bluematador

CASE STUDY

AUTOMATED ALERTING WITH ZERO CONFIGURATION WHEN MOVING TO KUBERNETES

Patrocinium™

Patrocinium Systems is an emergency event management platform providing real-time information about the personal safety of individuals during an emergency. Founded in 2015, Patrocinium's mission is to provide the public and responders with a flexible, cloud-based tool that reduces recovery time, cost, and loss of life during an emergency. Based in Washington D.C., Patrocinium's platform can serve diverse clients like oil rigs, airports, football stadiums, malls, schools, and office buildings small and large.

Due to the critical nature of their service, suffering a prolonged or significant outage is unacceptable for the Patrocinium team. As Jacob Tirey, Lead Site Reliability Engineer, puts it: "Because it is an emergency system it does not get used very often, but when it does get used it has to work. Our thresholds and SLAs for latency are very finely tuned. We need to make sure our system is online. That is why monitoring is key for us, probably more so than anyone. We can't really send out an apology letter like any other company would, there is extreme liability in our case. That is why we treat performance and uptime so seriously."

THE NEED: LESS NOISE, MORE ACTIONABLE ALERTS WHEN MOVING TO KUBERNETES

Patrocinium's platform is a collection of microservices – authentication, event streams coming in, alert streams going out, mobile device API endpoints, etc. – with very largely distributed applications talking to each other. That is why when Tirey first joined Patrocinium, he was immediately tasked with implementing a microservices-based infrastructure on Amazon Web Services using Docker and Kubernetes. He had a huge undertaking in front of him and there was no monitoring in place when he joined the team. Although expensive, for simplicity and ease of getting started he initially decided to go with a provider which offers an all-in-one solution around system monitoring, logging, APM, user sessions, etc. However, he quickly realized that for system monitoring, their existing solution left a lot to be desired. "With our prior provider there were so many alerts that weren't actionable. Being on call 24/7 gets old and having false positives is a real problem. I found I was getting woken up in the middle of the night for a bunch of nonsense. For this particular provider, being a jack of all trades but a master of none was a real problem," recalls Tirey. As a result, he made the decision to find and implement 'best of breed' solutions for each monitoring category, including finding a system monitoring tool with less noise and more actionable alerts.

NOTIFICATIONS THAT INFORM BUT DON'T CREATE ALERT FATIGUE

Supporting a team of nine developers, Tirey is responsible for the design and implementation of all the infrastructure. Additionally, Tirey is the sole on-call member right now, tasked with ensuring that Patrocinium meets its strict SLAs. After adopting Blue Matador, Tirey immediately found a reduction in noise and an increase in actionable alerts due to Blue Matador's hierarchy of notifications – Alerts, Warnings and Anomalies. According to Tirey, "Because I am the only person on-call right now, getting false positive alerts can really wear down morale. If you are a one man team and handling all the production issues and you're constantly being bombarded by non-actionable events it is going to wear you down. In contrast, I really like that Blue Matador has the concept of Alerts, Warnings and Anomalies and that Warnings and Anomalies don't alert by default. That has been really nice."

> *"It is nice having actionable alerts, that's probably the most important thing for me."*

BUSINESS CHALLENGE

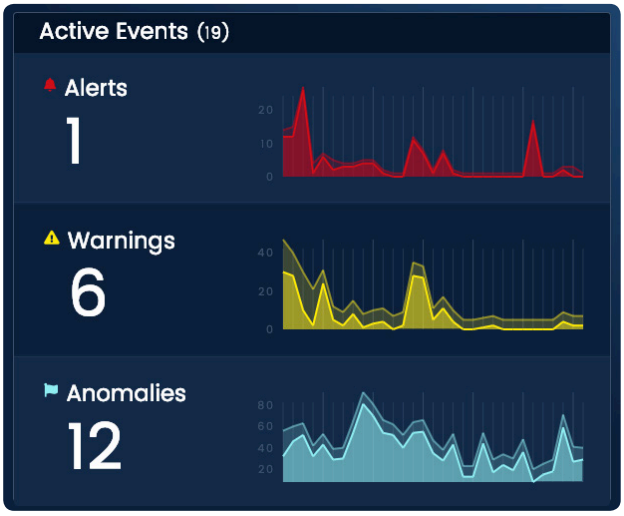
Providing actionable alerts and notifications when moving to Kubernetes and being the sole on-call team member with limited time to setup and configure notifications with a traditional monitoring tool

SOLUTION

In less than an hour, Blue Matador automatically setup actionable alerting and notifications for 140+ events in Patrocinium's Kubernetes clusters and AWS environment

RESULTS

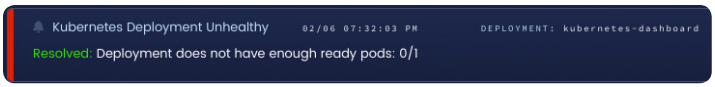
- Elimination of alert fatigue by providing only actionable alerts and notifications with no false positives
- Ability to address previous unknown issues proactively by investigating anomalies before they become incidents
- Confidence to continue to use more and more AWS services knowing that they will be automatically monitored without any configuration
- Time saved and speed to market increased by eliminating the manual process of setting up alerts and notifications with a typical monitoring tool



By only alerting when an issue is critical to the health of the system, Blue Matador helps Tirey be more proactive and stay focused on what is most important, not reacting to the typical stream of noise. In his own words, "Blue Matador hasn't had the false positive problem. That is probably the best thing when you're one person trying to keep your sanity, actionable alerts is key. Blue Matador's concept of Alerts, Warnings and Anomalies enables me to filter out the noise. Other providers just alert for any anomalies."

PROACTIVE NOTIFICATIONS THAT DISCOVER PREVIOUSLY UNKNOWN ISSUES

The Patrocinium team builds and deploys everyday and embraces the philosophy of DevOps. To ensure that the dev team continues to move at a rapid pace, Tirey looks to Blue Matador to help him be more proactive in addressing potential issues. For instance, he has found that when deployments fail in his Kubernetes cluster, Blue Matador will automatically alert him. "Blue Matador will actually alert that the deployment is unhealthy before the Kubernetes watcher catches it," says Tirey.



And Blue Matador's anomaly detection allows him to address potential issues proactively. A few anomalies have been identified that he wouldn't have known to investigate before Blue Matador. "I received consistent anomaly notifications regarding resolv.conf errors that I didn't know was a thing...I had no idea we were generating this error in our Kubernetes cluster. It has been a persistent issue in our cluster for quite some time and I had no idea," recalls Tirey. He has been able to look into these anomalies and address the issues before it turned into an alert.

COMPREHENSIVE INTEGRATIONS WITH AWS COVERING ALL THE BASES

As Patrocinium's platform continues to deepen and expand and new features are added, they are going to start using additional AWS services very soon, like API Gateway, Lambda, SNS, SQS, EFS, etc. For Tirey, it is nice to know that Blue Matador monitors each of these services out-of-the-box. "In the past when we discovered that our prior provider wasn't monitoring everything, we then had to worry 'is this service being monitored?' Now we know that Blue Matador is pretty much monitoring everything. It is very rare that I go into an architectural planning meeting where we are discussing using a new service or tool and I have to worry if it is going to be monitored," says Tirey.

One AWS service where Patrocinium has really seen a strong improvement is in the accuracy and depth of the notifications they receive in AWS' Relational Database Service (RDS). As Tirey recalls, "Coming from another provider, they did not monitor everything in RDS. In the CloudWatch metrics they just pulled four different metrics and that is it. We had an outage that relied on connection throughput. It would have been a really good indicator that something was wrong, but they didn't monitor for it. We've found that Blue Matador catches a lot more CloudWatch metrics."

AUTOMATED, INTELLIGENT OUT-OF-THE-BOX ALERTING THAT SAVES TIME

Due to the breadth of events automatically notified for, Patrocinium has found that Blue Matador has saved them a lot of time and effort. By automating their alerting, Tirey has gained a lot of time back to focus on his core responsibilities: "I don't want to spend time setting up thresholds for each database, each server, what is too little memory, etc. I don't want to be setting manual triggers on all my metrics. I can just install the agent and forget it. The ease of install and ease of use has been great."

Looking back, Blue Matador was exactly what the Patrocinium team was looking for – a product that was fully configured from the outset and didn't need constant maintenance. Referring to his experience getting started with Blue Matador, Tirey said, "Blue Matador's setup was exactly what I was looking for. I install the agent and I run it in the command. I've got Kubernetes monitoring with a single daemonset deployment. I've got AWS monitoring from just providing some IAM credentials."

> *"We were fully up and running with Blue Matador in less than an hour."*

As the lead Site Reliability Engineer, Tirey's ultimate goal is to ensure that Patrocinium's development team continues to rapidly deploy new features to improve their emergency event management platform while maintaining their strict uptime requirements. Blue Matador is allowing him to achieve this goal.

+1 385 355 0135 info@bluematador.com
3630 W South Jordan Pkwy Ste 201
South Jordan, UT 84009