Leveraging automation to assist in the deployment of Service Control Policies

aws partner network

Executive Summary

The client is a multinational financial services corporation looking to apply service control policies across their AWS organization.

Key Challenge/Problem Statement

The Customer is currently moving away from a manual blacklist/whitelist process for AWS services within their AWS Organization. The process of updating Service Control Policies (SCP) to deny access to unauthorized services or services that were not in use required the manual parsing of AWS Access Reports for each OU.

Proposed Solution and Architecture

AWS and Vertical Relevance worked together to build automation scripts to perform analysis of proposed SCP changes and their effect on AWS service access and were designed to be run as part of the Customer's SCP deployment pipeline. In addition, 2 IAM permissions boundaries were developed that would make delegated IAM roles more secure.

All changes to individual OU's SCPs were centralized in a single GitHub repository. A manifest file exists in the repository regarding which SCPs are currently deployed and the OU(s) in which they are deployed. When a pull request was merged into the Master branch, an automated pipeline would trigger that would gather all the changes made to the SCPs and cross-reference that with the manifest file in order to generate a "resolved manifest" which is divided into 4 sections; Create, Add, Update, and Remove. The names and paths of the SCPs with their deploy targets are contained within these different sections.

In order to determine if any of the proposed SCP changes would block access to AWS services that are currently in use, the analyzer script extracts the AWS account numbers and the paths of the SCPs that are to be deployed into those accounts. For each AWS account, the script generates an AWS access report. For each SCP that is to be added/updated for an AWS account, the script parses the SCP and determines whether each statement allows or denies an AWS service. This allow/deny list is then compared to the access report which outputs any instance where an SCP statement denies a service that is in-use. This process is repeated for each AWS account and the output is captured in a Python dictionary that is then returned to the calling deployment script.

Once the analysis is complete, logic within the SCP deployment script is able to determine if the pipeline should proceed with deployment or not based on how many in-use services might be blocked. If the pipeline fails, the deployment of the SCPs is halt;ed until a new pull request containing any fixes is merged to the Master branch of the repository.

About the Client

The client is an American multinational financial service corporation. It is one of the largest asset managers in the world with $2.46 trillion in assets under management with a combined total customer asset value number of $6.7 trillion. The Customer operates a brokerage firm, manages a large family of mutual funds, provides fund distribution and investment advice, retirement services, Index funds, wealth management, cryptocurrency, securities execution and clearance, and life insurance.

To complement the Service Control Policies that were deployed into the AWS Organization, AWS and Vertical Relevance developed a pair of IAM permissions boundaries that would be attached to delegated roles within certain accounts. The first permissions boundary, DelegatedAdminPermissionsBoundary, limited the permissions of the role to only creating and managing IAM roles if a second permissions boundary was attached. The second permissions boundary, DelegatedDevPermissionsBoundary, bound the permissions of the role to only the AWS services and specific resources that needed to be managed.

Results

In the end, the Customer had a way to complement the service control policies that were deployed into the AWS organization.

Summary

By engaging AWS and Vertical Relevance, the Customer was able to automate deploying Service Control Policies across their AWS Cloud Organizations. Analysis of Service Control Policies before they are deployed into the Organization provides the advantage of increased confidence with each deployment, as well as, reduced time to remediation in cases where a Service Control Policy conflict occurs.

About Vertical Relevance

Vertical Relevance is a Financial Services focused (Wealth Management, Asset Management, Banking, Insurance) consulting firm helping with the design & delivery of effective transformation programs across people, process, & systems. With 10+ years of AWS & 20+ years of Financial Services experience, we understand the business needs & build solutions to meet sales, marketing, & compliance goals.

VERTICAL RELEVANCE