AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

FSI304

Policy as code: How to automate security and compliance

Shubham Shukla (he/him)
Vice President – Cloud Enablement
Goldman Sachs

Catherine Kim (she/her)
Vice President – Cloud Enablement
Goldman Sachs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Cloud enablement at Goldman Sachs

Continuous delivery – where we were

Gap analysis

Cloud fast track: policy as code

Quick demo

Current state

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Cloud enablement at Goldman Sachs

- 80+ team members
- Advisory, implementation, and security for cloud infrastructure
- Continuous delivery platform

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Houston, we have (had?) a problem

- AWS account acquisition
- Design reviews
- Manual security reviews
- Learn Goldman Sachs-specific modules/libraries

High-touch activity!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Wouldn’t it be nice if…

- Self-service
- Secure by design
- Cloud-native
- AWS account creation is an implementation detail

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Enter cloud fast track

- Self-service
- Shared responsibility
- Security by design – guardrails

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Quick demo (1/2)

```
import * as sqs from '@aws-cdk/aws-sqs';
import * as cdk from '@aws-cdk/core';

export class SqsStack extends cdk.Stack {
  constructor(scope: cdk.App, id: string, props?: cdk.StackProps) {
    super(scope, id, props);

    const queue = new sqs.Queue(this, 'SampleQueue', {
    });
  }
}
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Quick demo (2/2)


```
{
      "cft_properties": [
        {
          "allowed_values": [
            {
              "Fn::GetAtt": [
                "(Logical resource ID of KMS key created in the same stack)",
                "Arn“
              ]
            },
            {
              "Fn::GetAtt": [
                "(Logical resource ID of KMS key created in the same stack)",
                "KeyId“
              ]
            }
          ],
          "property": "KmsMasterKeyId",
          "required": true
        }
      ],
      "decision": "deny",
      "message": "Ensure SQS Queues use a KMS master key created in the same stack.",
      "policy_id": "sqs.queue_same_stack_kms_key",
      "type": "AWS::SQS::Queue",
      "controls": [],
      "resources": {
        "SampleQueue2FA9417D": []
      }
    }
}
```


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Where we are today

- Sandbox released October 2021
- 100+ sandbox pipelines
- Customer feedback
  - Support for additional AWS services
  - Guardrail-compliant constructs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Shubham Shukla
Shubham.Shukla@gs.com

Catherine Kim
Catherine.Kim@gs.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.