Search Guard Signals - Elasticsearch Alerting for Free

Daniel Gleim · 2025-11-19

Search Guard Signals - Elasticsearch Alerting for Free

Monitoring important changes in your data is essential—whether you're running a production Elasticsearch cluster or using it in a smaller, personal project. **SearchGuard Signals** is a **free alerting solution** for Elasticsearch and Kibana that helps detect and notify you of events that require your attention.

Stay Informed with Flexible Alert Rules

With Signals, you can define alert rules—known as *watches*—that monitor your Elasticsearch data and trigger notifications when certain conditions are met. These conditions can be simple, such as a value crossing a threshold, or more advanced, like detecting unusual patterns. Whether you are working with logs, metrics, or custom application data, Signals helps you catch issues as they happen.

One of Signals' key features is its flexibility in delivering notifications. Alerts can be sent through a variety of built-in channels, including email, Slack, PagerDuty, JIRA, webhooks, or even back into an Elasticsearch index. You can define multiple actions per alert and assign different severity levels to control how and when notifications are sent. For example, a warning might trigger a Slack message, while a critical alert could also send an email and open a PagerDuty incident. Signals can also notify you when a previously triggered condition is resolved.

Built-in Security and Easy Integration

Signals is fully integrated into the SearchGuard plugin. This allows alerting and security features to work together using the same role-based access control. You can manage who is allowed to create or edit

alerts, and rely on existing security settings like tenant isolation or field-level access control. Since Signals is bundled with SearchGuard, no additional installation is required.

User-Friendly Interface

Setting up alerts with Signals is straightforward. You can create and manage watches using the Kibana interface or the REST API. The Kibana UI offers both visual and text-based modes—either build conditions using a block-based editor or work directly with JSON. This flexibility makes it easy to set up alerting, whether you prefer a graphical workflow or need to automate tasks through scripts.

Conclusion

SearchGuard Signals is available under the Apache 2.0 license and is **free to use**, whether you're working with a small test cluster or a larger Elasticsearch environment. With built-in connectors, a user-friendly interface, and full integration into SearchGuard, Signals provides a reliable and accessible way to add alerting to your Elasticsearch setup—without the need for extra tools or licenses. Download Search Guard today and experience the future of Elasticsearch alerting!

This article was published on the Search Guard blog: https://search-guard.com/blog/search-guard-signals-elasticsearch-alerting-for-free/