23andMe Leverages AWS to Enforce Tagging Standard and Understand Cloud Spend

Overview

Leveraging Cloud Custodian and AWS Lambda to enforce their tagging standard enables 23andMe to associate their Cloud costs to their business initiatives.

Challenge

23andMe, Inc. ("23andMe") needed to improve their governance process to better manage costs, and recognized that enforcing their AWS tagging standard was critical to understanding their Cloud spend. Leveraging their relationship with BlueChipTek (Converge), 23andMe utilized resources to jointly develop a tagging enforcement system faster than if they only utilized their own internal staff.

Solution

After collaborating with 23andMe's Cloud Engineering team, Converge proposed:

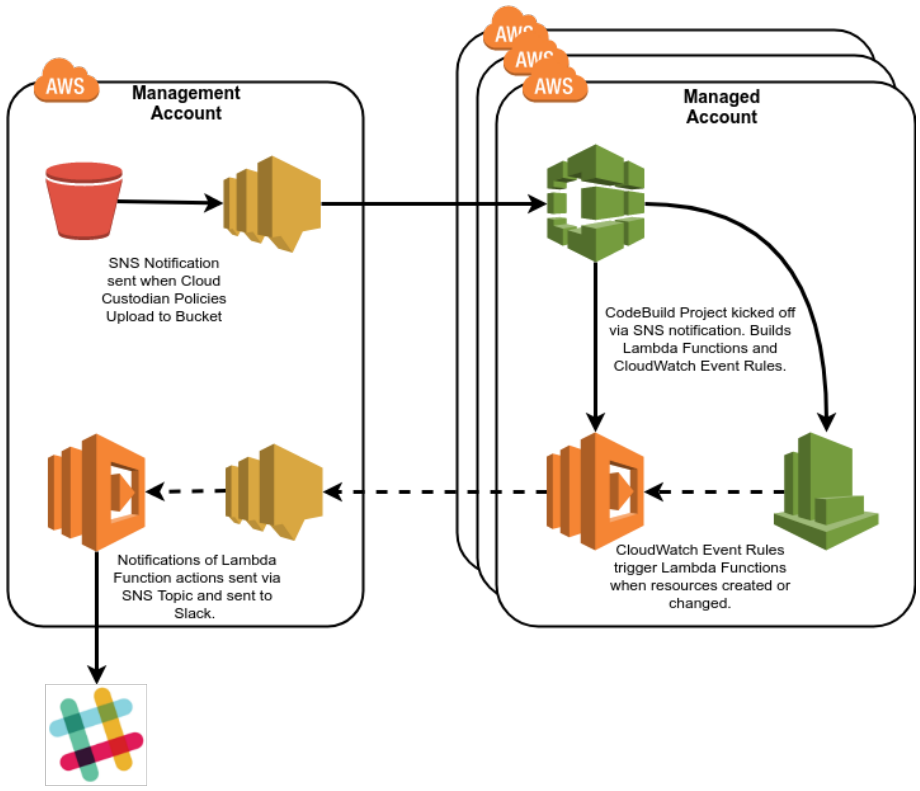
- Using serverless and event-driven architecture to evaluate the creation or modification of resources in order to take action if a resource did not meet the tagging standard.
- Leveraging Cloud Custodian (open-source software) to create and manage the serverless infrastructure.
- Utilizing Slack to notify resource creators about actions that would be taken against non-conformant resources.
- Creating a pipeline utilizing AWS DevOps services to push out new changes to each of 23andMe's AWS accounts.

A parallel effort to tag existing resources was also performed leveraging the AWS Tag Editor, which allows for bulk tagging of resources across multiple regions at once.

AWS Services Used in Solution

- CloudWatch Event rules were used to trigger Lambda Functions to evaluate created or modified resources. When a resource doesn't conform to the tagging standard, the Lambda Function takes action by sending a message via Slack, shutting down or deleting the resource.
- Lambda Functions and CloudWatch Event rules were deployed into each AWS account allowing the utilization of Cloud Custodian and its YAML based policy language.
- A central S3 bucket was utilized to upload new policy files. This created a pipeline for updates and application of new policies into each of the AWS accounts. SNS notifications kick off the CodeBuild Project in each account. The CodeBuild project then runs Cloud Custodian using the new policy file.
- Cloud Custodian was enabled to send Slack messages via a Lambda Function to process SNS notifications sent from each AWS account. Custom Python code was written to take the SNS notifications sent via Cloud Custodian and transform them into something consumable by 23andMe AWS users.

The following diagram provides a basic architecture overview:



While CloudFormation was used to deploy resources in the master AWS account, CloudFormation StackSets were used to deploy the CodeBuild Project to individual AWS accounts. This will soon be automated every time a new AWS account is added to the 23andMe AWS Organization. The CodeBuild Project will create the Cloud Custodian Lambda Functions and CloudWatch Event rules when an AWS account is created.

Results & Benefits

As a result of this solution, there has been a dramatic reduction of untagged resources, providing 23andMe the ability to understand their AWS spend, how it relates to their business, and what areas they need to optimize.

This project laid the foundation to utilize Cloud Custodian to enforce other policies in the realm of security and account management.