clearscale

aws PARTNER Premier Tier Services

Cryptocurrency Exchange Migrates to Scalable and Cost-efficient Logging and Monitoring Solution

POLONIEX

Executive Summary

Poloniex is a one-stop shop for cryptocurrency trading. Users have access to more than 400 cryptocurrencies and over 10 million NFTs through Poloniex. Everything is safeguarded by a multi-layered risk management system, which includes offline storage in air-gapped cold storage, and clients can reach customer support 24/7 with any issues related to their assets.

Recently, Poloniex decided to migrate from its legacy Splunk monitoring solution. The company wanted to take advantage of Amazon OpenSearch with Kibana, which required help from ClearScale, an AWS Premier Tier Services partner with deep cloud monitoring experience. ClearScale was able to upgrade Poloniex's log collection and analyzing capabilities, as well as reduce the company's spend in an area that had the potential to escalate quickly.

"The monitoring solution we envisioned required a combination of technologies that we didn't have the time or capacity to figure out. We left ClearScale in charge and ended up with a new data parsing process and monitoring solution that is a significant upgrade over what we were using before."

Cory Farinella, Director of Technical Operations, Poloniex

The Challenge

Prior to switching to Amazon OpenSource, Poloniex relied on a self-managed Splunk installation that was hosted in an existing AWS account. The problem was that the log analyzing solution was not optimized, particularly when it came to scalability, availability, and fault tolerance. The Splunk cluster was built on a few AWS instances, and the indices were configured improperly – logs from multiple sources were being sent to the same single index.

Poloniex also wanted to get away from Splunk licensing fees. Splunk no longer supports self-hosted installations, and it was going to take too much effort for the company to extend its license. Furthermore, the internal team was more familiar with Amazon OpenSearch. The individual who had initially configured Splunk for Poloniex was no longer with the company.

Last, Poloniex was growing fast – the company was ingesting 750-1,300 GB of log data every day and expected this figure to grow 10x the following year. Moving to a new Splunk cloud licensing plan to support that growth would incur millions of dollars in fees.

For these reasons, Poloniex was ready to build a new centralized logging solution based on Elasticsearch with data visualization built on Kibana dashboards. ClearScale stepped in and helped the client achieve its goals.

The ClearScale Solution

In place of the legacy Splunk solution, ClearScale used the latest version of OpenSearch as the log collecting and indexing core. The cloud solutions provider set up a cluster using the latest generation of AWS Graviton2 instances. This provided an optimal cost-to-performance ratio for the client. Once everything was ready, ClearScale imported data from S3 into the cluster. ClearScale decided to use the VPC-based deployment variant to ensure secure communication between Poloniex's workloads running on ECS clusters and OpenSearch.

ClearScale also deployed and configured log forwarding for the new OpenSearch solution. ClearScale engineers had to write the data parsing routines for Fluentd for each of 70+ individual logs discovered and documented by Poloniex. The reason is because the client's applications generated several types of logs in different formats. This made it difficult to come up with a unified way to send and index logs in OpenSearch without implementing a proactive sanitization and sorting process.

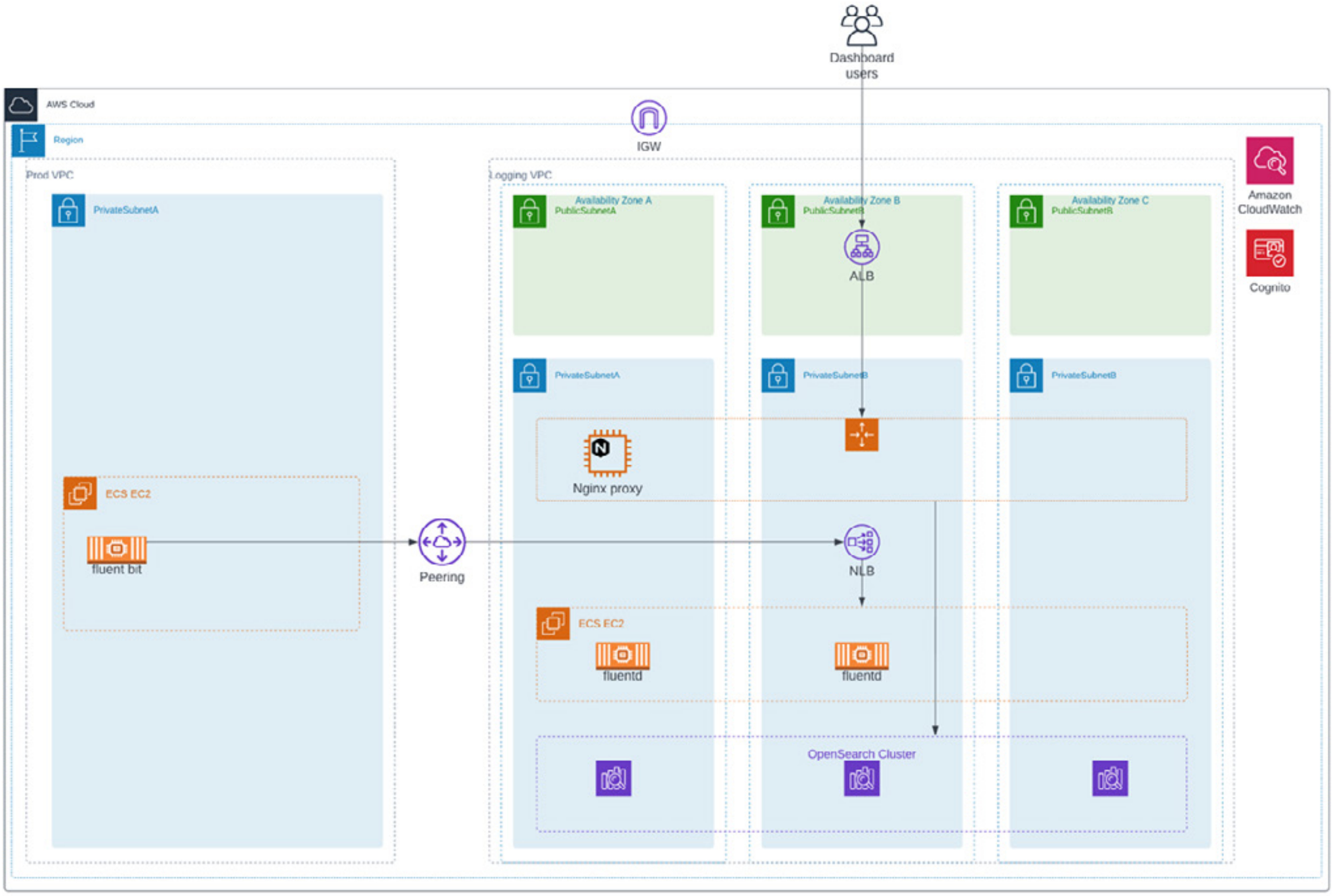
Fluentd was crucial for parsing log data "on the fly," but ClearScale had to develop a more custom solution. Fluentd is written in Ruby and is prone to crashes, which makes it a poor choice for use as a sidecar in ECS clusters. Fluentd's sibling, fluentbit, on the other hand, is written in C and is lightweight, performant, and stable. The downside of fluentbit is that it lacks the variety of data parsing and formatting capabilities of Fluentd.

That's why ClearScale developed a combined solution:

- Deployed fluentbit as a sidecar on the ECS clusters. Fluentbit, in combination with AWS FireLens driver, picks logs and sends them to Fluentd, which is deployed as a separate auto-scaling group with EC2 micro instances.
- Fluentd does all the parsing and data preparation work before passing everything on to OpenSearch as a standard, indexable JSON document.

This combined pipeline ensured maximum performance without compromising fault tolerance or scalability. Outside of the parsing pipeline, ClearScale recreated the existing Splunk dashboards, alerts, and monitoring rules.

Architecture / Diagrams



The Benefits

By switching from Splunk to OpenSearch, Poloniex was able to free itself from rigid licensing and take advantage of pay-as-you-go pricing from AWS. Poloniex now only pays for AWS resources used to run its OpenSearch cluster and helper services. The client's new monitoring and logging solution also leverages AWS managed services. Internal developers spend much less time dealing with administrative overhead, freeing them up for more important priorities.

Consequently, Poloniex is prepared to scale as needed to meet customer demand. The leadership team doesn't have to worry about growing too fast. Every component within the new monitoring solution is built with scalability in mind. As cryptocurrency adoption expands across the world, this ability to grow quickly and cost-effectively will be essential.