NATIVE AWS SECURITY-LOGGING CAPABILITIES

"What are the native AWS security-logging capabilities?"

Overview

Each AWS service provides operational metrics or log files to provide insight into how the service is operating. Additionally, many AWS services generate security log data, including audit logs for access, configuration changes, and billing events. However these security logging capabilities are described in multiple whitepapers, service documentation, and presentations. This document consolidates this information to provide a high-level overview of the native AWS audit log capabilities. For more information about logging for regulatory compliance, please see the whitepaper *Security at Scale: Logging in AWS*.

The following sections assume basic knowledge of the AWS platform and a general understanding of audit and access logs.

General Best Practices

When working with log files in any environment, the following best practices apply:

- Enable audit and access logging capabilities wherever available.
- Leverage secure, durable storage for log files to ensure log files are not accidentally lost, stolen, or tampered with.
- Create and implement log lifecycle policies for storing, aggregating, analyzing, archiving, and deleting log data.
- Leverage meaningful names to organize log data when consolidating logs into a single location.
- Analyze logs, create actionable reports, and configure appropriate alerting to get the most out of log data.

Application on the AWS Platform

The following section describes the native AWS security-logging capabilities and provides service-specific log recommendations.

AWS CloudTrail

AWS CloudTrail provides a history of AWS API calls for an account, and facilitates security analysis, resource change tracking, and compliance auditing of an AWS environment. CloudTrail is an essential service for understanding AWS use, and should be enabled in every region[1] for all AWS accounts regardless of where services are deployed. CloudTrail delivers log files to a designated Amazon Simple Storage Service (Amazon S3) bucket approximately every five minutes, along with option log file integrity validation,[2] and can be configured to trigger an Amazon Simple Notification Service (Amazon SNS) message when new log files are delivered or to send events directly to AWS CloudWatch Logs or AWS Lambda for immediate processing.

AWS Config

AWS Config creates an AWS resource inventory, including configuration history, configuration change notification, and relationships between AWS resources. AWS Config provides a timeline of resource configuration changes for specific services. If multiple changes are made within a short period of time, only the cumulative result of these changes will be recorded. Change snapshots are stored in a specified Amazon S3 bucket and can be configured to send Amazon SNS notifications when AWS resource changes are detected.

Enable AWS Config if you want to track changes to resources configuration, answer questions about resource configurations, demonstrate compliance either at a specific point in time or over a period of time, troubleshoot, or perform security analysis. When processing configuration change notifications, leverage AWS Lambda or Amazon Simple Queue Service (SQS) with workers to process, filter, and consolidate change notifications and alerting.

---

[1] Only enable the default *include-global-service-events* option in one region to avoid generating duplicate records for global services such as AWS Identity and Access Management (IAM) and Amazon CloudFront in every region. For more information, see https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-regional-and-global-services

[2] Log file validation is recommended optional feature that helps customers determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it. For more information, see https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-enabling.html

AWS Detailed Billing Reports

Detailed billing reports break down costs by the hour, day, or month; by each account in an organization; by product or product resource, or by customer-defined tags. Billing reports can be useful to determine how AWS resources are being consumed and to audit an organization's consumption of AWS services. AWS publishes detailed billing reports up to several times a day in comma-separated value (CSV) format to a specified S3 bucket.

Use the *detailed billing report with resources and tags*[3] (with meaningful tags, such as those for cost centers, departmental billing codes, or product names) to improve the accuracy of cost allocation reports and simplify billing reconciliation processes.[4] In addition to using detailed billing reports, consider additional proactive billing monitoring and alerting options like creating Amazon CloudWatch billing alerts.[5]

Amazon S3 Access Logs

S3 access logging records individual requests made to Amazon S3 buckets and can be useful for analyzing traffic patterns, troubleshooting, and security and access auditing. It can also help an organization learn about it customer base, set lifecycle policies, define access policies, and understand Amazon S3 charges. Amazon S3 access logs are delivered to a designated target S3 bucket on a best effort basis.[6]

Elastic Load Balancing Access Logs

Elastic Load Balancing access logging records individual requests made to your load balancer and can be useful for analyzing traffic patterns, troubleshooting, and security and access logging. These logs also provide request processing durations which can be used to improve user experiences, discover user-facing load balancer generated errors, and debug communication between load balancers and back-end webservers. Elastic Load Balancing access logs are delivered to a designated target S3 bucket at user requested 5 or 60 minute intervals.

Amazon CloudFront Access Logs

Amazon CloudFront access logging records individual requests made to CloudFront distributions and can be useful for analyzing traffic patterns, troubleshooting, and security and access auditing. It can also help an organization learn about its customer base, set lifecycle policies, define access policies, and understand CloudFront charges. CloudFront access logs are delivered to a designated target S3 bucket on a best effort basis.[6]

Amazon Redshift Logs

Amazon Redshift logs capture information about database connections, user activity, and changes to user definitions. These logs facilitate security monitoring, troubleshooting, and database auditing activities. Amazon Redshift logs are delivered to a designated target S3 bucket.

Amazon Relational Database Service (RDS) Logs

Amazon Relational Database Service (RDS) logs capture information about database access, performance, errors, and operation. These logs facilitate security, performance, and operation analysis of your AWS managed databases. Customers can view, watch, or download these database logs using the Amazon RDS console, the AWS Command Line Interface, or the Amazon RDS API. Additionally, log files can be queried through DB engine-specific database tables. Consider implementing an automated process to export Amazon RDS access logs into a central access log repository like Amazon S3 or Amazon CloudWatch Logs.

Amazon VPC Flow Logs

Amazon VPC Flow Logs captures information about the IP traffic going to and from Amazon Virtual Private Cloud (Amazon VPC) network interfaces and can be applied at the VPC, subnet, or individual Elastic Network Interface level. Flow log data is stored using Amazon CloudWatch Logs and can be exported using Amazon CloudWatch streams for additional analytics or visualization of network traffic flows.[7] Enable Amazon VPC Flow Logs for debugging or when organizational legal or security policies require capturing network flow data.

---

[3] http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/detailed-billing-reports.html#reportstagsresources

[4] See the AWS Tagging Strategies Solution Brief for more information.

[5] For a description of other reporting, alerting and budgeting options available on the platform, explore the AWS Billing and Cost Management webpage (see the *Resources* section).

[6] http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html

[7] https://github.com/awslabs/cloudwatch-logs-subscription-consumer

Centralized Log Management Options

AWS offers several different options for centrally managing log data. The majority of AWS audit and access log data is delivered to user-specified Amazon S3 buckets. Consider consolidating S3-based logs into a single, secured bucket with meaningful prefix names to make it easier to organize, consolidate, and manage access to log files across AWS services and accounts for processing and analysis. Amazon CloudWatch Logs provides a centralized service for storing and aggregating log data, with rudimentary alerting through CloudWatch alerts. AWS Partner Network members offer feature rich log management solutions that integrate directly with many or all of these audit log capabilities.

Resources

AWS Multiple Account Billing Strategy	https://d0.awsstatic.com/aws-answers/AWS_Multi_Account_Billing_Strategy.pdf AWS Solution Brief on best practices for managing billing with multiple accounts.
AWS Multiple Account Security Strategy	https://d0.awsstatic.com/aws-answers/AWS_Multi_Account_Security_Strategy.pdf AWS Solution Brief on security best practices and implementation strategies for multiple AWS accounts
AWS Tagging Strategies	https://d0.awsstatic.com/aws-answers/AWS_Tagging_Strategies.pdf AWS Solution Brief on resource tagging best practices
AWS Billing and Cost Management	http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-what-is.html AWS User Guide that includes details on usage monitoring and Consolidating Billing
AWS Security Best Practices	http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf AWS whitepaper on security best practices
CloudTrail User Guide	http://awsdocs.s3.amazonaws.com/awscloudtrail/latest/awscloudtrail-ug.pdf
Security at Scale: Logging in AWS	https://d0.awsstatic.com/whitepapers/aws-security-at-scale-logging-in-aws.pdf AWS whitepaper on PIA call logging and monitoring using AWS CloudTrail, with specific callouts to PCI DSS, ISO 27001, and FedRAMP