splunk>

GETTING STARTED GUIDE

GETTING STARTED WITH SPLUNK® FOR APPLICATION MANAGEMENT

A step-by-step guide to improving application insight

Introduction

Applications are the lifeblood of your organization. They support the processes that engage your customers, partners and employees. And all of these applications need to deliver an exceptional experience—because an app that's down can cost your organization thousands of dollars per minute.

This guide outlines some of the insights you can gain by using Splunk software to monitor your application stack and troubleshoot problems that affect uptime and performance.

Benefits of better application management

Building great apps take more than intuitive design. They need to be reliable, available, responsive, error-free and capable of scaling. It's also important to know what aspects of your application are used frequently. That way, business and development teams can prioritize new features and enhance application design, and DevOps teams can provide sufficient capacity relative to demand.

When an application fails, it's often because of changes that took place in the application or underlying infrastructure. Two of the most common examples:

- A bug is introduced into an application
- Configuration changes are made to underlying infrastructure

Your best defense is to inventory all the components of both the application and the infrastructure that supports it. That way, you can quickly triage problems, monitor the entire stack and understand the impact of usage—not only with application execution, but of the infrastructure as well.

Getting started

If you're already using Splunk software to monitor your key infrastructure components, you're ahead of the game. Many of the data sources you're collecting and analyzing are the same ones you need for application monitoring and troubleshooting.

When you're identifying data sources:

- **Think about your developer, operations and business teams**
  - **Developers** want to understand how apps are being used and where there are performance problems, so they can quickly isolate bugs and deliver new and improved apps.
  - **Operations teams** are often the "first line of defense" for app issues, as they need to quickly triage and isolate problems. These stakeholders want to proactively monitor applications and infrastructure to find leading indicators of potential issues.
  - **Business stakeholders** want to understand whether applications are delivering against service-level agreements and key performance indicators.
- **Accelerate onboarding and analyzing your data with Splunk Apps**
  - There are hundreds of apps on Splunkbase that you can install to your Splunk instance. Search for the key infrastructure types you have, as well as other IT operations and APM tools.
  - Installing apps is quick and easy. The interface guides you through the steps, and many apps have wizards that help you collect and index data.
- **Support all application platforms**—more apps are being delivered through web browsers and on mobile platforms. Gaining insight into the end user experience is important, and you should ensure you're collecting the right data sources. For example, mobile SDKs are an effective way to mine machine data from mobile apps.
- **Get insights into supporting infrastructure**—some application components are accessible to you; others—such as data from a PaaS- or SaaS-based application component—aren't. You may not gain insight from within the component, but you can use wire data to gain insight on transaction length, type and payload.

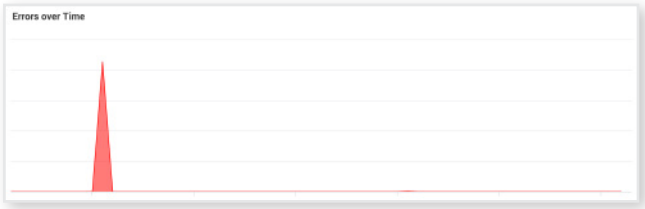
Data Sources Table

Data Type	Where to Find It	What It Can Tell You
OS, virtualization and container logs and metrics	Syslog via management interfaces, APIs, etc.	Health, performance and availability of underlying infrastructure
Web and application server logs and metrics	Log4j, popular web servers (such as Apache), application servers (such as WebSphere and NGINX)	Usage, clickstream insights, relationships between application components, configuration changes
Database logs and metrics	Logs for databases	Usage, database errors, configuration changes, specific queries and source of queries
Network and other infrastructure logs	Network device managers, message queues, other device logs	Additional insight on availability, performance and usage of supporting infrastructure
Application logs	Defined by application developers	Anything that developers want to log that helps them assess app execution. Developers evolve their logging over time to include key value pairs, so they can associate usage and other attributes
Mobile client data	Mobile app SDKs	Insight on app usage, performance, crashes and other items from the perspective of the mobile app user
Wire data	Wire data probes (software based)	Communication between app component, application response times and payload of applications (even when you may not have direct visibility to some app components)
APM data	APM tools	End user response time, byte-code level insight on app execution, JVM, .NET, php, node.js server performance metrics
API components	API data	Usage, performance and payload of APIs

Using Splunk for Application Management

1) Get Baselines of Infrastructure Performance

- **What to look for:** Errors in log files
- **Why?** You can perform real-time analysis that provides immediate insight into problems. Additionally, log files often provide insight into why the error occurred
- **Example search:** ... ERROR | timechart count



---

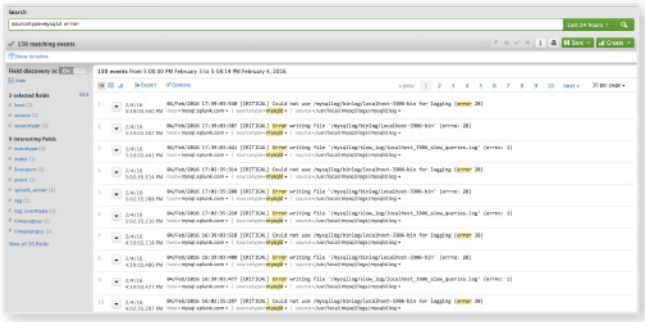
2) Monitor for Application Usage Trends

- **What to look for:** HTTP status codes as a proxy for number of web pages served
- **Why?** You can get insight into when, who and what people are doing with your application
- **Example search:** sourcetype=access* | timechart count

---

3) Monitor Application Transactions

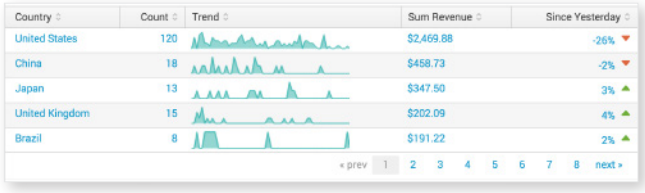
- **What to look for:** Correlate timestamps of various application and infrastructure components to assess response time and status
- **Why?** You can understand performance as well as identify downtime
- **Example search:** sourcetype=access* | timecharg avg(time_taken)



---

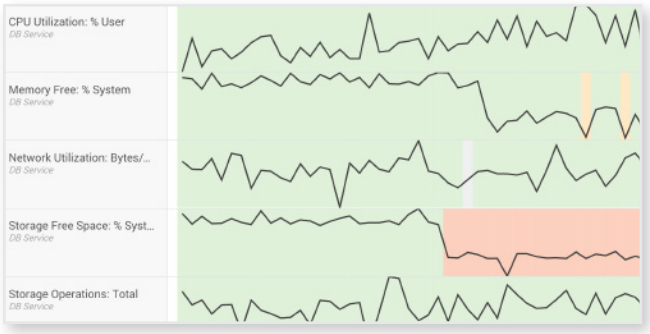
4) Add User and Customer Context

- **What to look for:** Correlation between a customer ID, transaction ID and a customer name in an external data source
- **Why?** This enables you to add business context to dashboards and alerts, which line of business (LOB) stakeholders find especially useful
- **Example search:** .... | sum(revenue)



4) Measure and manage to SLAs and KPIs

- **What to look for:** KPIs and SLAs that the business and IT are aligned on
- **Why?** Present SLAs and KPIs to prioritize alert and communication application outcomes to business stakeholders



CUSTOMER SPOTLIGHT

ENERNOC

EnerNOC is a Boston-based provider of energy intelligence software that helps its customers—electric power grid operators, businesses and utilities—optimize energy use. The company's Energy Intelligence Software (EIS) platform continuously monitors real-time energy data, including data from more than 30,000 energy sensors and smart meters. The company had built an application to analyze data from system and web logs, but it was difficult to scale and frequently crashed.

The firm now uses Splunk software to monitor consumption and output for demand-response events while tracking performance of the data-collection infrastructure to meet SLAs. With views into the platform's public and private cloud components, administrators can perform workload and user analytics in real time and over large historical data sets.

Splunk Enterprise monitors core platform services, ensuring that data is processed, with high error-free throughput and near zero latency. In addition, Splunk Enterprise plays a vital role in creating a dynamic DevOps environment. Using Splunk Enterprise for real-time metrics, EnerNOC's developers and QA team test code in staging environments to gauge functionality, scalability and performance under peak loads. The DevOps team then relies on the same Splunk dashboards to further refine applications the moment they are placed into production to preserve reliability and customer satisfaction.

Summary

Effective application management isn't just a "nice to have"—it's critical to the success of your organization. Using this guide and data sources you may already be analyzing, you can quickly optimize your application uptime, performance and delivery.

Try Splunk Cloud or Splunk Enterprise for free or learn more about application delivery.
Already have Splunk? Download Splunk Apps on Splunkbase.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com