Chrome File Edit View History Bookmarks People Tab Window Help 100% Mon 10:46 AM

console.aws.amazon.com/iam/home?region=us-east-1#/groups/swa?section=permissions

aws Services Resource Groups kcfdaniel Global Support

Manage Group Permissions

Edit Permissions

The policy generator enables you to create policies that control access to Amazon Web Services (AWS) products and resources. For more information about creating policies, see Overview of Policies in Using AWS Identity and Access Management.

Effect Allow Deny

1. **AWS Service** Amazon API Gateway

3. **Actions** 1 Action(s) Selected

Amazon Resource Name (ARN) arn:aws:execute-api:us-east-1:927601418139:itchzfxj23/*/GET/*

2. AWS Organizations
AWS Price List
AWS Resource Groups
AWS Security Token Service
AWS Serverless Application Repository
AWS Service Catalog
AWS Shield
AWS Snowball
AWS Step Functions
AWS Support
AWS Trusted Advisor
AWS WAF
AWS WAF Regional
AWS XRay
Alexa for Business
Amazon API Gateway
Amazon AWS Cloud Contact Center
Amazon AppStream
Amazon Athena
Amazon Chime
Amazon Cloud Directory
Amazon CloudFront
Amazon CloudSearch
Amazon CloudWatch
Amazon CloudWatch Events
Amazon CloudWatch Logs
Amazon Cognito Identity
Amazon Cognito Sync
Amazon Cognito User Pools
Amazon Comprehend
Amazon DynamoDB
Amazon DynamoDB Accelerator (DAX)
Amazon EC2
Amazon EC2 Container Registry
Amazon EC2 Container Service
Amazon ElastiCache

All Actions (*)
InvalidateCache
Invoke

4.

wildcard (*) matching all API stages
account ID
API ID
wildcard (*) matching all API resources
region

5. set the correct ARN (important).
Use the correct region, account ID, API ID,
This example allows users to make
GET requests to all the resources of the API.

6. Add Statement

Effect	Action	Resource	
Allow	execute-api:Invoke	arn:aws:execute-api:us-east-1:927601418139:itchzfxj23/*/GET/*	Remove

7.

Cancel Previous Next Step