splunk> turn data into doing®

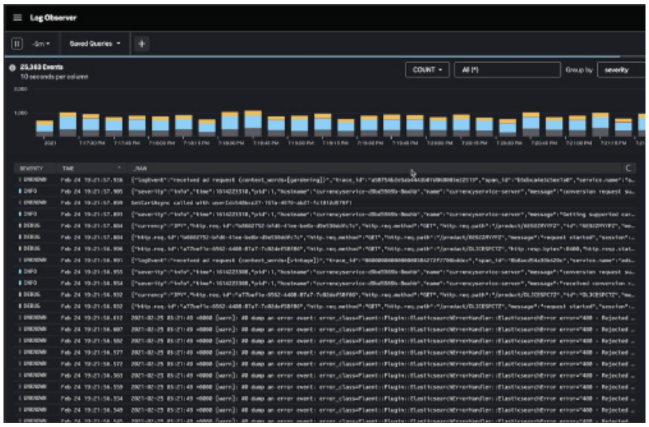
PRODUCT BRIEF

Splunk Log Observer

Fast, intuitive log investigations for DevOps teams

Key Benefits

- **Better customer experience:** Harness the power of a unified observability solution to monitor mission critical applications and quickly understand and optimize customer experience.
- **Improved developer productivity:** No-code log exploration reduces time to value 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 easily manage logs, lowering overall logging cost and optimizing control over their organization's log use.
- **Better cross-team collaboration:** Build an operational center of excellence and address any use case with all of your metrics, trace, event and log data centralized on Splunk.



```
UNKNOWN  Feb 24 19:21:57.936  {"logEvent":"received ad request (context_words=[gardening])","trace_id":"[illegible]","span_id":"[illegible]","service.name":"a…
INFO     Feb 24 19:21:57.905  {"severity":"info","time":1614223318,"pid":1,"hostname":"currencyservice-[illegible]","name":"currencyservice-server","message":"conversion request su…
UNKNOWN  Feb 24 19:21:57.899  GetCartAsync called with userId=[illegible]
INFO     Feb 24 19:21:57.893  {"severity":"info","time":1614223318,"pid":1,"hostname":"currencyservice-[illegible]","name":"currencyservice-server","message":"Getting supported cur…
DEBUG    Feb 24 19:21:57.884  {"currency":"JPY","http.req.id":"[illegible]","http.req.method":"GET","http.req.path":"/product/[illegible]","id":"[illegible]","me…
DEBUG    Feb 24 19:21:57.884  {"http.req.id":"[illegible]","http.req.method":"GET","http.req.path":"/product/[illegible]","message":"request started","session":…
DEBUG    Feb 24 19:21:56.996  {"http.req.id":"[illegible]","http.req.method":"GET","http.req.path":"/product/[illegible]","http.resp.bytes":8400,"http.resp.stat…
UNKNOWN  Feb 24 19:21:56.991  {"logEvent":"received ad request (context_words=[vintage])","trace_id":"[illegible]","span_id":"[illegible]","service.name":"ads…
INFO     Feb 24 19:21:56.955  {"severity":"info","time":1614223308,"pid":1,"hostname":"currencyservice-[illegible]","name":"currencyservice-server","message":"conversion request su…
INFO     Feb 24 19:21:56.954  {"severity":"info","time":1614223308,"pid":1,"hostname":"currencyservice-[illegible]","name":"currencyservice-server","message":"received conversion r…
DEBUG    Feb 24 19:21:56.932  {"currency":"JPY","http.req.id":"[illegible]","http.req.method":"GET","http.req.path":"/product/[illegible]","id":"[illegible]","me…
DEBUG    Feb 24 19:21:56.932  {"http.req.id":"[illegible]","http.req.method":"GET","http.req.path":"/product/[illegible]","message":"request started","session":…
UNKNOWN  Feb 24 19:21:56.612  2021-02-25 03:21:49 +0000 [warn]: #0 dump an error event: error_class=Fluent::Plugin::ElasticsearchErrorHandler::ElasticsearchError error="400 - Rejected …
UNKNOWN  Feb 24 19:21:56.607  2021-02-25 03:21:49 +0000 [warn]: #0 dump an error event: error_class=Fluent::Plugin::ElasticsearchErrorHandler::ElasticsearchError error="400 - Rejected …
UNKNOWN  Feb 24 19:21:56.582  2021-02-25 03:21:49 +0000 [warn]: #0 dump an error event: error_class=Fluent::Plugin::ElasticsearchErrorHandler::ElasticsearchError error="400 - Rejected …
UNKNOWN  Feb 24 19:21:56.577  2021-02-25 03:21:49 +0000 [warn]: #0 dump an error event: error_class=Fluent::Plugin::ElasticsearchErrorHandler::ElasticsearchError error="400 - Rejected …
UNKNOWN  Feb 24 19:21:56.572  2021-02-25 03:21:49 +0000 [warn]: #0 dump an error event: error_class=Fluent::Plugin::ElasticsearchErrorHandler::ElasticsearchError error="400 - Rejected …
UNKNOWN  Feb 24 19:21:56.563  2021-02-25 03:21:49 +0000 [warn]: #0 dump an error event: error_class=Fluent::Plugin::ElasticsearchErrorHandler::ElasticsearchError error="400 - Rejected …
UNKNOWN  Feb 24 19:21:56.558  2021-02-25 03:21:49 +0000 [warn]: #0 dump an error event: error_class=Fluent::Plugin::ElasticsearchErrorHandler::ElasticsearchError error="400 - Rejected …
UNKNOWN  Feb 24 19:21:56.554  2021-02-25 03:21:49 +0000 [warn]: #0 dump an error event: error_class=Fluent::Plugin::ElasticsearchErrorHandler::ElasticsearchError error="400 - Rejected …
UNKNOWN  Feb 24 19:21:56.549  2021-02-25 03:21:49 +0000 [warn]: #0 dump an error event: error_class=Fluent::Plugin::ElasticsearchErrorHandler::ElasticsearchError error="400 - Rejected …
```

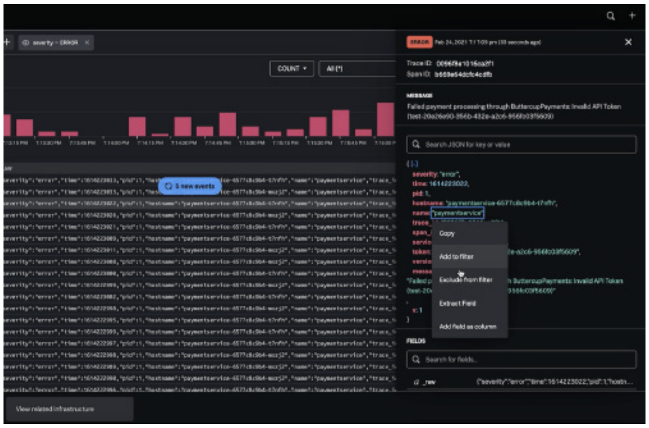
Splunk Log Observer is the industry's leading logging solution for DevOps, extending the value of a team's existing Splunk solutions. It's designed to enable DevOps, SRE and platform teams to understand the "why" behind application and cloud infrastructure behavior. Investigations are intuitive, require 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.

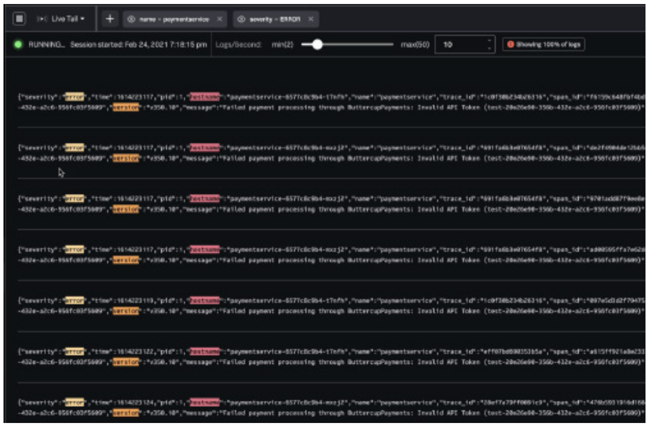
Log Observer Connect: Consolidate your tools. Leverage the power of Splunk Enterprise data in Splunk Observability Cloud. Log Observer Connect lets observability users explore the data you're already sending to your existing Splunk instances with Splunk Log Observer's intuitive no-code interface for faster troubleshooting, root-cause analysis and better cross-team collaboration.

Key capabilities



Trace ID: 0096f8e1016ea2f1
Span ID: b659e54dcfc4cdfb

MESSAGE
Failed payment processing through ButtercupPayments: Invalid API Token (test-20e26e90-356b-432e-a2c6-956fc03f5609)



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 — search, 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. You can also explore related content from Splunk Enterprise in other Splunk Observability Cloud products such as Splunk Infrastructure Monitoring and Splunk APM.

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 the most out of your existing Splunk data by connecting it to your observability workflow via Log Observer. Get started today with a free trial of Splunk Observability Cloud.

For more information check out our docs site

Get started today with a free trial of Splunk Observability Cloud.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com