AWS SECURE INITIAL ACCOUNT SETUP

"How do I ensure I set up my AWS account securely?"

Overview

AWS provides many account-level security options and tools that enable customers to meet their security objectives and implement the appropriate controls for their business functions. This document provides baseline security guidance for AWS accounts to help customers gain confidence that they have securely set up and initialized an account according to AWS best practices. For additional security guidance on managing multiple AWS accounts, see the AWS Organizations User Guide.

The following sections assume basic knowledge of AWS accounts, AWS Identity and Access Management (IAM), AWS CloudTrail, Amazon CloudWatch, AWS Config, and Amazon Simple Storage Service (Amazon S3).

General Best Practices

When setting up access to a service provider, there are some universal security measures that are necessary in order to create a secure system:

- Create a strategy to control permissions at the user level, and grant the minimum set of permissions necessary (*least privilege*) to complete a job role or task.
- Monitor and audit your users, and regularly review privileges. Leverage AWS native security-logging capabilities and configure additional logging as necessary.
- Identify which individuals should interact with the service provider regarding billing, security, and operations matters, and grant authorization accordingly.
- Ensure continuous communication with the service provider, even if individuals change roles or leave the company. For example, use email distribution lists and company phone numbers rather than personal email addresses or mobile phone numbers.
- For consistency across multiple accounts, use AWS CloudFormation or a configuration tool to automatically set up logging and monitoring features for new accounts upon creation.

Security on the AWS Cloud

An AWS account security baseline should include how to communicate with AWS, how to manage and control user access within the account, and how to monitor and audit user activities. The following sections describe key methods and services to help manage each of these aspects of account security.

Communication with AWS

When a customer creates a new AWS account, AWS captures the primary contact information that it will use for all communication about the account, unless alternate contacts are also added. AWS accounts can include alternate contacts for Billing, Operations, and Security. These contacts will receive copies of relevant notifications and serve as secondary communication points if the primary contact is unavailable. When setting up communication channels with AWS, keep the following best practices in mind:

- Configure the AWS account contact information with a corporate email distribution list (e.g. *aws-<org_name>@yourdomain.com*) and company phone number rather than an individual user's email address or personal cell phone.
- Configure the account's alternate contacts to point to a group rather than an individual. For example, create separate email distribution lists for billing, operations, and security and configure these as Billing, Security, and Operations contacts in each active AWS account. This ensures that multiple people will receive AWS notifications and be able to respond, even if someone is on vacation, changes roles, or leaves the company.
- Sign up for an AWS support plan that aligns with your organization's support expectations. Business and Enterprise support plans provide additional contact mechanisms (web, chat, and phone) that are especially useful when a customer needs an immediate response from AWS.

AWS Identity and Access Management (IAM)

AWS recommends using IAM to securely control access to AWS resources. IAM is a free service that allows customers to grant granular permissions, and incorporates capabilities for multi-factor authentication (MFA), identity federation, and record logging. Create a foundational IAM strategy early on and keep the following best practices in mind:

- Create a strong root account password, enable physical MFA on the root account, and create a process for storing and retrieving these credentials only when absolutely necessary. For day-to-day interaction with AWS, use IAM user credentials instead.
- If you have root account access keys, remove them and use IAM roles or user access keys instead.
- Ensure you have a documented process for adding and removing authorized users. Ultimately, it should fully integrate with an organization's existing employee provisioning/de-provisioning process.
- Create IAM groups that reflect organizational roles, and use managed policies to grant specific technical permissions as required.
- If you have an existing identity federation provider, you can use the AWS Security Token Service to grant external identities secure access to your AWS resources without having to create IAM users.

Logging and Auditing

AWS provides several different tools to help customers monitor their account activities and trends. AWS recommends all customers enable the following features:

- Create a security email distribution list to receive security-related notifications. This will make it easier to configure and manage monitoring notifications associated with the monitoring services described below.
- Create an Amazon Simple Notification Service (Amazon SNS) topic for security notifications and subscribe the security email distribution list to the topic. This will make it easier to create and manage security-related alerts.
- Enable CloudTrail in all AWS Regions, which by default will capture global service events. Enable CloudTrail log file integrity validation and send logs to a central S3 bucket that your security team owns.
- Configure CloudTrail integration with Amazon CloudWatch Logs and launch the provided AWS CloudFormation template to create CloudWatch alarms for security and network-related API activity.
- Enable AWS Config. Use the predefined rules `CLOUD_TRAIL_ENABLED` and `RESTRICTED_INCOMING_TRAFFIC` to notify the security SNS topic if CloudTrail is disabled for the account or if someone creates insecure security group rules.
- Create an S3 bucket for storing monitoring data and configure the bucket policy to allow the appropriate services (CloudTrail, AWS Config) to store AWS log and configuration data. For multiple accounts, use a single bucket to consolidate this data and restrict access appropriately.

Billing and Cost Monitoring

AWS forecasting and budgeting services help you accurately plan and monitor your usage and spending levels. Here are steps to establish a baseline for your account:

- Configure AWS usage and billing reports to get detailed information regarding trends in your account activity.
- Designate an email distribution list that will receive billing notifications.
- Create an SNS topic for budget notifications and subscribe to the billing email distribution list to this topic.
- Create one or more budgets in your account and configure notifications if forecasted spending exceeds your budgeted usage.

Resources

AWS Overview of Security Processes	http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf
IAM in Practice	https://d0.awsstatic.com/aws-answers/AWS_IAM_in_Practice.pdf