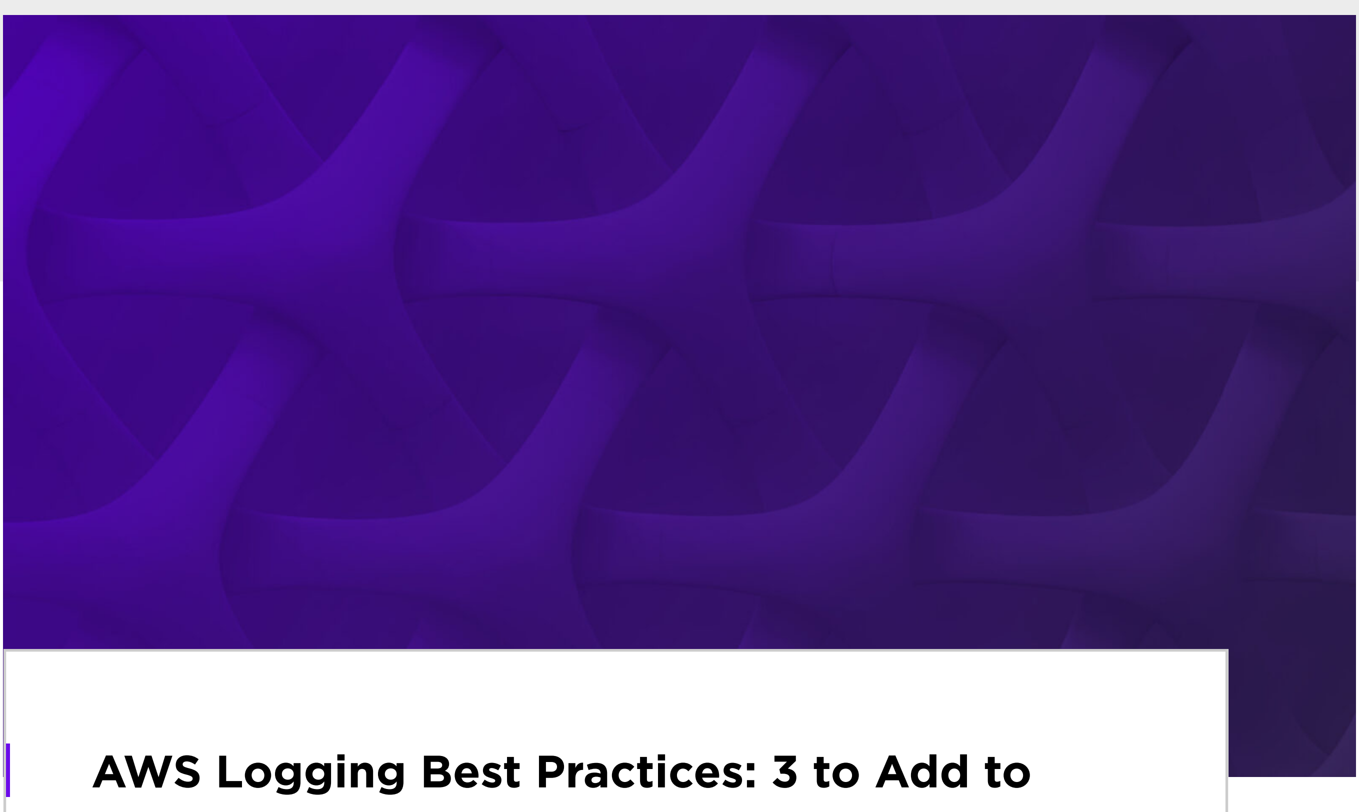

AWS Logging Best Practices: 3 to Add to Your Checklist

January 28, 2020
by SentinelOne

Logging and monitoring should be critical components of your organization's IT governance. Without logging in place, troubleshooting technical issues is more difficult, and gaining operational insight and intelligence is almost impossible.

Logging is as important as ever in the era of the cloud, especially when your organization uses Amazon Web Services (AWS). If you agree that logging is important, then this post is for you.

Today we'll explore three AWS logging best practices — only three because I'd like to keep this post simple. We'll also discuss how you could follow these best practices using various AWS services. After you read this post, consider checking if your organization follows any of these practices on AWS. Are there gaps you could fix?

Let's start with some logging fundamentals on AWS.

Getting Started With AWS Logging Best Practices

Let me introduce you to AWS CloudTrail and AWS CloudWatch. These logging and monitoring services are your starting point in the realm of AWS logging. Before we get into logging best practices, you should definitely check these services out and start using them as soon as you can. If you don't use them, you're practically blind to what's happening on AWS. It's kind of like driving a car with your eyes closed!

Let's start with a high-level overview of CloudTrail next.

AWS CloudTrail, Your Cloud's Audit Repository

AWS CloudTrail is an audit logging service that keeps track and records AWS application program interface (API) calls, actions, and changes on AWS. In other words, when you configure CloudTrail correctly, you can keep track of everything under the ~~sun~~ cloud of your organization.

CloudTrail is enabled by default, and it logs all activities and events for 90 days. If you need more than 90 days, then you'll have to configure CloudTrail to deliver those events to an Amazon S3 bucket. I strongly recommend retaining your logs with CloudTrail because this is a prerequisite for the three best practices I'll cover later on.

Let's move on and take a look at AWS CloudWatch.

AWS CloudWatch, Your Logging and Monitoring Service

AWS CloudWatch is a group of logging and monitoring services that gives your organization logging and monitoring superpowers. CloudWatch collects all kinds of operational metrics from other AWS data sources and can even consume your application's logs with some additional configuration.

You can use CloudWatch Logs Insights, an interactive graphical reporting and log analytics tool, to search and analyze CloudTrail logs. CloudWatch can monitor many other AWS services and log sources with CloudWatch Events. If you haven't heard about CloudWatch Events, I strongly recommend that you check it out because it's yet another prerequisite for automating your operational responses to log events with AWS Step Functions and AWS Lambda.

Now, with the basics out of the way, let's move on to the logging best practices.

> **AWS CloudWatch is a group of logging and monitoring services that gives your organization logging and monitoring superpowers.**

Best Practice #1: Always Log Whenever You Can.

The first rule of ~~Fight Club~~ logging is always generating logs whenever you can. In other words, treat logging as a critical non-functional requirement.

How would you follow this practice on AWS?

CloudTrail is enabled by default on AWS. This sounds like the "always log" part is taken care of, doesn't it? Not so fast!

CloudTrail is enabled by default for your AWS master account only, but not for any other provisioned AWS accounts. This means CloudTrail might not be logging everything as you'd expect. All those additional AWS accounts, their API calls, configuration events, and changes could be flying under the radar right at this moment. And things flying under the radar is not an option.

You need a central management and policy engine, and that's exactly what AWS Organizations is. With AWS Organizations, you can manage and standardize AWS account configurations, policies, compliance, and even CloudTrail configurations. All you need is an Organization Trail policy to make sure all AWS accounts and their actions are logged. Additionally, when you configure this policy, you can centralize all CloudTrail your logs in one S3 bucket, which is an additional best practice that I recommend you do.

Before we move on to the next best practice, one more thing about the "always log" part. Is your CloudTrail logging events in all AWS regions, even in the regions you aren't using at the moment? If your answer is "no" or "maybe," please log in to AWS and fix your CloudTrail config to cover all AWS regions as soon as you can. The bottom line is, always log whenever and wherever you can on AWS.

My next logging best practice is all about log life cycle management.

Best Practice #2: Pay Attention to Your Log Life Cycle Management and Log Availability.

This practice is about making sure your log is available at all times and managing the life cycle of your logs properly. In other words, pay attention to where, when, and how you store, archive, and back up your log files. And if your log files contain sensitive information, it's important to delete those logs securely. Let's see how you could follow this best practice on AWS.

When you configure CloudTrail to retain logs longer than 90 days, the logs are transferred to an AWS S3 bucket. S3 is a highly available and super-durable storage service with data life cycle management and secure deletion capabilities. You should be covered, as long as you configure S3 Object Lifecycle Management on your S3 bucket accordingly. S3 also takes care of both the high availability and the secure deletion part of the best practice, which makes your life a bit easier. S3 can also help you with the next best practice.

> **S3 is a highly available and super-durable storage service with data life cycle management and secure deletion capabilities.**

Best Practice #3: Keep Your Logs Secure.

This practice focuses on the security of your logs. After all, log files are important events and actions. In some cases they could even contain sensitive data. Therefore, preserving log file confidentiality and integrity is important. If you don't currently follow this practice on AWS, then read the next paragraph carefully.

S3 provides various encryption options for your logs. To keep it simple, I'll give you the easiest "encrypt-to-go" option: encrypt your log files using S3 server-side encryption (S3-SSE) with S3-managed keys. This means AWS S3 does all the data encryption, key management, and key rotation so you don't have to worry about it. A word of caution before you take any actions here: make sure you choose an encryption option that meets your organization's policies, and factor in any applicable regulatory and compliance requirements.

How about preserving the integrity of your logs? Check your CloudTrail configuration, and enable log file integrity validation. And while you're at it, turn on multi-factor authentication for deleting logs. With log integrity validation, you can make sure log files aren't changed without your knowledge, and multi-factor prevents any accidental deletions of those logs. This is another great practice on its own.

Wrapping Up

In summary, we've covered CloudTrail and CloudWatch, two of the most important logging and monitoring services you need to know on AWS. We also went through three logging best practices, and I gave you pointers on how you could follow these practices on AWS.

I have a confession to make. Even though this post is about three best practices, I've actually given you more than three best practices for your checklist. I also want you to login to AWS and make sure you're getting the most out of CloudTrail and CloudWatch. And while you're at it, check out Scalyr's log management solution to extend your logging capabilities. This article on logging best practices can also be helpful, and this white paper on logging is worth a look.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Getting Started Quickly With Groovy Logging