awsmarketplace

Security

Quickly Search all Enterprise Log Data on AWS

The challenge of aggregating and searching log data at cloud scale

The machine logs produced by activity in your Amazon Web Services (AWS) environment contain a multitude of insights that can help your organization improve security posture, comply with regulatory requirements, perform forensic evidence following security incidents, and more. However, searching across all logs produced by an enterprise-scale AWS deployment can be challenging. In addition to their massive scale and dynamic resources, most of these architectures leverage several accounts spanning several AWS regions, further complicating the task. Manual processes designed to parse this data and deliver the insights that the business needs are typically slow, human capital-intensive, and error-prone.

The AWS Solution

AWS CloudTrail records all the API calls made to your AWS services. This data is securely delivered to your Amazon S3 bucket (Figure 1), where it can be used for purposes including compliance, security analysis, and other enterprise initiatives. Using the AWS Management Console, command line interfaces, or software development kits (SDKs) you can set rules to receive a notification each time a new log file is delivered. You can also choose to define rules that automatically delete log files or move them to even more cost-effective AWS storage solutions at specified intervals. CloudTrail log files are protected by server-side encryption while they are stored in your Amazon S3 bucket. You can also use log file integrity validation with CloudTrail, which allows you to detect whether a log file was unchanged, deleted, or modified since CloudTrail delivered it to the specified Amazon S3 bucket. Other services such as Amazon Web Application Firewall (WAF), Elastic Load Balancing, Application Load Balancer, and Amazon VPC Flow Logs provide detail on the traffic that flowed through the service. In addition to all the log files produced by AWS you also have access to all the log files produced by your third-party or custom applications running in your AWS account.

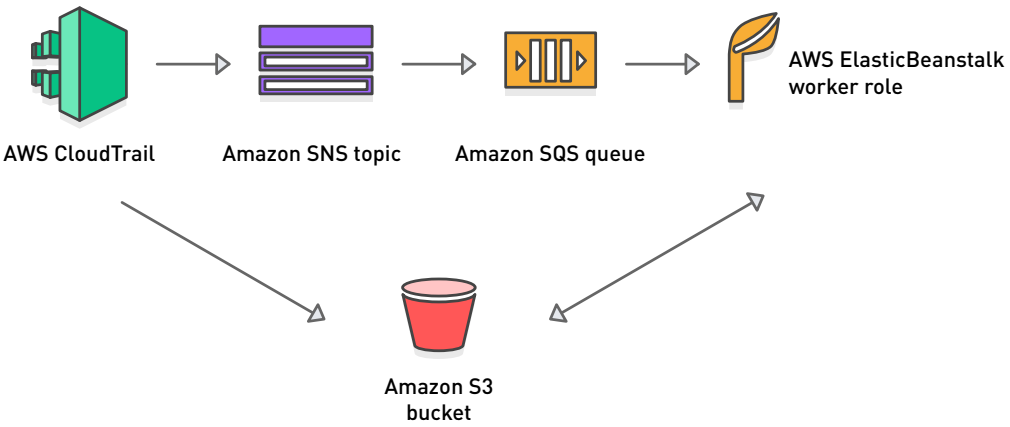

Figure 1: A basic log analysis solution using AWS CloudTrail

Search across AWS Regions, accounts, and services with solutions from AWS Marketplace

Building on the functionality provided by AWS CloudTrail, third-party solutions from AWS Marketplace (Figure 2) simplify the process of searching across enterprise log data by unifying logs across AWS accounts and Regions, while also applying custom metrics and machine learning to correlate information for visibility across your AWS environment. By leveraging these tools, you can much more easily interpret the log data produced by your AWS services and other applications in your AWS environment, including web servers and third-party/custom applications. This allows you to determine which actions need to be taken to remain secure and in compliance with regulatory requirements. They also provide pre-defined filters for common inquiries, such as:

- Who launched a specific Amazon EC2 Instance
- When unauthorized access attempts occurred
- All activity associated with a particular IP address
- Code and/or configuration changes that create security or compliance risks

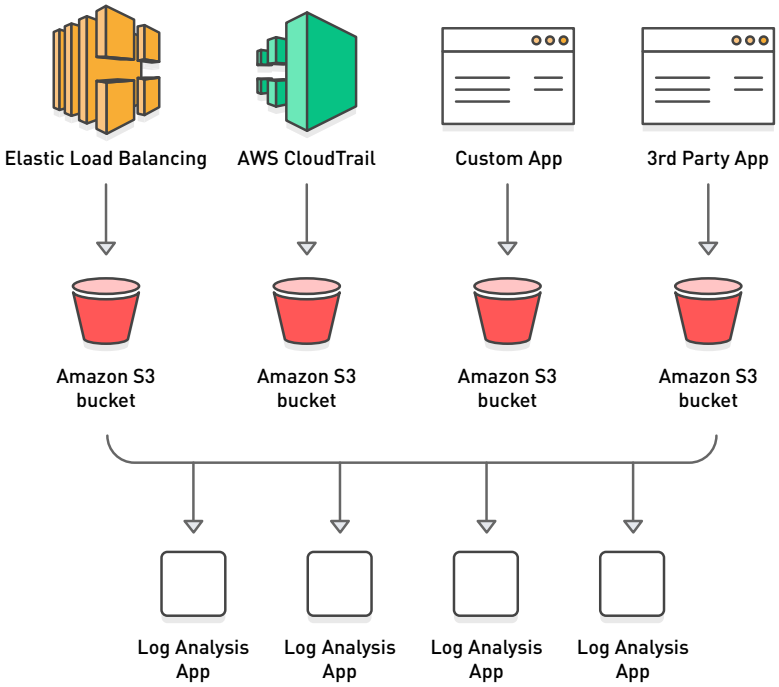

Figure 2: Log analysis applications from AWS Marketplace make it easier to search, correlate and act across your enterprise log data on AWS

In addition, these solutions allow you to see which users took which actions and when they took them, giving you greater context for incident response and digital forensics. They also can help you normalize raw log data with varying formats, including JSON and plaintext, so you can gain a holistic view of your AWS environment without spending excessive time on data transformation. Together, these features make it significantly easier to correlate and find the relationships between events across your AWS environment. This helps you determine the root cause of security incidents and prioritize the actions needed to prevent future incidents. Searches can be turned into real-time reports, and fine-grained access controls enable you to share reports with users without impacting who can access production systems. Use logging and monitoring tools from AWS Marketplace to quickly search, correlate and act across your enterprise log data on AWS.

Get Started with Logging and Monitoring Software in AWS Marketplace

Find and deploy the solution you need in minutes

Save money with pay-as-you-go pricing

Scale globally across all AWS Regions