APPLICATION LOGS:

Software applications generate logs when something occurs within (or affects) the application.

APPLICATION SPECIFIC LOGS:

An application-specific log format is a custom format created by a developer or software vendor to log events, errors, transactions, or debug information in a way that makes sense only to that specific application.

There are

Internal applications

External applications

Internal application events:

- Memory leaks
- Non-existent path errors
- Unhandled exceptions in the code
- A system crash

External application events:

- Disk space warnings
- Server reboots
- Lost network access

Application Log Types

- **Access logs:** Provide a record of all requests made to your application. For example, every time a user tries to load a page or download a file, an entry is made in the access log. This can be extremely useful in understanding user behavior and identifying potential security threats.
- **Authentication logs:** Record every attempt to log into your application. They detail whether the login attempt was successful or not and which user was trying to gain access. For instance, if a particular user is making numerous failed login attempts, this could indicate a possible brute force attack on your system.
- **Authorization logs:** Keep track of what actions each authenticated user is permitted to perform. Say a user attempts to delete a record, but they do not have the necessary permissions. This would be logged in the authorization log, providing a clear audit trail of user activities.

Example Log:

```
192.168.1.25 - - [06/Jul/2025:06:30:15 +0000] "GET /index.html HTTP/1.1" 200 3056

192.168.1.25 - - [06/Jul/2025:08:30:17 +0000] "POST /login HTTP/1.1" 401 1283
```

Compatibility: No

Solution:

Parse → Normalize → Reformat (to JSON/Syslog/etc.)

Advantage of Application specific log:

- Human-readable
- Contains business-specific terms

Disadvantage:

- No JSON/XML structure
- Not recognized by log tools unless custom parser is made
- No severity level or source IP