

eBPF Notes

TJ Robinson

October 29, 2025

1 What is eBPF?

- eBPF (extended Berkeley Packet Filter)

1.1 Logs vs. Metrics vs. Observability

- Logs: Detailed, unstructured, aggregated data about individual events.
 - Useful for troubleshooting and forensic analysis.
 - Can be voluminous and harder to analyze at scale.
- Metrics: Aggregated, structured data for to monitor a program or system performance at a specific point in time.
 - Useful for identifying trends and triggering alerts.
 - Typically less detailed but more efficient to store and query.
- Observability: Combines logs, metrics, and traces to provide a comprehensive view of system behavior.
 - Capacity to ask arbitrary questions and receive complex answers about a system's state.

1.2 Namespaces & Cgroups

Both are fundamental for containerization and resource management in Linux.

- Namespaces: Isolate system resources for processes (e.g., PID, network, mount).
 - inside a namespace, you experience the operating system like there were no other tasks running on the computer

- Cgroups: Control and limit resource usage (CPU, memory, I/O) for process groups.
 - gives you fine grain control over resource usage like CPU, disk I/O, network, and etc.

Tracepoints are static marks in the kernel code that can be used to inject code to inspect the kernel's execution.