AWS re:Invent

DOP312-R

Customize AWS CloudFormation with open-source tools

Luis Colon
Senior Developer Advocate
AWS CloudFormation

Ryan Lohan
Software Development Engineer
AWS CloudFormation

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Agenda

Increasing community engagement

Review of some tools available

Focus: Resource providers

Where to go from here

Increasing community engagement

Already a passionate, engaged community

- Many GitHub projects
- Documentation contributions
- Over 1,400 members in Slack channel
  - Twitter DM: @luiscolon1 or @thedanblanco - send your email address
- New GitHub organization, plus projects in other GitHub locations
  - https://github.com/aws-cloudformation
- All links we'll discuss today will be here also:
  https://github.com/aws-cloudformation/awesome-cloudformation

Public coverage roadmap

Search or jump to... / Pull requests Issues Marketplace Explore

aws-cloudformation / aws-cloudformation-coverage-roadmap

Unwatch 90 Star 414 Fork 7

Code Issues 181 Pull requests 0 Projects 1 Security Insights Settings

coverage-roadmap
Updated 3 days ago

Filter cards + Add cards Fullscreen Menu

16 Researching

- AWS::IAM::User-Tags
  #69 opened by avatarworf
  security identity co...
- AWS::Logs::LogGroup tag support
  #77 opened by kjpgit
  management & gov...
- AWS::SSM::Document-NewAttribute (Name)
  0 of 1
  #115 opened by azec-pdx
  management & gov...
- AWS::ApiGateway::Stage-MethodSetting-EnableDetailedCloudWatchMetrics
  #100 opened by pawelaugustyn
  networking & cont...

6 We're working on it

- AWS::S3::Bucket Transition - DEEP_ARCHIVE doesn't work
  #161 opened by rjpereira
  storage
- Create AWS::MediaConvert::* Resources
  #114 opened by ngamradt-turner
  other AWS services
- AWS::ECS::TaskDefinition - allow support for memory swap per container
  #153 opened by luiseduardocolon
  compute
- AWS::CloudWatch::Alarm - allow tags
  #64 opened by Limess
  management & gov...

7 Coming Soon

- AWS::Lambda::Function-Code-ZipFile
  #80 opened by rclark
  compute
- AWS::SNS::Topic (allow tags)
  #7 opened by luiseduardocolon
  app integration
- AWS::Events::Rule -> Target -> EcsParameters (new properties) (support for scheduled tasks)
  #23 opened by luiseduardocolon
  management & gov...
- AWS::CodePipeline::Pipeline-Tags
  #95 opened by farski
  dev tools
- AWS::ApiGateway::DomainName- (new parameter)

32 Shipped

- AWS::Cognito::UserPool-LambdaConfig (new properties)
  #59 opened by patrickgreenwell
  security identity co...
- AWS::Cognito::ResourceServer
  #173 opened by jacintoArias
  security identity co...
- AWS::Cognito::UserPoolDomain
  #58 opened by dehli
  security identity co...
- AWS::Events::Rule->EventBusName
  #138 opened by mbotmcc
  app integration
- AWS::Config::RemediationConfiguration - Please add support for auto-remediation

Authoring

Many snippets, sample templates from docs

- Doc team also accepts contributions
- cfn-flip – switches from JSON to/from YAML

Other sources of samples

- https://github.com/awslabs/aws-cloudformation-templates
- AWS solutions/quickstarts
- https://github.com/aws-quickstart
- https://github.com/widdix/aws-cf-templates
- https://asecure.cloud/

https://asecure.cloud/

AWS CodePipeline: Grant Permissions to Approve or Reject Manual Approval Actions

Overview

Configure & Deploy

Sources & Documentation

Overview

An IAM policy that grants permissions to approve or reject manual approval actions in a specific pipeline

Configuration Templates

Policy | CloudFormation | AWS CLI

Missing Parameters

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "codepipeline:PutApprovalResult"
            ],
            "Resource": [
                "arn:aws:codepipeline:::/*/*"
            ],
            "Effect": "Allow"
```

Actions

Deploy to AWS Account

Save to File

Add to Stack

Customize Policy

region *

AWS Region. Use * to indica

accountId *

Authoring utilities

https://github.com/iann0036/AWSConsoleRecorder

Console Recorder for AWS

Boto3 (Python) | CloudFormation | Terraform | Troposphere | CDK (TS) | AWS CLI

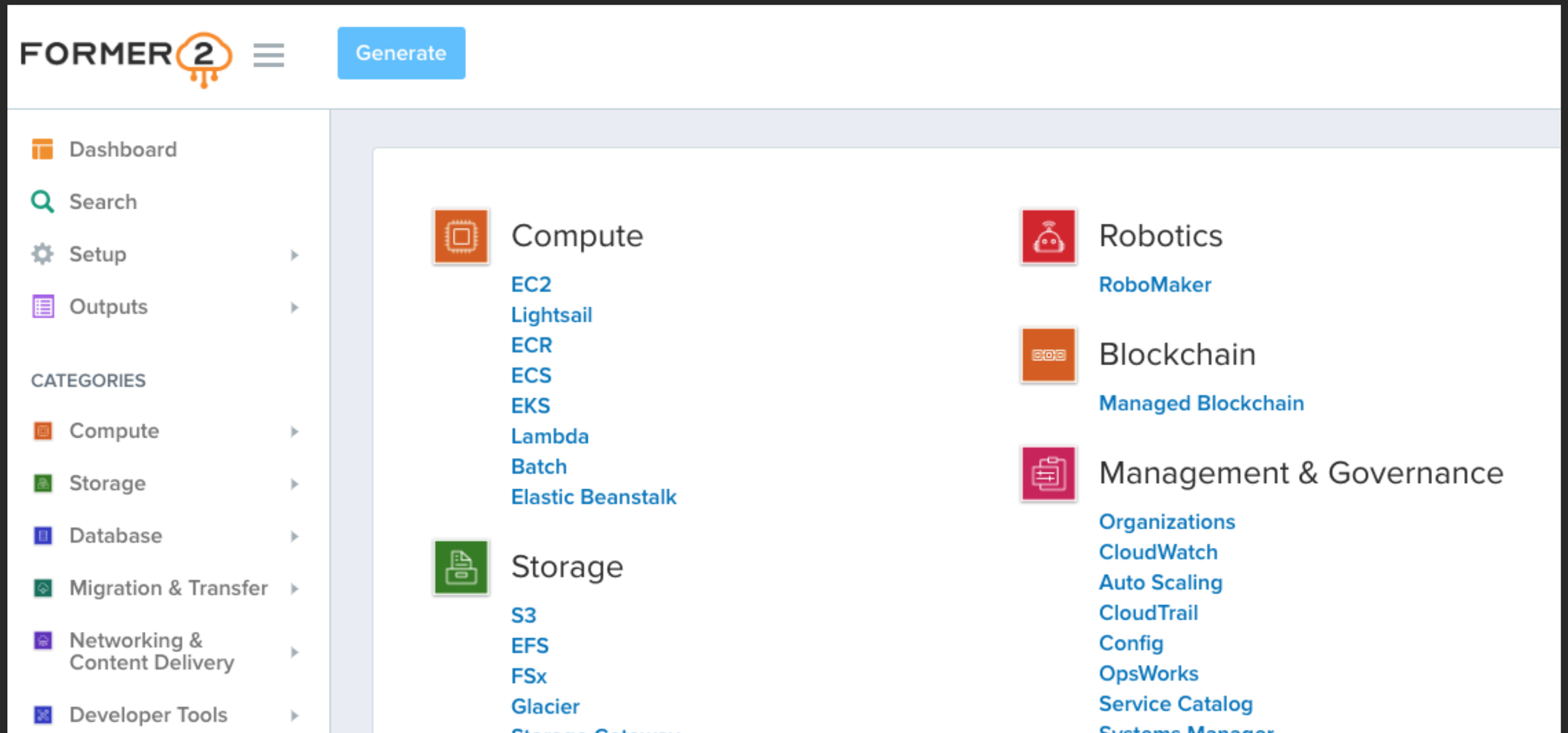
IAM | JavaScript | Go SDK (v1) | Settings

```yaml
AWSTemplateFormatVersion: "2010-09-09"
Metadata:
    Generator: "console-recorder"
Description: ""
Resources:
    ec2dfb7acb:
        Type: "AWS::EC2::SecurityGroup"
        Properties:
            GroupDescription: "launch-wizard-2 created 2019-01-05T22:59:03.991+11:00"
            GroupName: "launch-wizard-2"
            VpcId: "vpc-0125f564"

    ec2ccd5ceb:
        Type: "AWS::EC2::Instance"
        Properties:
```

Authoring utilities

https://github.com/iann0036/former2



Authoring utilities

https://github.com/aws-cloudformation/cfn-python-lint

```yaml
AWSTemplateFormatVersion: "2010-09-09"
Description: A sample template
Errors:
  Catch: Missing
Parameters:
  myParam:
    Type: String
    Default: String
    Description: String
Resources:
  ## Missing Properties
  MyEC2Instance1:
    Type: "AWS::EC2::Instance1"
  ## Fake Properties Key on main level
  ## Bad sub properties in BlockDeviceMappings/Ebs and NetworkInterfaces
  MyEC2Instance:
    Type: "AWS::EC2::Instance"
    Properties:
      ImageId: "ami-2f726546"
      InstanceType: t1.micro
      KeyName: 1
      FakeKey: MadeYouLook
      BlockDeviceMappings:
```

Severity	Provider	Description	Line
Warning	Cfn-Lint	Top level item Errors isn't valid	3:1
Warning	Cfn-Lint	Parameter myParam not used	6:1
Warning	Cfn-Lint	Invalid Type AWS::EC2::Instance1 for resource MyEC2Instance1	12:1
Warning	Cfn-Lint	Properties not defined for resource MyEC2Instance1	12:1
Warning	Cfn-Lint	Invalid Property FakeKey for resource MyEC2Instance	18:1
Warning	Cfn-Lint	Invalid Property BadSubX2Key for resource MyEC2Instance	26:1

Testing

Cfn-lint – use headless in pipelines

Cfn-nag – focused on security rules

https://github.com/stelligent/cfn_nag

Taskcat – test across regions

CLI tools

awscfncli – https://github.com/Kotaimen/awscfncli
Stacker – https://github.com/cloudtools/stacker
Sceptre – https://github.com/Sceptre/sceptre

```
Commands:
  create          Creates a stack or a change set.
  delete          Deletes a stack or a change set.
  describe        Commands for describing attributes of stacks.
  estimate-cost   Estimates the cost of the template.
  execute         Executes a Change Set.
  generate        Prints the template.
  launch          Launch a Stack or StackGroup.
  list            Commands for listing attributes of stacks.
  new             Commands for initialising Sceptre projects.
  set-policy      Sets Stack policy.
  status          Print status of stack or stack_group.
  update          Update a stack.
  validate        Validates the template.
```

Code generation

CDK – https://github.com/aws/aws-cdk
SAM – https://github.com/awslabs/serverless-application-model
Stelligent Mu – for deploying ECS/EKS container-based microservices
https://github.com/stelligent/mu
Others
- Language specific – for example, Troposphere (Python)
  https://github.com/cloudtools/troposphere
- SparkleFormation (Ruby)
  https://github.com/sparkleformation
- VaporShell (PowerShell)
  https://github.com/scrthq/VaporShell

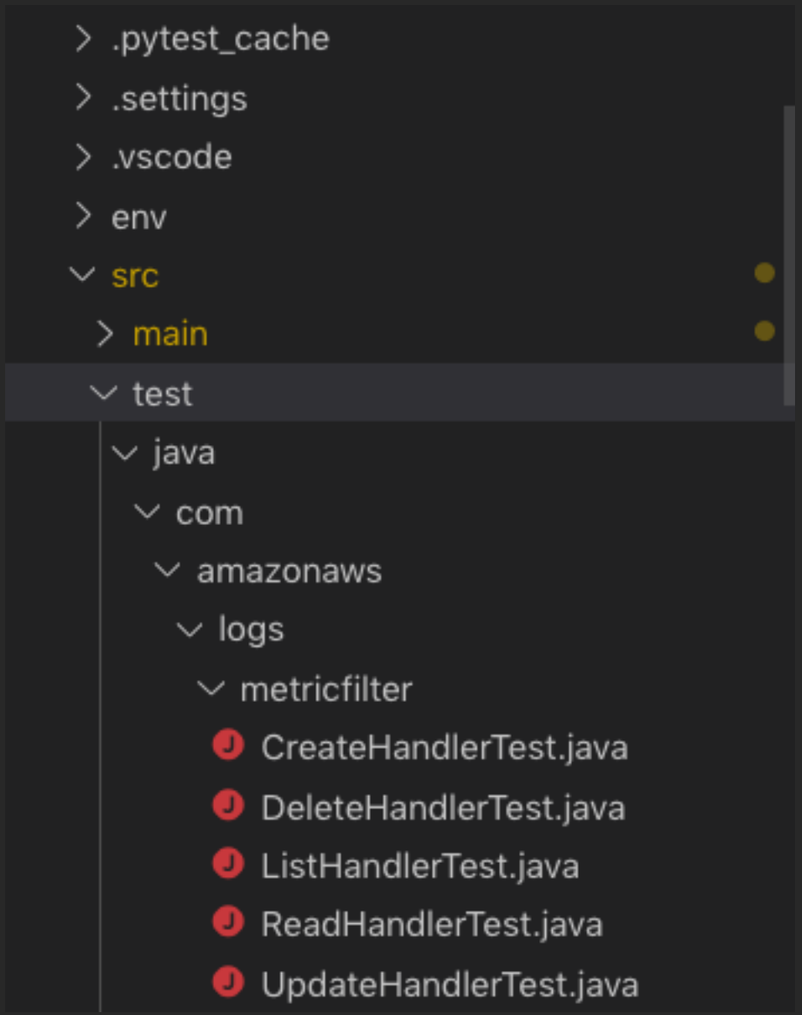
New AWS CloudFormation CLI

Initialize resource provider projects with sample code; build system support

Leverages SAM to enable local testing

Validates resource provider definitions

As a developer, focus first on developing your schema and then focus on the APIs require to create, update, and describe your resources



Schema-driven development

Start with JSON schema – define properties, requirements, permissions, data types

Based on that definition, initial code assets and scaffolding can be generated to aid in testing and code quality

More handlers, to enable resource to inherit features like change sets & rollbacks

Specifications are updated so that tools like validation/linters and CDK can leverage the resource

Invocations are managed by new runtime, like native first-class resource types

```
},
"MetricTransformations": {
  "description": "MetricTransformation",
  "type": "array",
  "minItems": 1,
  "maxItems": 1,
  "items": {
    "type": "object",
    "properties": {
      "DefaultValue": {
        "type": "number",
        "minimum": 1,
        "maximum": 9999
      },
      "MetricName": {
        "type": "string",
        "pattern": "^[.\\-_/#A-Za-z0-9]+$"
      },
      "MetricNamespace": {…
      },
      "MetricValue": {…
      }
    },
    "required": [
      "MetricName",
      "MetricNamespace",
      "MetricValue"
    ]
```

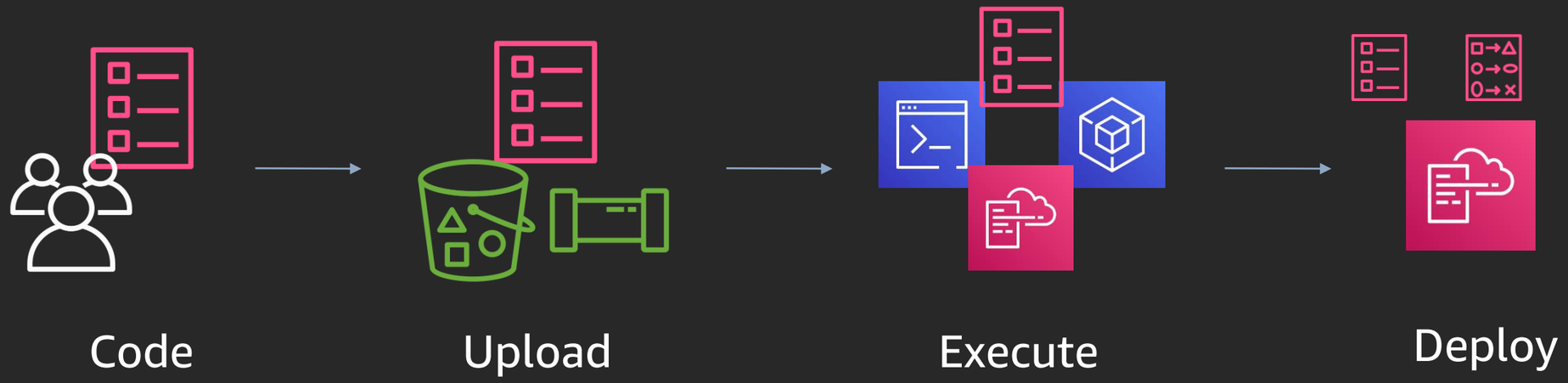
Demo

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Looking forward

Encourage and support more community involvement
- Creating win-wins
- More feedback, more frequently

Cover more use cases for our customers



We welcome your involvement

Our dedicated GitHub org

https://github.com/aws-cloudformation

Public coverage roadmap

https://github.com/aws-cloudformation/aws-cloudformation-coverage-roadmap

AWS CloudFormation

https://aws.amazon.com/cloudformation/

AWS CloudFormation Slack channel:

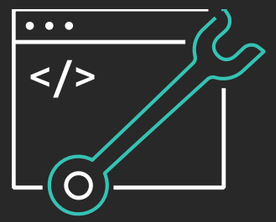
Twitter DM to @luiscolon1 or @thedanblanco with your email

Q&A

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learn DevOps with AWS Training and Certification

Resources created by the experts at AWS to propel your organization and career forward



Take free digital training to learn best practices for developing, deploying, and maintaining applications

Classroom offerings, like DevOps Engineering on AWS, feature AWS expert instructors and hands-on activities

Validate expertise with the **AWS Certified DevOps Engineer - Professional** or **AWS Certified Developer - Associate** exams

Visit aws.amazon.com/training/path-developing/

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws training and certification

Thank you!

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Please complete the session survey in the mobile app.

AWS re:Invent

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws