Threat Stack anchors disaster recovery for its authentication service on Amazon Aurora

Case Study

Executive Summary

Threat Stack migrated a key component of the Threat Stack Cloud Security Platform from a single-location deployment of Cassandra DataStax to the MySQL engine on Amazon Aurora. This allowed the agent registration service to take advantage of multi-region availability for recovery.

The Challenge

In today's world, business can't stop for power outages or natural disasters especially when it's the business of security. The Threat Stack Cloud Security Platform collects telemetry at every layer of the infrastructure stack, including applications. to help customers achieve cloud security and compliance with ease.

The solution works when agents in the customer environment send security events to the platform. Before they can enter, the events must pass an authentication service which uses secrets and keys stored in a database to validate the agent of origin and determine if it can be trusted.

The authentication service runs off a single-point deployment of Cassandra DataStax, which means that if the database goes down due to a disaster no events can enter or get validated.

The Solution

Threat Stack rebuilt their authentication service on Amazon Aurora, which allowed them to establish a secondary replica in a different region. Now, in the event of a disaster, they can easily promote the secondary to act as the primary. The team used the migration as an opportunity to include improved functionality to their authentication service as well.

> "Our customers rely on Threat Stack for security and compliance in their cloud infrastructure, so availability and scale are paramount. That said, we also must continue to innovate. Our use of Amazon Aurora allowed us to reduce manual processes and reduce time-to-scale from days to minutes, which helps keep our engineers focused on building great new services."
>
> — Christopher Ford,
> Vice President of Product at Threat Stack

About Threat Stack

Threat Stack is the leader in cloud security and compliance for infrastructure and applications, helping global enterprises securely leverage the business benefits of the cloud with proactive risk identification and real-time threat detection across cloud workloads.

The Threat Stack Cloud Security Platform® delivers full stack security observability across the cloud management console, host, container, orchestration, managed containers, and serverless layers.

> "We chose Amazon Aurora because we wanted a data store to support availability cross-region, so in the instance of a downed datacenter our customers can still authenticate."
>
> – Jennifer Kim, Lead Software Engineer for Threat Stack

Results and Benefits

Amazon Aurora helps Threat Stack keep its authentication service up and running smoothly even in the event of a disaster.

Established a disaster recovery plan

When the authentication server was running on Cassandra, there was no process in place for dealing with a natural disaster or power outage. If the datacenter that housed the database went down, the Threat Stack agent would not be able to authenticate which means events wouldn't make it into the platform, so customers would lose visibility into their infrastructure.

"We wanted to be vigilant about not running into that scenario," explained Kim. "We chose Amazon Aurora because we wanted a data store to support cross-region replicas that would allow us to maintain functionality in the instance of a downed datacenter, and Amazon Aurora makes it easy to flip from one to the other."

Improved scalability and agility

Before moving to Amazon Aurora, the Threat Stack team would go to great lengths to avoid needing to upgrade to a larger instance. "When we were on Cassandra, scaling was a scary thing," said Kim, "because the process took longer and required more manual engineering effort on our part to stream in the new nodes, roll them into the cluster, etc." Now with Amazon Aurora, it just takes a couple of minutes to make the necessary updates.

Reduced database administration activities

As a result of the move to Amazon Aurora, the team that oversees the authentication service has also gained the benefits of a fully managed service. Whereas they used to be responsible for hardware provisioning, software patching, and updates themselves, AWS takes care of database management tasks for them. The platform includes built-in features that automatically and continuously monitor and back up data as well. It gives the IT team peace of mind the database is running smoothly and allows them to focus on more business-critical issues.

Learn more

Amazon Aurora is a MySQL and PostgreSQL-compatible relational database built for the cloud, that combines the performance and availability of traditional enterprise databases with the simplicity and cost-effectiveness of open source databases. Amazon Aurora is up to five times faster than standard MySQL databases and three times faster than standard PostgreSQL databases. It provides the security, availability, and reliability of commercial databases at 1/10th the cost.