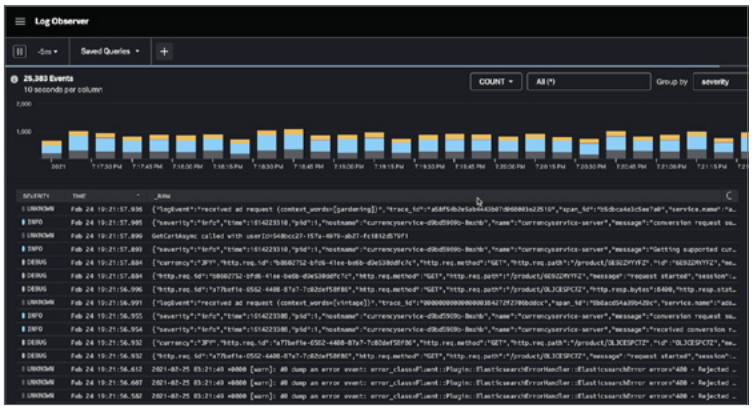
Splunk Log Observer

Fast, intuitive log investigations for DevOps teams

Key Benefits

- **Better customer experience:** Harness the power of observability to quickly understand the observed customer experience and why it's occurring.
- **Improved developer productivity:** No-code log exploration reduces time to learn new products and provides insights to identify problems as they unfold in real time.
- **Shorter downtime episodes:** Connect application performance and infrastructure monitoring with logs in context. A single click reveals what's going on and why.
- **Enhanced log management:** Infinite logging allows DevOps teams to helm log management, lowering overall logging cost and optimizing control over their organization's log use.

Splunk Log Observer is the industry's leading logging solution designed for DevOps. Part of Splunk Observability Cloud, Splunk Log Observer is designed to enable DevOps, SRE and platform teams to understand the "why" behind application and cloud infrastructure behavior. Investigations are intuitive, require no additional coding and empower teams to readily combine real-time log data with metrics and traces to gain immediate insights.



Architecture

Integrated observability data and experience: Splunk Log Observer is part of the Splunk Observability Cloud, which provides a single, consistent user experience across all metric, trace and log data. Use one seamless and streamlined workflow during the whole life cycle of issues for monitoring, troubleshooting, investigation and resolution. Whether you're a frontend developer who needs to know what end customers are experiencing, a backend developer building the most performant APIs and services or an SRE who's frequently on call, you get the context-rich insight you need to collaborate with the people who can quickly resolve outages. You can also leverage deep insights to proactively prevent issues from arising.

Infinite logging: With Splunk Log Observer, you get maximum control over your logging data. Quickly add logging sources, like Kubernetes, AWS Cloudwatch, CGP Stackdriver, OpenTelemetry sources, FluentBit/Fluentd, Splunk forwarders and others. Sophisticated pipeline management lets you store all data while indexing and adding context for higher value data. Combined, you get context-enriched logs with the ability to handle all your logs in an efficient, cost-effective manner.

Key capabilities

Intuitive no-code log exploration: Point and click your way through log investigations. In-context log data is easy to search, filter and visualize, and related content offers single-click access to metrics and traces correlated to log data.

Live tail: Get a real-time view of logs easily sorted based on attributes you define. Offering to sample real-time logs makes readability even easier.

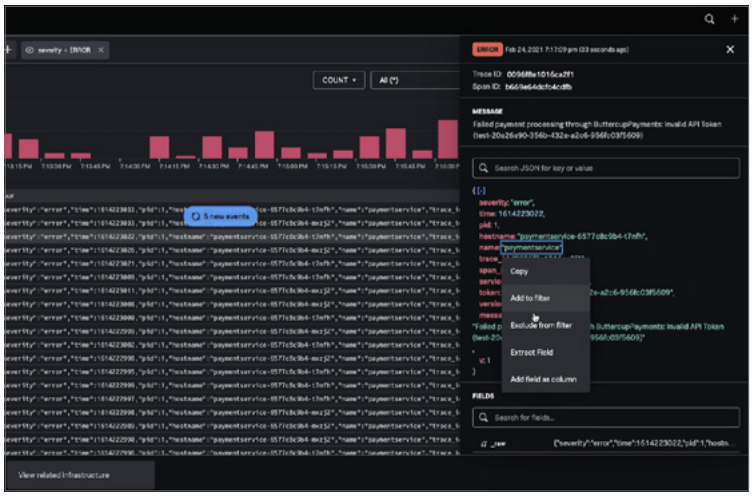
Save and share queries: Save useful queries and enable others to use those queries to accelerate their log investigations.

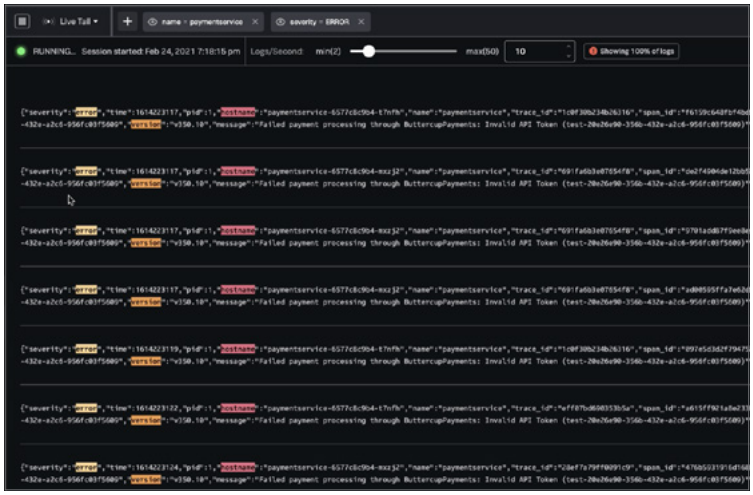
Integrates your DevOps-driven logging sources: Connect to AWS Cloudwatch, OpenTelemetry, GCP Stackdriver and Kubernetes in minutes using a wizard. Splunk Log Observer shapes data from these formats, making them simpler to searc h, explore and contextualize related metrics and traces in the Splunk Observability Cloud.

Related content: As part of the Splunk Observability Cloud, logs, metrics and traces work in correlation with each other. Related content pointers are provided during log exploration, so your investigations are intuitive — with no dead-ends.

Infinite logging: Splunk Log Observer permits you to store all your logs. High-value logs are indexed, shaped with context about the data and are ready for real-time analysis, while lower-value logs are placed in a customer-owned storage location.

Pipeline management: Add additional context to logs, extract fields and apply actions to provide the proper treatment for logs so they can be easily explored.





Get started today with a free trial of Splunk Infrastructure Monitoring.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

21-18281-Splunk-Log Observer-PB-103