

لینک های راهنما جهت نصب و پیکربندی استک ELK

https://www.elastic.co/guide/en/elastic-stack/current/installing-elastic-stack.html

https://dzone.com/articles/installing-the-elk-stack-on-windows

لینک های راهنما جهت طراحی خط لوله پردازش داده

https://www.elastic.co/guide/en/logstash/current/configuration.html

/https://www.bmc.com/blogs/logstash-using-data-pipeline