
AWS
re:Invent
DECEMBER 2 – 6, 2024 | LAS VEGAS, NV

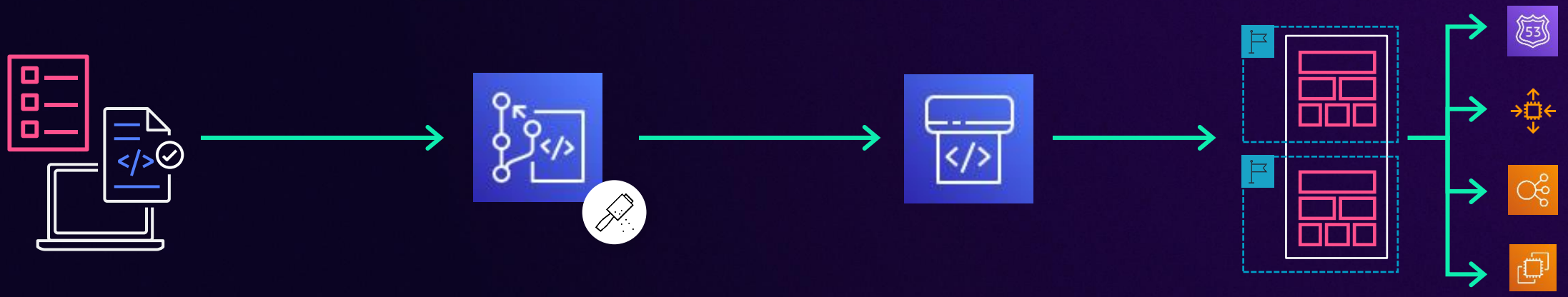
COP407

Coding for proactive controls with AWS CloudFormation

David Killmon
(he/him)
Principal Engineer
AWS CloudFormation

Ben Perak
(he/him)
Principal Product Manager
AWS CloudFormation

Provisioning and managing IaC



1. Code
2. Commit
   Git push/PR
3. Execute CI/CD test and deployment
4. Resources provisioned through CloudFormation

The increasing role of deployment safety

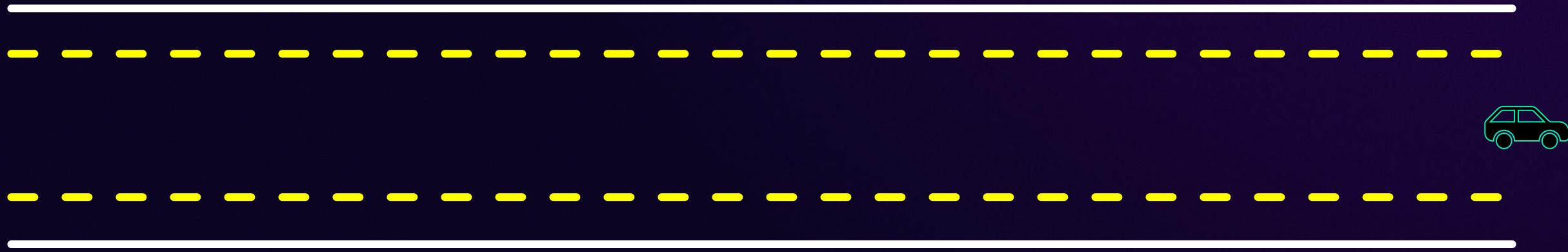
AS IAC AUTHORING EVOLVES, ENSURING SAFE DEPLOYMENTS IS CRITICAL

- As customers empower their development team to use different methods to author templates, the need for guardrails increases
- Infrastructure-as-Code authoring is evolving with new layers of abstraction and the use of gen AI tools
- Increasing role of guardrails to force best practice configurations

The increasing role of deployment safety

AS IAC AUTHORING EVOLVES, ENSURING SAFE DEPLOYMENTS IS CRITICAL

- As customers empower their development team to use different methods to author templates, the need for guardrails increases
- Infrastructure-as-Code authoring is evolving with new layers of abstraction and the use of gen AI tools
- Increasing role of guardrails to force best practice configurations



Introduction to CloudFormation Hooks

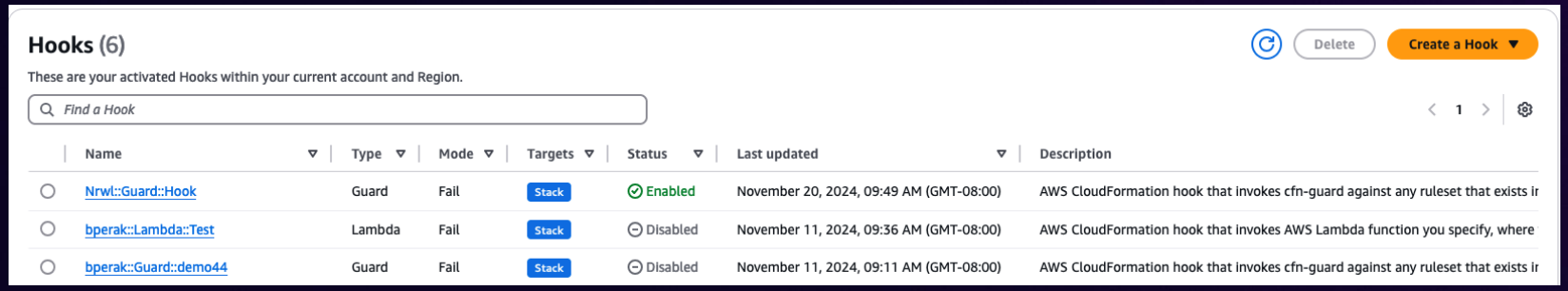
SHIFT LEFT PROACTIVE CONTROLS

Template

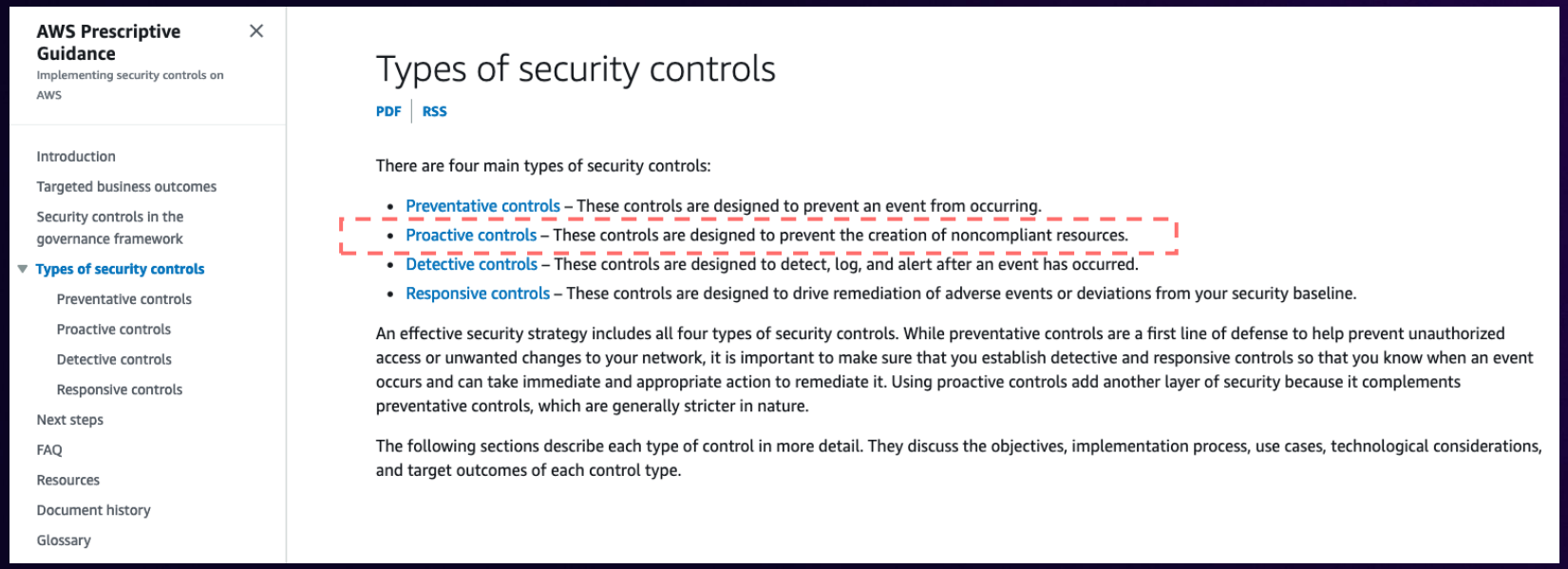
```
AWSTemplateFormatVersion: "2010-09-09"
Resources:
  S3Bucket:
    Type: AWS::S3::Bucket
    Properties: {}
```

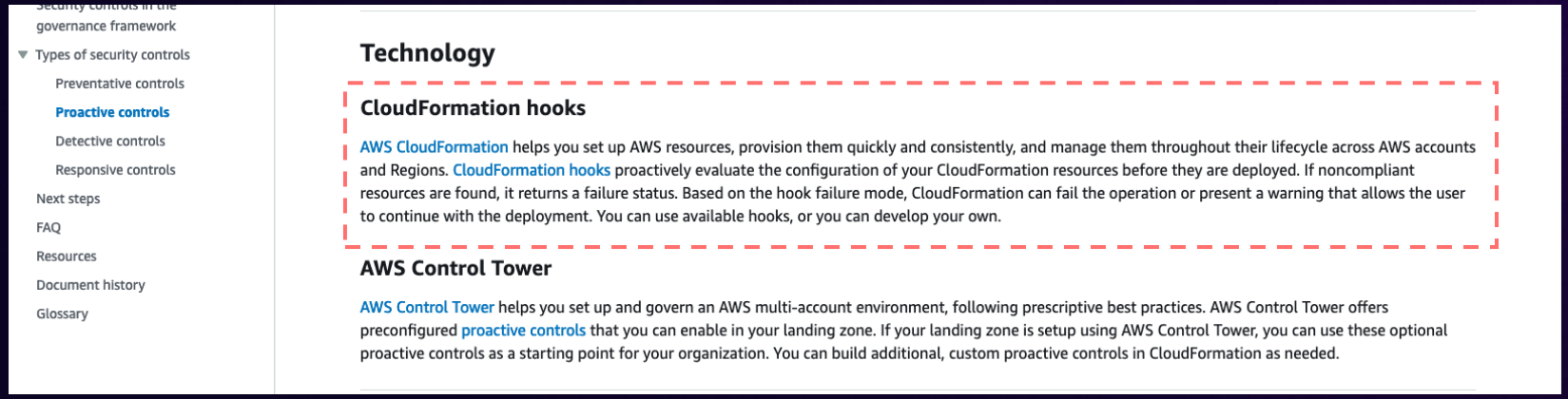
```
resultStatus = HookStatus.FAILED;
resultMessage = "Bucket Encryption not enabled for bucket with name: " + bucket.getBucketName();
```

Registered Hooks



CloudFormation Hooks in the AWS Controls Narrative





Use case #2: Prevent accidental operation impacts

Original template

```
AWSTemplateFormatVersion: "2010-09-09"
Resources:
  myASG:
    Type: AWS::AutoScaling::AutoScalingGroup
    Properties:
      MinSize:  1
      MaxSize:  100
      DesiredCapacity:  50
      LaunchTemplate:
          LaunchTemplateId: !Ref myLaunchTemplate
          Version: !Ref myLaunchTemplateVersionNumber
      VPCZoneIdentifier: !Ref Subnets
```

Change set

```
AWSTemplateFormatVersion: "2010-09-09"
Resources:
  myASG:
    Type: AWS::AutoScaling::AutoScalingGroup
    Properties:
      MinSize:  1
      MaxSize:  10
      DesiredCapacity:  50
      LaunchTemplate:
          LaunchTemplateId: !Ref myLaunchTemplate
          Version: !Ref myLaunchTemplateVersionNumber
      VPCZoneIdentifier: !Ref Subnets
```

Operational impacts often happen by making configuration mistakes. Prevent impacts by evaluating prior resource configurations against “to-be” configurations.

Hook result

```
status = HookStatus.FAILED
message = f"The ASG change you are making is greater than 50% of the original value."
```

Use case #3: Drive cost governance and best practices

CCOE and Cloud Cost Management professionals want to be notified when unnecessary spend occurs

Template

```
AWSTemplateFormatVersion: "2010-09-09"
Resources:
  MyInstance:
    Type: AWS::EC2::Instance
    Properties:
       ImageId: "ami-79fd7eee"
       InstanceType: "p3dn. 24xlarge"
```

Hook result

```
status = HookStatus.FAILED
message = f"The EC2 instance you are provisioning is not covered by an Savings Plan or Reserved Instance."
```

```
status = HookStatus.FAILED
message = f"The EC2 instance you are provisioning is not allowed in a Sandbox environment."
```

New features

Support for new use cases

- Template Hook invocations – inspect an entire template
- Change set Hook invocations – surface violations early, and often
- Cloud Control API Hook invocation – extend hooks beyond CloudFormation

Simplifying the developer experience

- New console and onboarding workflows
- Managed Hook for Guard
- Managed Hook for invoking an AWS Lambda function
- New CloudFormation resources to provision Guard/Lambda Hooks

Let’s code!

Thank you!

Please complete the session survey in the mobile app

David Killmon
killmond@amazon.com

Ben Perak
bperak@amazon.com