2. Mention 10 best practises when logging. Why is log formatting necessary?

The 10 important thing to be considered during logging are as follows:

- **Log only what's needed. Don't log everything**

  i.e Don't log too much or Too little

  Logging too much can cause storage volume sortage and it will really become hard to get any value from it.

  Too little log will risk not being able to troubleshoot problems.

- **Don't log sensitive information**

  i.e we should be aware of what not to log like

  If anyone gets the sensitive data from the log, then our system could be vulnerable and can help others to breach the security system.

  Some information should not be logged like:

  - Personally Identifiable Information (PII)
  - Business Names and Contact Informations
  - Financial Data (Back Accounts, Card Details, etc)
  - Passwords, security keys, secrets, etc

- **Format logs so they are easily parsable and readable**

  Use standard date and time format. Most probably UTC.

  Add more context to the logs Logging Practises.

- **Separation of concerns for logs**

  The log level is used to denote the severity of each event in the system.

  Using different log levels like **FATAL < ERROR < WARN < INFO < DEBUG < TRACE** can help to distinguish the troubleshooting priority too.

  E.g.

  ```
  2012-05-23T15:02:27Z | ERROR | access to /home/test/index.html is forbidden. Client:
  202.123.22.23
  2018-03-22T11:34:12Z | WARN | The plugin xyz is deprecated and will be removed
  from future releases.
  ```

  Include developer-friendly log messages (short and sweet)

- **Centralize logs**

  It is mandatory to keep these logs preserved both locally and in central storage to make it hard for intruders and cybercriminals to access both locations and delete evidence of their activity at the same time.

  It helps us prevent breaches from going unnoticed.

  Logs can generate from multiple servers

  Accessing each server to retrieve the logs is painful

- **Log rotation**

  Eg. with logrotate utility, you can configure to rotate your logs with configuration as such

  ```
  /var/log/nginx/access.log {
    Daily
    Rotate 7
    Size 20M
    Compress
  }
  ```

  Log rotate can help us to take logs of the applications Daily/Weekly, keeping the require amount of logs 7 logs weekly, determine the size of the log, helps to compress the log, etc

- **Using Recommended Tools**

  Using recommended tools can help to get log in more efficient way like

  - Logging Frameworks

    We can use tools like JavaScript, TypeScript, Java, Golang, etc

  - Log inspection/aggregation/monitoring tools

    We can use CLI tools, Cloud tools, SEIM tools and others like ELK stack, Loggly, etc

- **Using the English Language**

  Some tools and terminal consoles do not support printing and storing log messages with certain Unicode characters. Hence localization and other advanced features may be challenging at the logging level.

  Therefore, make sure you stick to the English language and always use a widely accepted character set for writing log messages.

- **Make each log message unique across the system**

  One mistake that most developers make is to copy-paste the same log message in multiple files while letting the final log aggregate fill with similar log lines coming from multiple different parts of the system.

Doing that,, it is not easy to trace the exact location that triggered the event in the code.
At least mentioning the log source with the log message to make the final log lines look different from each other.

- **Set up alerts and push notifications when critical incidents occur**
  Almost all the log monitoring tools include features to define custom thresholds at certain levels.
  When the system hits those levels, the monitoring tool will proactively detect them with the help of log data and notify SysAdmins via alarms, push notifications APIs (e.g. Slack Audit Logs API), emails, etc.
  Also they can be preconfigured to trigger automated processes like dynamic scaling, system backup, changeovers, etc.

Why is log formatting necessary ?

Generally when logs are generated,
The problem with log files is they are unstructured text data which makes it difficult to generate meaningful information by just looking at the logs.
Log formatting is necessary

- Process log files for analytics or business intelligence
- Searching log files
- To generate more meaningful information.
- To set severity levels such as “**FATAL, ERROR, CRITICAL**”,etc so that we can focus on specific logs to solve.
- To solve problems like filtering all logs by a certain customer or transaction and allow additional analytics