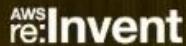


DEV317

# Deep Dive on AWS CloudFormation

Anil Kumar, Senior Product Manager  
Luis Colon, Senior Developer Advocate

November 28, 2017



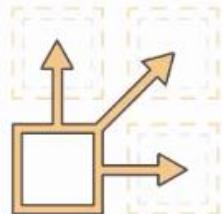
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## THEMES *for this session*



System Admins:  
Safety Guardrails



System Admins:  
Provisioning at scale



Developers:  
Test and Validate



Developers:  
Serverless Apps

# AGENDA

*What to expect from this session*

Learn how to...



- Protect stacks and monitor resources for changes



- Provision AWS resources across accounts and regions



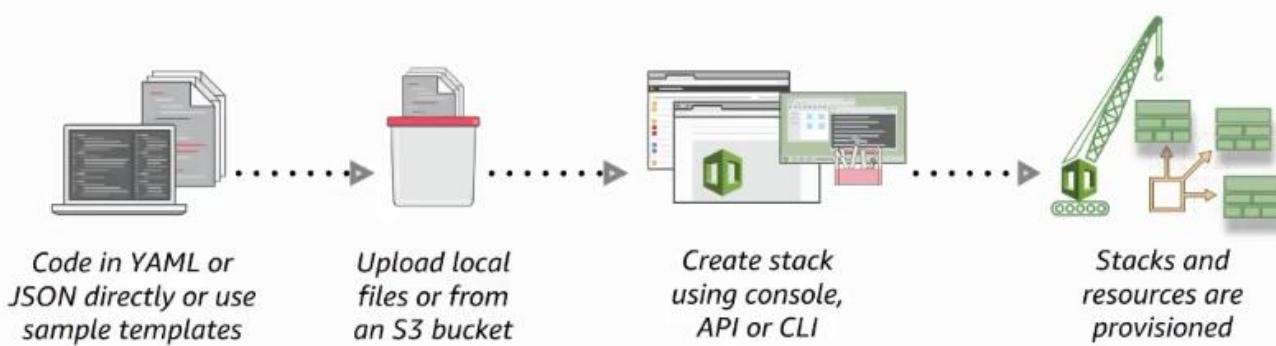
- Improve deployment reliability with validation



- Options to create and deploy serverless apps

## AWS CLOUDFORMATION AT A GLANCE

Enables provisioning and management of your infrastructure



**CloudFormation** CF is an infrastructure as code service by AWS, it allows you to provision your resources as well as be able to manage the entire lifecycle of those resources on AWS. You simply create your YAML or JSON files where you define the configuration on the resources you want to configure on AWS, upload the templates, then leverage the CF API to create your stacks.

# AWS CLOUDFORMATION AT A GLANCE



Over 350,000 AWS customers use AWS CloudFormation.



Over 75% of the top 10,000 highest spend AWS customers use AWS CloudFormation.



Over 2.4M AWS CloudFormation stacks are managed by AWS customers on AWS CloudFormation.

## AGENDA

*What to expect from this session*

Learn how to...



- **Protect stacks** and monitor resources for changes



- Provision AWS resources across accounts and regions



- Improve deployment reliability with validation

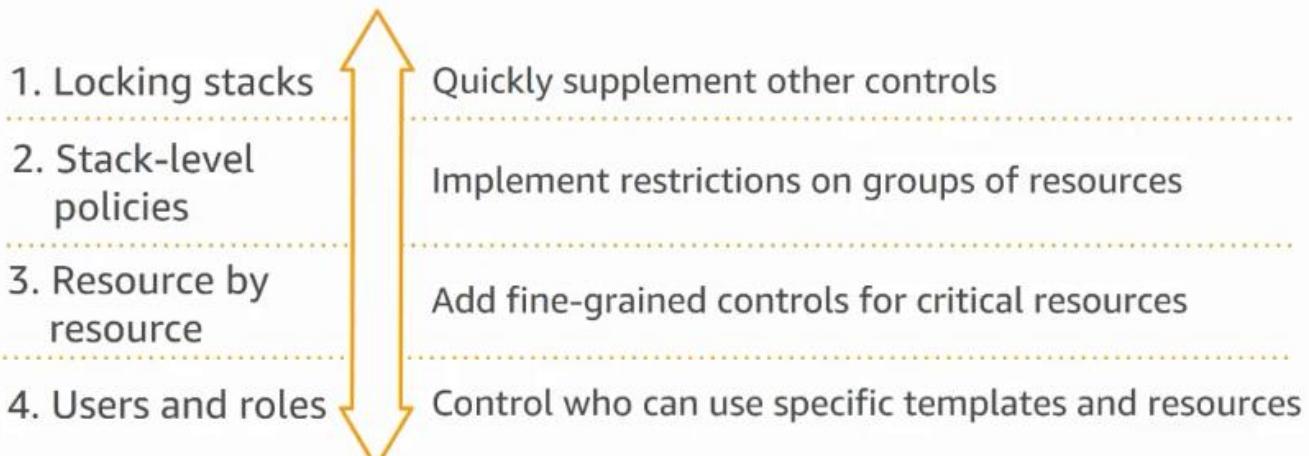


- Options to create and deploy serverless apps

# PROTECTING STACKS AND RESOURCES



Implementing **multiple layers** of guardrails



## 1. STACK TERMINATION PROTECTION



### Advanced

You can set additional options for your stack, like notification options and a stack policy. Learn more.

#### Notification options

No notification

New Amazon SNS topic

Topic

Email

Existing Amazon SNS topic

Existing topic ARN

#### Overview

#### Outputs

#### Resources

#### Events

**Stack name:** AppPipeline

**Stack ID:** arn:aws:cloudformation:123456789012:stack/AppPipeline/1234567890123456

**Status:** CREATE\_COMPLETE

**Status reason:**

**Termination protection:** Enabled

IAM Roles

Termination Protection  Enabled  
 Disabled

*ideal for **critical** stacks*



AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

After enabling Termination Protection as above when you try to delete this API, your DELETE stack API call will fail. You will have to disable the Termination Protection on the stack again before your DELETE stack API call can succeed.

## 2. STACK LEVEL POLICIES

```
{  
  "Statement" : [  
    {  
      "Effect" : "Deny",  
      "Action" : "Update:*",  
      "Principal": "*",  
      "Resource" : "*",  
      "Condition" : {  
        "StringEquals" : {  
          "ResourceType" : ["AWS::RDS::DBInstance"]  
        }  
      }  
    },  
    {  
      "Effect" : "Allow",  
      "Action" : "Update:*",  
      "Principal": "*",  
      "Resource" : "*"  
    }  
  ]  
}
```

*Example: only prevent updates to  
all RDS database instances*



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## 3. RESOURCE LEVEL POLICIES

```
{  
  "AWSTemplateFormatVersion": "2010-09-09",  
  "Resources": {  
    "myVolume": {  
      "Type": "AWS::EC2::Volume",  
      "DeletionPolicy": "Snapshot",  
      "Properties": {  
        "AvailabilityZone": "us-east-1a",  
        "Size": "200"  
      }  
    }  
  }  
}
```

*Example: deletion policy to  
backup/snapshot an EC2 volume*



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



This can be used on S3 buckets that you don't want to delete

## 4. USING IAM POLICIES



```
{  
    "Effect": "Allow",  
    "Action": ["cloudformation>CreateStack"]  
},  
{  
    "Effect": "Deny",  
    "Action": ["cloudformation>CreateStack"]  
    "Condition": {  
        "ForAnyValue:StringLike": {  
            "cloudformation:ResourceType": ["AWS::IAM::*"]  
        }  
    }  
}
```

Example: **deny** CreateStack  
operation for IAM resources



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## AGENDA

*What to expect from this session*

Learn how to...



- Protect stacks and **monitor resources for changes**



- Provision AWS resources across accounts and regions



- Improve deployment reliability with validation



- Options to create and deploy serverless apps



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



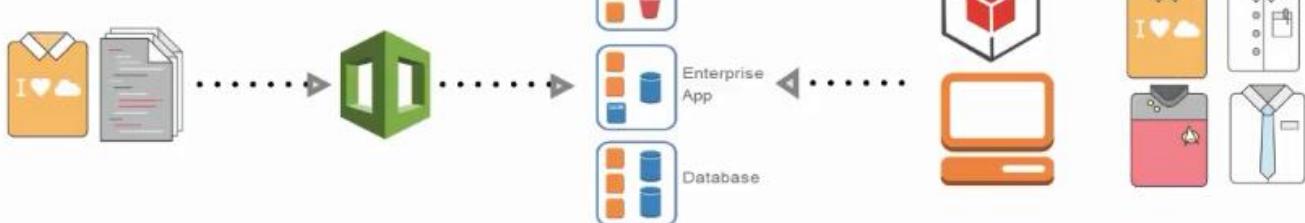
# MONITORING STACKS AND RESOURCE CHANGES

Implementing **multiple layers** of guardrails



- |                                  |  |
|----------------------------------|--|
| 1. Detecting configuration drift | Tracking changes made outside of CloudFormation to stack resources |
| 2. Dynamic monitoring            | Monitoring during the stack creation and update                    |
| 3. Recording changes             | Assess, audit, and evaluate configurations                         |

## CONFIGURATION DRIFT



Planned changes can be properly tested...

**IN CASE OF  
EMERGENCY  
BREAK GLASS**

...but not all changes can be planned!

## CONFIGURATION DRIFT DEFINED



Any changes made outside of AWS CloudFormation to one or more resources contained in a stack that modify the expected configuration values of resources would cause **drift** in the stack.

The change can be any of the following:

- Modifying stack resource property values
- Modifying default values of stack resources
- Deleting stack resources

## CONFIGURATION DRIFT DEFINED



### Key Concepts

- Expected values: stated in CloudFormation templates & defaults
- Current values: live configuration values of resources provisioned
- Drift = difference between Expected and Current values

## CONFIGURATION DRIFT: SIDE EFFECTS



### Stack Operation

- Can cause the stack update operation to fail
- Move the stack to a state in which you cannot update or delete the stack



*Delays in infrastructure updates*

### Audit and Compliance

- Divergence from your approved architecture
- Unaccounted changes, not reflected in your source code (templates)



*Fragile change control; non-compliance*



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## WHAT DO WE NEED?



A feature that allows you to detect and view changes made outside of CloudFormation to AWS resources managed by CloudFormation.

*Visibility*



*Detect & Compare*

## DRIFT DETECTION – COMING SOON



**Coming soon in 2018**, Configuration drift detection capability in AWS CloudFormation will be generally available in all AWS commercial regions.

### AWS CLOUDFORMATION DRIFT DETECTION DEMO

```
drift % aws cloudformation create-stack --stack-name events --template-body file:///events.yaml
{
  "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-11e7-be7
7-50d502dc688e"
}
drift % cat events.yaml
---
Resources:
  Events:
    Type: "AWS::DynamoDB::Table"
    Properties:
      KeySchema:
        -
          AttributeName: EventId
          KeyType: HASH
      AttributeDefinitions:
        -
          AttributeName: EventId
```

```
Resources:
Events:
  Type: "AWS::DynamoDB::Table"
  Properties:
    KeySchema:
      -
        AttributeName: EventId
        KeyType: HASH
    AttributeDefinitions:
      -
        AttributeName: EventId
        AttributeType: S
  ProvisionedThroughput:
    ReadCapacityUnits: 20
    WriteCapacityUnits: 20
EventQueue:
  Type: "AWS::SQS::Queue"
drift %
```

```
drift % aws cloudformation describe-stacks --stack-name events | less
```

```
{
  "Stacks": [
    {
      "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-11e7-be77-50d502dc688e",
      "DriftInformation": {
        "LastCheckTimestamp": "2017-11-21T01:14:33.611Z",
        "StackDriftStatus": "NOT_DRIFTED"
      },
      "Tags": [],
      "EnableTerminationProtection": false,
      "CreationTime": "2017-11-21T00:51:42.630Z",
      "StackName": "events",
      "NotificationARNs": [],
      "StackStatus": "CREATE_COMPLETE",
      "DisableRollback": false,
      "RollbackConfiguration": {}
    }
  ]
}
```

```
{  
    "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-  
11e7-be77-50d502dc688e",  
    "DriftInformation": {  
        "LastCheckTimestamp": "2017-11-21T01:14:33.611Z",  
        "StackDriftStatus": "NOT_DRIFTED"  
    },  
    "Tags": [],  
    "EnableTerminationProtection": false,  
    "CreationTime": "2017-11-21T00:51:42.630Z",  
    "StackName": "events",  
    "NotificationARNs": [],  
    "StackStatus": "CREATE_COMPLETE",  
    "DisableRollback": false,  
    "RollbackConfiguration": {}  
}  
]  
:
```

```
drift % aws cloudformation describe-stacks --stack-name events | less  
drift % aws cloudformation detect-stack-drift --stack-name events  
{  
    "StackDriftDetectionId": "731c5fa0-ce59-11e7-a99b-50d502d3d48e"  
}  
drift % aws cloudformation describe-stack-drift-detection-status --stack-drift-detection-id 731c5  
fa0-ce59-11e7-a99b-50d502d3d48e  
{  
    "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-11e7-be7  
7-50d502dc688e",  
    "StackDriftDetectionId": "731c5fa0-ce59-11e7-a99b-50d502d3d48e",  
    "StackDriftStatus": "NOT_DRIFTED",  
    "Timestamp": "2017-11-21T01:15:23.675Z",  
    "DetectionStatus": "DETECTION_COMPLETE",  
    "DriftedStackResourceCount": 0  
}  
drift %
```

```
drift % aws cloudformation describe-stack-resource-drifts --stack-name events | less
```

```
{  
  "StackResourceDrifts": [  
    {  
      "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-  
11e7-be77-50d502dc688e",  
      "ActualProperties": "{\"ReceiveMessageWaitTimeSeconds\":0,\"DelaySeconds\":0,\"Message  
RetentionPeriod\":345600,\"MaximumMessageSize\":262144,\"VisibilityTimeout\":30,\"QueueName\":\"  
events-EventQueue-T0U5BUNQEMG1\"}",  
      "ResourceType": "AWS::SQS::Queue",  
      "Timestamp": "2017-11-21T01:15:24.310Z",  
      "PhysicalResourceId": "https://sns.us-east-1.amazonaws.com/376991696843/events-EventQ  
ueue-T0U5BUNQEMG1",  
      "StackResourceDriftStatus": "NOT_DRIFTED",  
      "ExpectedProperties": "{\"ReceiveMessageWaitTimeSeconds\":0,\"DelaySeconds\":0,\"Message  
RetentionPeriod\":345600,\"MaximumMessageSize\":262144,\"VisibilityTimeout\":30,\"QueueName\":\"  
events-EventQueue-T0U5BUNQEMG1\"}",  
      "PropertyDifferences": []  
    },  
    ...  
  ]  
}
```

```
},  
{  
  "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-  
11e7-be77-50d502dc688e",  
  "ActualProperties": "{\"TableName\":\"events-Events-1A6CYGLS0DA35\",\"ProvisionedThro  
ughput\":{\"ReadCapacityUnits\":20,\"WriteCapacityUnits\":20},\"AttributeDefinitions\":[{\"Attrib  
uteName\":\"EventId\",\"AttributeType\":\"S\"}],\"KeySchema\":[{\"AttributeName\":\"EventId\",\"K  
eyType\":\"HASH\"]}]",  
  "ResourceType": "AWS::DynamoDB::Table",  
  "Timestamp": "2017-11-21T01:15:24.821Z",  
  "PhysicalResourceId": "events-Events-1A6CYGLS0DA35",  
  "StackResourceDriftStatus": "NOT_DRIFTED",  
  "ExpectedProperties": "{\"TableName\":\"events-Events-1A6CYGLS0DA35\",\"ProvisionedTh  
roughput\":{\"ReadCapacityUnits\":20,\"WriteCapacityUnits\":20},\"AttributeDefinitions\":[{\"Attr  
ibuteName\":\"EventId\",\"AttributeType\":\"S\"}],\"KeySchema\":[{\"AttributeName\":\"EventId\",\"K  
eyType\":\"HASH\"]}]",  
  "PropertyDifferences": []  
},  
...  
]
```

```
drift % aws dynamodb update-table --table-name events-Events-1A6CYGLS0DA35 --provisioned-throughp  
ut ReadCapacityUnits=50,WriteCapacityUnits=50
```

```
        "LastIncreaseDateTime": 1511227606.278,
        "ReadCapacityUnits": 20,
        "LastDecreaseDateTime": 1511227575.543
    },
    "TableSizeBytes": 0,
    "TableName": "events-Events-1A6CYGLS0DA35",
    "TableStatus": "UPDATING",
    "KeySchema": [
        {
            "KeyType": "HASH",
            "AttributeName": "EventId"
        }
    ],
    "ItemCount": 0,
    "CreationDateTime": 1511225507.831
}
}
drift %
```

```
drift % aws cloudformation detect-stack-resource-drift --stack-name events --logical-resource-id Events | less
```

```
{
    "StackResourceDrift": {
        "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-11e7-be77-50d502dc688e",
        "ActualProperties": "{\"TableName\":\"events-Events-1A6CYGLS0DA35\",\"ProvisionedThroughput\":{\"ReadCapacityUnits\":50,\"WriteCapacityUnits\":50},\"AttributeDefinitions\":[{\"AttributeName\":\"EventId\",\"AttributeType\":\"S\"}],\"KeySchema\":[{\"AttributeName\":\"EventId\",\"KeyType\":\"HASH\"]}]",
        "ResourceType": "AWS::DynamoDB::Table",
        "Timestamp": "2017-11-21T01:28:39.083Z",
        "PhysicalResourceId": "events-Events-1A6CYGLS0DA35",
        "StackResourceDriftStatus": "MODIFIED",
        "ExpectedProperties": "{\"TableName\":\"events-Events-1A6CYGLS0DA35\",\"ProvisionedThroughput\":{\"ReadCapacityUnits\":20,\"WriteCapacityUnits\":20},\"AttributeDefinitions\":[{\"AttributeName\":\"EventId\",\"AttributeType\":\"S\"}],\"KeySchema\":[{\"AttributeName\":\"EventId\",\"KeyType\":\"HASH\"]}]",
        "PropertyDifferences": [
    }
```

```
ut\" : {\"ReadCapacityUnits\":50, \"WriteCapacityUnits\":50}, \"AttributeDefinitions\":[{\"AttributeNa  
ame\":\"EventId\", \"AttributeType\":\"S\"}], \"KeySchema\":[{\"AttributeName\":\"EventId\", \"KeyTy  
pe\":\"HASH\"]}],  
    \"ResourceType\": \"AWS::DynamoDB::Table\",  
    \"Timestamp\": \"2017-11-21T01:28:39.083Z\",  
    \"PhysicalResourceId\": \"events-Events-1A6CYGLS0DA35\",  
    \"StackResourceDriftStatus\": \"MODIFIED\",  
    \"ExpectedProperties\": {\"TableName\":\"events-Events-1A6CYGLS0DA35\", \"ProvisionedThrough  
put\":[\"ReadCapacityUnits\":20, \"WriteCapacityUnits\":20], \"AttributeDefinitions\":[{\"Attribut  
eName\":\"EventId\", \"AttributeType\":\"S\"}], \"KeySchema\":[{\"AttributeName\":\"EventId\", \"Key  
Type\":\"HASH\"]}]}},  
    \"PropertyDifferences\": [  
        {  
            \"PropertyPath\": \"/ProvisionedThroughput/WriteCapacityUnits\",  
            \"ActualValue\": \"50\",  
            \"ExpectedValue\": \"20\",  
            \"DifferenceType\": \"NOT_EQUAL\"  
        },  
        {  
            \"PropertyPath\": \"/ProvisionedThroughput/ReadCapacityUnits\",  
            \"ActualValue\": \"50\",  
            \"ExpectedValue\": \"20\",  
            \"DifferenceType\": \"NOT_EQUAL\"  
        }  
    ]  
},  
:  
:
```

```
hput\":[{\"ReadCapacityUnits\":20, \"WriteCapacityUnits\":20}, \"AttributeDefinitions\":[{\"Attribut  
eName\":\"EventId\", \"AttributeType\":\"S\"}], \"KeySchema\":[{\"AttributeName\":\"EventId\", \"Key  
Type\":\"HASH\"]}]}},  
    \"PropertyDifferences\": [  
        {  
            \"PropertyPath\": \"/ProvisionedThroughput/WriteCapacityUnits\",  
            \"ActualValue\": \"50\",  
            \"ExpectedValue\": \"20\",  
            \"DifferenceType\": \"NOT_EQUAL\"  
        },  
        {  
            \"PropertyPath\": \"/ProvisionedThroughput/ReadCapacityUnits\",  
            \"ActualValue\": \"50\",  
            \"ExpectedValue\": \"20\",  
            \"DifferenceType\": \"NOT_EQUAL\"  
        }  
    ]  
},  
:  
:
```

Now CF has detected that the stack has drifted due to the out-of-band change made

```
drift % aws cloudformation detect-stack-resource-drift --stack-name events --logical-resource-id  
Events | less  
drift % aws cloudformation describe-stacks --stack-name events | less
```

```
{  
  "Stacks": [  
    {  
      "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-  
11e7-be77-50d502dc688e",  
      "DriftInformation": {  
        "LastCheckTimestamp": "2017-11-21T01:28:39.083Z",  
        "StackDriftStatus": "DRIFTED"  
      },  
      "Tags": [],  
      "EnableTerminationProtection": false,  
      "CreationTime": "2017-11-21T00:51:42.630Z",  
      "StackName": "events",  
      "NotificationARNs": [],  
      "StackStatus": "CREATE_COMPLETE",  
      "DisableRollback": false,  
      "RollbackConfiguration": {}  
    }  
  ]
```

```
{  
  "Stacks": [  
    {  
      "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-  
11e7-be77-50d502dc688e",  
      "DriftInformation": {  
        "LastCheckTimestamp": "2017-11-21T01:28:39.083Z",  
        "StackDriftStatus": "DRIFTED"  
      },  
      "Tags": [],  
      "EnableTerminationProtection": false,  
      "CreationTime": "2017-11-21T00:51:42.630Z",  
      "StackName": "events",  
      "NotificationARNs": [],  
      "StackStatus": "CREATE_COMPLETE",  
      "DisableRollback": false,  
      "RollbackConfiguration": {}  
    }  
  ]
```

```
drift % aws dynamodb update-table --table-name events-Events-1A6CYGLS0DA35 --provisioned-throughput ReadCapacityUnits=20,WriteCapacityUnits=20
```

```
        "LastIncreaseDateTime": 1511227618.652,
        "ReadCapacityUnits": 50,
        "LastDecreaseDateTime": 1511228570.714
    },
    "TableSizeBytes": 0,
    "TableName": "events-Events-1A6CYGLS0DA35",
    "TableStatus": "UPDATING",
    "KeySchema": [
        {
            "KeyType": "HASH",
            "AttributeName": "EventId"
        }
    ],
    "ItemCount": 0,
    "CreationDateTime": 1511225507.831
}
}
drift %
```

```
drift % aws cloudformation detect-stack-resource-drift --stack-name events --logical-resource-id Events | less
```

```
-be77-50d502dc688e",
    "ActualProperties": "{\"TableName\":\"events-Events-1A6CYGLS0DA35\",\"ProvisionedThroughput\":{\"ReadCapacityUnits\":20,\"WriteCapacityUnits\":20},\"AttributeDefinitions\":[{\"AttributeName\":\"EventId\",\"AttributeType\":\"S\"}],\"KeySchema\":[{\"AttributeName\":\"EventId\",\"KeyType\":\"HASH\"]}]",
    "ResourceType": "AWS::DynamoDB::Table",
    "Timestamp": "2017-11-21T01:48:17.416Z",
    "PhysicalResourceId": "events-Events-1A6CYGLS0DA35",
    "StackResourceDriftStatus": "NOT_DRIFTED",
    "ExpectedProperties": "{\"TableName\":\"events-Events-1A6CYGLS0DA35\",\"ProvisionedThroughput\":{\"ReadCapacityUnits\":20,\"WriteCapacityUnits\":20},\"AttributeDefinitions\":[{\"AttributeName\":\"EventId\",\"AttributeType\":\"S\"}],\"KeySchema\":[{\"AttributeName\":\"EventId\",\"KeyType\":\"HASH\"]}]",
    "PropertyDifferences": [],
    "LogicalResourceId": "Events"
}
:
```

```
drift % aws cloudformation detect-stack-resource-drift --stack-name events --logical-resource-id Events | less
drift % aws cloudformation describe-stack-resources --stack-name events | less
```

```
{  
  "StackResources": [  
    {  
      "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-  
11e7-be77-50d502dc688e",  
      "ResourceStatus": "CREATE_COMPLETE",  
      "DriftInformation": {  
        "StackResourceDriftStatus": "NOT_DRIFTED"  
      },  
      "ResourceType": "AWS::SQS::Queue",  
      "Timestamp": "2017-11-21T00:51:57.944Z",  
      "StackName": "events",  
      "PhysicalResourceId": "https://sns.us-east-1.amazonaws.com/376991696843/events-EventQ  
ueue-T0U5BUNQEMG1",  
      "LogicalResourceId": "EventQueue"  
    },  
    {  
      :  
    }  
  ]  
}
```

```
  "LogicalResourceId": "EventQueue"  
  },  
  {  
    "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-  
11e7-be77-50d502dc688e",  
    "ResourceStatus": "CREATE_COMPLETE",  
    "DriftInformation": {  
      "StackResourceDriftStatus": "NOT_DRIFTED"  
    },  
    "ResourceType": "AWS::DynamoDB::Table",  
    "Timestamp": "2017-11-21T00:52:20.505Z",  
    "StackName": "events",  
    "PhysicalResourceId": "events-Events-1A6CYGLS0DA35",  
    "LogicalResourceId": "Events"  
  }  
]  
:  
:
```

```
drift % aws dynamodb delete-table --table-name events-Events-1A6CYGLS0DA35  
{  
  "TableDescription": {  
    "TableArn": "arn:aws:dynamodb:us-east-1:376991696843:table/events-Events-1A6CYGLS0DA35",  
    "ProvisionedThroughput": {  
      "NumberOfDecreasesToday": 0,  
      "WriteCapacityUnits": 20,  
      "ReadCapacityUnits": 20  
    },  
    "TableSizeBytes": 0,  
    "TableName": "events-Events-1A6CYGLS0DA35",  
    "TableStatus": "DELETING",  
    "ItemCount": 0  
  }  
}  
drift %
```

```
drift % aws cloudformation detect-stack-resource-drift --stack-name events --logical-resource-id  
Events | less
```

```
{
  "StackResourceDrift": {
    "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-11e7-be77-50d502dc688e",
    "ResourceType": "AWS::DynamoDB::Table",
    "Timestamp": "2017-11-21T01:51:09.417Z",
    "PhysicalResourceId": "events-Events-1A6CYGLS0DA35",
    "StackResourceDriftStatus": "DELETED",
    "LogicalResourceId": "Events"
  }
}
(END)
```

## DRIFT DETECTION – CONSOLE WALKTHROUGH (1/8)



CloudFormation > Stacks

Create Stack Actions Design template

Filter: Active ▾ By Stack Name

Showing 22 stacks

Stack Name	Created Time	Status	Drift Status	Description
Drift-DEMO	2017-11-21 12:05:53 UTC-0800	CREATE_COMPLETE	NOT_DRIFTED	
SQS-Drift-DEMO-BETA	2017-11-14 09:57:57 UTC-0800	CREATE_COMPLETE	DRIFTED	
createChange	2017-11-10 10:08:06 UTC-0800	CREATE_COMPLETE	NOT_CHECKED	
CreateChange	2017-11-10 10:08:54 UTC-0800	CREATE_COMPLETE	NOT_DRIFTED	
testCreateChange	2017-11-10 09:58:09 UTC-0800	REVIEW_IN_PROGRESS	NOT_CHECKED	
SQS-Drift-DEMO	2017-11-08 10:03:09 UTC-0800	CREATE_COMPLETE	DRIFTED	
DynamoDB-Drift	2017-11-08 18:12:29 UTC-0800	CREATE_COMPLETE	DRIFTED	
DynamoDB_Events	2017-11-08 19:44:48 UTC-0800	ROLLBACK_COMPLETE	NOT_CHECKED	

Overview Outputs Resources Events Template Parameters Tags Stack Policy Change Sets

Stack name: Drift-DEMO  
 Stack ID: arn:aws:cloudformation:us-east-1:260496401202:stack/Drift-DEMO/B465cf80-cef7-11e7-bb30-50d5033d80fe  
 Status: CREATE\_COMPLETE  
 Status reason:  
 Termination protection: Disabled  
 Drift status: NOT\_DRIFTED View details  
 Last drift check time: 2017-11-21 12:07:16 UTC-0800



## DRIFT DETECTION – CONSOLE (2/8)



Screenshot of the AWS CloudFormation console showing the Stacks page. A context menu is open over the 'Drift-DEMO' stack, with the option 'Detect drift for current stack' highlighted.

Stack Name	Last Updated	Status	Drift Status	Description
Drift-DEMO	2017-11-10 10:08:53 UTC-0800	CREATE_COMPLETE	NOT_DRIFTED	
SQS-Drift-DEM	2017-11-09 10:57:57 UTC-0800	CREATE_COMPLETE	DRIFTED	
createChange	2017-11-09 10:08:06 UTC-0800	CREATE_COMPLETE	NOT_CHECKED	
CreateChange	2017-11-10 10:08:54 UTC-0800	CREATE_COMPLETE	NOT_DRIFTED	
testCreateChange	2017-11-10 09:59:09 UTC-0800	REVIEW_IN_PROGRESS	NOT_CHECKED	
SQS-Drift-DEMO	2017-11-09 10:03:09 UTC-0800	CREATE_COMPLETE	DRIFTED	
DynamicDB-Drift	2017-11-08 15:12:29 UTC-0800	CREATE_COMPLETE	DRIFTED	
sns-drift-example	2017-11-08 10:44:48 UTC-0800	PENDING_COMPLETE	NOT_CHECKED	

Stack name: Drift-DEMO  
Stack ID: arn:aws:cloudformation:us-east-1:260496401202:stack/Drift-DEMO/8485d680-0ef7-11e7-bb30-50d5033d80fe  
Status: CREATE\_COMPLETE  
Status reason:  
Termination protection: Disabled  
Drift status: NOT\_DRIFTED View details  
Last drift check time: 2017-11-21 12:07:16 UTC-0800

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

## DRIFT DETECTION – CONSOLE (3/8)



Screenshot of the AWS CloudFormation console showing the Stacks page. A modal dialog box titled 'Detect drift' is open over the 'Drift-DEMO' stack.

Detect drift

Detecting drift could take several minutes, depending on the number of resources present in a stack. Drift detection will continue for this stack, even if you close this window.

Stack name: Drift-DEMO  
Detection status:   
Drift status:   
Last drift check time:

Stack name: Drift-DEMO  
Stack ID: arn:aws:cloudformation:us-east-1:260496401202:stack/Drift-DEMO/8485d680-0ef7-11e7-bb30-50d5033d80fe  
Status: CREATE\_COMPLETE  
Status reason:  
Termination protection: Disabled  
Drift status: NOT\_DRIFTED View details  
Last drift check time: 2017-11-21 12:07:16 UTC-0800

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

## DRIFT DETECTION – CONSOLE (4/8)



Screenshot of the AWS CloudFormation console showing the 'Detect drift' dialog box. The dialog box displays the following information:

- Stack name: Drift-DEMO
- Detection status: DETECTION\_COMPLETE
- Drift status: DRIFTED (highlighted with a yellow arrow)
- Last drift check time: 2017-11-21 12:17:22 UTC-0800

The main CloudFormation interface shows the stack 'Drift-DEMO' with status CREATE\_COMPLETE and last drift check time 2017-11-21 12:16:08 UTC-0800.

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## DRIFT DETECTION – CONSOLE (5/8)



Screenshot of the AWS CloudFormation console showing the 'Drift Details' page for the stack 'Drift-DEMO'.

**Overview**

Stack name: Drift-DEMO  
Stack ID: arn:aws:cloudformation:us-east-1:260496401202:stack/Drift-DEMO/B465d680-cef7-11e7-bb30-50d5033d80fe  
Status: CREATE\_COMPLETE  
Drift status: DRIFTED  
Last drift check time: 2017-11-21 12:17:24 UTC-0800

**Resource drift status**

Logical ID	Physical ID	Type	Resource drift status	Timestamp
DLO	https://sqs.us-east-1.amazonaws.com/26...	AWS::SQS::Queue	NOT_DRIFTED	2017-11-21 12:17:23 UTC-0800
Queue	https://sqs.us-east-1.amazonaws.com/26...	AWS::SQS::Queue	MODIFIED	2017-11-21 12:17:24 UTC-0800

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## DRIFT DETECTION – CONSOLE (5/8)



CloudFormation > Stacks > Stack Detail > Drift Detail

### Drift Details: Drift-DEMO

**Overview**

Stack name: Drift-DEMO  
Stack ID: arn:aws:cloudformation:us-east-1:260496401202:stack/Drift-DEMO/8465d680-cef7-11e7-bb30-50d5033d80fe  
Status: CREATE\_COMPLETE  
Drift status: ⚠ DRIFTED  
Last drift check time: 2017-11-21 12:17:24 UTC-0800

**Detect drift for current stack**

**Resource drift status**

**Detect drift for resource**

Logical ID	Physical ID	Type	Resource drift status	Timestamp
DLQ	https://sqs.us-east-1.amazonaws.com/26...	AWS::SQS::Queue	<span style="color: green;">✓ NOT_DRIFTED</span>	2017-11-21 12:17:23 UTC-0800
Queue	https://sqs.us-east-1.amazonaws.com/26...	AWS::SQS::Queue	<span style="color: orange;">⚠ MODIFIED</span>	2017-11-21 12:17:24 UTC-0800

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## DRIFT DETECTION – CONSOLE (6/8)



### Resource drift status

**Detect drift for resource**

**Filter: All**

	Logical ID	Physical ID	Type	Resource drift status	Timestamp
<input type="checkbox"/>	DLQ	https://sqs.us-east-1.amazonaws.com/26...	AWS::SQS::Queue	<span style="color: green;">✓ NOT_DRIFTED</span>	2017-11-21 12:17:23 UTC-0800
<input checked="" type="checkbox"/>	Queue	https://sqs.us-east-1.amazonaws.com/26...	AWS::SQS::Queue	<span style="color: orange;">⚠ MODIFIED</span>	2017-11-21 12:17:24 UTC-0800

**Expected**

```
{
    "ReceiveMessageWaitTimeSeconds": 0,
    "DelaySeconds": 20,
    "RedrivePolicy": {
        "deadLetterTargetArn": "arn:aws:sqs:us-ea",
        "maxReceiveCount": 10
    },
    "MessageRetentionPeriod": 345600,
    "MaximumMessageSize": 262144,
    "VisibilityTimeout": 60,
    "QueueName": "Drift-DEMO-Queue-T63J7LA6V4"
}
```

**Current**

```
{
    "ReceiveMessageWaitTimeSeconds": 0,
    "DelaySeconds": 20,
    "KmsMasterKeyId": "alias/aws/sqs",
    "MessageRetentionPeriod": 345600,
    "MaximumMessageSize": 262144,
    "VisibilityTimeout": 600,
    "KmsDataKeyReusePeriodSeconds": 300,
    "QueueName": "Drift-DEMO-Queue-T63J7LA6V4"
}
```

**Differences (4)**

Select all | Clear

- /RedrivePolicy - REMOVE
- /VisibilityTimeout - NOT\_EQUAL
- /KmsMasterKeyId - ADD
- /KmsDataKeyReusePeriodSeconds - ADD

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## DRIFT DETECTION – CONSOLE (7/8)



### Resource drift status

Detect drift for resource



Filter: All ▾

	Logical ID	Physical ID	Type	Resource drift status	Timestamp
<input type="checkbox"/>	DLQ	https://sqs.us-east-1.amazonaws.com/26...	AWS::SQS::Queue	<span>● NOT_DRIFTED</span>	2017-11-21 12:17:23 UTC-0800
<input checked="" type="checkbox"/>	Queue	https://sqs.us-east-1.amazonaws.com/26...	AWS::SQS::Queue	<span>⚠ MODIFIED</span>	2017-11-21 12:17:24 UTC-0800

**Expected**

```
{
    "ReceiveMessageWaitTimeSeconds": 0,
    "DelaySeconds": 20,
    "RedrivePolicy": {
        "deadLetterTargetArn": "arn:aws:sqs:us-",
        "maxReceiveCount": 10
    },
    "MessageRetentionPeriod": 345600,
    "MaximumMessageSize": 262144,
    "VisibilityTimeout": 60,
    "QueueName": "Drift-DEMO-Queue-T63J7LA6V4"
}
```

**Current**

```
{
    "ReceiveMessageWaitTimeSeconds": 0,
    "DelaySeconds": 20,
    "KmsMasterKeyId": "alias/aws/sqs",
    "MessageRetentionPeriod": 345600,
    "MaximumMessageSize": 262144,
    "VisibilityTimeout": 600,
    "KmsDataKeyReusePeriodSeconds": 300,
    "QueueName": "Drift-DEMO-Queue-T63J7LA6V4"
}
```

**Differences (4)**

Select all | Clear

- /RedrivePolicy - REMOVE
- /VisibilityTimeout - NOT\_EQUAL
- /KmsMasterKeyId - ADD
- /KmsDataKeyReusePeriodSeconds - ADD



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## DRIFT DETECTION – CONSOLE (8/8)



### Resource drift status

Detect drift for resource



Filter: All ▾

	Logical ID	Physical ID	Type	Resource drift status	Timestamp
<input checked="" type="checkbox"/>	DLQ	https://sqs.us-east-1.amazonaws.com/26...	AWS::SQS::Queue	<span>⚠ DELETED</span>	2017-11-21 12:19:35 UTC-0800
<input type="checkbox"/>	Queue	https://sqs.us-east-1.amazonaws.com/26...	AWS::SQS::Queue	<span>⚠ MODIFIED</span>	2017-11-21 12:17:24 UTC-0800



### Resource drift status

Detect drift for resource



Filter: All ▾

	Logical ID	Physical ID	Type	Resource drift status	Timestamp
<input type="checkbox"/>	DLQ	https://sqs.us-east-1.amazonaws.com/26...	AWS::SQS::Queue	<span>⚠ DELETED</span>	2017-11-21 12:19:35 UTC-0800
This resource has been deleted.					
<input type="checkbox"/>	Queue	https://sqs.us-east-1.amazonaws.com/26...	AWS::SQS::Queue	<span>⚠ MODIFIED</span>	2017-11-21 12:17:24 UTC-0800



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## 2. DYNAMIC MONITORING USING ROLLBACK TRIGGERS

*Revert changes impacting performance*



Integrate application- and stack resource-level alarms from Amazon CloudWatch



Monitor these alarms while updating stacks



If alarms fire, AWS CloudFormation automatically rolls back



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## 2. DYNAMIC MONITORING USING ROLLBACK TRIGGERS

*Revert changes impacting performance (An example (1/2))*



### 1. BUILD A ROLLBACK TRIGGER

batch-service-rollbacktrigger.json

```
{  
  "RollbackTriggers": [  
    {  
      "Arn": "arn:aws:cloudwatch:us-east-  
2:xxxxxxxxxx:alarm:SQSQueueDepth",  
      "Type": "AWS::CloudWatch::Alarm"  
    }  
  ],  
  "MonitoringTimeInMinutes": 10  
}
```



### 2. UPDATE STACK USING THAT ROLLBACK TRIGGER

```
aws cloudformation update-stack --region us-east-2 \  
--stack-name ImageProcService \  
--template-body file://batch-service.yml \  
--parameters file://batch-service-config.json \  
--rollback-configuration file://batch-service-  
rollbacktrigger.json
```

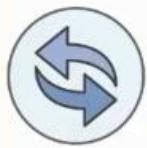


© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## 2. DYNAMIC MONITORING USING ROLLBACK TRIGGERS

*Revert changes impacting performance (An example (2/2))*



If in ALARM state,  
CloudFormation  
automatically  
rolls back

Stack Name	Created Time	Status	Description					
ImageProcService	2017-09-19 10:15:53 UTC-0700	UPDATE_ROLLBACK_COMPLETE						
Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets
2017-09-19	Status	Type	Logical ID	Status reason				
▶ 11:08:31 UTC-0700	UPDATE_ROLLBACK_COMPL	AWS::CloudFormation::Stack	ImageProcService					
ETE								
▶ 11:08:29 UTC-0700	UPDATE_ROLLBACK_COMPL	AWS::CloudFormation::Stack	ImageProcService					
ETE_CLEANUP_IN_PROGRESS								
▶ 11:08:29 UTC-0700	UPDATE_COMPLETE	AWS::ECS::Service	service					
▶ 11:07:28 UTC-0700	UPDATE_IN_PROGRESS	AWS::ECS::Service	service					
▶ 11:07:11 UTC-0700	UPDATE_ROLLBACK_IN_PROGRESS	AWS::CloudFormation::Stack	ImageProcService					
GRESS								
▶ 11:03:09 UTC-0700	UPDATE_COMPLETE	AWS::ECS::Service	service					
▶ 11:02:08 UTC-0700	UPDATE_IN_PROGRESS	AWS::ECS::Service	service					
▶ 11:02:04 UTC-0700	UPDATE_IN_PROGRESS	AWS::CloudFormation::Stack	ImageProcService					
			User Initiated					



AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

## 3. RECORD & MONITOR STACK CHANGES WITH AWS CONFIG

- Record configuration changes to CloudFormation stacks
- Track current and historical stack configuration
- Get notified via Amazon SNS when changes occur
- Maintain audit compliance and governance controls

Resource type

- ACM
- Certificate
- AutoScaling
- AutoScalingGroup
- LaunchConfiguration
- ScalingPolicy
- ScheduledAction
- CloudFormation
- Stack
- CloudFront
- Distribution



AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Config will record all the configuration changes that happens to all of its supported resource types like CF stacks.

### 3. RECORD & MONITOR STACK CHANGES WITH AWS CONFIG

*See changes using AWS Config timeline*

CloudFormation Stack MyProd-01-DynamoDBTable-01  
on November 19, 2017 2:28:38 PM Pacific Standard Time (UTC-08:00)

Manage resource Now View Details

Configuration Details

Amazon Resource Name	arn:aws:cloudformation:us-east-1:827326825706:stack/MyProd-01-DynamoDBTable-01/2:c967340-cd73-11e7-b792-500c212ff5fd	Stack Name	MyProd-01-DynamoDBTable-01
Resource type	AWS::CloudFormation::Stack	Stack Status	UPDATE_COMPLETE
Resource ID	arn:aws:cloudformation:us-east-1:827326825706:stack/MyProd-01-DynamoDBTable-01/2:c967340-cd73-11e7-b792-500c212ff5fd	Disable Rollback	false
Resource name	MyProd-01-DynamoDBTable-01	Notification ARNs	None
Availability zone	Regional		
Created on	November 19, 2017 1:47:01 PM		
Tags (4)	DynamoDB-Table:01 Prod 01 UseCase-StoreSem... Team:ProdApp1		

### 3. RECORD & MONITOR STACK CHANGES WITH AWS CONFIG

*Drill down further to see details*

Changes 3

Configuration Changes 2

Field	From	To
Configuration.lastUpdatedTime	"Nov 19, 2017 10:01:14 PM"	"Nov 19, 2017 10:10:10 PM"

SupplementaryConfiguration.StackResourceSummaries.0

Object	logicalResourceId: "Messages" physicalResourceId: "MyProd-01-DynamoDBTable-01-Messages-1/KX626YII9Y54" resourceType: "AWS::DynamoDB::Table" lastUpdatedTimestamp: "Nov 19, 2017 10:01:50 PM" resourceStatus: "UPDATE_COMPLETE"
--------	---

Relationship Changes 1

Field	From	To
AWS::DynamoDB::Table	"MyProd-01-DynamoDBTable-01-Messages-1/KX626YII9Y54"	"MyProd-01-DynamoDBTable-01-Messages-1/KX626YII9Y54"

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

### 3. RECORD & MONITOR STACK CHANGES WITH AWS CONFIG

Pre-built AWS Config rule: **cloudformation-stack-notification-check**

- Verify whether stacks are sending SNS notifications



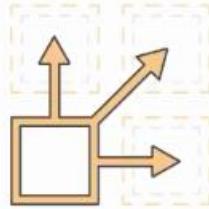
The screenshot shows the AWS Config Rules interface. It's Step 2: Rules of a three-step setup. The 'cloudformation-stack-notification-check' rule is highlighted with a blue border and an orange arrow pointing to it from the top right. The rule details are visible: it checks if CloudFormation stacks send event notifications to an SNS topic. Other rules like 'acm-certificate-expiration-check' and 'dynamodb-autoscaling-enabled' are also listed.

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



System Admins:  
Safety Guardrails



System Admins:  
Provisioning at scale

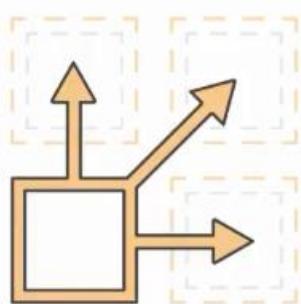


Developers:  
Test and Validate



Developers:  
Serverless Apps

## PROVISIONING AT SCALE

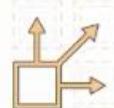


As enterprises grow, many leverage  
multiple accounts and regions

- Create boundaries for critical resources
  - Some regions or accounts may need to be restricted or isolated
- Reduce availability risks
  - Spreading traffic geographically

# PROVISIONING AT SCALE

*Let's look at few customer profiles*



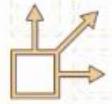
Customer Profile	#1	#2	#3
	<ul style="list-style-type: none"><li>• 2800+ accounts and wants to grow to 10,000 accounts</li></ul>	<ul style="list-style-type: none"><li>• 180+ accounts</li></ul>	<ul style="list-style-type: none"><li>• 19 accounts and plans to have 40 accounts</li></ul>
	<ul style="list-style-type: none"><li>• Deploy in nine AWS Regions and wants to be in 11 regions</li></ul>	<ul style="list-style-type: none"><li>• Deploy in selective regions</li></ul>	<ul style="list-style-type: none"><li>• Multiple regions</li></ul>
	<ul style="list-style-type: none"><li>• VPC, EC2, IAM, Subnet, Security Groups, and more</li></ul>	<ul style="list-style-type: none"><li>• VPC, IAM, CloudTrail, AWS Config</li></ul>	<ul style="list-style-type: none"><li>• VPC, Security Groups, IAM roles, CloudTrail</li></ul>

## PROVISIONING AT SCALE: CHALLENGES



- Multiple, manual operations can be error-prone
- Home-grown, multi-account, multi-region scripts add maintenance
- Third party tooling adds cost

# STACKSETS



Create and update stacks in **multiple** accounts and regions using a **single** operation



## CORE CONCEPTS

Three target accounts across three regions which delegate trust to the administrator account

Implements nine stack instances

done from an administrator account with an assumable IAM role

the **stackset** is a single global template



AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

You need to have a master account that is where you control everything and where you actually deploy the stack sets from. Then you will have a variety of target accounts in possibly different regions. This means that we can deploy 9 stack instances in a single operation. You can also have several accounts associated with an organization using AWS Organizations so that you can deploy to all the accounts using an organizationID in a single operation. The administrator account will have an assumed IAM Role, and the target accounts are going to delegate trust to that admin account.

# PROVISIONING AT SCALE WITH STACKSETS



## Set up new accounts with defaults

- Enable CloudTrail for all regions; use admin's S3 bucket
- Set up AWS Config rules to properly tag resources
- Set up AWS KMS keys

## Deploy identical infrastructure for globally used apps

- Manage app stacks across multiple regions
- Use CFN to speed up new region setup

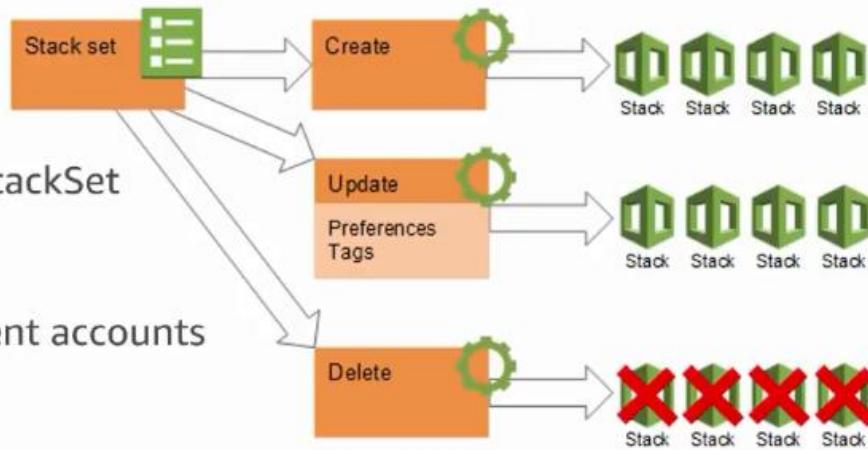
## Business Continuity/Disaster Recovery

- Configure Amazon S3 bucket replication
- Provision Amazon RDS read replicas

# STACKSET OPERATIONS

## Operations

- Create StackSet
- Update StackSet
- Delete stack and StackSet



## Options

- Maximum concurrent accounts
- Failure tolerance
- Retain stacks

## STACKSETS: EARLY ADOPTER FEEDBACK

*"[It] has simplified our continuous deployment initiative, allowing centralized management of pipelines deploying solutions across multiple functional AWS accounts. [It] greatly reduced project complexity while providing greater control"*

- Kevin Price, Architect, GE Appliance

*"[It] has been instrumental for us in our quest to deliver compliance, security, and audit requirements for the entirety of our AWS estate"*

- Joe Jarman, SRE, HIVE (Centrica, parent co. of British Gas)

*"[It] presents the opportunity for significant time savings while increasing adherence to golden configurations across multiple accounts."*

- Aater Suleman, CEO, Flux7

## STACKSETS DEMO

The screenshot shows the AWS CloudFormation Manager interface with the URL <https://cte-wc.console-beta.us-west-2.usd.us-east-1.amazonaws.com/cloudformation/stackssets/home?region=us-east-1&stackSetId=StackSets%20Beta>. The browser tabs include 'CloudFormation Manager' and 'AWS Console-SidG'. The main navigation bar has 'Services' and 'Resource Groups' selected. Below the navigation is a search bar and user information. The main content area is titled 'Stack sets' and shows a table of 10 stack sets. The table columns are 'Stack set name', 'Stack set ID', and 'Description'. The rows list various stack sets such as 'enableCT', 'enableCT2', 'enableConfig', etc., each with a detailed description of its purpose.

Stack set name	Stack set ID	Description
enableCT	enableCTd42a7f3e-2d5d-41d9-a01b-99772f0d566b	Enable AWS CloudTrail
enableCT2	enableCT2.cdf56a4a-a2cd-4e8a-a7a8-192883ca7d32	Enable AWS CloudTrail. This template creates a CloudTrail trail, an Amazon S3 bucket where logs are published.
enableConfig	enableConfig.38415615-e093-4975-840a-a1de02f4dace	Enable AWS Config
enableConfig2	enableConfig2.c6c313ce-3ea5-4d1b-b138-e8b652997d55	Enable AWS Config
mystackset0717	mystackset0717.a64d42e4-bf85-43c4-bce2-1fc75d732a82	Enable AWS CloudTrail
mystackset2	mystackset2:920b4cd8-ecde-4ee0-901b-7b226db14e45	Enable AWS CloudTrail
mystackset3	mystackset3:37196c74-a2b3-4f49-eee3-c4844f54a842	Enable AWS CloudTrail
mystackset4	mystackset4:dff794c7e-4ef6-4088-bda5-e10d4d3abd1c	Enable AWS CloudTrail
mystacksetforCloudTrail	mystacksetforCloudTrail:136d3391-7f38-43ec-9141-dedad3cc1f29	Enable AWS CloudTrail
testRole	testRole.5dfa7003-17bb-4f40-8420-d747409591ba	Configure the AWSCloudFormationStackSetExecutionRole to support AWS CloudFormation StackSets in a multi-account environment.

Create A New Stack set

https://rfs-us-console-beta.us-west-2.iad.iad.proxy.amazon.com/cloudformation/stacksets/home?region=Test#stacksets

AWS Console-SidG demo1 demo2 ppburner1 ppburner2 StackSets Beta

Services Resource Groups

CloudFormation Stack sets Create stack set

### Create stack set

**Select template**

**Select template**

A stack set is a container for a set of AWS CloudFormation stacks across multiple AWS accounts and regions. Choose the template that describes the stack sets that you want to create.

Select a sample template from the following templates

Upload a template to Amazon S3

Specify an Amazon S3 template URL

**CloudFormation sample templates**

**Enable AWS CloudTrail**

AWS CloudTrail captures AWS API calls and related events made by or on behalf of an AWS account, and delivers log files to an Amazon S3 bucket that you specify.

[View template](#)

**Enable AWS Config**

AWS Config keeps track of all changes to your resources by invoking the Describe or the List API call for each resource in your account. The service uses those same...

[View template](#)

**Add config rule root-account-mfa-en...**

Add an AWS Config rule to determine whether the root user has multi-factor authentication (MFA) enabled for console sign-in.

[View template](#)

**Add config rule cloudtrail-enabled**

Add an AWS Config rule to determine whether CloudTrail is enabled for an account.

[View template](#)

**Add config rule eip-attached**

Add an AWS Config rule to determine whether all available elastic IP addresses (EIPs) are in use by VPCs or elastic network interfaces (ENIs).

[View template](#)

**Add config rule encrypted-volumes**

Add an AWS Config rule to determine whether all or specific EBS volumes within an account are encrypted with a (optional) key.

[View template](#)

Create A New Stack set

https://rfs-us-console-beta.us-west-2.iad.iad.proxy.amazon.com/cloudformation/stacksets/home?region=Test#stacksets

AWS Console-SidG demo1 demo2 ppburner1 ppburner2 StackSets Beta

Set deployment options

A stack set is a container for a set of AWS CloudFormation stacks across multiple AWS accounts and regions. Choose the template that describes the stack sets that you want to create.

Select a sample template from the following templates

Upload a template to Amazon S3

Specify an Amazon S3 template URL

**CloudFormation sample templates**

**Enable AWS CloudTrail**

AWS CloudTrail captures AWS API calls and related events made by or on behalf of an AWS account, and delivers log files to an Amazon S3 bucket that you specify.

[View template](#)

**Enable AWS Config**

AWS Config keeps track of all changes to your resources by invoking the Describe or the List API call for each resource in your account. The service uses those same...

[View template](#)

**Add config rule root-account-mfa-en...**

Add an AWS Config rule to determine whether the root user has multi-factor authentication (MFA) enabled for console sign-in.

[View template](#)

**Add config rule cloudtrail-enabled**

Add an AWS Config rule to determine whether CloudTrail is enabled for an account.

[View template](#)

**Add config rule eip-attached**

Add an AWS Config rule to determine whether all available elastic IP addresses (EIPs) are in use by VPCs or elastic network interfaces (ENIs).

[View template](#)

**Add config rule encrypted-volumes**

Add an AWS Config rule to determine whether all or specific EBS volumes within an account are encrypted with a (optional) key.

[View template](#)

[Cancel](#) [Next](#)

Create A New Stack set

Stack set name: EnableCloudTrailInDevAccts

Parameters

### Trail Configuration

Enable log file validation: false

Include global service events: false

Is this a multi-region trail: false

### Delivery Notifications

Send notifications to SNS: false

Notification Email (optional):

[Cancel](#) [Previous](#) [Next](#)

Create A New Stack set

Services > Resource Groups > Create stack set

CloudFormation > Stack sets > Create stack set

**Create stack set**

Select template

Specify details

**Set deployment options**

Configure options to deploy stacks to your accounts and regions. Stacks are deployed to regions in sequence, and across accounts in parallel. You can specify the order in which stacks are deployed within regions, the maximum number of accounts in which to deploy in parallel, and failure tolerance.

Tags

Review

**Set deployment options**

Specify accounts

Identify accounts or organizational units in which you want to create stacks.

- Deploy stacks in accounts
- Deploy stacks in AWS organizational units. Learn more
- Upload a list of valid accounts in which stacks can be deployed

Enter valid account numbers:

**Specify regions**

Choose the regions in which you want to deploy stacks. Stacks are deployed in these regions in the order that you specify in the deployment order box.

Available regions	Deployment order			
US East (N. Virginia) US West (Oregon) EU (Ireland) US West (N. California)	Add →	Remove	Move up	Move down

Create A New Stack set

https://cfn-ws-console-beta.us-west-2.railroad.proxy.amazonaws.com/cloudformation/stackssets/home?region=Test&#3F;stacksets

AWS Console-SidG demo1 demo2 pburner1 pburner2 Sibburner3 AWS cons... StackSets Beta

Deploy stacks in accounts

Deploy stacks in AWS organizational units. Learn more  
ou-mt95-m2zuhp5

Upload a list of valid accounts in which stacks can be deployed

Specify regions

Choose the regions in which you want to deploy stacks. Stacks are deployed in these regions in the order that you specify in the deployment order box.

Available regions

- EU (Ireland)
- US West (N. California)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)
- US East (Ohio)
- South America (Sao Paulo)
- Asia Pacific (Sydney)
- EU (Frankfurt)
- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- EU (London)
- Canada (Central)

Deployment order

- US East (N.Virginia)
- US West (Oregon)

Add ➔ Remove Add all ➔ Move up Move down Reset

Deployment options

Maximum concurrent accounts  By number  By percentage  
1 Number of accounts per region to which you can deploy stacks at one time.

Create A New Stack set

https://cfn-ws-console-beta.us-west-2.railroad.proxy.amazonaws.com/cloudformation/stackssets/home?region=Test&#3F;stacksets

AWS Console-SidG demo1 demo2 pburner1 pburner2 Sibburner3 AWS cons... StackSets Beta

Choose the regions in which you want to deploy stacks. Stacks are deployed in these regions in the order that you specify in the deployment order box.

Available regions

- EU (Ireland)
- US West (N. California)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)
- US East (Ohio)
- South America (Sao Paulo)
- Asia Pacific (Sydney)
- EU (Frankfurt)
- Asia Pacific (Seoul)
- Asia Pacific (Mumbai)
- EU (London)
- Canada (Central)

Deployment order

- US East (N.Virginia)
- US West (Oregon)

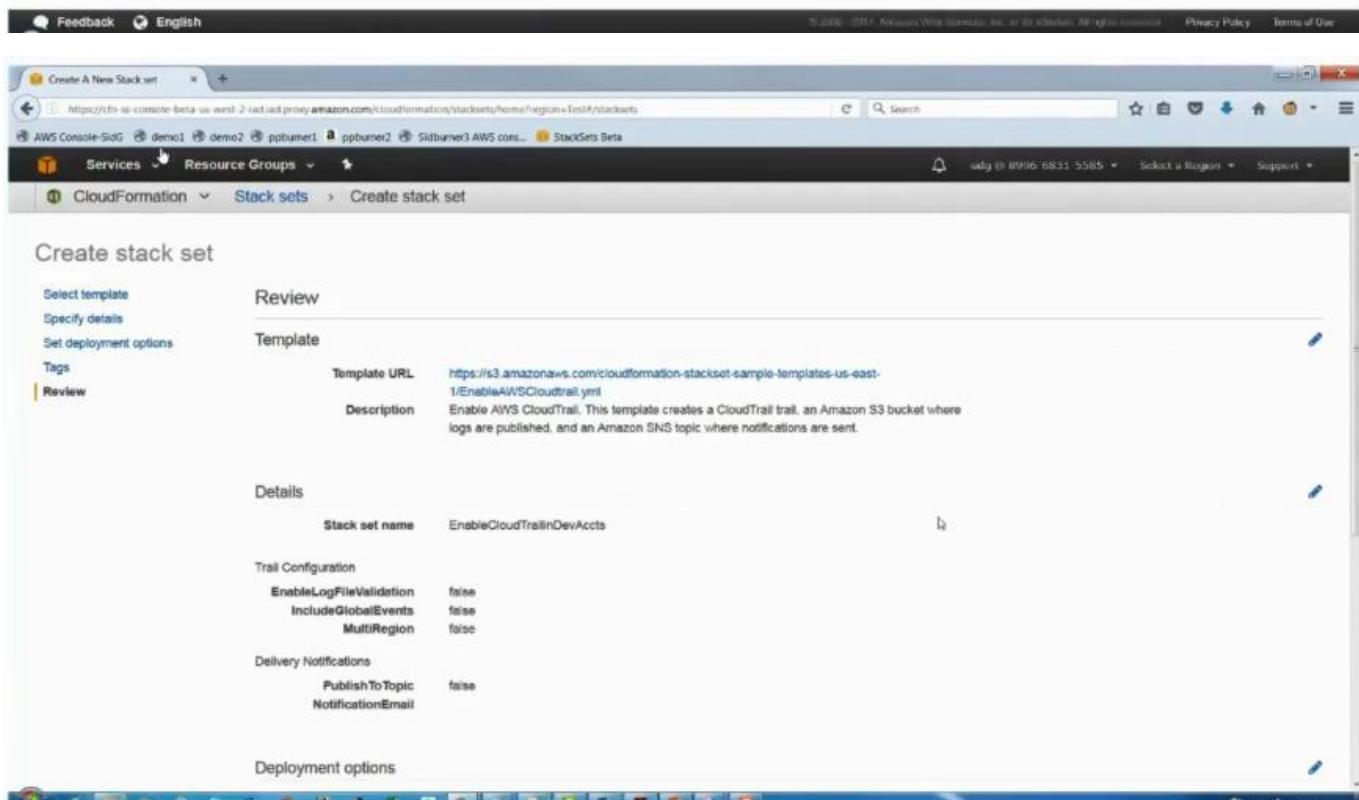
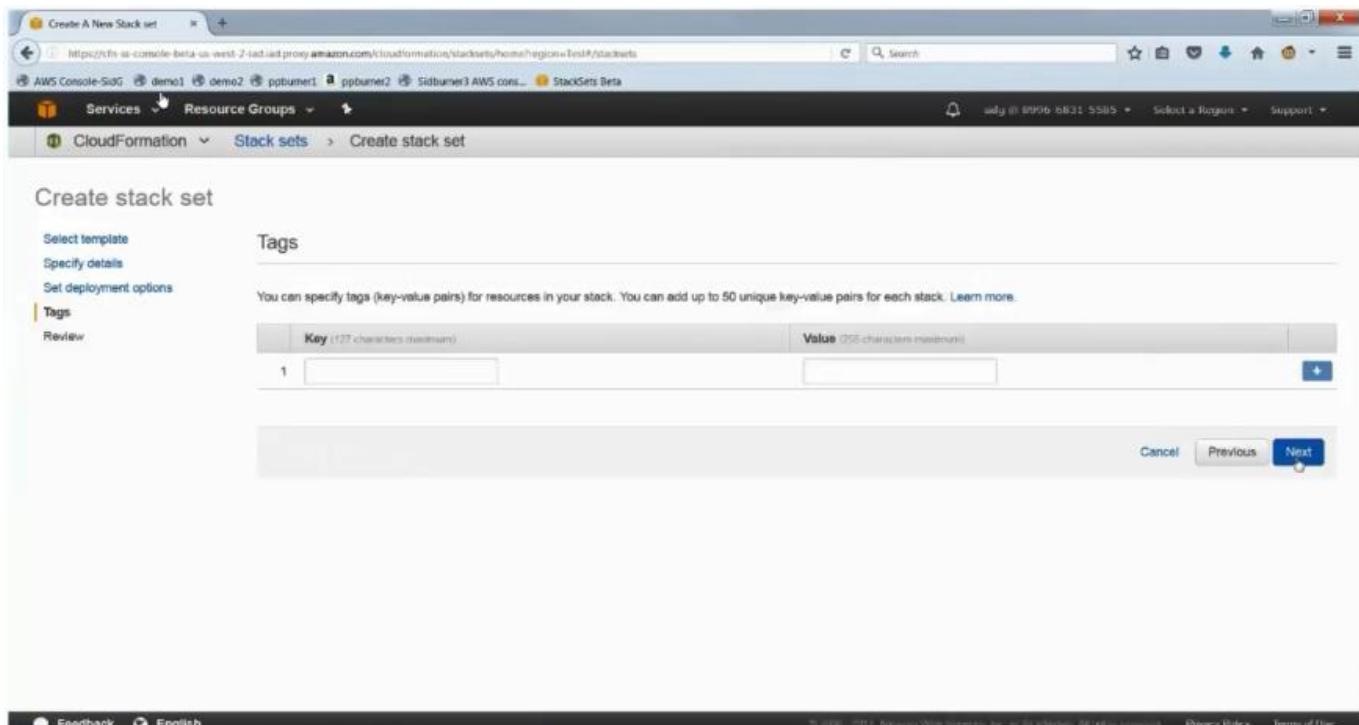
Add ➔ Remove Add all ➔ Move up Move down Reset

Deployment options

Maximum concurrent accounts  By number  By percentage  
5 Number of accounts per region to which you can deploy stacks at one time.

Failure tolerance  By number  By percentage  
5 Number of accounts, per region, for which stacks can fail before CloudFormation stops the operation in that region. If CloudFormation stops the operation in one region, it does not continue in other regions.

Cancel Previous Next



Create A New Stack set

https://ch-w-console-beta.us-west-2.iad.iad.proxy.amazon.com/cloudformation/stacksets/home?region=Test&stackset=

AWS Console-SidG demo1 demo2 pburner1 pburner2 Sdburner3 AWS cons... StackSets Beta

Trail Configuration

EnableLogFileValidation	false
IncludeGlobalEvents	false
MultiRegion	false

Delivery Notifications

PublishToTopic	false
NotificationEmail	

Deployment options

Accounts	179314946985, 197366921397, 086768435266, 137118073555, 816794622732
Deployment order	US East (N.Virginia), US West (Oregon)
Estimated stack count	10
Maximum concurrent accounts	5
Failure tolerance	5

Tags

Key	Value
No tags	

Cancel Previous Create

Feedback English

© 2006 - 2017 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Stack set properties

https://ch-w-console-beta.us-west-2.iad.iad.proxy.amazon.com/cloudformation/stacksets/home?region=Test&stackset=

AWS Console-SidG demo1 demo2 pburner1 pburner2 Sdburner3 AWS cons... StackSets Beta

Services Resource Groups Select a Region Support

CloudFormation Stack sets Stack set properties

Delete stack set Manage stack set

EnableCloudTrailinDevAccts

Stack set name: EnableCloudTrailinDevAccts

Stack set ID: EnableCloudTrailinDevAccts:12d0d0eb-ba74-424e-99ab-968de733643b

Description: Enable AWS CloudTrail. This template creates a CloudTrail trail, an Amazon S3 bucket where logs are published, and an Amazon SNS topic where notifications are sent.

Template Parameters Tags Operations

Operation ID	Operation type	Created time	Completed time	Status	Actions
3886c245-63b4-40ff-9739-e3ff43cfac3	CREATE	2017-07-20 11:35:02 UTC-0700		RUNNING	Stop

Stacks

Stack set properties

https://cfn-us-console-beta.us-west-2.iad.us-east-1.amazonaws.com/cloudformation/stacksets/home?region=Test#stacksets

AWS Console-SidG demo1 demo2 pburner1 pburner2 Sidburner3 AWS cons... StackSets Beta

**Stack set name:** EnableCloudTrailInDevAccts

**Stack set ID:** EnableCloudTrailInDevAccts:12d00deb-ba74-424e-99ab-968de733643b

**Description:** Enable AWS CloudTrail. This template creates a CloudTrail trail, an Amazon S3 bucket where logs are published, and an Amazon SNS topic where notifications are sent.

Template

Parameters

Tags

Operations

Operation ID	Operation type	Created time	Completed time	Status	Actions
3866c245-63b4-40ff-9739-e3ff43cfaac3	CREATE	2017-07-20 11:35:02 UTC-0700		RUNNING	Stop

Stacks

AWS account	AWS region	Stack name	Status	Status reason
No stack instances found				

Feedback English

© 2017 AWS. All rights reserved. AWS is a trademark of Amazon.com, Inc., or its affiliates. All rights reserved. Privacy Policy Terms of Use

Stack set properties

https://cfn-us-console-beta.us-west-2.iad.us-east-1.amazonaws.com/cloudformation/stacksets/home?region=Test#stacksets

AWS Console-SidG demo1 demo2 pburner1 pburner2 Sidburner3 AWS cons... StackSets Beta

**EnableCloudTrailInDevAccts**

**Stack set name:** EnableCloudTrailInDevAccts

**Stack set ID:** EnableCloudTrailInDevAccts:12d00deb-ba74-424e-99ab-968de733643b

**Description:** Enable AWS CloudTrail. This template creates a CloudTrail trail, an Amazon S3 bucket where logs are published, and an Amazon SNS topic where notifications are sent.

**Template**

```
AWSTemplateFormatVersion: 2010-09-09
Description: Enable AWS CloudTrail. This template creates a CloudTrail trail, an Amazon S3 bucket where logs are published, and an Amazon SNS topic where notifications are sent.

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Labels:
          - Trail Configuration
        Parameters:
          - MultiLogFileValidation
          - IncludeGlobalEvents
          - MultiRegion
      - Labels:
          - Delivery Notifications
        Parameters:
          - PublishToTopic
          - NotificationEmail
    ParameterLabels:
      EnableLogFileValidation:
        default: Enable log file validation
      IncludeGlobalEvents:
        default: Include global service events
      MultiRegion:
        default: Is this a multi-region trail
      PublishToTopic:
        default: Publish logs to an SNS topic
      NotificationEmail:
        default: Email address for notifications
```

Delete stack set Manage stack set

Stack set properties

https://cfn-us-console-beta.us-west-2.iad.iad.proxy.amazon.com/cloudformation/stacksets/home?region=Test#/stacksets

AWS Console-SidG demo1 demo2 ppburner1 ppburner2 ppburner3 AWS cons... StackSets Beta

TrailBucketLibrary

Type: AWS::CloudTrail::Trail

Properties:

- TrailBucketName: !Ref TrailBucket
- DevTopicName: !Ref
- Publish
- !GetAtt TrailTopic.TopicName
- !Ref ARN: !Ref Value

IsLogging: true

EnableLogFileValidation: !Ref EnableLogFileValidation

IncludeGlobalServiceEvents: !Ref

- MultiRegion
- true
- !Ref IncludeGlobalEvents

MultiRegionTrail: !Ref MultiRegion

▼ Parameters

Key	Value
EnableLogFileValidation	false
IncludeGlobalEvents	false
MultiRegion	false
NotificationEmail	
PublishToTopic	false

► Tags

Stack set properties

https://cfn-us-console-beta.us-west-2.iad.iad.proxy.amazon.com/cloudformation/stacksets/home?region=Test#/stacksets

AWS Console-SidG demo1 demo2 ppburner1 ppburner2 ppburner3 AWS cons... StackSets Beta

includeGlobalEvents	false
MultiRegion	false
NotificationEmail	
PublishToTopic	false

▼ Tags

Key	Value
No values found.	

▼ Operations

Operation ID	Operation type	Created time	Completed time	Status	Actions
3866c245-53b4-40ff-9739-e3ff43cfac3	CREATE	2017-07-20 11:35:02 UTC-0700		RUNNING	Stop

► Stacks

AWS account	AWS region	Stack name	Status	Status reason	Status	Action
No stack instances found						All

Stack set properties

https://cfn-us-console-beta.us-west-2.iad.iad.proxy.amazon.com/cloudformation/stacksets/home?region=Test&stackset=

AWS Console-SidG demo1 demo2 pbumer1 ppbumer2 Sidburner3 AWS cons... StackSets Beta

Tags

Operations

Operation ID	Operation type	Created time	Completed time	Status	Actions
3866c245-63b4-40ff-9739-e3ff43cfac3	CREATE	2017-07-20 11:35:02 UTC-0700		RUNNING	Stop

Stacks

AWS account	AWS region	Stack name	Status	Status reason
066768435266	us-east-1	StackSet-62ae663d-a999-4037-a929-a8e64ea29387	CURRENT	
066768435266	us-west-2	StackSet-6af1a434-8883-44aa-967d-4470f60bab17	OUTDATED	User initiated operation
137118073555	us-east-1	StackSet-d31402fa-5630-4fe9-b34d-e047fce807e	CURRENT	
137118073555	us-west-2	StackSet-9e2a4df5-575f-4bbc-ac2b-1af542994db9	OUTDATED	User initiated operation
179314948985	us-east-1	StackSet-ddd85772-1979-4cf4-ad0f-35140b486e33	CURRENT	
179314948985	us-west-2	StackSet-71e18f6-4f9f-455f-e834-157b6234b960	OUTDATED	User initiated operation
197366821397	us-east-1	StackSet-71e18f6-4f9f-455f-e834-157b6234b960	CURRENT	
197366821397	us-west-2	StackSet-a7817157-5118-4b19-b717-cca7b39ad59c	OUTDATED	User initiated operation
816794622732	us-east-1	StackSet-a7817157-5118-4b19-b717-cca7b39ad59c	CURRENT	
816794622732	us-west-2	StackSet-d2cec253-35e6-48d0-8fa7-50bcd680ae1	OUTDATED	User initiated operation

Stack set properties

https://cfn-us-console-beta.us-west-2.iad.iad.proxy.amazon.com/cloudformation/stacksets/home?region=Test&stackset=

AWS Console-SidG demo1 demo2 pbumer1 ppbumer2 Sidburner3 AWS cons... StackSets Beta

Tags

Operations

Operation ID	Operation type	Created time	Completed time	Status	Actions
3866c245-63b4-40ff-9739-e3ff43cfac3	CREATE	2017-07-20 11:35:02 UTC-0700		RUNNING	Stop

Stacks

AWS account	AWS region	Stack name	Status	Status reason
066768435266	us-east-1	StackSet-62ae663d-a999-4037-a929-a8e64ea29387	CURRENT	
066768435266	us-west-2	StackSet-6af1a434-8883-44aa-967d-4470f60bab17	OUTDATED	User initiated
137118073555	us-east-1	StackSet-d31402fa-5630-4fe9-b34d-e047fce807e	CURRENT	
137118073555	us-west-2	StackSet-9e2a4df5-575f-4bbc-ac2b-1af542994db9	OUTDATED	User initiated
179314948985	us-east-1	StackSet-ddd85772-1979-4cf4-ad0f-35140b486e33	CURRENT	
179314948985	us-west-2	StackSet-09954257-6697-4af0-bfc8-59234ee4a690	OUTDATED	User initiated
197366821397	us-east-1	StackSet-71e18f6-4f9f-455f-e834-157b6234b960	CURRENT	
197366821397	us-west-2	StackSet-fd77b6ab-a759-4146-95e8-61557a63817a	OUTDATED	User initiated
816794622732	us-east-1	StackSet-a7817157-5118-4b19-b717-cca7b39ad59c	CURRENT	
816794622732	us-west-2	StackSet-d2cec253-35e6-48d0-8fa7-50bcd680ae1	OUTDATED	User initiated

Stack set properties

https://cfn-us-west-2-radial.proxy.amazon.com/cloudFormation/stacksets/home?region=Test&stackset=

AWS Console-SidG demo1 demo2 ppburner1 ppburner2 Sidburner3 AWS cons... StackSets Beta

Tags

Operations

Operation ID	Operation type	Created time	Completed time	Status	Actions
3866c245-63b4-40ff-9739-e3ff43cfaac3	CREATE	2017-07-20 11:35:02 UTC-0700	2017-07-20 11:38:32 UTC-0700	SUCCEEDED	

Stacks

Status: ALL

AWS account	AWS region	Stack name	Status	Status reason
066768435266	us-east-1	StackSet-62ae663d-a999-4037-a929-a8e64ea29367	CURRENT	
066768435266	us-west-2	StackSet-6af1a434-8883-44aa-967d-4470f50be617	CURRENT	
137118073555	us-east-1	StackSet-d31402fa-5630-4fe9-b34d-e047fce807e	CURRENT	
137118073555	us-west-2	StackSet-9a2e4df5-575f-4bbc-aa20-1af642994db9	CURRENT	
179314948985	us-east-1	StackSet-ddd85772-1979-4cf4-ad0f-35140b486e33	CURRENT	
179314948985	us-west-2	StackSet-09964257-6697-4af0-bf78-59234ee4a690	CURRENT	
197366821397	us-east-1	StackSet-71e18ff6-4f9f-4551-e634-157b6234b960	CURRENT	
197366821397	us-west-2	StackSet-fd77b6ab-a759-4146-95e8-61557a63817a	CURRENT	
816794622732	us-east-1	StackSet-a7817157-5118-4bf9-b717-cca7b39ad59c	CURRENT	
816794622732	us-west-2	StackSet-d22ec253-35a6-48d0-8fa7-50bcdff680ae1	CURRENT	

Stack set properties

https://cfn-us-west-2-radial.proxy.amazon.com/cloudFormation/stacksets/home?region=Test&stackset=

AWS Console-SidG demo1 demo2 ppburner1 ppburner2 Sidburner3 AWS cons... StackSets Beta

Services Resource Groups

CloudFormation Stack sets Stack set properties

Delete stack set Manage stack set

### EnableCloudTrailinDevAccts

Stack set name: EnableCloudTrailinDevAccts

Stack set ID: EnableCloudTrailinDevAccts:12d0d0eb-ba74-424e-99ab-968de733643b

Description: Enable AWS CloudTrail. This template creates a CloudTrail trail, an Amazon S3 bucket where logs are published, and an Amazon SNS topic where notifications are sent.

Template

Parameters

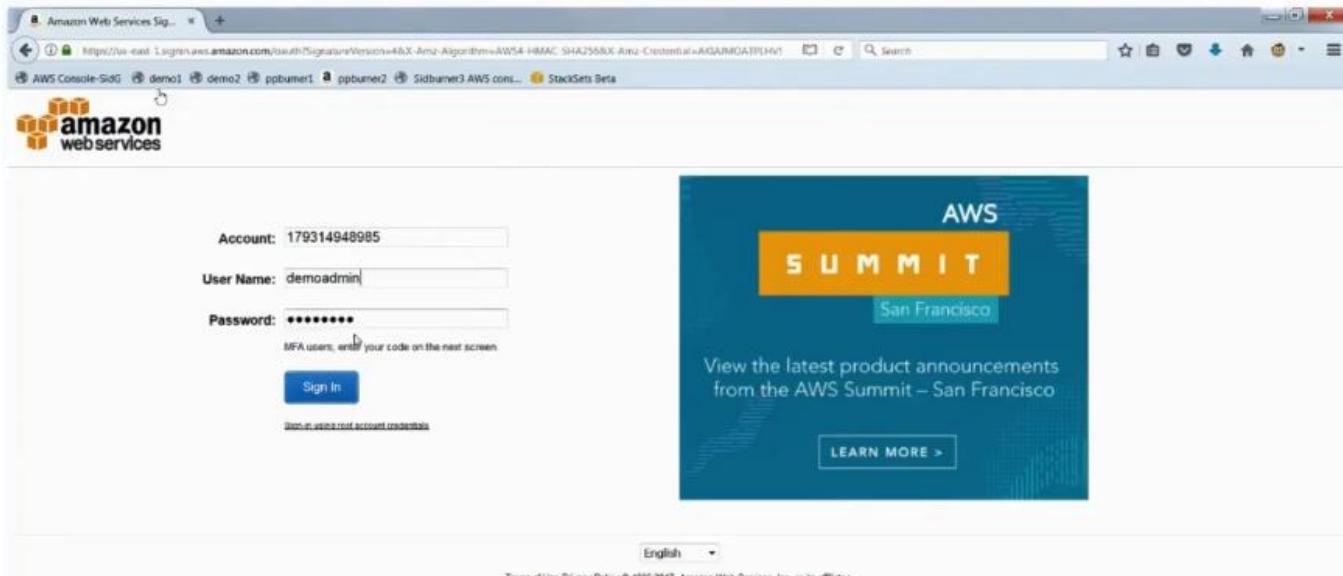
Tags

Operations

Operation ID	Operation type	Created time	Completed time	Status	Actions
3866c245-63b4-40ff-9739-e3ff43cfaac3	CREATE	2017-07-20 11:35:02 UTC-0700	2017-07-20 11:38:32 UTC-0700	SUCCEEDED	

Stacks

Status: ALL



The screenshot shows the AWS Management Console homepage. It features a search bar for 'AWS services', a 'Recently visited services' section with links to Config, IAM, and CloudFormation, and a 'Build a solution' section with six quick-start options: Launch a virtual machine, Build a web app, Host a static website, Connect an IoT device, Start a development project, and Register a domain. On the right, there are 'Helpful tips' for managing costs and creating organizations, and sections for exploring AWS products like the AWS Summit and Amazon Aurora. A 'Learn to build' section at the bottom provides step-by-step guides and labs.

CloudTrail Management C... https://us-west-2.console.aws.amazon.com/cloudtrail/home?region=us-west-2#/events

AWS Console-SidG demo1 demo2 ppbuhert1 ppbuhert2 Sidebar3 AWS cons... StackSets Beta

Services Resource Groups

API activity history

Trails

The following list includes the last 7 days of API activity for supported services. The list only includes API activity for create, modify, and delete API calls. For read-only API activity, go to your Amazon S3 bucket or CloudWatch Logs.

You can filter the list using the available attributes, and you can choose an event to see more detail about the event. Learn more.

Filter: Select attribute Enter lookup value Time range: Select time range

Event time	User name	Event name	Resource type	Resource name
2017-07-20, 10:50:09 AM	38abe48d-4479-406c-9e20-f2...	StartConfigurationRecorder		
2017-07-20, 10:50:05 AM	38abe48d-4479-406c-9e20-f2...	PutDeliveryChannel		
2017-07-20, 10:50:05 AM	38abe48d-4479-406c-9e20-f2...	StartConfigurationRecorder		
2017-07-20, 10:50:04 AM	38abe48d-4479-406c-9e20-f2...	PutConfigurationRecorder		
2017-07-20, 10:50:00 AM	38abe48d-4479-406c-9e20-f2...	PutBucketPolicy	S3 Bucket	stackset-30c4cae-46df-462b...
2017-07-20, 10:49:35 AM	38abe48d-4479-406c-9e20-f2...	CreateBucket	S3 Bucket	stackset-30c4cae-46df-462b...
2017-07-20, 10:49:35 AM	38abe48d-4479-406c-9e20-f2...	AttachRolePolicy	IAM Policy and 1 more	arn:aws:iam::aws:policy/service-role/AmazonCloudTrailFullAccess
2017-07-20, 10:49:34 AM	38abe48d-4479-406c-9e20-f2...	CreateRole	IAM Role	AROAIQJMAPKADOGTK2IL...
2017-07-20, 10:49:30 AM	38abe48d-4479-406c-9e20-f2...	CreateStack		
2017-07-20, 10:48:24 AM	0e42ec72-d82c-4aaa-8d88-e...	AttachRolePolicy	IAM Policy and 1 more	arn:aws:iam::aws:policy/service-role/AmazonCloudTrailFullAccess

Feedback English

Privacy Policy Terms of Use

CloudTrail Management C... https://us-west-2.console.aws.amazon.com/cloudtrail/home?region=us-west-2#/configuration

AWS Console-SidG demo1 demo2 ppbuhert1 ppbuhert2 Sidebar3 AWS cons... StackSets Beta

Services Resource Groups

API activity history

Trails

How does CloudTrail pricing work?

CloudTrail events can be processed by one trail for free. There is a charge for processing events by additional trails. For more information, see Pricing.

Add new trail

Name	Region	S3 bucket	Log file prefix	CloudWatch Logs Log group	Status
conduit-cloudtrail-179314948985	All	conduit-cloudtrail-logs	trail-logs		Green
StackSet-dd85772-1979-4c14-ad0f-35140b485e33-Trail-1SYVWADXKNZWRF	US East (N. Virginia)	stackset-dd85772-1979-4c14-ad0f-3514-trailbucket-12luwg5v2rcv			Green
StackSet-09954257-6697-4af0-bfc8-59234ee4a590-Trail-9IRNBOR5OUV2	US West (Oregon)	stackset-09954257-6697-4af0-bfc8-5923-trailbucket-dwxmy49ljsm			Green

Learn more

Pricing Documentation Forums FAQs

CloudTrail Management C... X

https://us-west-2.console.aws.amazon.com/cloudtrail/home?region=us-west-2#/configuration/trailStackSets/status-west-217031494885/trail@StackSet-0

AWS Console-SidG demo1 demo2 ppburner1 ppburner2 ppburner3 AWS cons... StackSets Beta

Services Resource Groups demoadmin (1793) 14/04 00:05 Origins Support

API activity history Trails Learn more

Trails > Configuration

StackSet-09954257-6697-4af0-bfc8-59234ee4a590-Trail-9IRN8OR5OUV2

Logging ON

Trail settings Edit

When a trail applies to all regions, the trail exists in all regions and delivers log files for all regions to one Amazon S3 bucket and an optional CloudWatch Logs log group. To see all of your trails, click Trails.

Apply trail to all regions No

Management events Edit

Management events are operations that occur on your AWS account and resources, such as the Amazon EC2 RunInstances API. Learn more.

ReadWrite events All

Data events Edit

Specify the S3 objects for which you want to log object-level operations. S3 object-level operations include APIs such as GetObject, DeleteObject, and PutObject. Additional charges apply. Learn more.

Configure

Amazon Web Services Sig... X

https://us-west-2.signin.aws.amazon.com/saml/SignatureVersion=4&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIMDAP1P34W/

AWS Console-SidG demo1 demo2 ppburner1 ppburner2 ppburner3 AWS cons... StackSets Beta



Account: 086768435266

User Name: demoadmin

Password: \*\*\*\*\*

MFA users: enter your code on the next screen.

Sign In

Sign in using root account credentials

  
AWS SUMMIT San Francisco  
View the latest product announcements from the AWS Summit – San Francisco  
LEARN MORE >

English ▼

Terms of Use Privacy Policy © 1996-2017, Amazon Web Services, Inc. or its affiliates.

AWS Management Console

https://console.aws.amazon.com/console/home?region=us-east-1

AWS Console-SidG demo1 demo2 ppburner1 ppburner2 Sidburner3 AWS cons... StackSets Beta

Services Resource Groups

AWS services

Find a service by name or feature (for example, EC2, S3 or VPC, storage)

Recently visited services

- CloudTrail
- Config
- AWS Organizations
- CloudFormation
- IAM

All services

Build a solution

Get started with simple wizards and automated workflows.

Launch a virtual machine With EC2 or Lightsail ~1-2 minutes	Build a web app With Elastic Beanstalk ~6 minutes	Host a static website With S3, CloudFront, Route 53 ~6 minutes
Connect an IoT device With AWS IoT ~5 minutes	Start a development project With CodeStar ~5 minutes	Register a domain With Route 53 ~3 minutes

See more

Learn to build

Learn to develop your solutions through step-by-step guides, labs, and videos.

See all

Helpful tips

Manage your costs

Get real-time billing alerts based on your cost and usage budgets. Start now.

Create an organization

Use AWS Organizations for policy-based management of multiple AWS accounts. Start now.

Explore AWS

New Product Announcements

View the latest announcements from the AWS Summit - San Francisco. Learn more.

Migrate from Oracle to Amazon Aurora

Learn how to migrate from Oracle to Amazon Aurora with minimal downtime. View project.

Introducing Amazon Kinesis Analytics

Easily process real-time, streaming data with Amazon Kinesis Analytics. Learn more.

CloudFormation Manager...

https://console-beta-us-west-2.railsoft.proxy.amazonaws.com/cloudformation/stacksets/home/?region=us-east-1

AWS Console-SidG demo1 demo2 ppburner1 ppburner2 Sidburner3 AWS cons... StackSets Beta

Services Resource Groups

CloudFormation Stack sets

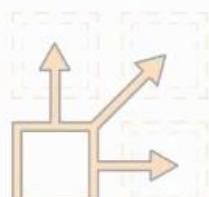
Create stack set Actions

By stack set name

Stack set name	Stack set ID	Description
enableCT	enableCT.d42a7f3e-2d5d-41d9-a01b-99772f05b60	Enable AWS CloudTrail
enableCT2	enableCT2.cdf65a4a-a2cd-4e8a-a7a5-192883ca7d32	Enable AWS CloudTrail. This template creates a CloudTrail trail, an Amazon S3 bucket where logs are published.
enableConfig	enableConfig.38415615-e093-4975-840a-a1da02f4dace	Enable AWS Config
enableConfig2	enableConfig2.cfc313ce-3aa8-4d1b-b13b-e6b65299755	Enable AWS Config
mystackset0717	mystackset0717.a54d42e4-bf85-43c4-bce2-1fc75d732a82	Enable AWS CloudTrail
mystackset12	mystackset12.920b4cd8-eccc-4eee-901b-7b226db14e45	Enable AWS CloudTrail
mystackset3	mystackset3.37198c74-a2b3-44b8-aee3-c4844f54a842	Enable AWS CloudTrail
mystackset4	mystackset4.dff794c7e-4ef5-4056-bda5-e10d4d3abdc	Enable AWS CloudTrail
mystacksetforCloudTrail	mystacksetforCloudTrail.136d3391-7f38-43ec-9141-dedad3cc1f29	Enable AWS CloudTrail
testRole	testRole.5dfa7003-17bb-4f40-8420-d747409591ba	Configure the AWSCloudFormationStackSetExecutionRole to support AWS CloudFormation StackSets in a managed way.



System Admins:  
Safety Guardrails



System Admins:  
Provisioning at scale



Developers:  
Test and Validate



Developers:  
Serverless Apps

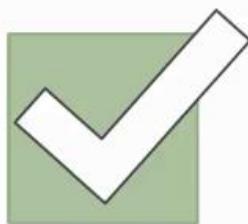
# INFRASTRUCTURE AS IS CODE!



Template code should be in a repo

- Track issues and history
- Commits can trigger test suites and builds
- Use tools and utilities for validation
- Hook into Jenkins, Ansible, Chef, Puppet, ...

## TESTING AND VALIDATING



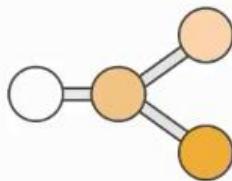
Keep track of what you are validating

- Environments: stage vs production
- Validate app code vs generated code separately

Automate validation often and log/alert

- Validate intermediate and end results

# VALIDATION PIPELINE



Run a set of customizable tests for logical and functional integrity against templates

- Integrates with an existing AWS CodeCommit repo
- Provisions and configures necessary services
  - AWS CodePipeline
  - AWS CodeBuild
  - AWS Lambda

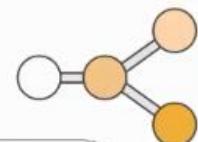
<http://docs.aws.amazon.com/solutions/latest/aws-cloudformation-validation-pipeline/>



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

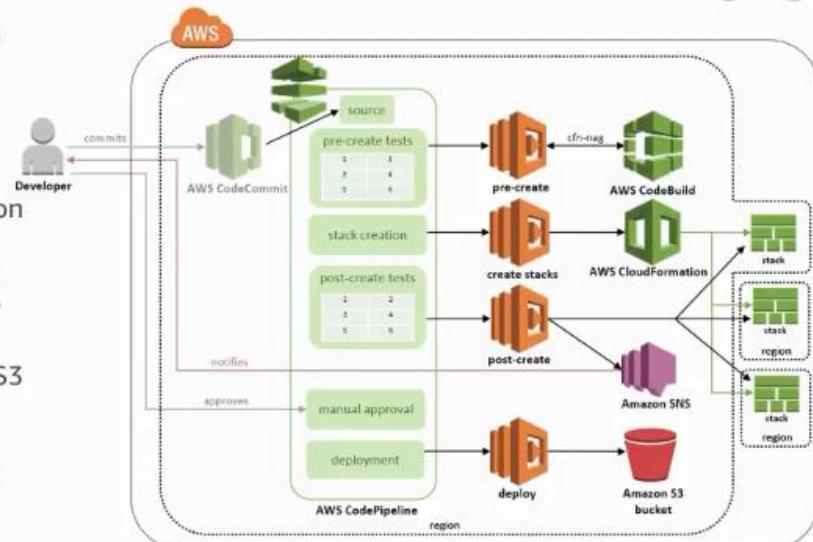


## REFERENCE IMPLEMENTATION



Triggered by a commit on your repo

1. Run logical pre-create tests, including syntax checks
2. Launch test stacks in multiple regions
3. Runs functional post-create sets on the test stacks
4. If tests are successful, an email is sent to indicate template is ready for approval
5. Final template is deployed to an S3 bucket, also storing CloudWatch data for each Lambda function
6. Deploy stack directly from the S3 bucket

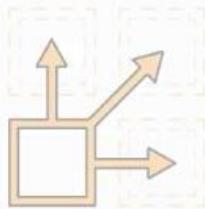


© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.





System Admins:  
Safety Guardrails



System Admins:  
Provisioning at scale



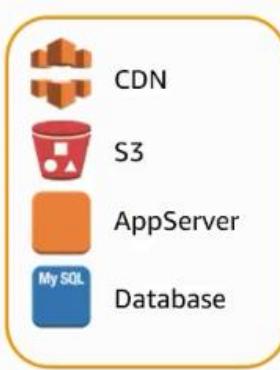
Developers:  
Test and Validate



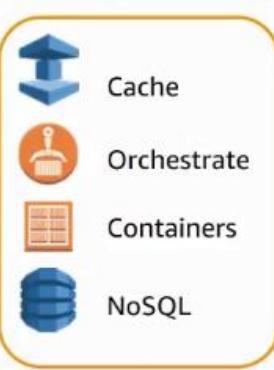
Developers:  
Serverless Apps

## WORKING ACROSS APP ARCHITECTURES

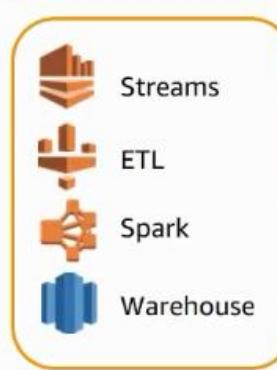
AWS CloudFormation can support many app types



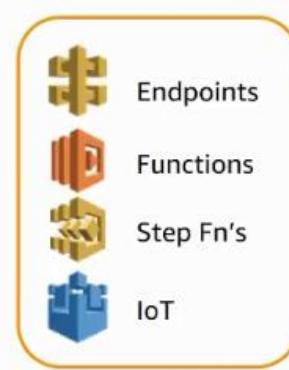
Multi-tier  
Transactional  
(Java, LAMP)



Microservices  
Transactional  
(Docker, K8s)



Big Data  
Analytical  
(Data lakes, Hubs)



...



AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## MODELING SERVERLESS APPS

Several options:

- Native serverless resource creation
- Serverless Application Model (SAM) transform
- Chalice Microframework

# SERVERLESS APPLICATION MODEL



Several options:

- AWS CloudFormation extension or “transform”
- Optimized for serverless apps
- Serverless resource types: functions, APIs, tables
- Supports anything AWS CloudFormation supports

# SERVERLESS FRAMEWORKS

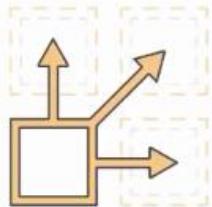


Apex	Lambda
Up	Lambdoku
Chalice	Shep
ClaudiaJS	Sparta
DEEP	Turtle
Gordon	Zappa
Gestalt	Lambdify
Iron Functions	Squeezee
Kappa	...



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.





System Admins:  
Safety Guardrails

System Admins:  
Provisioning at scale

Developers:  
Test and Validate

Developers:  
Serverless Apps

**AWS CloudFormation benefits many user segments in small and large organizations, for traditional and emerging application architectures**



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



## WHERE TO GO FROM HERE

Termination Protection	<a href="http://amzn.to/2y8KbjV">http://amzn.to/2y8KbjV</a>
Stack Policies	<a href="http://amzn.to/28JmWkT">http://amzn.to/28JmWkT</a>
Deletion Policy	<a href="http://amzn.to/1qtkrkq">http://amzn.to/1qtkrkq</a>
IAM Policy	<a href="http://amzn.to/2e345Tp">http://amzn.to/2e345Tp</a>
AWS Config	<a href="https://aws.amazon.com/config/">https://aws.amazon.com/config/</a>
Rollback Triggers	<a href="http://amzn.to/2zDV3GR">http://amzn.to/2zDV3GR</a>
StackSets	<a href="http://amzn.to/2zK0nGi">http://amzn.to/2zK0nGi</a>
Validation Pipeline	<a href="http://amzn.to/2hrz8rM">http://amzn.to/2hrz8rM</a>



DEV317

Deep Dive on AWS  
CloudFormation

**Remember to complete  
your evaluations! ☺**

Anil Kumar – [aanik@amazon.com](mailto:aanik@amazon.com)

[@anilsdomain](https://twitter.com/anilsdomain)

Luis Colon – [licolon@amazon.com](mailto:licolon@amazon.com)

[@luiscolon1](https://twitter.com/luiscolon1)



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

