Level 0 DFD Description

Log-Driven Incident Response System

The Level 0 Data Flow Diagram (DFD) presents a high-level overview of the **Log-Driven Incident Response System** and illustrates how the system interacts with external entities to detect incidents and respond to failures.

At this level, the entire system is represented as a **single process**, focusing on *what* the system does rather than *how* it does it internally.

External Entities and Interactions

1. **Application Services**
   Application Services continuously generate **application logs**, which are sent to the Log-Driven Incident Response System. Based on detected incidents, the system may trigger **recovery actions** (such as restarts or configuration fixes) back to the application services. The services also receive **status updates** after recovery actions are performed.
2. **System Executor**
   The System Executor is responsible for providing and configuring **automation playbooks**. These playbooks define the predefined recovery actions that the system can execute automatically when specific incident patterns are detected.
3. **On-call Engineer**
   The On-call Engineer acts as a human decision-maker in critical or uncertain situations. The system sends **failure alerts and approval requests** when incidents require manual intervention. The engineer reviews incidents and provides **manual approval or corrective input**, which guides the system's response.
4. **Notification Service**
   The Notification Service is used to deliver alerts and updates. The Log-Driven Incident Response System sends **notification requests** to this service, which then forwards **failure alerts, approval requests, and incident updates** to the On-call Engineer and relevant stakeholders.

Overall System Function

The Log-Driven Incident Response System acts as a central coordinator that:

- Collects logs from application services,
- Analyzes them to detect failures or anomalies,
- Executes automated recovery actions using configured playbooks,
- Notifies stakeholders through a notification service, and
- Escalates incidents to an on-call engineer when human approval or intervention is required.

This Level 0 DFD clearly defines the system boundaries and establishes how the system exchanges data with external entities without exposing internal processing details.