graylog

MAXIMUM UPTIME, PERFORMANCE, AND SECURITY WITH GRAYLOG

Category:
IT Ops platform

Industry:
Non-profit social services

Looking For:
Comprehensive solution, cost-effectiveness

Size:
1,400 employees

Every organization relies upon optimized and secure servers. Today's global business environment includes an often large, complex, and diverse network of hosts, often worldwide. In the cases where the organization is in the business of providing data, uptime, performance, security, 24 x7 is critical as is cost-efficiency of the server network.

"One of the most important shifts of this decade is the rise of interconnected data across distributed systems. This explosive growth not only sparked the need to rethink cloud and global IT strategies, but it also disrupted traditional development, DevOps and IT Ops practices."

Source: DevOps.com

EXAMPLE SITUATION

- Global internet company doing advanced research in social services areas.
- The company relies on a large, complex, and diverse network of hosts (hundreds of servers worldwide) to test the advanced algorithms, developed by company scientists, on a scale large enough to map to the usage patterns of mass populations.
- Uptime, performance, security, and cost-efficiency of the server network are critical to delivering data ontime.
- Hosts all required comprehensive monitoring to ensure they performed up to specification, driving the necessary services.
- The team relies on a trove of unique test data and sophisticated algorithms developed in pursuit of the company charter.
- Detecting, containing, and mitigating security issues and the resulting impact is challenging on a large and distributed host array.

  As a non profit company, cost is also an issue.

GRAYLOG IN ACTION

To ensure maximum uptime and peak performance while keeping costs manageable, IT teams in nonprofits and other similar industries (e.g., education, government, churches, etc.) rely on Graylog to ingest petabytes of data on a daily basis, making it easy to visualize and correlate across contexts.

SAVE TIME. REMOVE UNCERTAINTY. TRUST THE DATA.

To efficiently monitor the complete host network, the Graylog administrators implemented a plan for monitoring their infrastructure to make sure everything is operating correctly. The plan included a tracking dashboard that combines multiple

searches for their daily analysis of the complete host network.

For example, an indicator on one of the routers from green to red, the system administrator notes the spike on the widget charting all routers in the infrastructure and immediately drills down into the data, identifies the device causing the issue. The next step is to add the source ID into the parameter field and Graylog will display the results in a new tab. The sys admin clearly sees the root cause of the issue and quickly resolves it before there is any noticeable impact on company operations.

In these types of scenarios, companies have found that the dashboards significantly reduce the time to resolve application or service failure. Faster resolution brings the added benefit of better host maintenance, which extends the life of the host, resulting in reduced replacement costs and subsequently capital expenditure. While every company wants to save money, this is particularly useful for non profit companies, education, government, etc. where the bottom line is scrutinized to stretch every dollar.

LOWER OPS COSTS WITH ALERTS

The team also analyzes historical log data on a regular basis to identify potential areas of slowdown and system failures and set up alerts in place for anticipated issues. With Graylog, the team can take those logs and give correlated events across a diverse network of hosts and put in place basic alerting as well as correlating alerts when the hosts are talking across two different data streams.

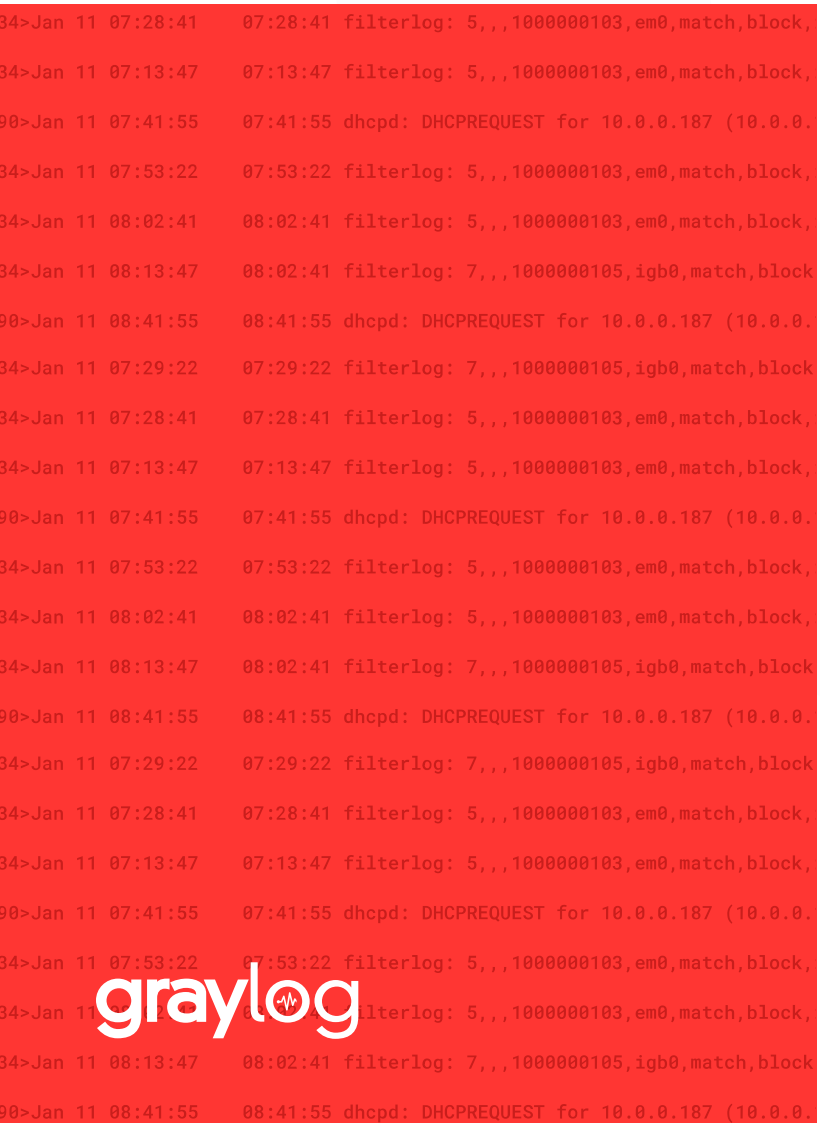
For any company, system security is paramount, and in this case scientific research is a competitive field. It is critical that the data is protected and this requires tight round-the-clock system security. The IT team wants to know when there is any activity indicating a breach.

Graylog's correlation engine can help find that type of activity and automatically trigger alerts in real time. These alerts come in multiple formats (e.g., text messages, emails and Slack messages, or even JIRA tickets). Alerts ensure that the team can take immediate action and protect the network and systems.

The team has put a holistic security monitoring and analysis strategy in place. With the added benefit of audit logs and role-based controls to demonstrate compliance in reports and monitoring privileged insiders in straightforward manner, Security is more comprehensive. Because Graylog can ingest nearly limitless log formats and sources — Syslog, GELF, AWS, Logstash, CEF, JSON, netflow, and of course raw text, among others it provides much more holistic security analysis than traditional SIEM tools.

SUMMARY

A globally-distributed array of computational hosts requires a flexible and comprehensive log management solution for monitoring as well as a solid overall security posture. Thanks to Graylog's support for the highest data volumes, exceptional performance, and straightforward customizability to suit specific needs and contexts, companies are able to explore data and lower ops costs by improving the security and stability of company IT assets and services.



graylog

ABOUT GRAYLOG

Graylog is a centralized log management platform for companies seeking seamless data collection and normalization from any data source, faster analysis, and greater affordability. Purpose-built for modern log analytics, Graylog removes complexity from IT operations, data exploration, error tracing, and threat hunting so you can quickly and easily find meaning in data and take action faster. Our customers enjoy increased productivity, improved performance, secure systems, and an empowered team.

www.graylog.com
sales@graylog.com

1301 Fannin St, Ste. 2140
Houston, TX 77002