



Data Monitoring

[How does monitoring work](#)

[Monitors](#)

[Notifications](#)

[Types of Alerts](#)

[Alert Response Overview](#)

[What can Alert Response do?](#)

[How can Alert Response help?](#)

[Alert Details](#)

[Alert Context](#)

[Context Cards](#)

[Set up Alert Response](#)

[Alert Page](#)

[Webhook connections](#)

[Alert Variables](#)

[Context Cards](#)

[Types of Context Cards](#)

[Anatomy of the Context Card](#)

How does monitoring work

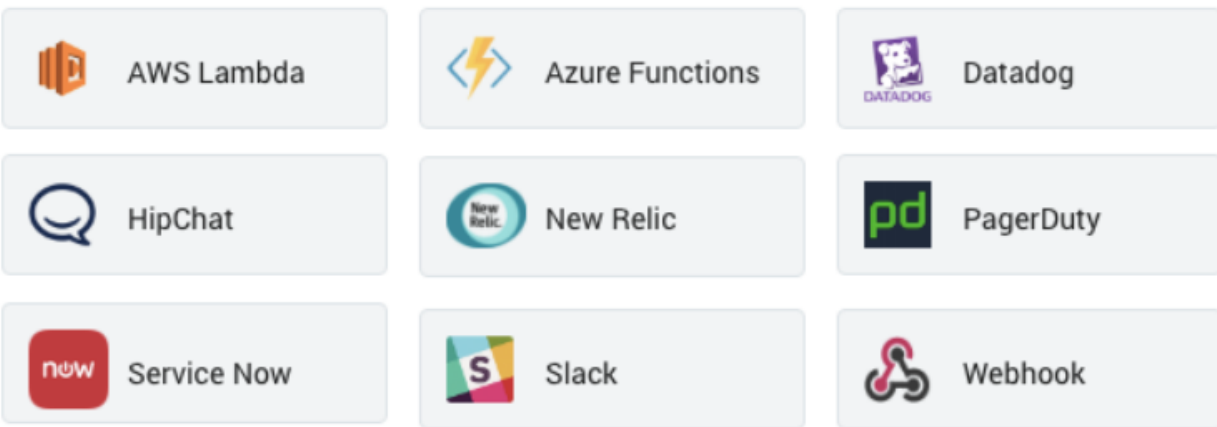
Monitors

- Allow users to set robust and **configurable alerting policies** that enable you to get notified
- Monitors track your **Metrics** or **Logs** data in **real time** and **send notifications** when noteworthy changes happen in production applications

Notifications

- Optional and available as an **alert** and **recovery** for each trigger condition you specify
 - **Critical**
 - **Warning**
 - **Missing Data**

Types of Alerts



- You can **schedule a search** and when a **condition is met**, it triggers an **alert**.
 - Email alert
 - Webhook
 - Save to index
 - Script action

Alert Response Overview

What can Alert Response do?

- Provides **contextual insights** about triggered alerts to **minimize the time** needed to investigate and resolve application failures

How can Alert Response help?

- Provides curated information to troubleshoot issues more quickly by providing two different types of information

Alert Details

- **Overview of the alert** that was triggered to help **understand the issue** and its potential impact
 - What is happening?
 - What is the potential impact?

Alert Context

- **System curated context** helps you understand **potential underlying symptoms** within the system that might be causing the issue.
 - What are the potential underlying symptoms within the system that might be causing the issue?
- Uses artificial intelligence and machine learning
- Finds interesting patterns in the data

Context Cards

- Log Fluctuation
- Dimensional Explanation
- Anomalies
- Benchmarks

Set up Alert Response

- When using Webhook connections offered by Sumo Logic for receiving notifications, need to provide the `alertResponseUrl`
- Monitor is triggered, it will generate a URL and provide it in the notification payload
 - Can be used to open **Alert Response**
- Example of Slack Payload

```

{
  "attachments": [
    {
      "pretext": "Sumo Logic Alert",
      "fields": [
        {
          "title": "Alert Page",
          "value": "{{alertResponseUrl}}"
        }
      ],
      "mrkdown_in": [
        "text",
        "pretext"
      ],
      "color": "#29A1E6"
    }
  ]
}

```

- Can also set up an Email alert

sumo logic

Monitor Name

Frontend-Errors Increase

[View Monitor](#)

Trigger Condition

Greater than or equal to 100.0 in the last 5 minutes

Time Range

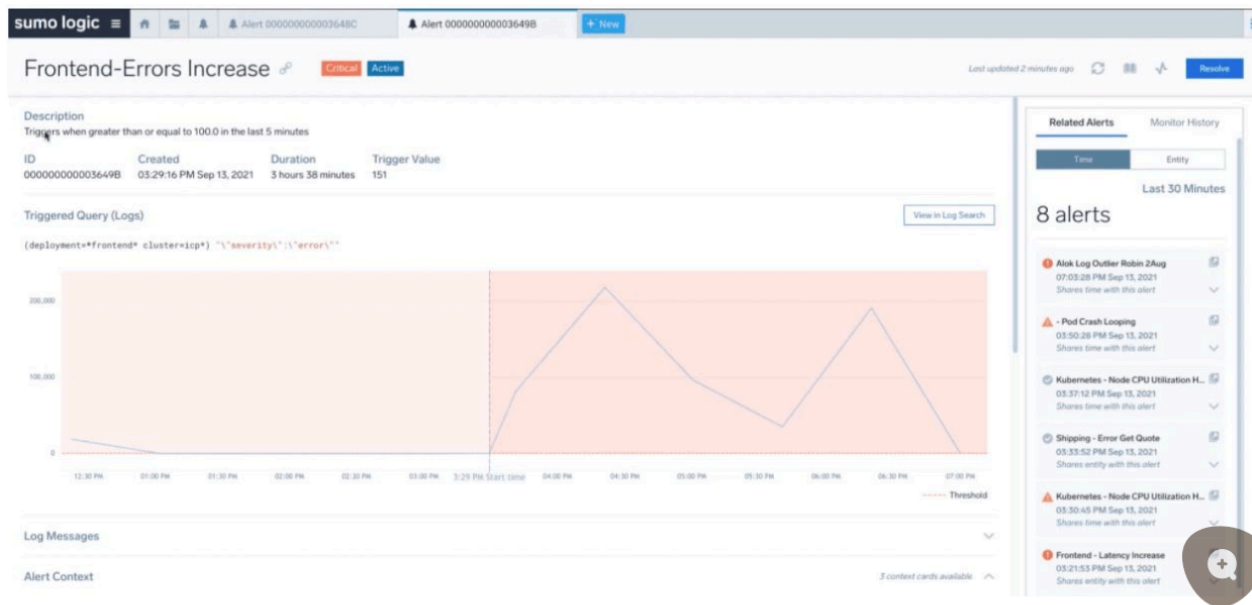
09/22/2021 04:31:25 PM PDT to 09/22/2021 04:36:25 PM PDT

Message

[View Alert](#)

- **View Alert** will take the user to the **Alert** page

Alert Page



- The **Alert details** section provides:
 - A chart to **visualize the alerting KPI** before and during the alert.
 - A **table** with the **raw data** that triggered the alert.
 - **Related alerts** firing in the system around the same time.
 - The **history of the given alert** being fired in the past.
 - Basic details about the alert like when it was fired and what triggered it.

Webhook connections

- Send **alerts to third-party** applications

Alert Variables

- **Variables are used as parameters** that allow you to customize the JSON payload object of your alert notifications.

Context Cards

Types of Context Cards

- Depending on the **type of data** the alert was based on, metrics or logs, you'll see different context cards

▼ Log Fluctuation Card

- Identify changes in **log patterns/signatures** that might help explain the underlying issue

▼ Anomaly Card

- Find **anomalies in metrics data** reported by various related entities over time

▼ Dimensional Explanation Card

- Analyze **app log data** and **surface dimensions** that might explain the **alert condition**

▼ Benchmark Card

- **Surface abnormalities** in data reported by various entities when **compared with other Sumo cohort**

Anatomy of the Context Card

- **Heading section**
 - Displays the **name** of the card and a **short description** of what it does
- **Summary section**
 - Displays a summary of the discovered data or signatures
- **Click to view details**
 - Provides an arrow option to expand or collapse the details
- **Click to open logs**
 - Provides links that **open the log messages** that are mapped to the given signature