

Splunk App for Amazon Web Services

Real-time Operational Insights and Analytics for Cloud Service

The Need for Cloud Control

Organizations that run part or all of their business applications in the cloud gain immediate benefits from the elastic scaling, fast time to market and pay-as-you-go model of cloud services. However, a lack of visibility into infrastructure performance, end-user response times and utilization of application features can create blind spots for cloud application owners.

The machine data generated by your cloud instances provides a definitive record of user transactions, customer behavior, machine behavior, security threats, fraudulent activity and more. Harnessing this data provides the operational visibility critical to running your applications in the cloud and delivers the insights you need for long-term business decision making.

Traditional Approaches to Monitoring Cloud Applications

Traditional data analysis, management and monitoring solutions are simply not engineered for the cloud environment. Typically, they rely on relational databases which limit them from properly scaling in the cloud. They also require data normalization to fit predefined schemas, which makes them less adaptable to the variety of languages and data formats that proliferate in AWS environments. Lastly, many of these tools are single-purpose solutions designed to solve a particular point problem. For example a Java monitoring solution that reports on a certain aspect of the health of your application cannot be easily extended to detect end-to-end user experience issues, or tell you which errors caused critical business transactions to fail or reveal which features of your application were most used.

Enter Splunk

Splunk Enterprise is the engine for machine data. It collects indexes and harnesses the machine data generated by your infrastructure and applications—whether they are located in your datacenter or in the cloud.

Use Splunk to gain rapid visibility, insights and intelligence across your infrastructure, applications and the business. Troubleshoot application problems and investigate security incidents in minutes instead of hours or days, avoid service degradation or outages, deliver compliance at lower cost and gain new business insights. Splunk provides new levels of operational visibility, informing critical business decisions and delivering a compelling competitive advantage.

Splunk Capabilities

Universally Index Machine Data from Virtually Any Source:

Splunk indexes machine data in real time from virtually any source, format or location without custom parsers or connectors. This includes live data from your packaged and custom applications, app servers, web servers, databases, physical or virtual networks, operating systems, storage and more. Splunk

indexes data from your cloud instances as well as your on-premise instances. Splunk's distributed architecture scales to the size of your machine data—no need to establish a predefined schema or to normalize your data.

Search, Investigate, Correlate: Splunk lets you search real-time and historical machine data from one place. Splunk not only lets you correlate information across various data types by time but its powerful search language helps you link transactions across multiple systems. It allows you to persist information about your cloud instances even after they have scaled down, so you have the complete historical picture for incident investigation. Powerful statistical and reporting commands let you detect anomalies, eliminate noise and update transaction counts and durations.

Add Knowledge: Splunk automatically discovers knowledge from your machine data at search time so you can start using new data sources immediately. You can also add context and meaning to your machine data by identifying, naming and tagging fields and data points. Add information from external sources such as asset management databases, configuration management systems and user directories, thereby providing context for your operational data and making it usable for driving business decisions.

Monitor and Alert: You can turn searches into real-time alerts that automatically trigger actions such as sending automated emails, running scripts, posting to RSS feeds, sending SNMP traps to your system management console or generating service desk tickets. You can base alerts on a variety of thresholds, trend-based conditions and complex patterns (such as abandoned shopping carts, brute force attacks and fraud scenarios).

Report and Analyze: Report builder lets you quickly build advanced charts, graphs and custom dashboards that show important trends, highs and lows and summaries of top values and frequency of occurrences. Drill down from anywhere in the visualizations to the raw events. Save reports, integrate them into dashboards and create PDFs on a scheduled basis to share with management, business users or other stakeholders.

Scale to Largest Infrastructures: Scale your Splunk installation from a single commodity Windows, Linux or Unix server, to index the most complex multi-geography, multi-datacenter infrastructure, generating tens of terabytes of data per day. The Splunk architecture is based on MapReduce and scales linearly across commodity servers to unlimited data volumes.

Secure Access to Data by Role: Information security and compliance requirements govern how far a given user's access to information can extend. Splunk gives authorized employees the view of the data they need, based on their role and usage need—whether for investigations, reports and dashboards, or analysis to improve IT operations and gain valuable business insights.

Customer Success

Cie Games

Developers of Car Town, currently ranked #12 among social games by monthly active users, leverage Splunk to model and monitor user experience. Cie Games run their entire operations in Amazon Web Services and use Splunk's real-time dashboards to know exactly what's happening within the game at any time. Splunk is used to calculate the new user funnel, user retention rates, detect monetization triggers, monitor the successful launch of new features or content, figure out which ads and promotions are most compelling and even calculate royalty payments from promotions to various automotive brands.



"For us it wasn't a matter of proving ROI with Splunk. The value is obvious. It's incredible that we're able to analyze so much data so quickly. We can really ask Splunk almost any question about our business and get an answer in minutes. We can truly say we're a data driven business. Splunk gives us that ability—and in doing so, delivers a strategic advantage."

Matt Winkler,
Monetization Analyst, Cie Games

TransGaming

TransGaming is the global leader in the deployment and distribution of electronic entertainment across multiple platforms. Working with the industry's leading developers and publishers, TransGaming enables and distributes their games for Smart TV set-top boxes, Mac computers and Linux/CE platforms. TransGaming uses Splunk to generate operational and business analytics around GameTree TV. This on-demand smart TV gaming platform runs entirely on AWS and offers an unparalleled user experience on the next generation of set-top boxes and connected consumer electronic (CE) devices. Splunk is used by developers extensively to locate root causes of user experience issues and by business users for operational analytics around game usage, unique users, game play times and user experience.



"Splunk gives us confidence and helps us get answers quickly. They provide much needed visibility into our operations—helping not only developers but also business users with critical and unique insights."

Roberto Monge,
Chief Architect, TransGaming Inc.

Shopify

Shopify, a large SaaS online retail platform, uses Splunk extensively to monitor on-premise and AWS based instances of their nginx/Ruby on Rails application. They use Splunk for centralized logging, operational troubleshooting and get extensive insights into their application data. They also use Splunk for various fraud detection and avoidance mechanisms helping to reduce the processing cost of fraudulent registrations.



"We had zero insights into our data before Splunk. Our very first install reduced the time required for a common customer support function by 87% ! "

Dale Neufeld
Network Security Ninja, Shopify

Optimizely

Optimizely is a dramatically easier way for you to improve your website through A/B testing. Optimizely runs on AWS and uses Splunk extensively as part of its service to aggregate and process results of website testing.



"We investigated many other options to aggregate and process results, but none came close to the scale or speed of Splunk."

Features	Splunk Free	Splunk Enterprise
Maximum indexing volume per day	500MB	Unlimited (based on license)
Universal, real-time indexing	•	•
Real-time and historical search	•	•
Reporting	•	•
Knowledge mapping	•	•
Dashboards	•	•
Monitoring and alerting		•
Distributed search		•
Data forwarding and receiving	•	•
Role-based access controls		•
Single sign-on		•
Developer APIs	•	•
Community Apps	•	•
Enterprise Apps		•
Standard support	•	
Enterprise support		•

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.