1. List some logging and visualization tools available in the market with the preferred scenario to use one over other.

Some of the tools for logging and visualization are as follows

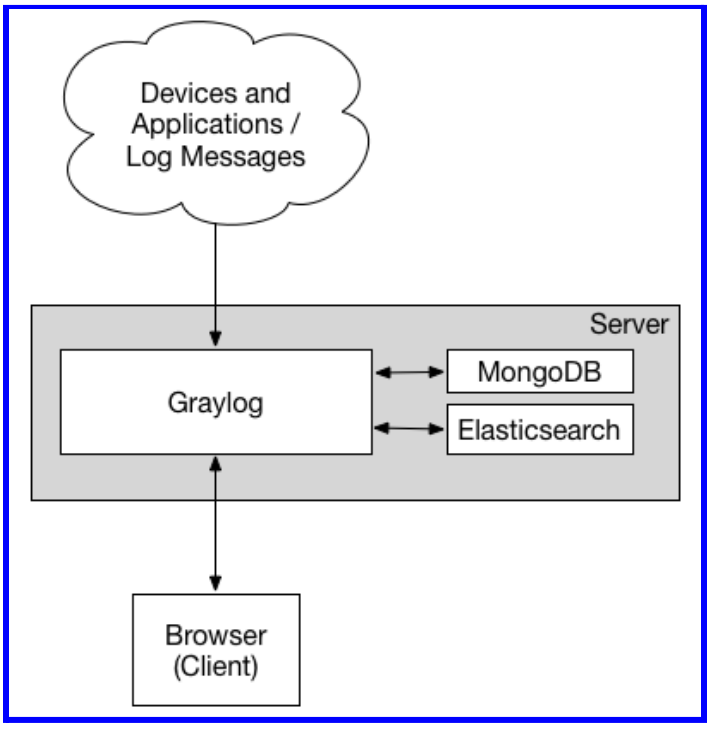
- **Graylog**
- **ELK (**Elasticsearch, Logstash and Kibana**)**
- **Splunk**
- **Datadog**

The feature of each log management tool for which it has been choose in the market is as follows

Graylog

The Graylog software centrally captures, stores, and enables real-time search and log analysis against terabytes of machine data from any component in the IT infrastructure and applications.

The software uses a three-tier architecture and scalable storage based on Elasticsearch and MongoDB.



This is a minimum to be used for smaller, non-critical, or test setups. None of the components are redundant, and they are easy and quick to set up.

Features of Graylog

- Ksystemlog can ingest any structured data, including log messages and network traffic.
- Provides a fully customizable dashboard with numbers of a widget.
- Use standard Boolean search terms for selecting fields and data types.
- Send real-time alert notifications to admin in various ways like email, text, and Slack.
- Graylog usually contains sensitive and regulated data so that the system itself remains accessible, secure, and speedy.
- Has predefined templates to display data.

Benefits over other tools

- **Real-time Answers and fast.**
- **Empower non-tech users**
- **Lower operations costs**
- **Explore your data**

ELK (Elasticsearch, Logstash and Kibana)

Elastic Stack, commonly abbreviated as ELK, is a popular three-in-one log centralization, parsing, and visualization tool that centralizes large sets of data and logs from multiple servers into one server.
ELK stack comprises 3 different products:

Logstash

Logstash is a free and open-source data pipeline that collects logs and events data and even processes and transforms the data to the desired output.

Elasticsearch

Built on Apache Lucene, Elasticsearch is an open-source and distributed search and analytics engine for nearly all types of data – both structured and unstructured.

Kibana

Data is finally passed on to Kibana, which is a WebUI visualization platform that runs alongside Elasticsearch. Kibana allows you to explore and visualize time-series data and logs from elasticsearch.

Features of Elastic Stack

- Clustering and high availability
- Automatic node recovery
- Index lifecycle management
- Secure settings and many more …..

Benefits over other tools

- **It is interoperable**

It can interoperate with other tools to get the job done.

- **It is open-source**

The Elastic Stack is a collection of open-source projects. If you want to deploy it yourself to test it out, you can.

- **It is managed**

If you have the money or don't want to spend any time maintaining your ELK Stack, you can subscribe to a managed service and reduce your time to value.

- **Parting thoughts**

There are many use cases with ELK, and you can break your deployment up into small parts if needed.

Splunk is a software platform widely used for monitoring, searching, analyzing and visualizing the machine-generated data in real time.

It performs capturing, indexing, and correlating the real time data in a searchable container and produces graphs, alerts, dashboards and visualizations.

Features of Splunk

- **Dashboards and Visualizations**

  Customized dashboards and data visualizations give voice to your data.

- **Monitoring and Alerting**

  Continuous monitoring of events, conditions, and critical KPIs helps keep your operations running smoothly.

- **Reporting**

  Reports can be created in real time, scheduled to run at any interval and used in your dashboards.

- **Machine Learning Toolkit (MLTK)**

  Use pre-built Splunk machine learning analytics for identifying use cases or create your own custom machine learning models to tackle impactful issues or opportunities in your company.

Benefits over other tools

- **Accelerate Your Digitization**

  Whether you're just starting to digitize, or you were born in the cloud, innovate with confidence with purpose-built solutions driven by AI and machine learning.

  Splunk solutions provide everything you need to ensure your digital initiatives succeed.

- **Ensure Business Resilience**

  Empower your people to predict, identify and solve problems in real time.

  Answer questions across business, IT, DevOps and security functions with world-class investigative capabilities, intuitive visualizations and seamless collaboration.

- **Meet the Data Opportunities of Today and Tomorrow**

  It’s flexible platform and purpose-built solutions scale with you as your data and organization evolve

Datadog Log Management, also referred to as Datadog logs or logging, provides decoupling log ingestion from indexing.

This enables you to cost-effectively collect, process, archive, explore, and monitor all of your logs without limitations, also known as Logging without Limits*.

Features of Datadog

- **See across systems, apps, and services**

With turn-key integrations, Datadog seamlessly aggregates metrics and events across the full devops stack.

- **Analyze and explore log data in context**

Quickly search, filter, and analyze your logs for troubleshooting and open-ended exploration of your data.

- **Visualize traffic flow in cloud-native environments**

Understand performance using meaningful, human-readable tags.

- **Build real-time interactive dashboards**

More than summary dashboards, Datadog offers all high-resolution metrics and events for manipulation and graphing. And many more …...

Benefits over other tools

- **Customizable Dashboard**

The dashboard used in the Datadog can be easily customizable as per the requirements.

- **Easy installation**

The configuration and installation of the Datadog tool are easy as it uses the SaaS service.

- **Cheaper than others**

The implementation of the tool is cheap.

There are also many more log management and visualization tools like, **LOGalyze, Glogg, GoAccess, Frontail, Multitail, Logwatch, Nagios, etc** which are open-source and efficient to use.