How do you read application logs and dashboards when something breaks?

3 November 2026 · 5 min read · blogs.iictp.org/how-to-read-application-logs

Start from the symptom, find the time it began, then use the dashboard to see what changed and the logs to see why. Work from the broad view to the specific request, and write down what you learn as you go.

TL;DR The short version

- When something breaks, start from the symptom, find when it began, use dashboards to see what changed and logs to see why.
- Check the four golden signals first: latency, traffic, errors and saturation.
- Structured logs and correlation IDs make filtering possible, and passwords, tokens and personal data must never appear in logs.

Read online, listen to it, or change the text size: https://blogs.iictp.org/how-to-read-application-logs

What do the log levels mean?

DEBUG is detail for developers, INFO records normal events, WARN flags something unusual that did not fail, and ERROR records a failure. In production, ERROR and WARN entries are usually the first place to look.

What should you check first on a dashboard?

Look at the four golden signals from the Google SRE book: latency, traffic, errors and saturation. Compare them with normal. A jump in errors that starts exactly when a release went out points to the release.

How do you find the right log lines?

1. Pin down the time window of the problem.
2. Filter by service and by level.
3. Search for the request, user or correlation ID from a failing example.
4. Follow that ID through every service it touched.

Why do structured logs and correlation IDs help?

Structured logs, written as key-value fields instead of free text, can be filtered and counted. A correlation ID carried through every service lets you reconstruct one request across the whole system. See observability versus monitoring.

What should never appear in logs?

Passwords, tokens, full card numbers and other personal data. Logs are copied to many places and kept for a long time, so sensitive values become a second leak. Mask or leave them out.

Related credential: Associate Technical Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. Beyer, B., Jones, C., Petoff, J. and Murphy, N. R. (eds.) (2016). Site Reliability Engineering, chapter 6, “Monitoring Distributed Systems”. O’Reilly Media.
2. OWASP. Logging Cheat Sheet. cheatsheetseries.owasp.org.

Published by IICTP, an independent technical credential body, on 3 November 2026. The current version of this post is at https://blogs.iictp.org/how-to-read-application-logs. More guides: blogs.iictp.org.