From left in the photo:
Kazutaka Yokoyama
General Manager, Server Infrastructure Division

Yudai Kaneda
Group Leader, Infrastructure Server Platform Group
Server Infrastructure Division

SUCCESS STORY

OBSERVABILITY | AUTOMOTIVE AND MANUFACTURING

Hino Computer System centralizes network log data for full operational visibility

At Hino Computer System Co., Ltd. ("Hino Computer System"), the system development company of the Hino Motors Group, log data output from various network devices across the main office and factory sites was scattered across multiple locations, making it difficult to detect faults and respond to incidents in a timely manner. To address this, the company decided to overhaul its log monitoring platform. The goal was to enable administrators to explore the data in greater detail, accelerating the identification and analysis of problem areas. As a result, the company centralized its siloed log data and made it actionable and accessible within a secure environment, enhancing overall observability.

Reduced log search time from 30 minutes to just seconds

Elastic Cloud enabled the company to centralize log data, which was previously scattered across devices in multiple business units, into the Server Infrastructure Division at the head office. This dramatically shortened log search times.

Created a secure environment via a private network connection with Microsoft Azure

By connecting to Microsoft Azure over a private network, the company was able to centralize its log data within a secure environment without exposing it to the internet.

Achieved “data democratization” and autonomous data use by on-site teams

The implementation of Elastic Cloud enabled “data democratization,” giving teams across departments the ability to access and use data independently, without relying on centralized control.

The ability to respond to incidents was hindered by network logs being scattered across multiple locations

Hino Computer System is a system subsidiary of Hino Motors, and its Corporate Server Infrastructure Division supports the group's overall network infrastructure, including security environments. However, as the group's business expanded, the network environment grew more complex, and the ability to grasp system load conditions and manage logs across multiple departments had almost reached its limits.

Yudai Kaneda, leader of the Infrastructure Server Platform Group in the Server Infrastructure Division, explained the previous infrastructure management platform, saying, "Log information was collected and stored individually in each system, but they essentially remained scattered across the servers. Because of that, to determine what had happened and where, we first had to access servers and devices in multiple locations and gather the logs."

When an incident occurs, it is essential to identify the cause as quickly as possible. However, under the previous infrastructure management platform, just collecting log data scattered across systems was time-consuming, and the system used to analyze it responded slowly. Kaneda recalls, "It took 20 to 30 minutes just to analyze one hour of logs and display the results."

In addition, storing large volumes of log data long-term across multiple servers was difficult. Older logs were sometimes moved to other media or, in the worst cases, overwritten. As a result, referencing and analyzing past logs during incidents was extremely challenging.

Elastic's flexibility and scalability stood out

To overcome these challenges, the company began evaluating Elastic toward the end of 2024. During the selection process, the team also compared solutions from other vendors. Elastic was ultimately chosen for its extensive track record in log management and its strength as a platform capable of performing high-speed searches across massive datasets. A decisive factor was its capability to store hundreds of gigabytes of daily network logs long-term at low cost while still enabling immediate search.

Elastic's flexibility and scalability were also critical. Kazutaka Yokoyama,

The scalability of Elastic Cloud, which allowed us to start small and expand as needed, was a major advantage.

Kazutaka Yokoyama
General Manager,
Server Infrastructure
Division

elastic

general manager of the Corporate Server Infrastructure Division, recalls, "The ability to customize dashboards and freely make the information we needed visually accessible was an advantage not found in other packaged products. It also aligned with our approach of starting small and expanding the scope once we saw success."

Meeting strict security requirements for log data management was another important consideration. To meet Hino Motors Group's stringent security standards, placing log data in external cloud environments needed to be avoided as much as possible.

Elastic Cloud addressed this concern by connecting to the group's Microsoft Azure environment via Azure Private Link, allowing data to be transferred within a private network without traversing the internet. Kaneda explained, "The ability to build a secure environment without exposing data externally encouraged us to adopt a cloud-based solution."

Open source roots make Elastic easy to understand and work with

The implementation project progressed in three stages: building the log data platform, replacing the existing environment, and finally optimizing it. Beyond simply collecting logs, the team also devised ways to process the data so it could be used effectively in day-to-day operations. For example, they performed a series of tasks to rewrite the logs into a format that on-site engineers could understand intuitively, such as converting network logs from bytes to bits for visual accessibility.

To address the wide range of challenges encountered during development, Kaneda's team advanced the project with support from partner companies and Elastic. Elastic's extensive public documentation also proved valuable.

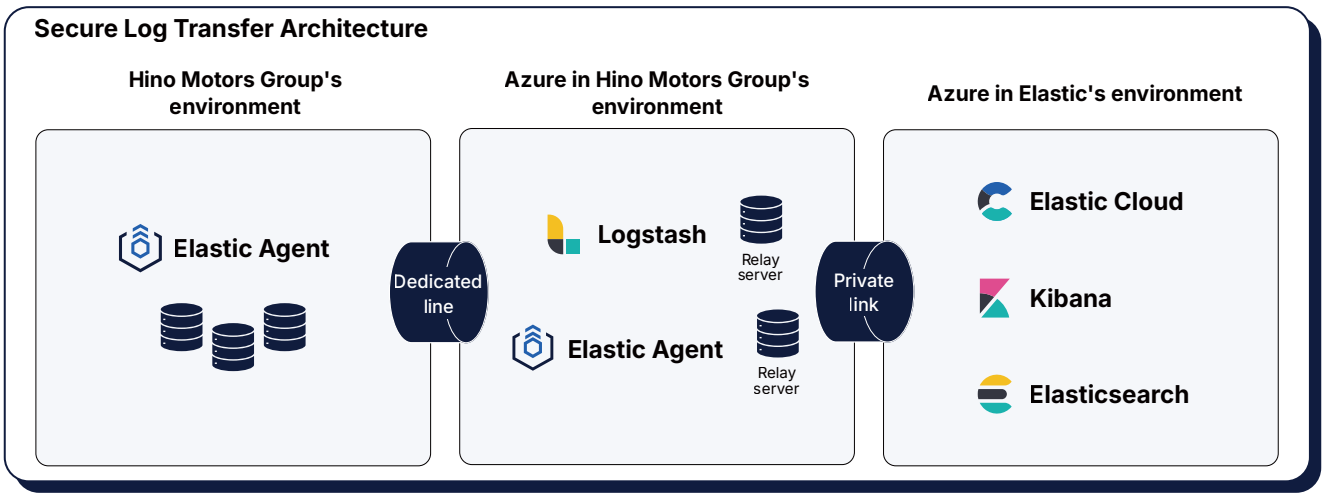
"Because Elastic has open source origins, you can dig deep and find solutions on your own," Kaneda notes. "Even when something is unclear, having a foundation that lets you rely on the community and documentation to find answers yourself is extremely reassuring when promoting in-house development."

On-site administrators can independently customize dashboards

After implementation, the most significant change was the dramatic reduction in log query time. What once took nearly 30 minutes to display, an hour's worth of logs can now be searched in seconds or a few minutes. This has led to dramatically faster response times during incidents.

"With faster queries, we've been able to significantly reduce the burden on on-site operations staff," Kaneda says. "Even when issues occur, we can instantly visualize the situation and investigate the cause — adjusting conditions as needed in order to understand it from all angles. This capability has been extremely well received."

The operation of the log management platform has also delivered major benefits. By leveraging Elastic Cloud's tiered hot/frozen architecture, the company has achieved a balance between cost efficiency and convenience. Recent data is stored on high-speed



storage, while older data is moved to low-cost object storage — an approach that is extremely logical and a great fit for managing log data, where the frequency of use drops sharply over time.

Kaneda notes, "Even with data in the cost-optimized frozen tier, we have no complaints about search speed." This allows the company to keep costs down while making it easy to conduct analysis, such as looking back and investigating incidents from three months earlier.

Running log management on Elastic Cloud has also produced benefits that Yokoyama and Kaneda did not anticipate. Initially, operations staff in each business unit used the prebuilt dashboards, but they soon began customizing them to fit their own workflows, eventually taking the initiative to develop new features themselves. Kaneda reflects, "On-site staff who weren't network engineers learned how to configure the management tools and began writing their own search queries. It truly felt like 'data democratization' was happening."

Among the features developed by on-site teams are tools that convert log data into more readable formats and automatically send email alerts when the bandwidth usage of specific devices exceeds 80%. As teams autonomously make use of Elastic's data platform, the value of the log data continues to grow.

Plans to expand beyond log monitoring

Looking ahead, the Server Infrastructure Division plans to expand its Elastic Cloud–based log data operations across the entire group, extending into additional domains. Hino Motors is preparing for a business integration with Mitsubishi Fuso Truck and Bus Corporation, and improving the efficiency of network infrastructure management after the integration is also in view.

At the same time, the company is exploring applications of rapidly advancing AI technologies. "We believe AI can be used to analyze historical log data through machine learning," Kaneda says. "For example, we expect it will enable us to take proactive security measures by comparing current network anomalies with past incident or attack patterns."

Yokoyama adds, "As part of supporting on-site teams, we plan for the Server Infrastructure Division to lead internal study sessions and training on Elastic Cloud. We also expect Elastic to continue providing the same level of support as before."

Beyond network logs, potential applications continue to expand, ranging from application-level operations management to security log monitoring and analysis through security information and event management (SIEM).

In closing, Kaneda pointed out, “Elastic’s platform continues to reveal new possibilities for us, and as we expand its use across the organization, we see even greater potential ahead.”

Elastic’s open source origins — and the wealth of technical information available online — were extremely appealing from a development standpoint.

Yudai Kaneda
Group Leader,
Infrastructure Server
Platform Group,
Server Infrastructure Division

SOLUTION

Elasticsearch

Elastic Cloud

Kibana

elastic