Automating the Management of the Operational Health of Cloud Accounts at Scale

Jamie Walls
Retail & Direct Bank
Cloud Engineering
What You Can Expect Today

- Challenges Faced in Cloud Environments at Scale
- Open-source Solutions and Implementation Details
- Custom Solutions When the Only Option is to Roll Up Your Sleeves
- Our “Shift Left” Philosophy to Cloud Account Management
Who I am

Jamie Walls
14 Years at Capital One

Roles Held
• Production Support
• Feature Delivery
• DevOps Support
• Cloud Engineering

What Drives Me
• Family
• Volunteerism
• Automating All the Things
Our Cloud Journey

Data Centers to Private Cloud to Public Cloud

Current State
Our Compliance Challenge

1. The cloud enables limitless capabilities

2. We empower our engineers

3. The banking industry is heavily regulated
Cloud Custodian: An Answer to Many of our Problems
What is Cloud Custodian?

Compliance & Cost Control Engine
Cloud Custodian enables users and entire organizations to be well managed in the cloud. It consolidates many of the ad-hoc scripts organizations have into a lightweight and flexible tool, with unified metrics and reporting. Custodian supports managing AWS, Azure, and GCP public cloud environments.

Open Source
Available free for anyone to use
https://cloudcustodian.io/
Available on Github.com

Python-based
Python 3 with 2.7 compatibility (until year end)

Run Anywhere
Can be run locally, on an instance, or Serverless in AWS Lambda.

Run on Any Schedule
Custodian can be configured to run in real-time, hourly, daily, weekly, or on any other schedule.

Simple DSL
Simple YAML DSL allows you to easily define rules to enable a well-managed cloud infrastructure, that's both secure and cost optimized.
Cloud Custodian DSL Example – Stop Unused EC2 Instances

- name: ec2-unused-stop-daily
  resource: ec2
  description: Find unused EC2 instances with 14 day average CPU utilization less than 1.5%, stop them, and mark for deletion in a week.
  filters:
  - type: metrics
    name: CPUUtilization
    days: 14
    value: 1.5
    op: less-than
  - type: instance-age
    days: 14
  - type: value
    key: "State.Name"
    value: "running"
    op: equal
  - "tag:aws:autoscaling:groupName": absent
  - type: value
    key: InstanceType
    value: ["t2.nano", "t2.micro", "t2.small", "t3.nano", "t3.micro", "t3.small"]
    op: not-in

actions:
- type: stop
  # Stop the instance
- type: mark-for-op
  tag: custodian_cleanup
  msg: "This EC2 instance has had less than 2 percent CPU utilization for over 14 days: {op}@{action_date}"
  op: terminate
  days: 7
Our Challenges Solved by Cloud Custodian

Security Enforcement
- No Public Resources
- Encryption Everywhere
- Patching

Backups
- EC2, EBS, RDS
- Snapshot Cleanups

Cost Control
- EC2 & RDS Nightly Shutdown
- Over-provisioned Resources
- ASG Resizing

Tagging
- Enforce tagging
- Auto-tag Creator
- Copy tags

Unused or Invalid Resource Cleanup
- EC2, EBS, RDS, ELB, Lambda, AMI
- "Spinning" ASGs

Account Maintenance
- Service Limit Increases
- Legacy VPC cleanup
Cloud Custodian Setup at Capital One

Hierarchy
- Enterprise
- Line of Business
- Account

Frequency
- Real-time
- Hourly
- Hourly Alternating Regions
- Daily
- Weekly
- Monthly

Notifications vs. Actions
- Prod
  - Fix or delete on create
  - Notify-only after an hour
- Non-Prod
  - Fix or delete

IAM Role Separation
- Enterprise – Read Only w/ selective modify
- Line of Business – Modify & Terminate

Logging
- Slack notifications for failures
“With great power comes great responsibility”

max-resources-percent: 5
or
max-resources: 3
Additional Operational Automation

**AWS Service Limit Increases**
- Cloud Custodian raises most
- Lambda function fills gaps

**Support Ticket Updates**
- High severity ticket notification
- Lambda function adds user ID and email

**Tag Validation**
- Lambda function builds validation list
- Custodian utilizes list

**Resource Owner Updates**
- Lambda function updates owner when he/she leaves the company

**Build Script Resource Lookup**
- AMI, Enterprise Security Groups, Subnets

**Bucket Policy Builder**
- Generates policy or build script
- Based on user input or access logs

**Multi-Account Monitoring App**
- Monitoring for cloud account failures
- View account growth trending

**Multi-Account Resource View App**
- Resource finder by tag or ID
- Resource comparisons
- Cost insights
“Shift Left” Approach to Solving Operational Problems

Lifecycle of a non-compliant cloud resource

Why focus on the problem when you can fix the source?
Where We Are Heading

Build Pipeline Updates
- Common enterprise pipeline
- Correct resource definitions
- Utilize lookups vs user input
- User input validation

Incident Ticket Integration
- Tickets to owning teams when resources fall out of compliance

Automated Rebuilding
- Automatically integrate new AMIs & SGs
- Automated regional failover

Terraform Enterprise
- Validation of build scripts
- Fail commits with non-compliant configurations

Smaller Accounts
- Shared VPC
- Single click account migration
Thank You

p.s. We’re hiring too
capitalonecareers.com

Jamie Walls – Find me on LinkedIn