Solution Brief

LOG MANAGEMENT

err0 simplifies log management

err0.io

Monitoring Blind Spot

Log management is impossible to operationalise because there's a lack of visibility into the complete catalog of log.

Today, many teams rely on what they've seen occurring, the tip of the iceberg. Therefore there are multiple critical events that aren't monitored, just because the DevOps & SRE teams don't know them.

Parsing & False Positive

The fundaments of log management is parsing logs using regular expression to match specific text and extract data. The efficiency of this process is crucial to all log management platform. A mismatch is a false positive, leading to a costly false alert.

Logs are unstructured data because there's no standardisation, no catalogs and, as consequence, no chain of communication for DevOps & SRE to be informed of log changes that would require them to update the log management configuration and settings.

err0 solution

err0 is a game-changer that transforms the ROI of your favorite Log Management platform:

- **Standard unique Error Code**
  - 100% match accuracy, no more false positive
  - 1 regex pattern to rule them all
- **Exhaustive error & log catalog**
  - All errors & logs are known, no blind spot
  - All errors & logs changes are tracked
- **Logs eXplanation**
  - Logs knowledge management
- **Log Management Configuration Automation**
  - Dynamic configuration based on error & log meta-data (ie. severity, priority, etc)

To learn more and test err0 visit
www.err0.io

How err0 works

1. CATALOG

Applying unique Id to all events

Use err0 open-source agent (github.com/Err0-io) to parse the source code and prepends a unique error code, as a text, to the message of every error and log. Once the proposed logId matches your expectations, then you can commit your code.

2. EXPLAIN

Making logs eXplainable

For each error code, err0 open-source agent captures meta-data and any preceding comment is use as a knowledge seed. Then stakeholders can easily contribute knowledge, so that it can be shared.

3. PRIORITIZE

Set severity and priority for important logs

Dynamically adjust the priority and severity of the error codes in err0 platform to ensure DevOps, SRE, Support and customers are aware of what they should be alerted on.

4. OPERATIONALISE

Automate log management configuration

With err0's API your favorite log management platform is automatically configured and maintained up to date, as information flows downstream.

How err0 solves challenges

Challenges	err0 Solutions
Maintenance	With err0 the configuration of the log management can be automated as part of the CD. One stable single regex to parse logs.
False positive	With the unique error code pattern, log parsing is efficient and 100% accurate. No more false positive.
Missed event	The conjunction of the unique error code pattern and the exhaustive log catalog enables to accurately trap all significant events.
Analysis	With err0 knowledge base, all stakeholders can easily share and access accurate knowledge on each error and log.
Searching	Thanks to the unique error code all searches are simple, efficient and accurate.
Correlation	The combination of unique error code enables to define and maintain efficient ML-based correlation and rules.
CyberSecurity	Compliance with NIST SP 800-92 is facilitated thanks to the unique error code, exhaustive log catalog, knowledge and dynamic configuration of monitoring and log management platforms.

To learn more and test err0 visit
www.err0.io

err0.io