1. List of logging and Visualization tools

- ELK stack: Elk stack consists of Elastic Search(for querying the logs) , Logstatch (for collecting logs from different sources) and Kibana for mainly visualization of the information collected through logs and for some monitoring too.

- SolarWinds log analyzer

- Datadog

- Graylog

2. 10 best practices while logging

- Aggregation of logs:
  The analysis of logs is difficultt to perform on individual machine or system when you the system is large and when it has large number or hosts or devices. Therefore , it is a good practice to collect and store the logs somewhere else in centralised location where the logs collected from the entire system can be analysed.

- Using structured log messages:
  Use of structured log messages can is needed where there are logs are created with different format. If the logs structured are structured and make easily readable, it makes logs analysis very easy. During the time of failures and problems these structured log messages are become helpful than unstructured messages. For example, JSON or key value parir can be used to structure the logs messages.

- Create meaningful log messages:
  If possible include the context in the log messages. Readable and useful log messages are key for faster troubleshooting. If logs contain only some error codes or ‘cryptic’ error messages it can be difficult to understand.

- Set different levels of in the log(FATAL, WARN, INFO, DEBUG, ERROR) :
  Setting different log levels like fatal, wran , info ,debug, error ,etc. Helps to analyse the logs faster by human. If there are “FATAL” flags in our logs, then we’d traverse the issue and rectify it. If it is just a warning or info then we would not consider them too much.

  These log levels help to highlight or differentiate the critical information from the large volume of records.

- Do not log any kind of credentials or sensitive information:
  Do not log any sensitive information like database url, api keys, authentication tokens etc in the logs. Since these logs are accessed by different people and different systems , these logs might become the loophole in our system any may be vulnerable.

- Review and rotate the logs periodically:
  If the logs are not reviewed periodically then there is no use of keeping those logs. Reviewing the logs periodically helps to find the issues and provide the status of the system.

- Make sure that the logging is not affecting the system itself:
  Logging takes both CPU and storage of the system. Logging shoul be done in such a way that it does not affect the system. Logs many affect the available memory of the system. The log files should be rotated and compressed regularly to prevent logging from overwhelming the system itself.