DEV317

# Deep Dive on AWS CloudFormation

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

November 28, 2017

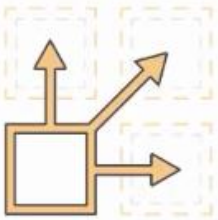
AWS re:Invent

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

aws

## THEMES *for this session*

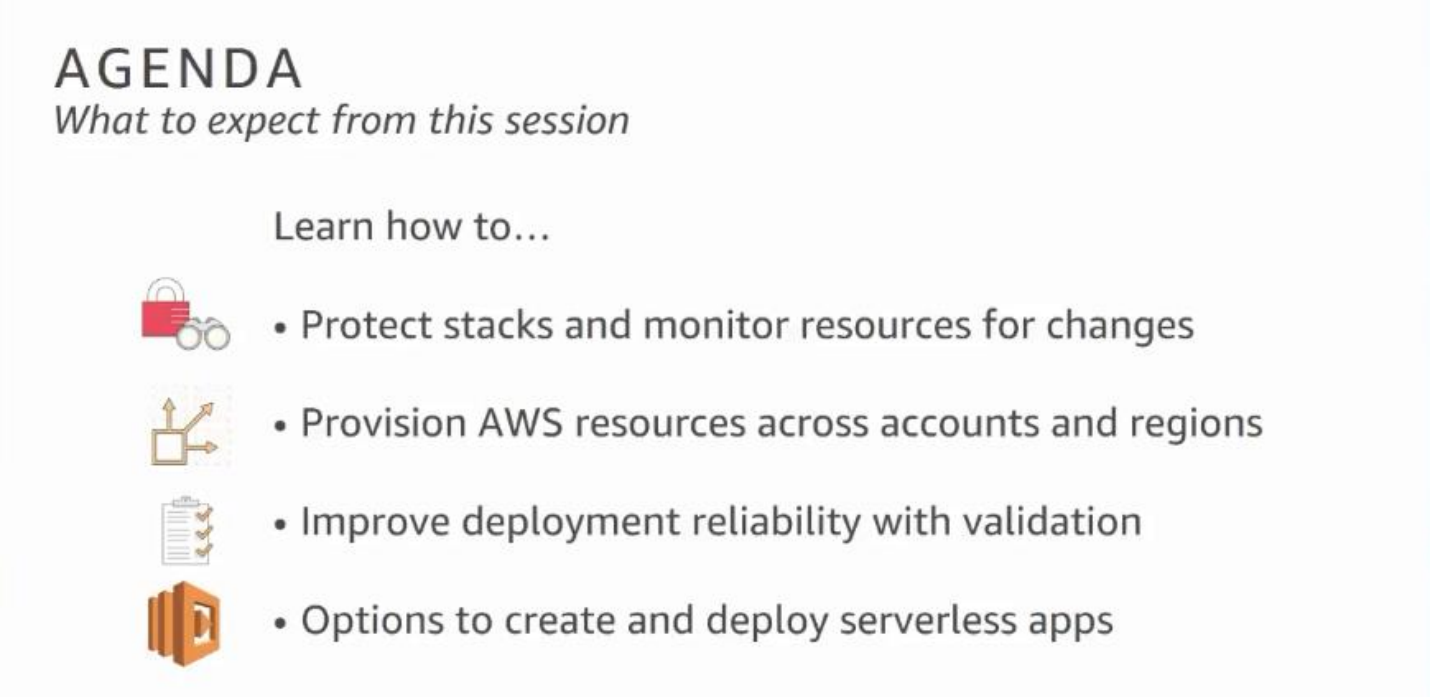
System Admins:
Safety Guardrails

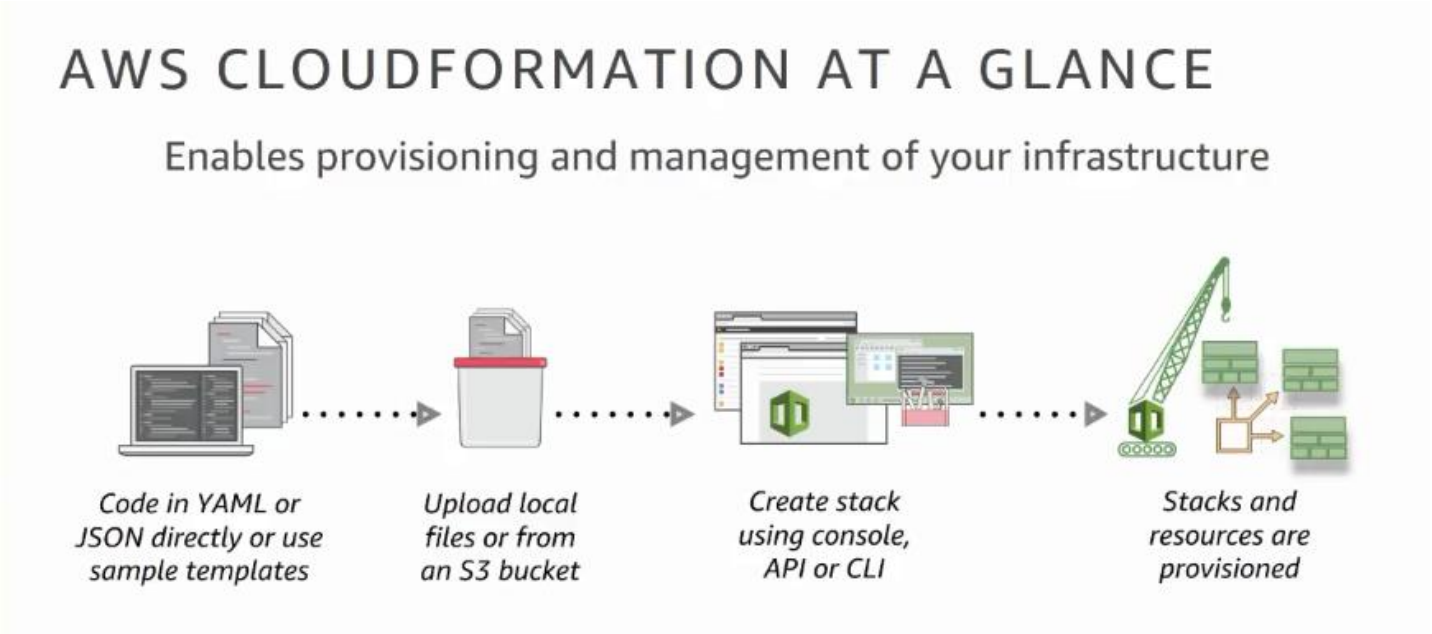


System Admins:
Provisioning at scale

Developers:
Test and Validate

Developers:
Serverless Apps




***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*

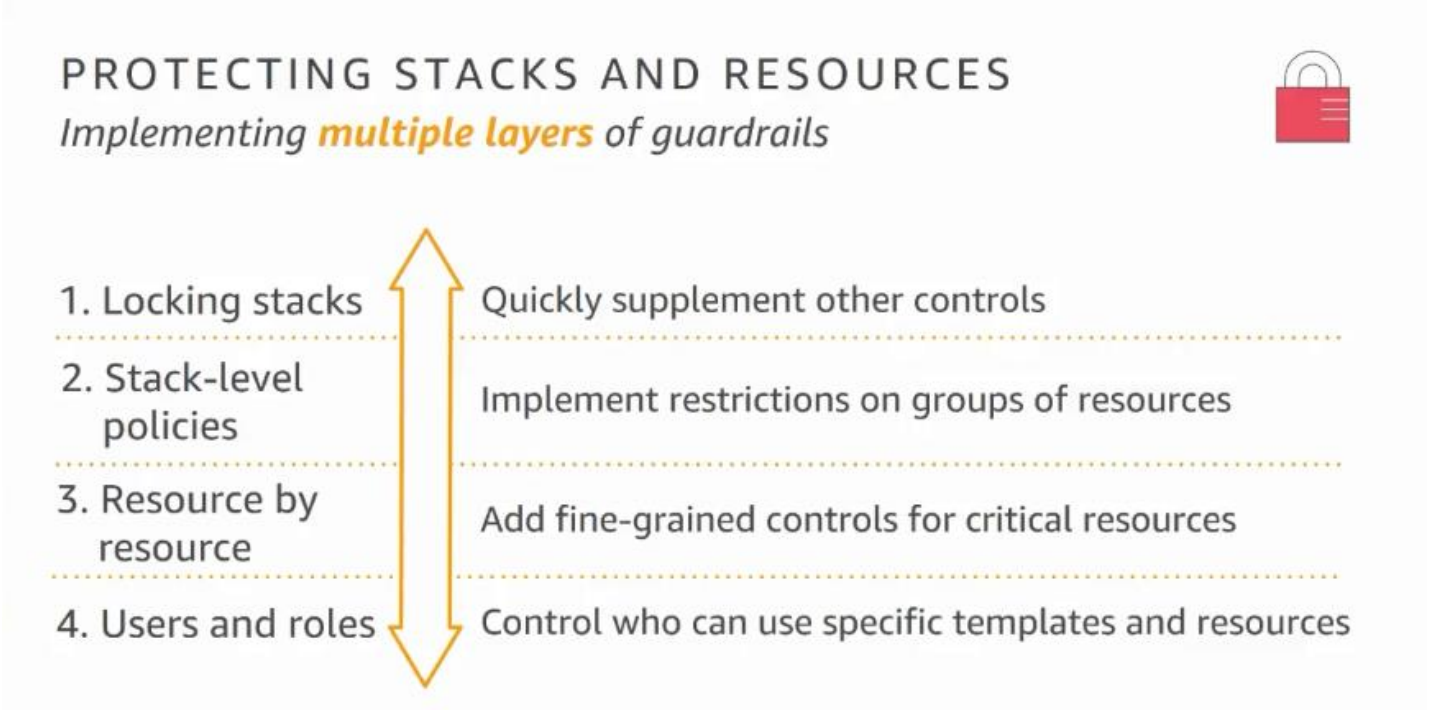
Learn how to…

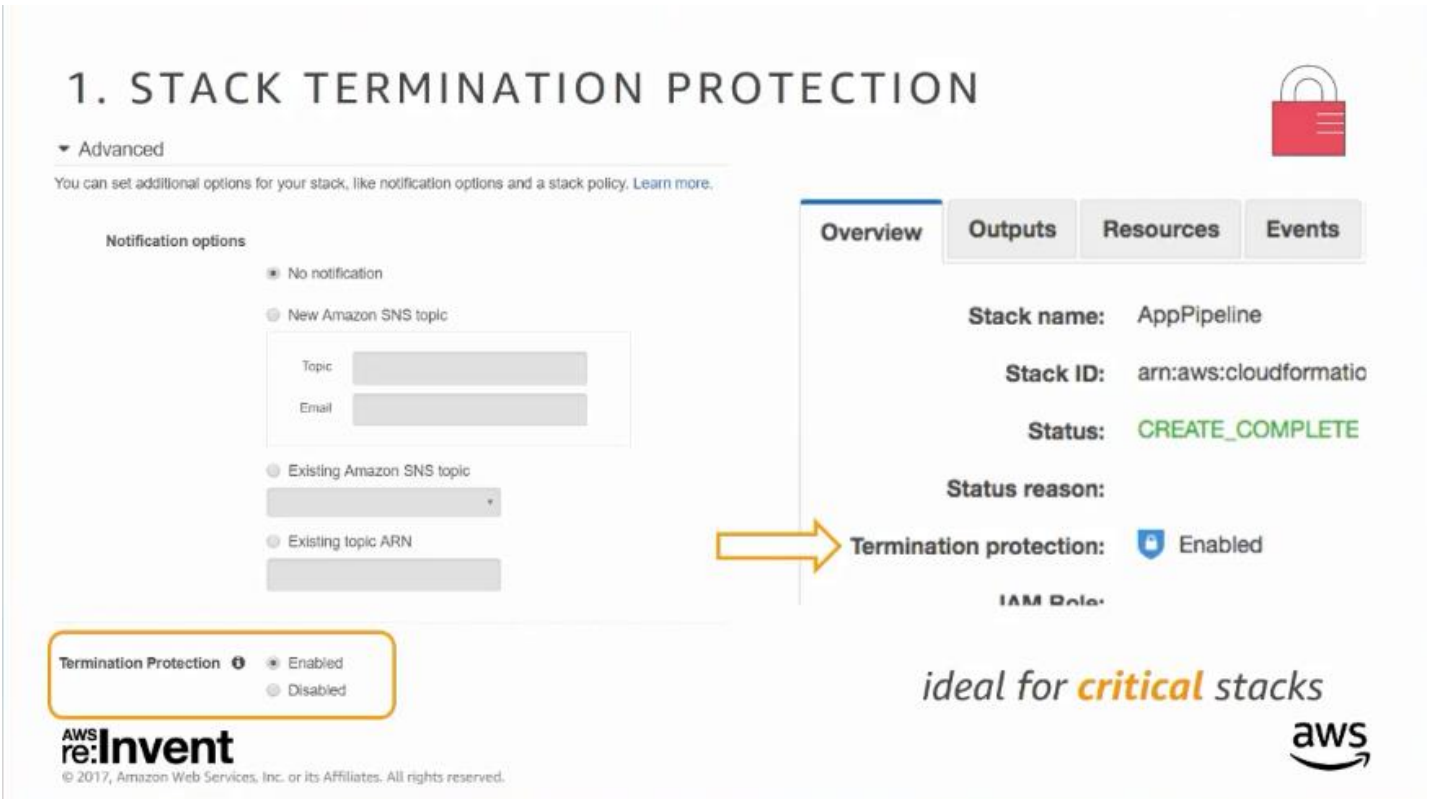
- **Protect stacks** and monitor resources for changes

- Provision AWS resources across accounts and regions

- Improve deployment reliability with validation

- Options to create and deploy serverless apps




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*

AWS re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
aws

## 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*

AWS re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
aws

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*

aws re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
aws

# 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 re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
aws

# 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…


…but not all changes can be planned!


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

## 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 you 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

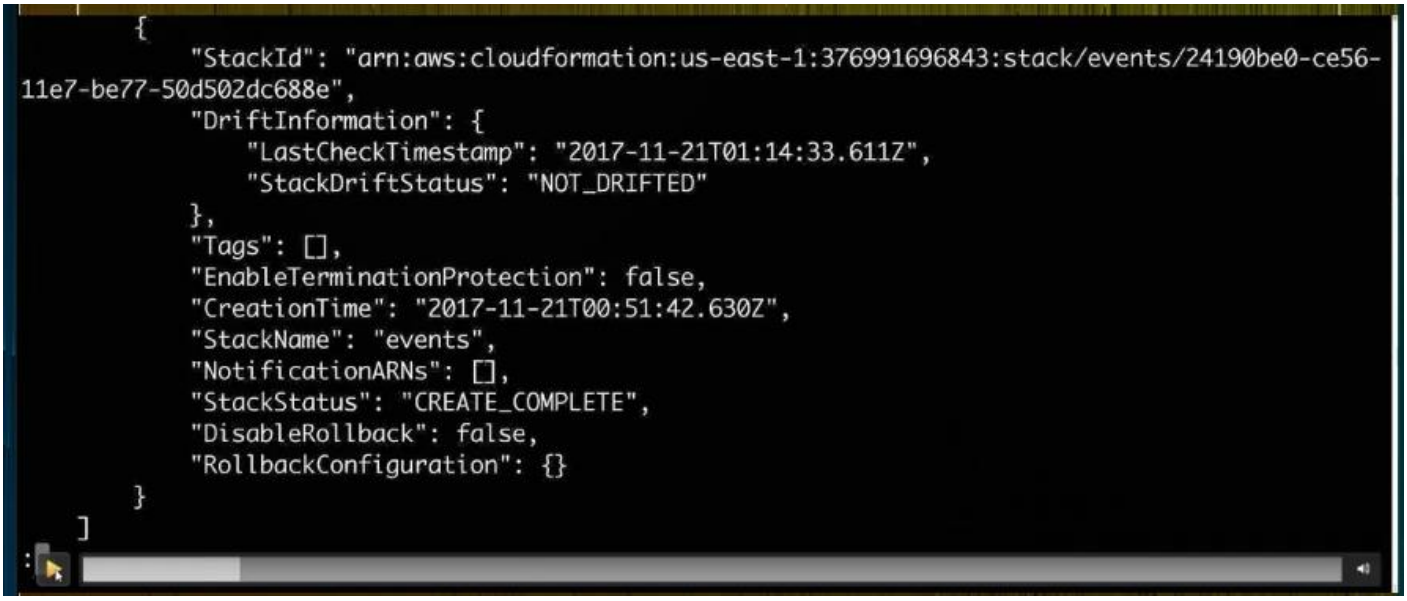
## DEMO

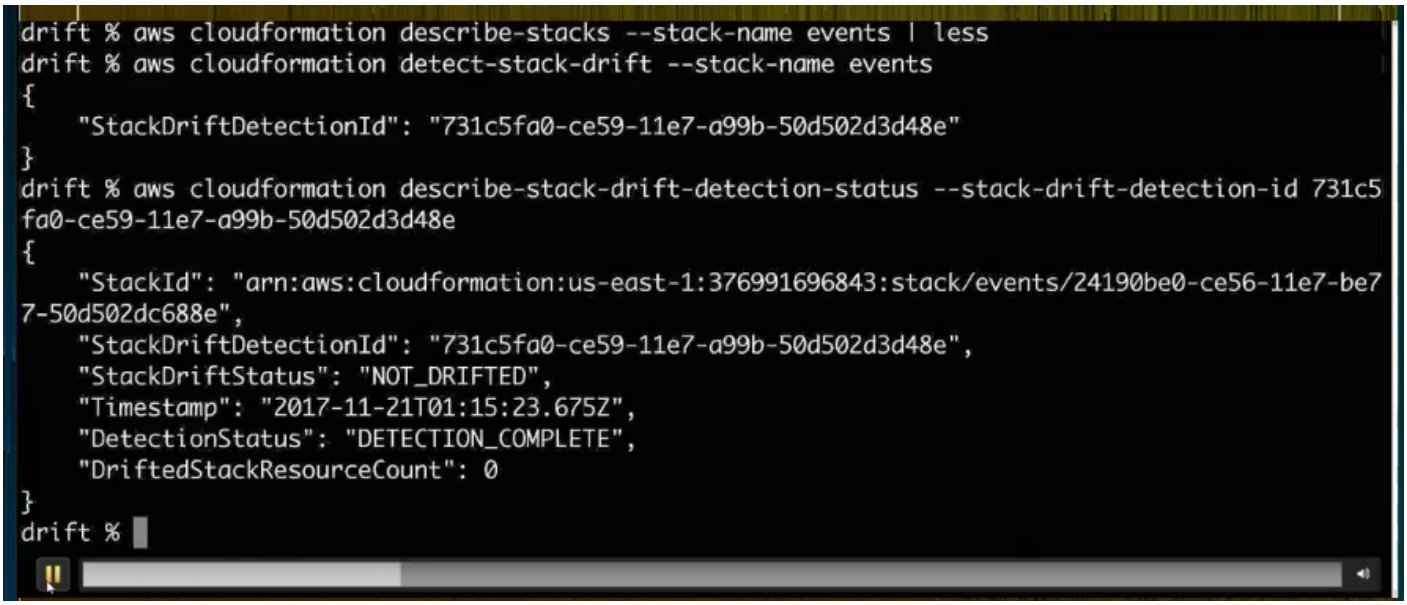
```
drift % aws cloudformation create-stack --stack-name events --template-body file:///./events.yaml
{
    "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-11e7-be7
7-50d502dc688e"
}
drift % cat events.yaml
---
Resources:
    Events:
        Type: "AWS::DynamoDB::Table"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

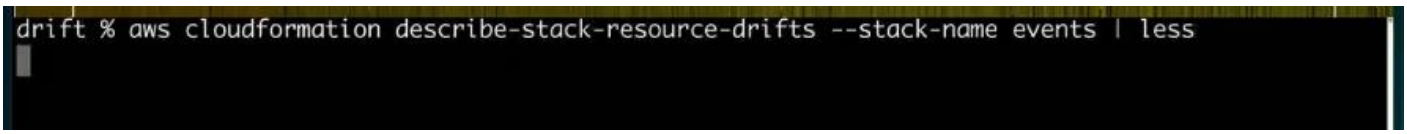
```
Resources:
    Events:
        Type: "AWS::DynamoDB::Table"
        Properties:
            KeySchema:
                -
                    AttributeName: EventId
                    KeyType: HASH
            AttributeDefinitions:
                -
                    AttributeName: EventId
                    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": {}
}
]

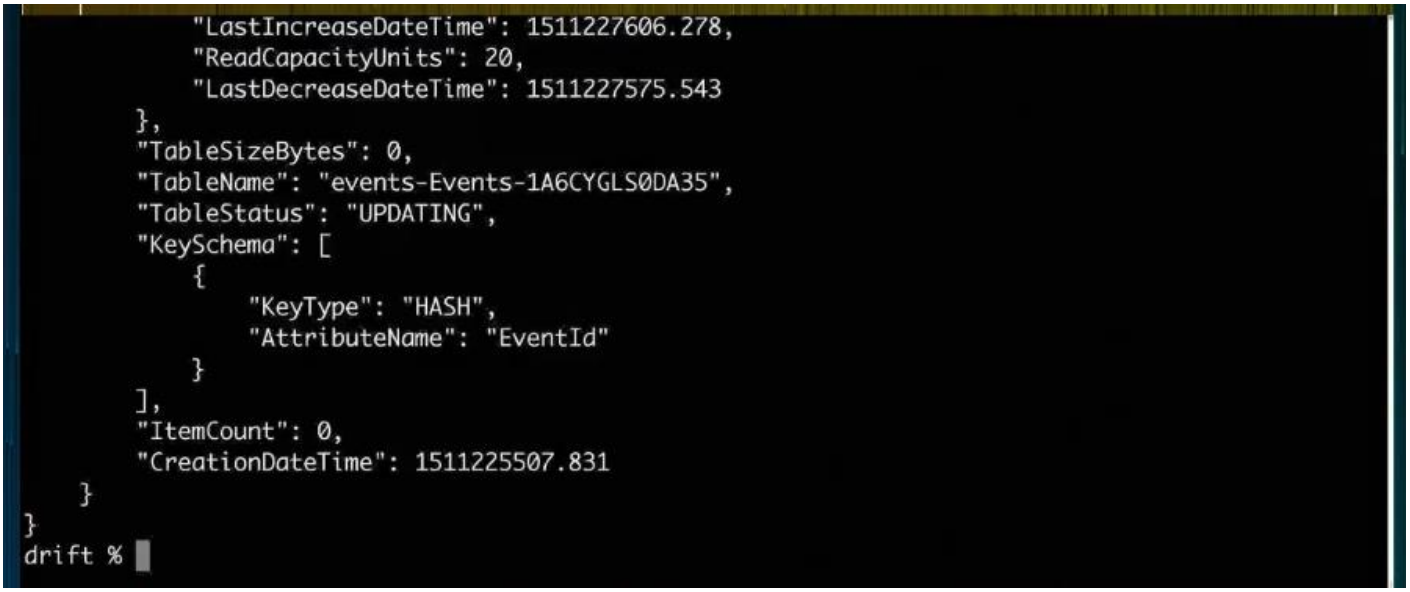

drift % aws cloudformation describe-stacks --stack-name events | less
drift % aws cloudformation detect-stack-drift --stack-name events
{
"StackDriftDetectionId": "731c5fa0-ce59-11e7-a99b-50d502d3d48e"
}
drift % aws cloudformation describe-stack-drift-detection-status --stack-drift-detection-id 731c5fa0-ce59-11e7-a99b-50d502d3d48e
{
"StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-11e7-be77-50d502dc688e",
"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

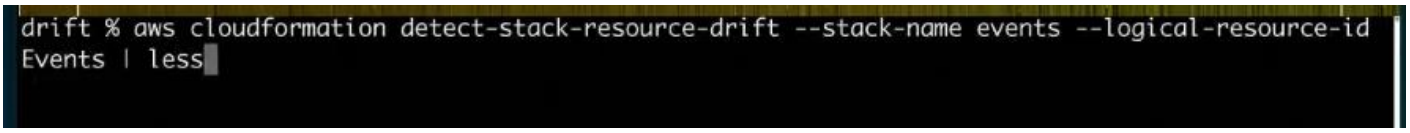
```
{
    "StackResourceDrifts": [
        {
            "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-
11e7-be77-50d502dc688e",
            "ActualProperties": "{\"ReceiveMessageWaitTimeSeconds\":0,\"DelaySeconds\":0,\"Messag
eRetentionPeriod\":345600,\"MaximumMessageSize\":262144,\"VisibilityTimeout\":30,\"QueueName\":\"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

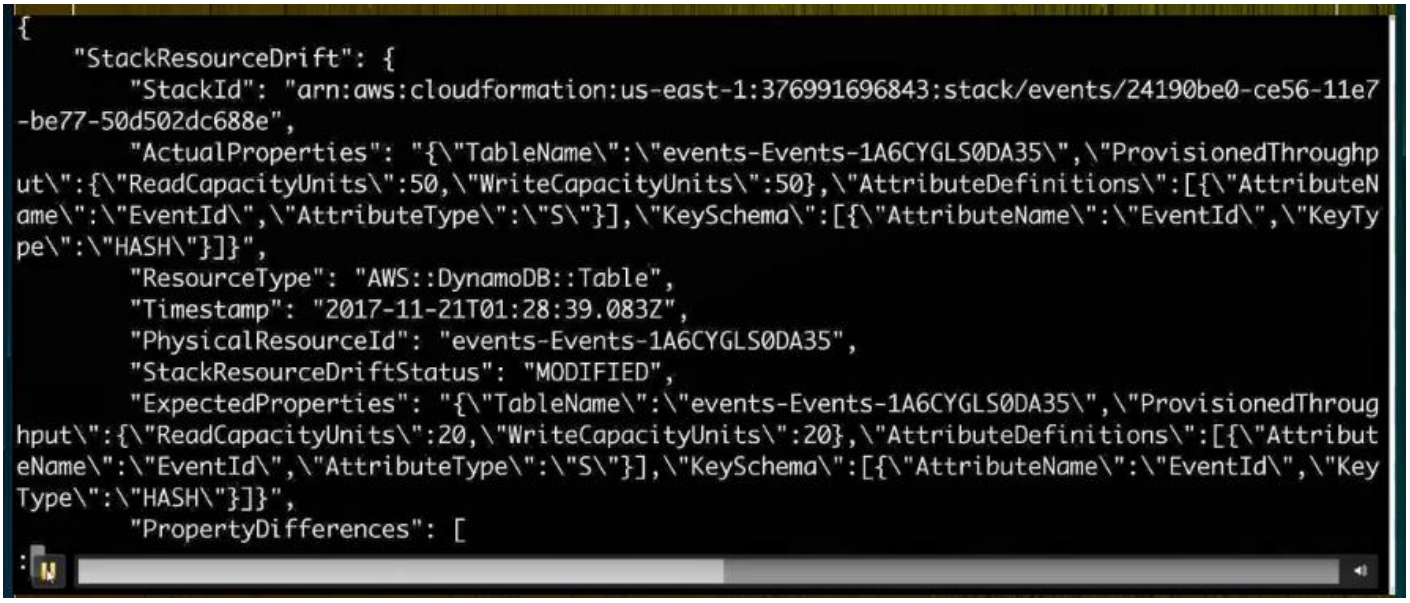
```
drift % aws dynamodb update-table --table-name events-Events-1A6CYGLS0DA35 --provisioned-throughp
ut ReadCapacityUnits=50,WriteCapacityUnits=50
```



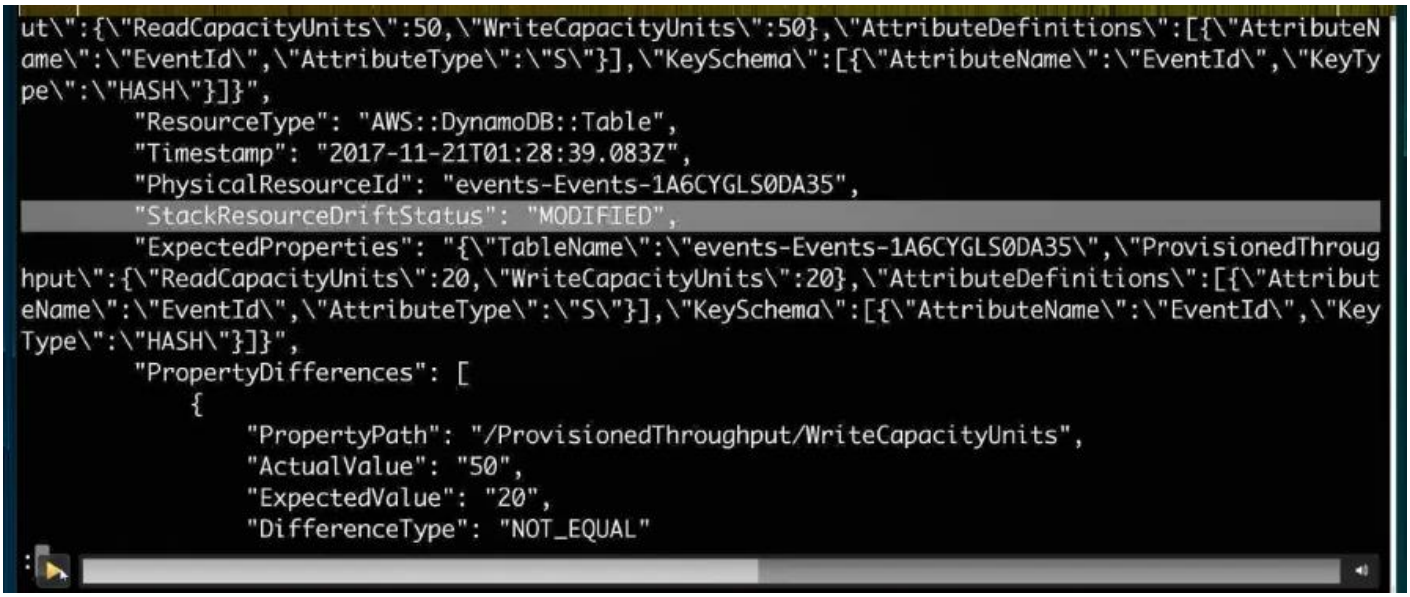
```
            "LastIncreaseDateTime": 1511227606.278,
            "ReadCapacityUnits": 20,
            "LastDecreaseDateTime": 1511227575.543
        },
        "TableSizeBytes": 0,
        "TableName": "events-Events-1A6CYGLS0DA35",
        "TableStatus": "UPDATING",
        "KeySchema": [
            {
                "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
```

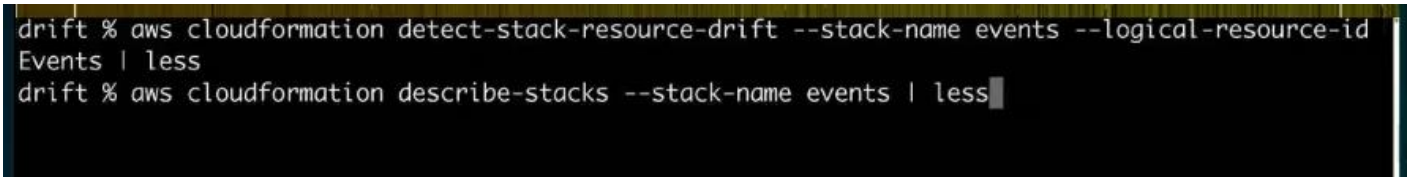


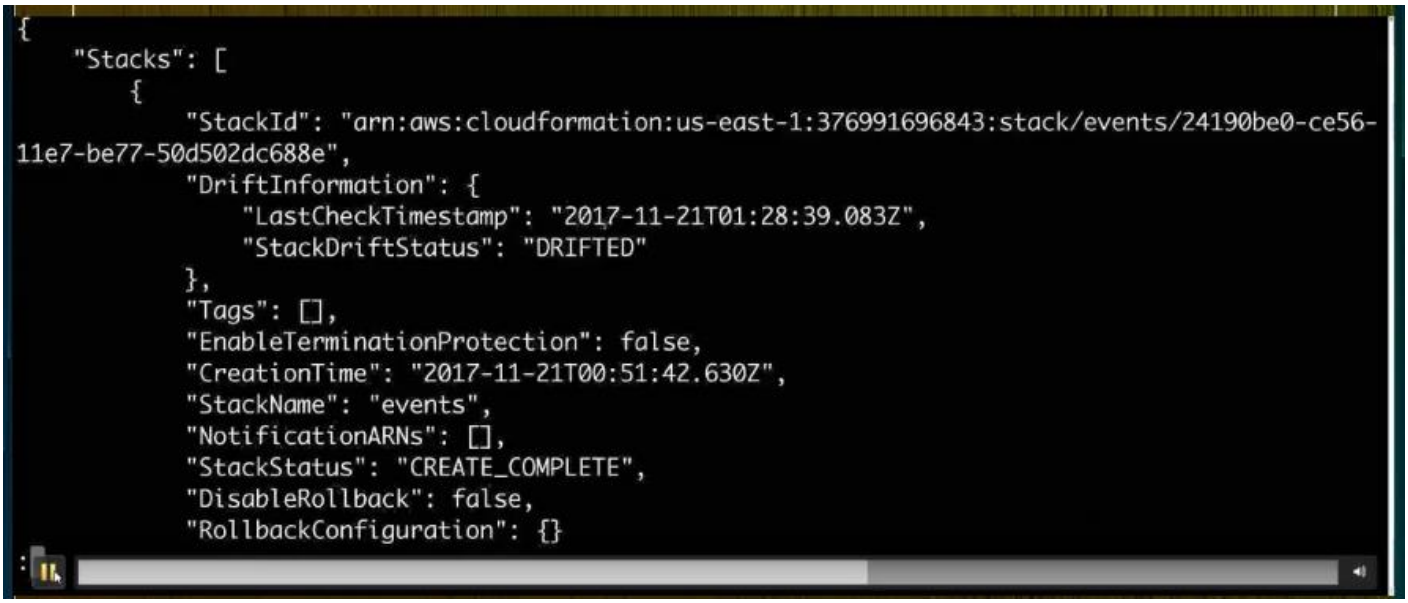
```
{
    "StackResourceDrift": {
        "StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-11e7
-be77-50d502dc688e",
        "ActualProperties": "{\"TableName\":\"events-Events-1A6CYGLS0DA35\",\"ProvisionedThroughp
ut\":{\"ReadCapacityUnits\":50,\"WriteCapacityUnits\":50},\"AttributeDefinitions\":[{\"AttributeN
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\",\"ProvisionedThroug
hput\":{\"ReadCapacityUnits\":20,\"WriteCapacityUnits\":20},\"AttributeDefinitions\":[{\"Attribut
eName\":\"EventId\",\"AttributeType\":\"S\"}],\"KeySchema\":[{\"AttributeName\":\"EventId\",\"Key
Type\":\"HASH\"}]}",
        "PropertyDifferences": [
:
```

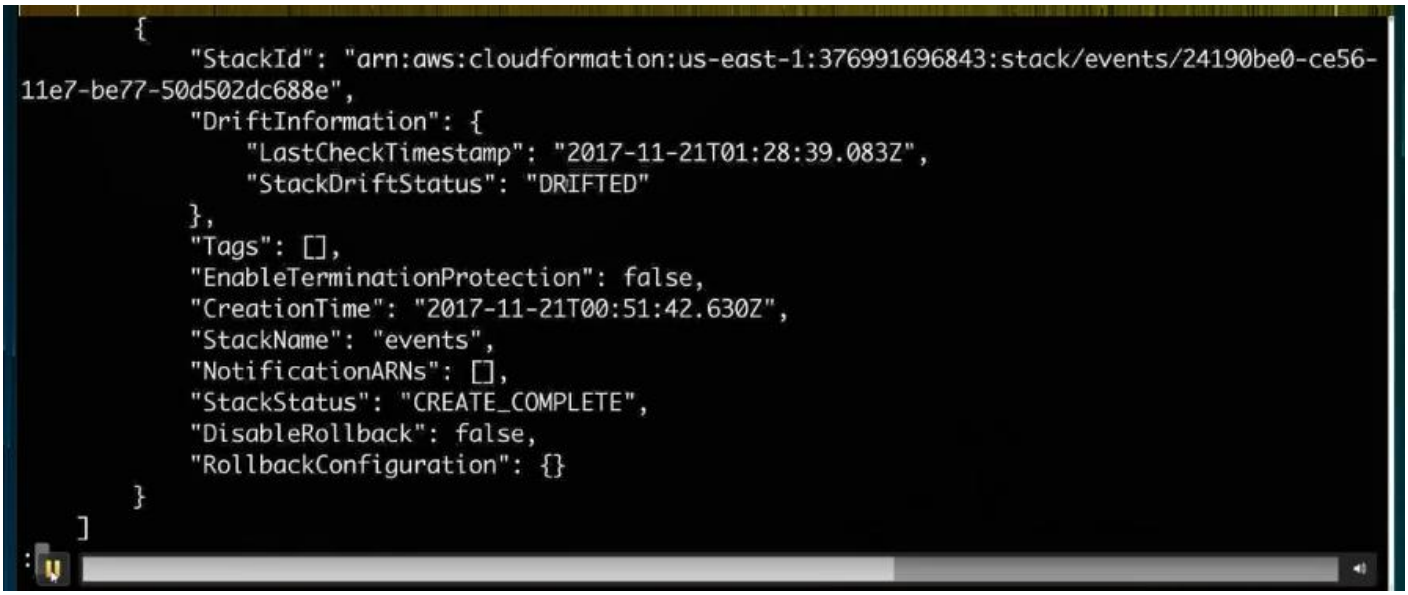




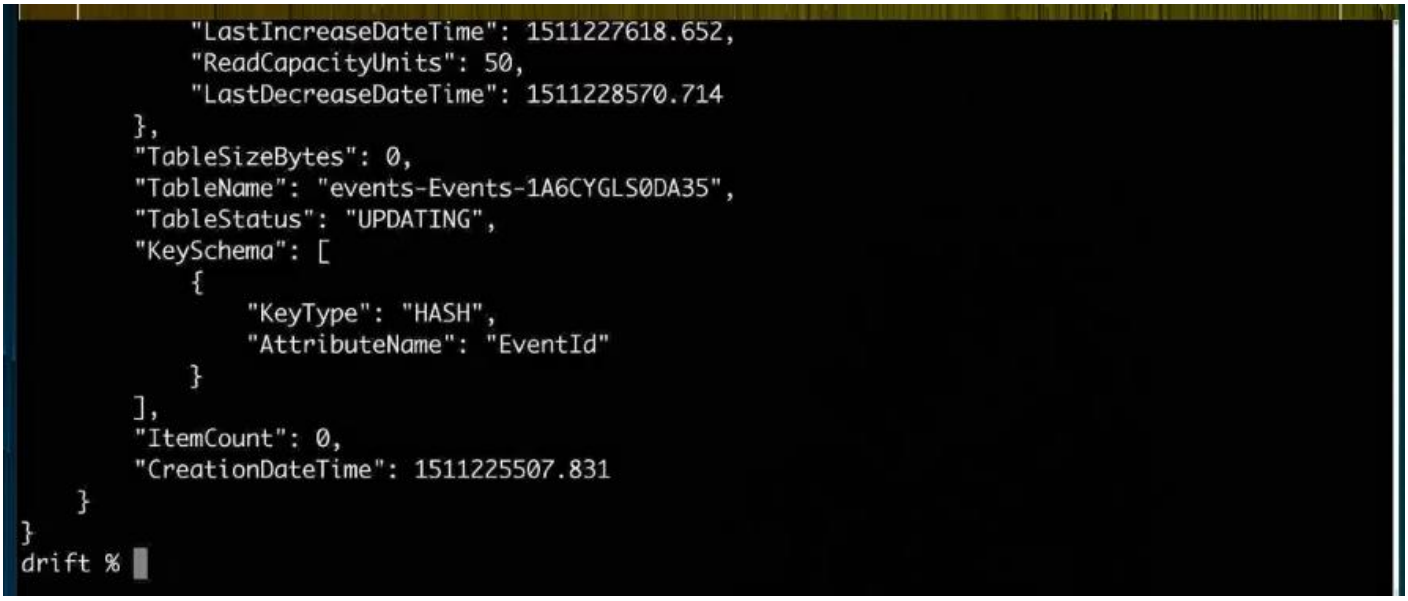
Now CF has detected that the stack as drifted due to the out-of-band change made



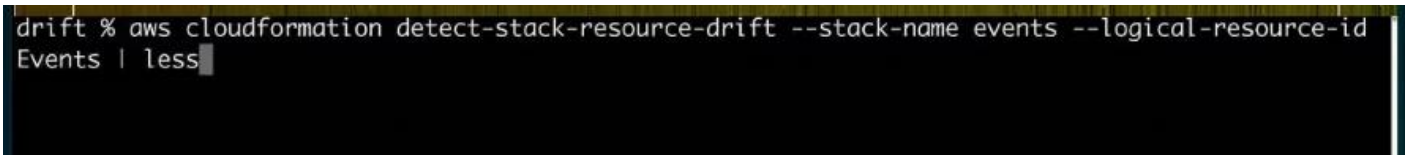


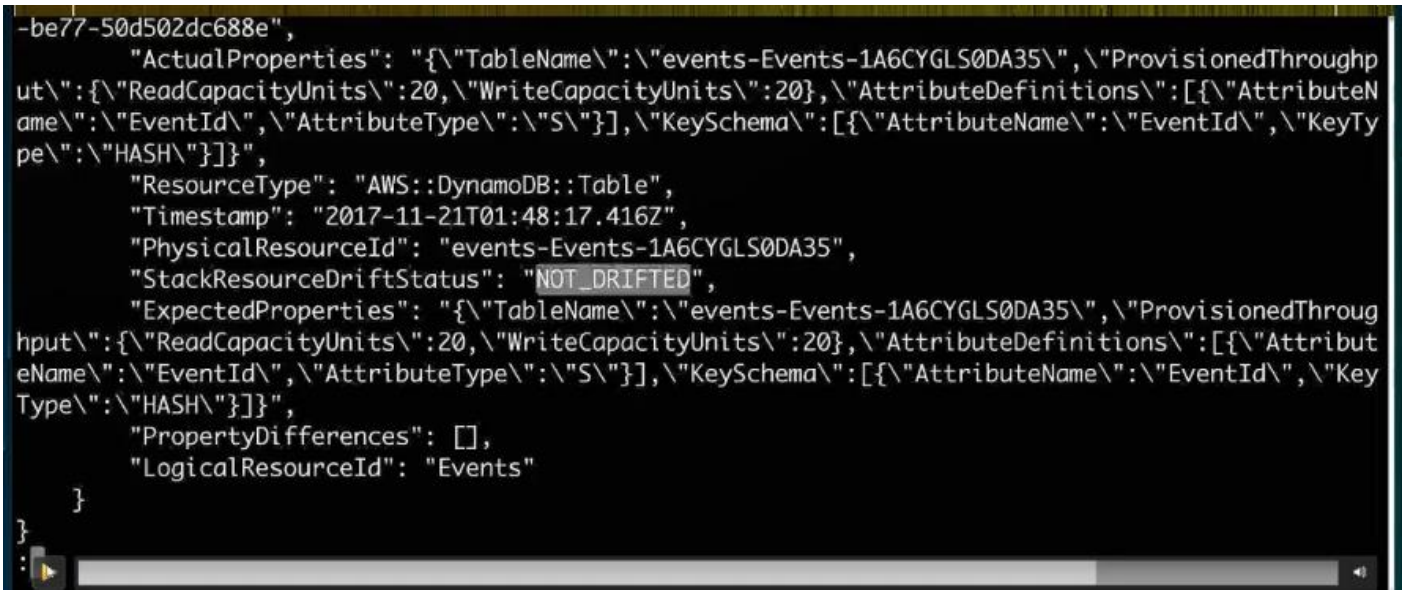

```
drift % aws dynamodb update-table --table-name events-Events-1A6CYGLS0DA35 --provisioned-throughput ReadCapacityUnits=20,WriteCapacityUnits=20
```



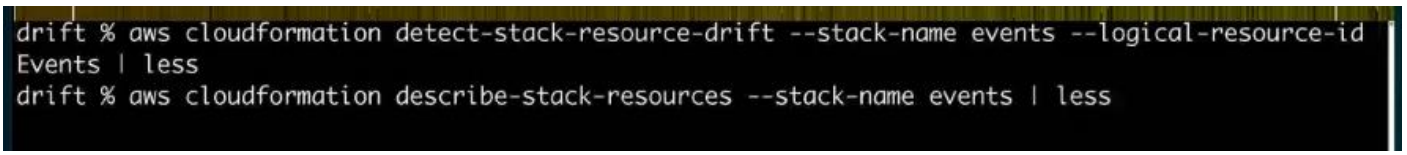
```
            "LastIncreaseDateTime": 1511227618.652,
            "ReadCapacityUnits": 50,
            "LastDecreaseDateTime": 1511228570.714
        },
        "TableSizeBytes": 0,
        "TableName": "events-Events-1A6CYGLS0DA35",
        "TableStatus": "UPDATING",
        "KeySchema": [
      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



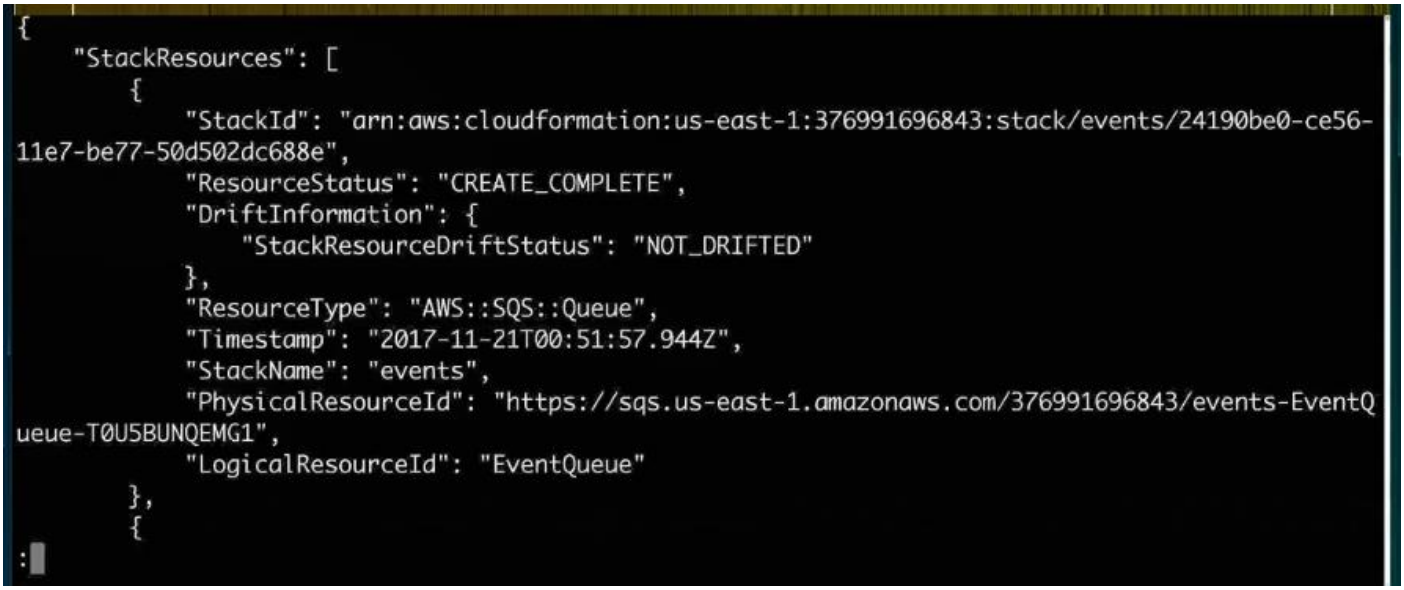
```
drift % aws cloudformation detect-stack-resource-drift --stack-name events --logical-resource-id
Events | less
```

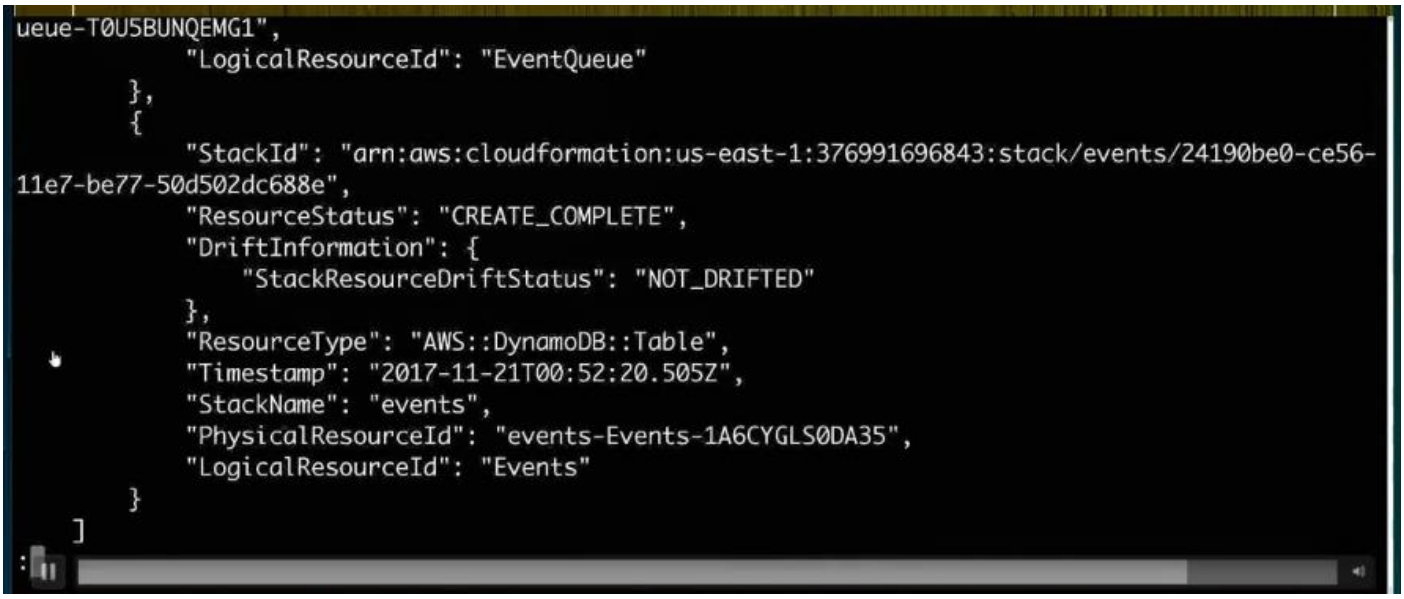


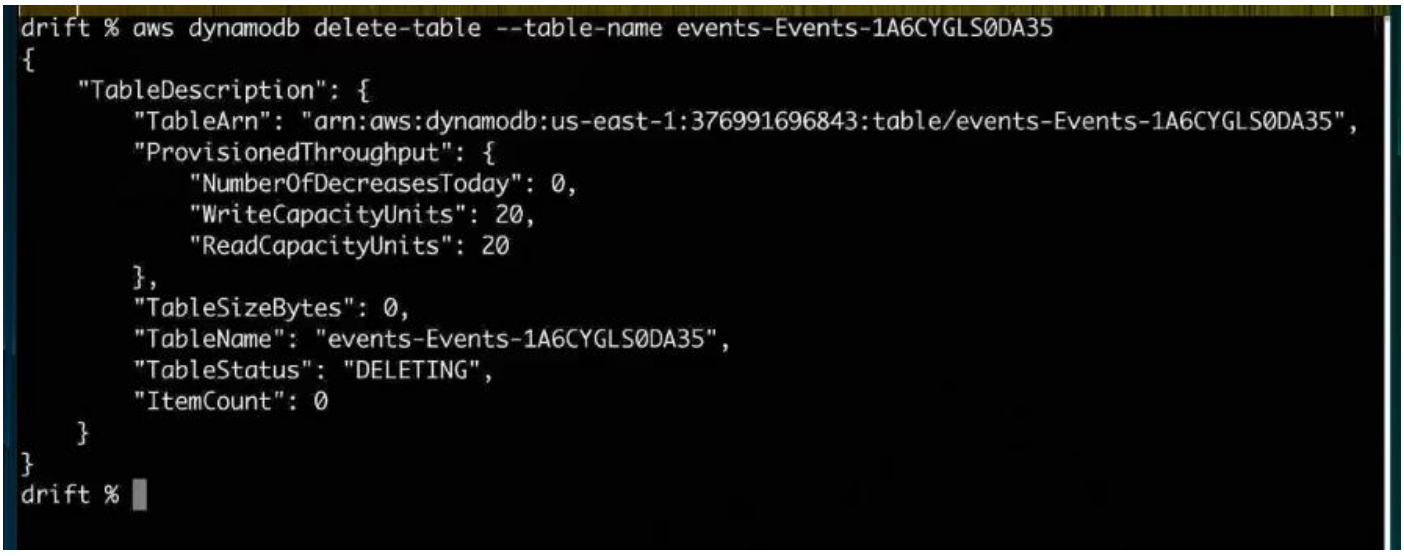
```
-be77-50d502dc688e",
        "ActualProperties": "{\"TableName\":\"events-Events-1A6CYGLS0DA35\",\"ProvisionedThroughp
ut\":{\"ReadCapacityUnits\":20,\"WriteCapacityUnits\":20},\"AttributeDefinitions\":[{\"AttributeN
ame\":\"EventId\",\"AttributeType\":\"S\"}],\"KeySchema\":[{\"AttributeName\":\"EventId\",\"KeyTy
pe\":\"HASH\"}]}",
        "ResourceType": "AWS::DynamoDB::Table",
        "Timestamp": "2017-11-21T01:48:17.416Z",
        "PhysicalResourceId": "events-Events-1A6CYGLS0DA35",
        "StackResourceDriftStatus": "NOT_DRIFTED",
        "ExpectedProperties": "{\"TableName\":\"events-Events-1A6CYGLS0DA35\",\"ProvisionedThroug
hput\":{\"ReadCapacityUnits\":20,\"WriteCapacityUnits\":20},\"AttributeDefinitions\":[{\"Attribut
eName\":\"EventId\",\"AttributeType\":\"S\"}],\"KeySchema\":[{\"AttributeName\":\"EventId\",\"Key
Type\":\"HASH\"}]}",
        "PropertyDifferences": [],
        "LogicalResourceId": "Events"
    }
}
:
```

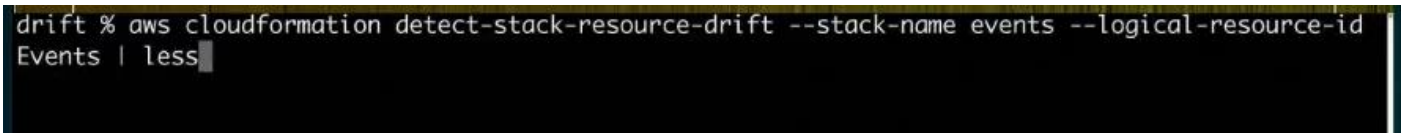


```
drift % aws cloudformation detect-stack-resource-drift --stack-name events --logical-resource-id
Events | less
drift % aws cloudformation describe-stack-resources --stack-name events | less
```


{
"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://sqs.us-east-1.amazonaws.com/376991696843/events-EventQueue-T0U5BUNQEMG1",
"LogicalResourceId": "EventQueue"
},
{
:

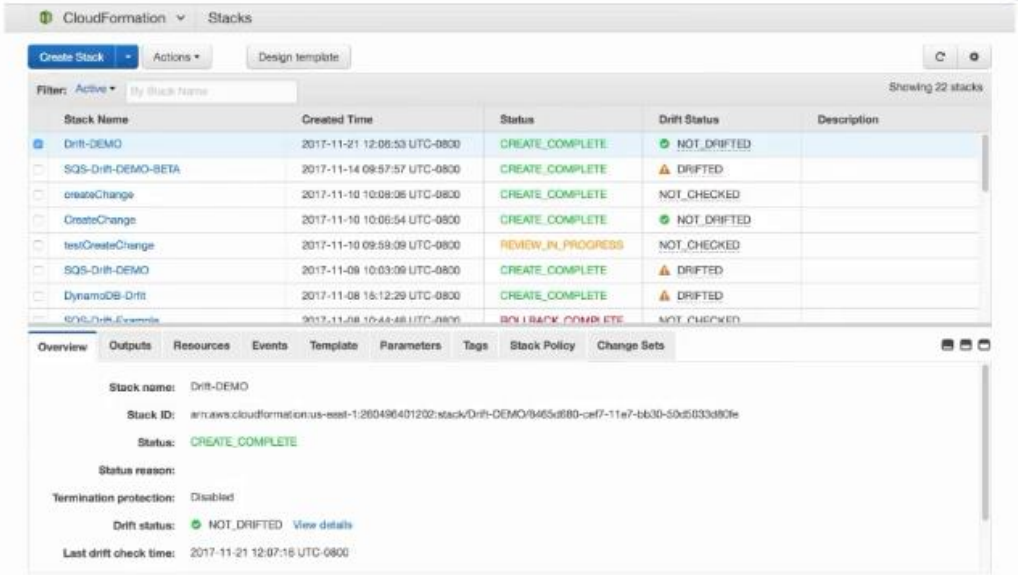

ueue-T0U5BUNQEMG1",
"LogicalResourceId": "EventQueue"
},
{
"StackId": "arn:aws:cloudformation:us-east-1:376991696843:stack/events/24190be0-ce56-11e7-be77-50d502dc688e",
"ResourceStatus": "CREATE_COMPLETE",
"DriftInformation": {
"StackResourceDriftStatus": "NOT_DRIFTED"
},
"ResourceType": "AWS::DynamoDB::Table",
"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)
```

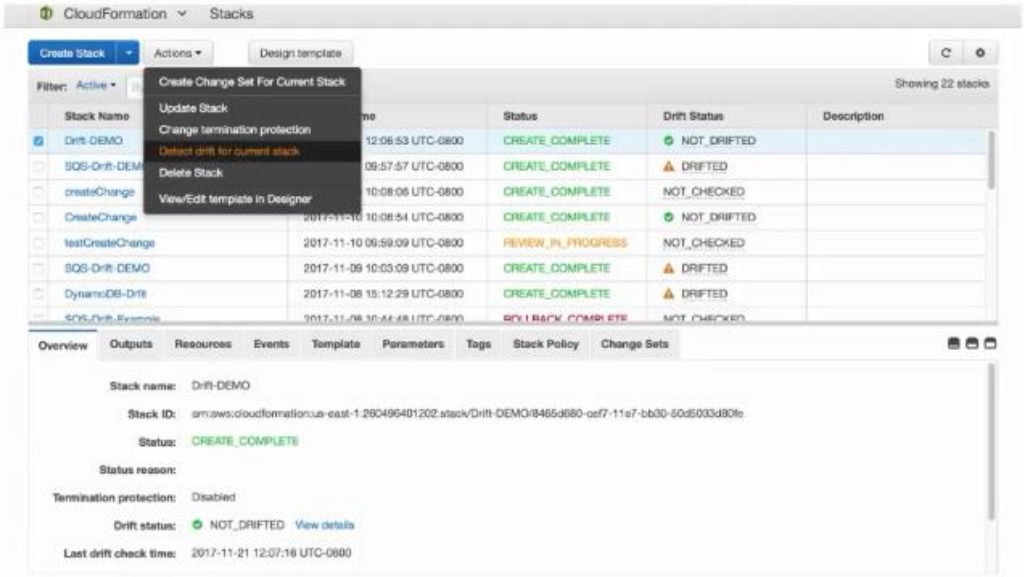

# DRIFT DETECTION – CONSOLE WALKTHROUGH (1/8)





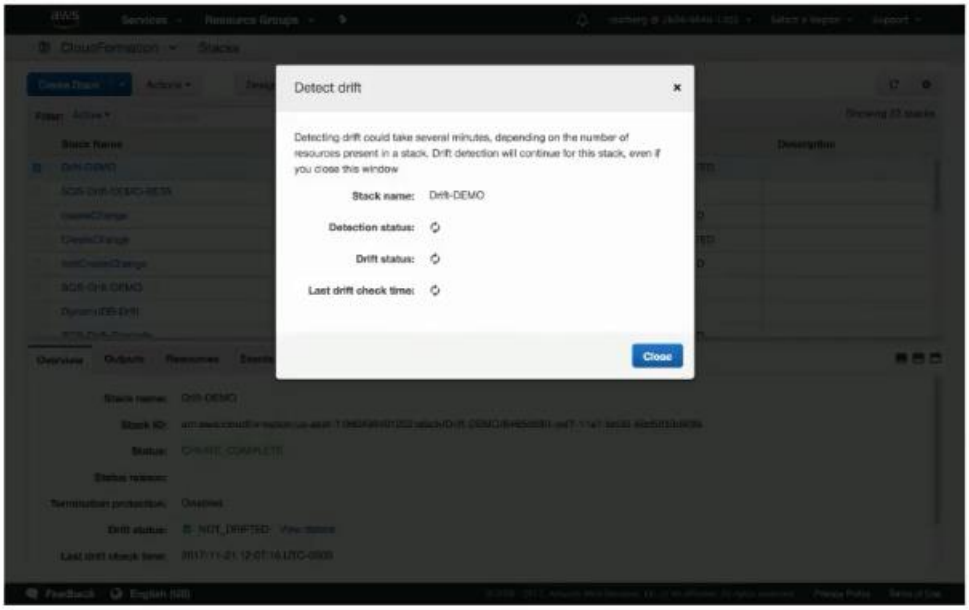
aws re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
aws

# DRIFT DETECTION – CONSOLE (2/8)



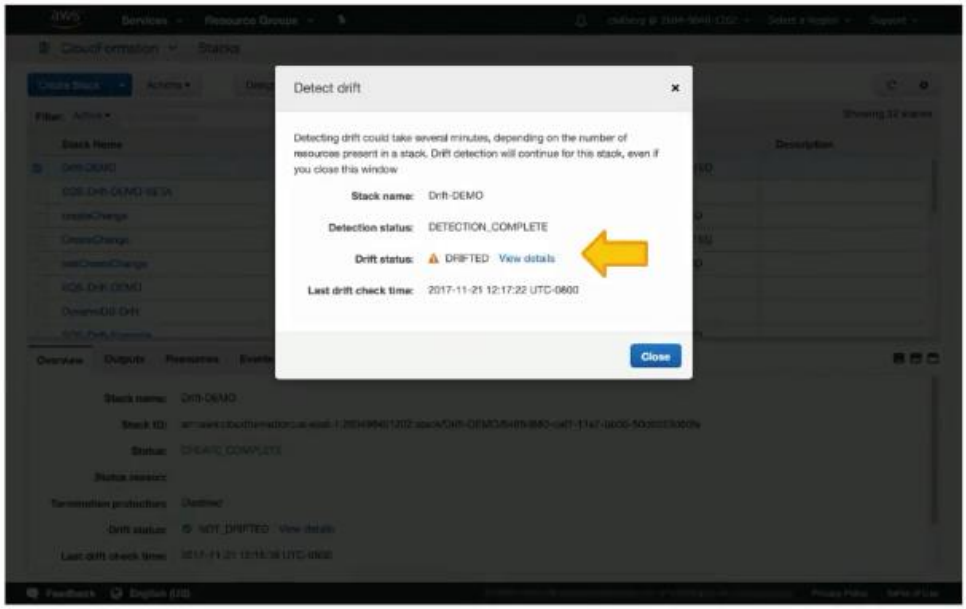

AWS re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
aws

# DRIFT DETECTION – CONSOLE (3/8)



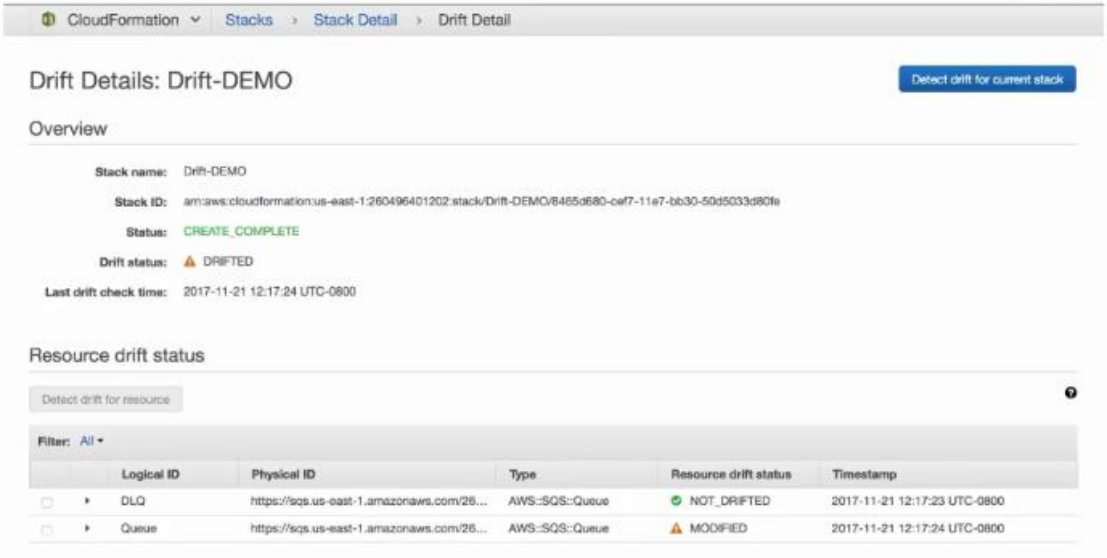

AWS re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
aws

# DRIFT DETECTION – CONSOLE (4/8)



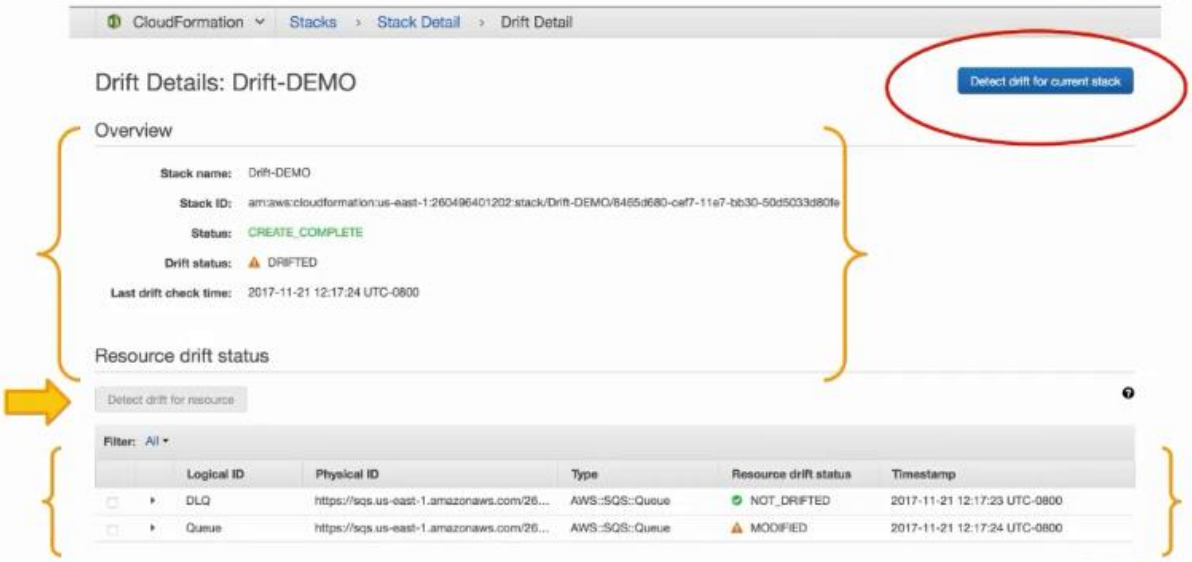

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# DRIFT DETECTION – CONSOLE (5/8)



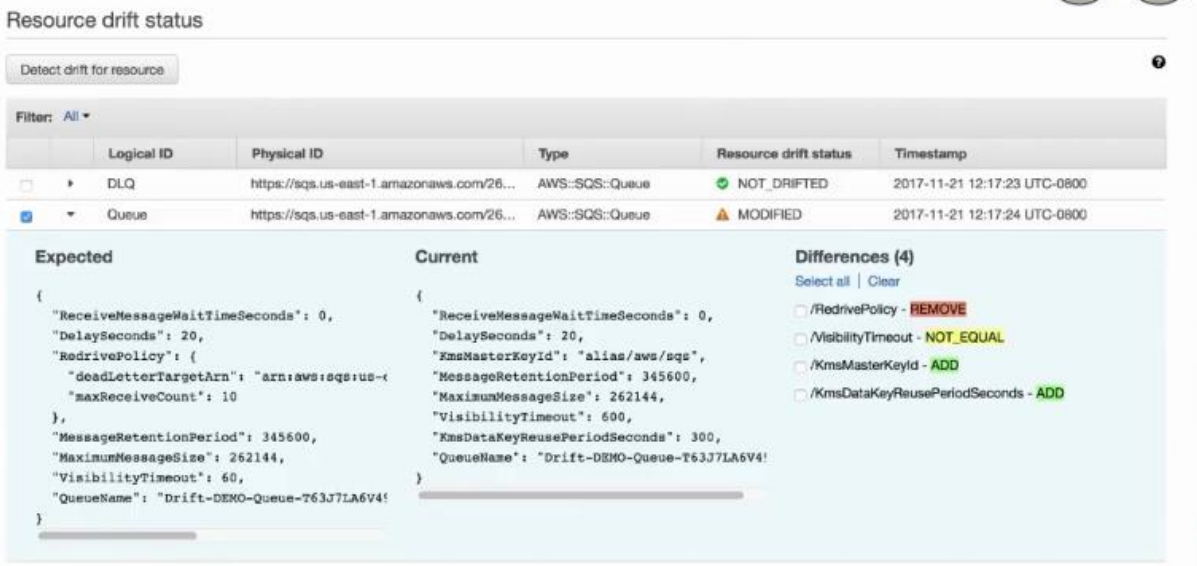

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# DRIFT DETECTION – CONSOLE (5/8)




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

# DRIFT DETECTION – CONSOLE (6/8)




© 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 |
|---|---|---|---|---|---|---|
| ☐ | ▸ | DLQ | 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 |

**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 |
|---|---|---|---|---|---|---|
| ☑ | ▸ | DLQ | https://sqs.us-east-1.amazonaws.com/26... | AWS::SQS::Queue | DELETED | 2017-11-21 12:19:35 UTC-0800 |
| ☐ | ▸ | Queue | https://sqs.us-east-1.amazonaws.com/26... | AWS::SQS::Queue | MODIFIED | 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 |
|---|---|---|---|---|---|---|
| ☐ | ▾ | DLQ | https://sqs.us-east-1.amazonaws.com/26... | AWS::SQS::Queue | DELETED | 2017-11-21 12:19:35 UTC-0800 |
| | | This resource has been deleted. | | | | |
| ☐ | ▸ | Queue | https://sqs.us-east-1.amazonaws.com/26... | AWS::SQS::Queue | MODIFIED | 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***

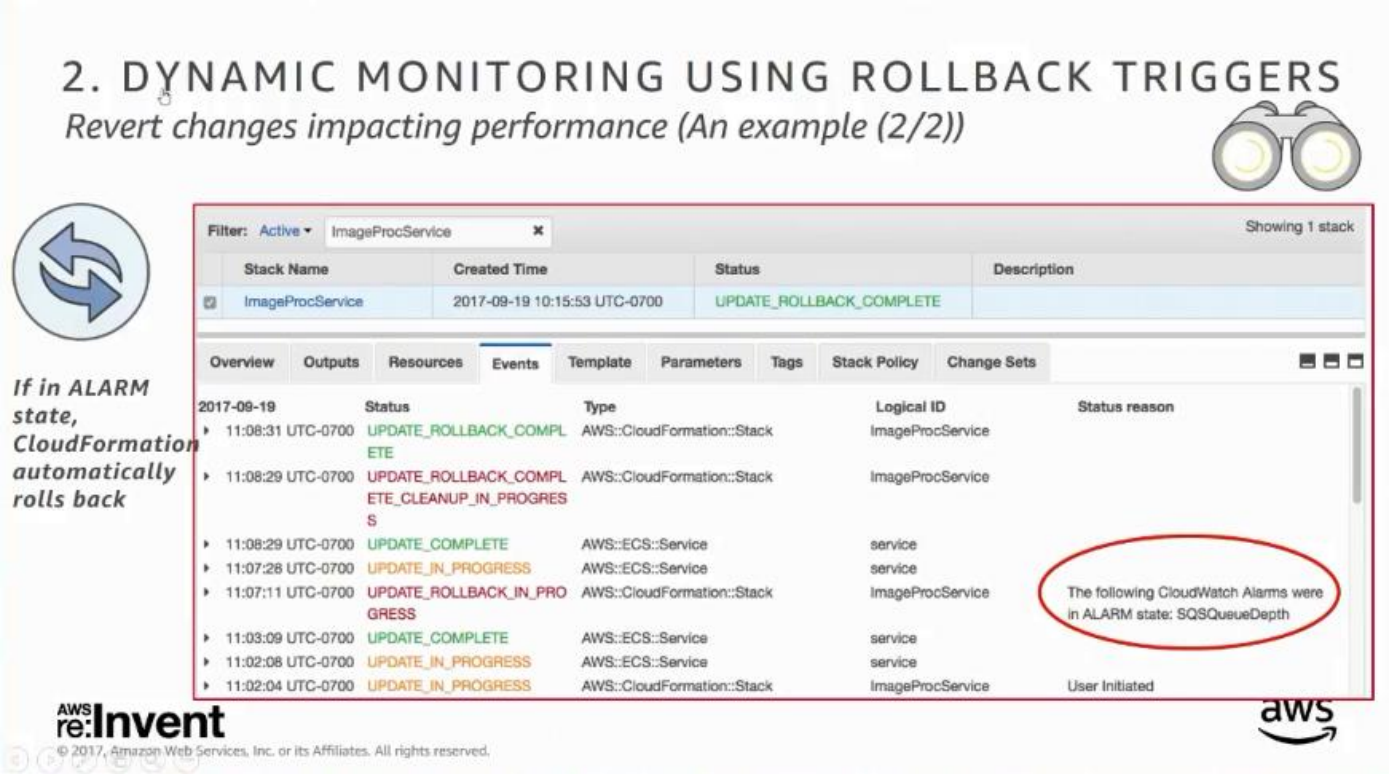
**batch-service-rollbacktrigger.json**

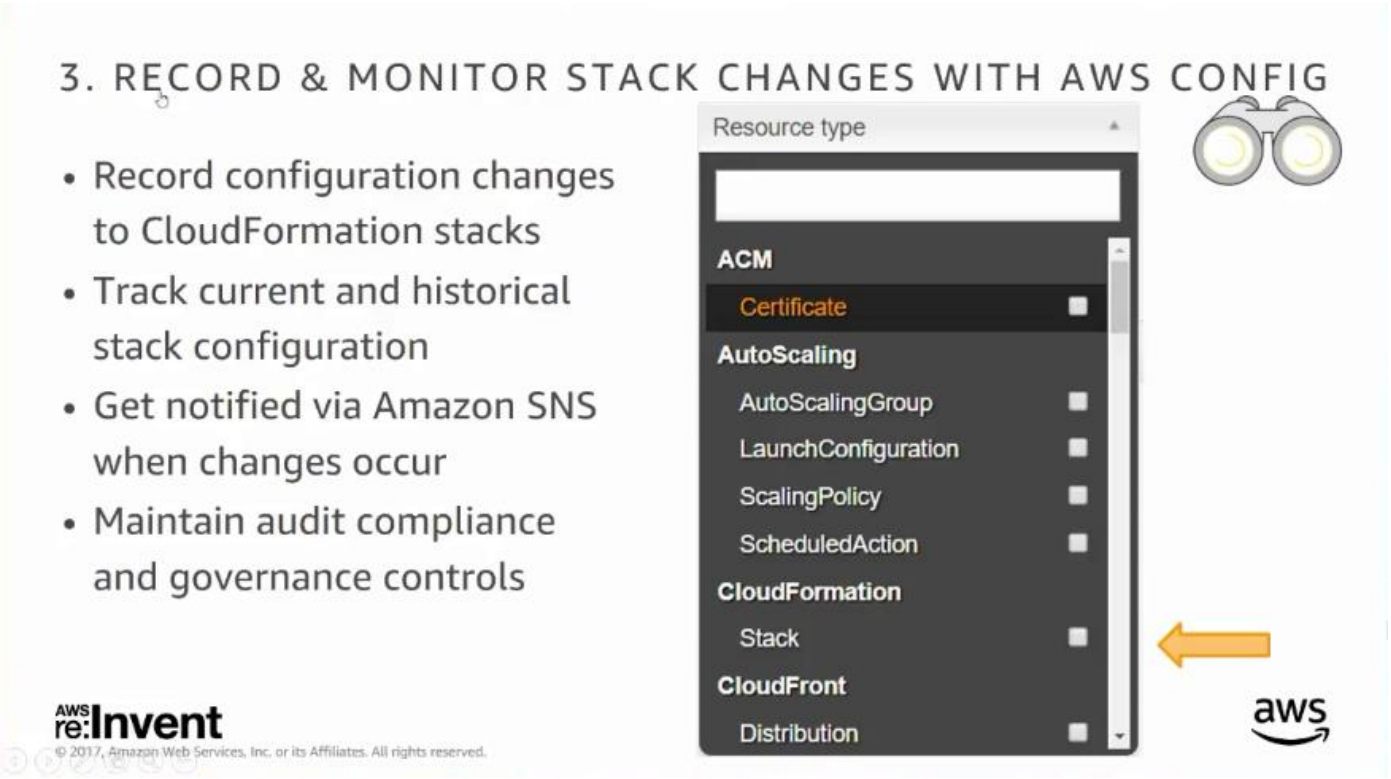
```
{
  "RollbackTriggers": [
    {
      "Arn": "arn:aws:cloudwatch:us-east-
2:xxxxxxxxxxxx:alarm:SQSQueueDepth",
      "Type": "AWS::CloudWatch::Alarm"
    }
  ],
  "MonitoringTimeInMinutes": 10
}
```

***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.

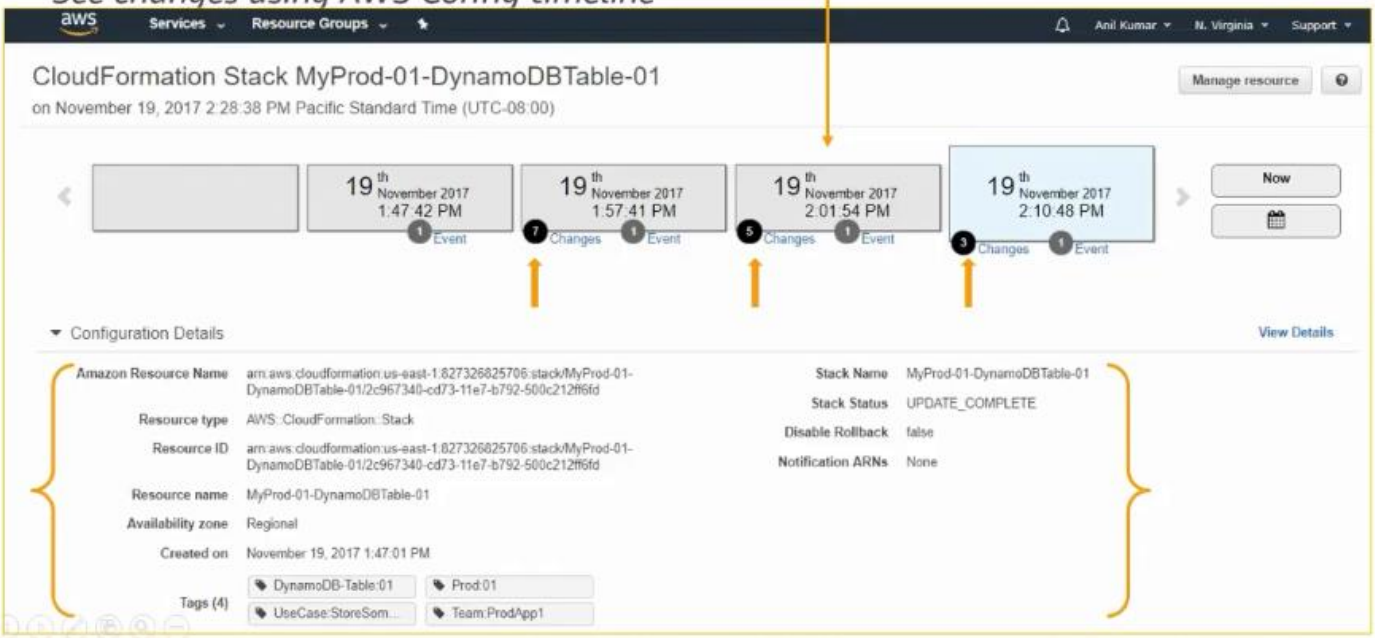



AWS Config will record all the configuration changes that happens to all of its supported resource types like CF stacks.

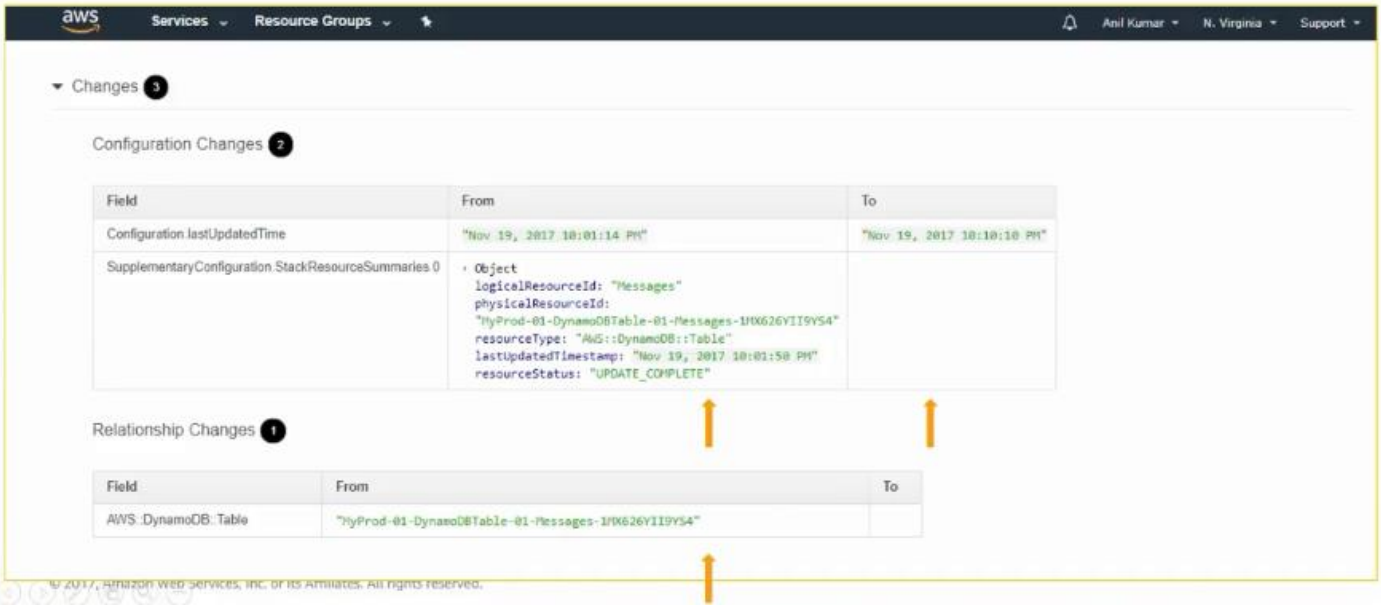
# 3. RECORD & MONITOR STACK CHANGES WITH AWS CONFIG

*See changes using AWS Config timeline*




# 3. RECORD & MONITOR STACK CHANGES WITH AWS CONFIG

*Drill down further to see details*

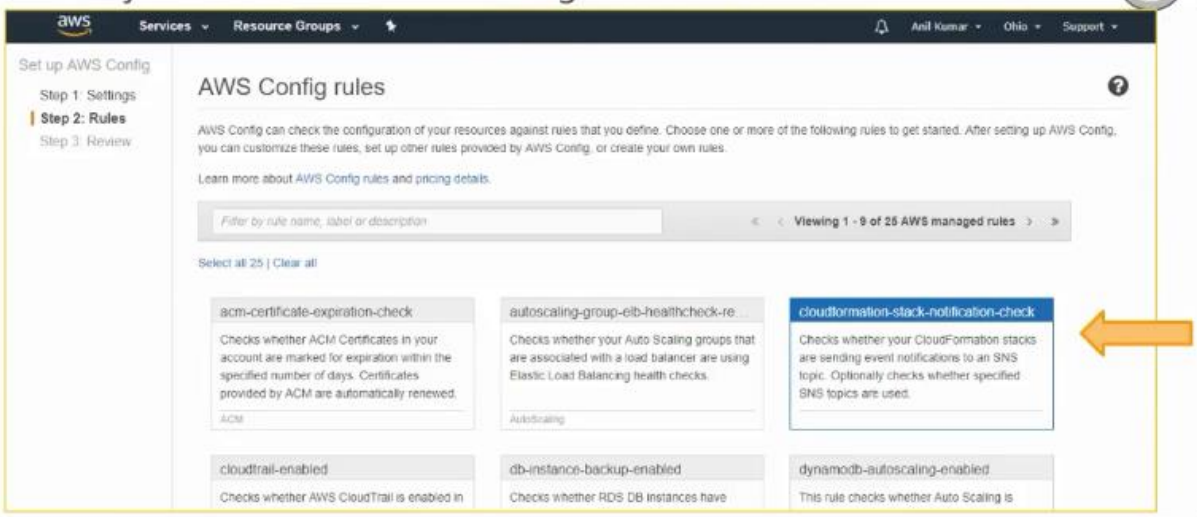



© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

# 3. RECORD & MONITOR STACK CHANGES WITH AWS CONFIG

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

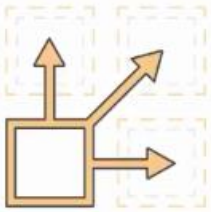
- Verify whether stacks are sending SNS notifications





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

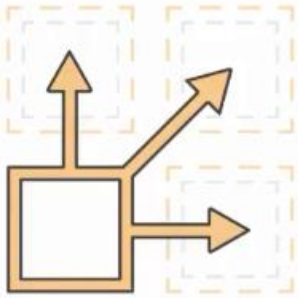

System Admins:
Safety Guardrails


**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

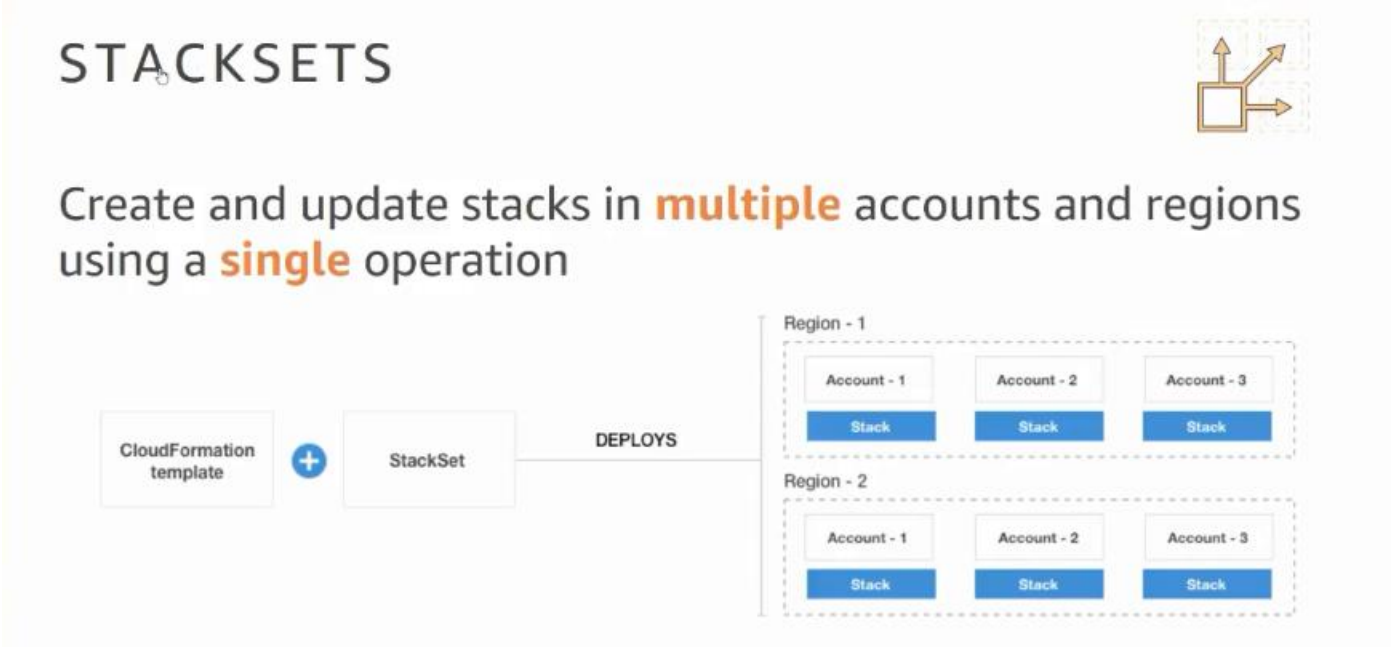
# PROVISIONING AT SCALE

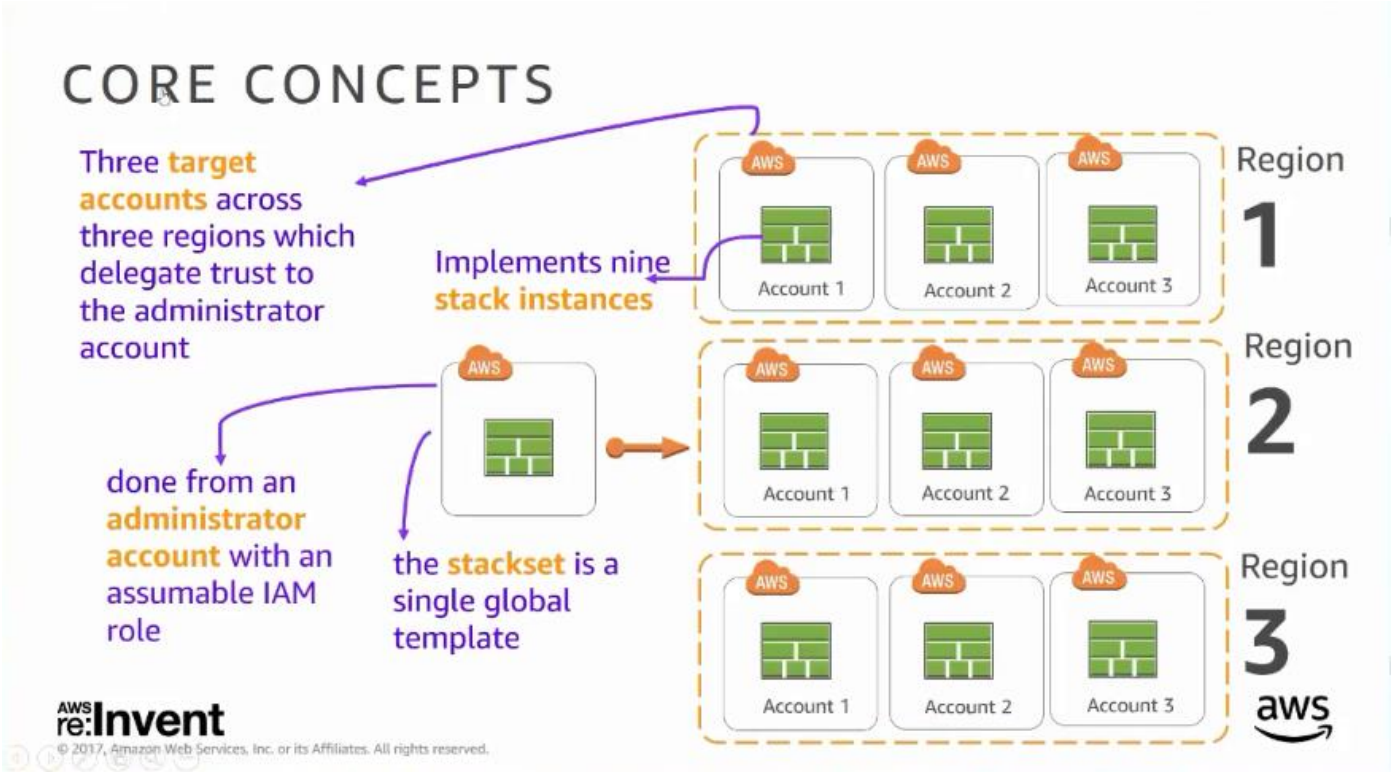
*Let's look at few customer profiles*

| Customer Profile | #1 | #2 | #3 |
|---|---|---|---|
| | • 2800+ accounts and wants to grow to 10,000 accounts | • 180+ accounts | • 19 accounts and plans to have 40 accounts |
| | • Deploy in nine AWS Regions and wants to be in 11 regions | • Deploy in selective regions | • Multiple regions |
| | • VPC, EC2, IAM, Subnet, Security Groups, and more | • VPC, IAM, CloudTrail, AWS Config | • VPC, Security Groups, IAM roles, CloudTrail |

# 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




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

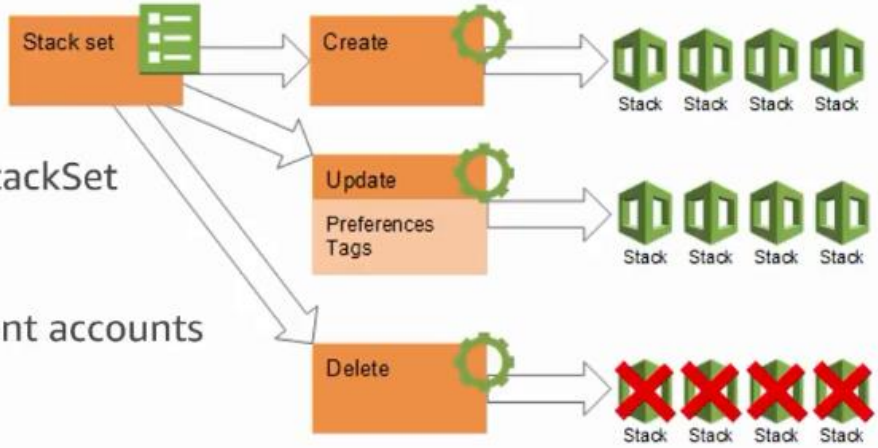
# STACKSET OPERATIONS

**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**

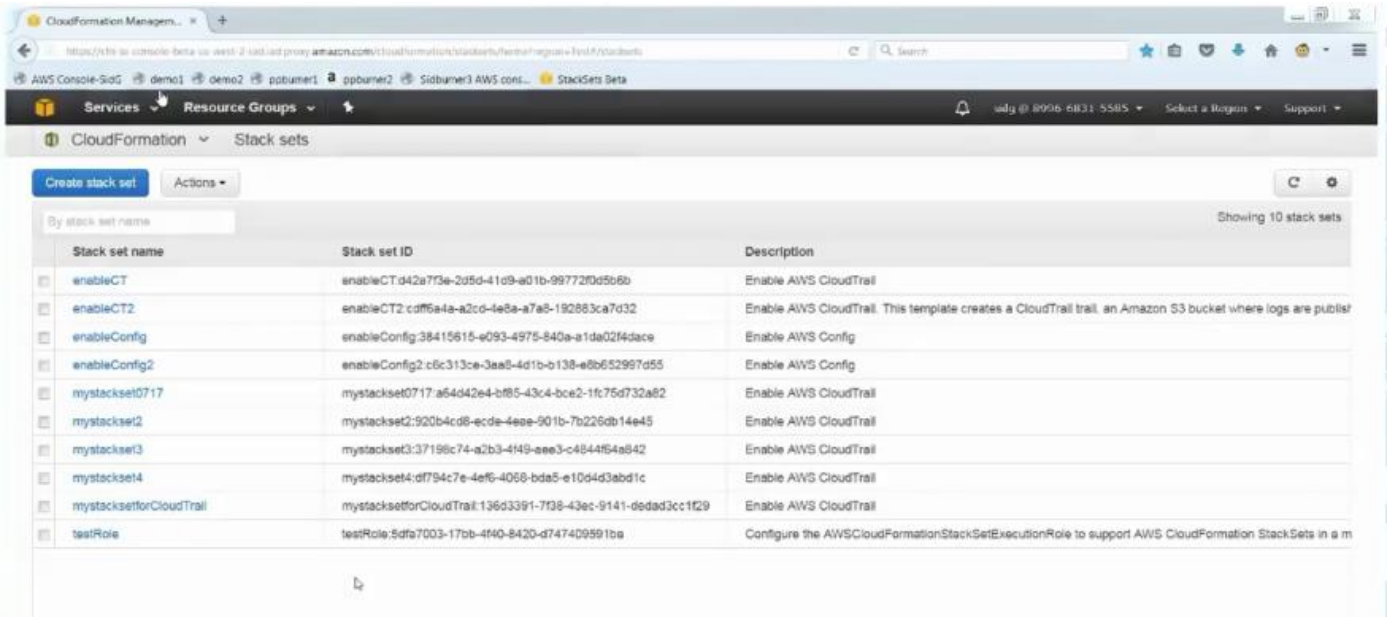
*"[It] has been instrumental for us in our quest to deliver compliance, security, and audit requirements for the entirety of our AWS estate"*

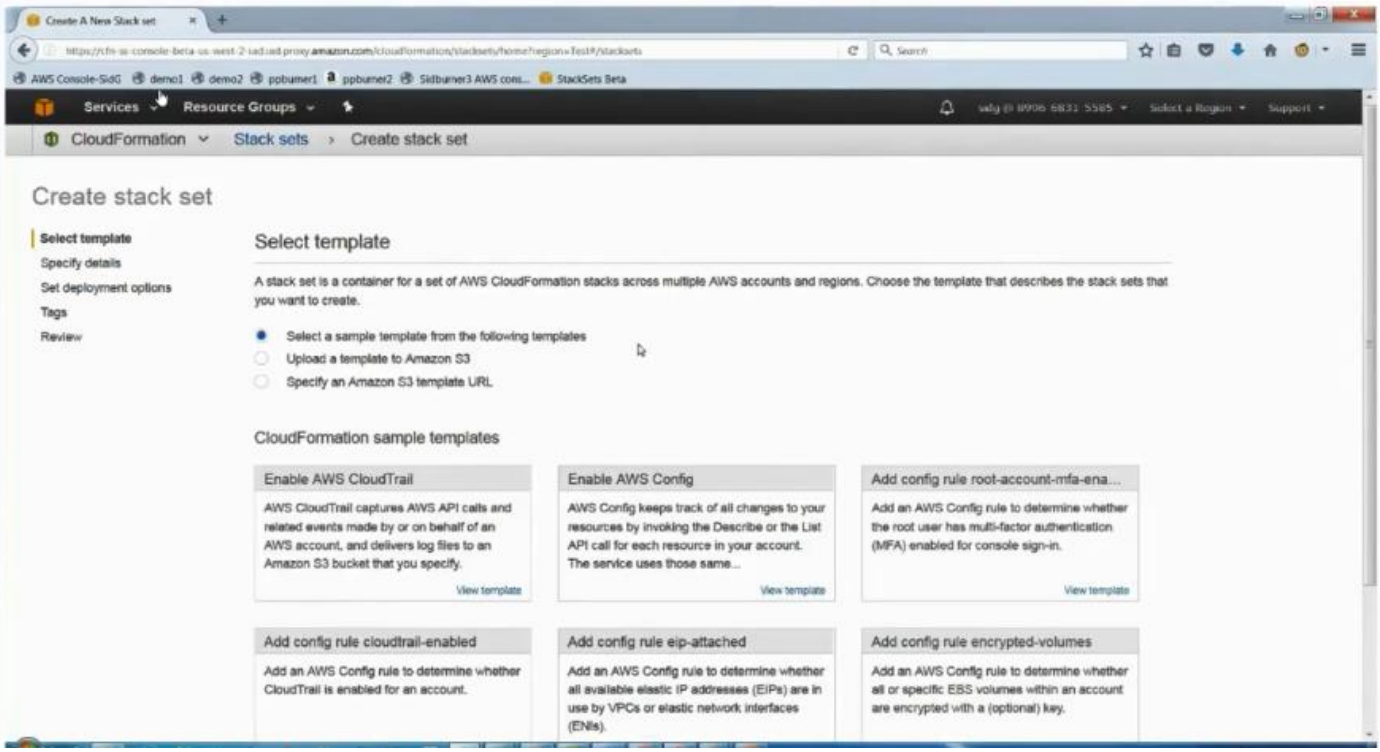
**- Joe Jarman, SRE, HIVE (Centrica, parent co. of British Gas)**

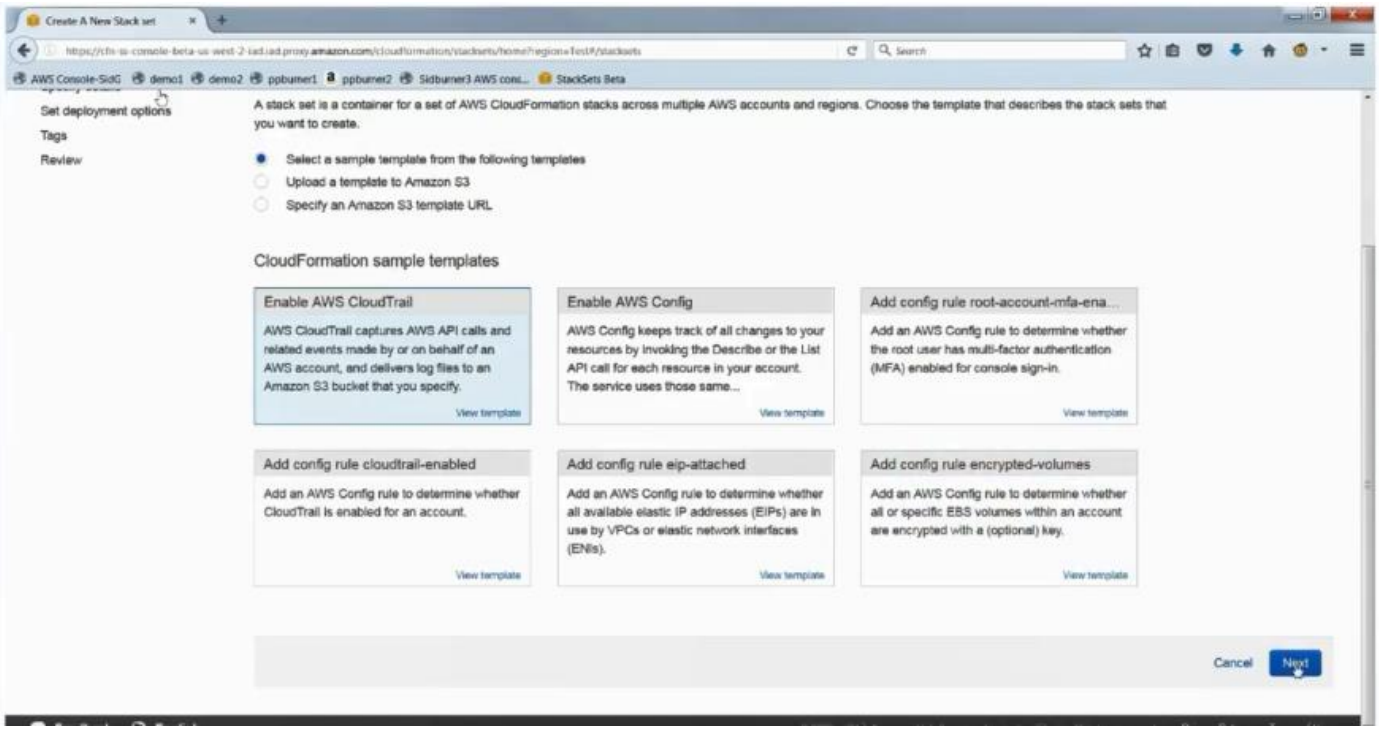
*"[It] presents the opportunity for significant time savings while increasing adherence to golden configurations across multiple accounts."*

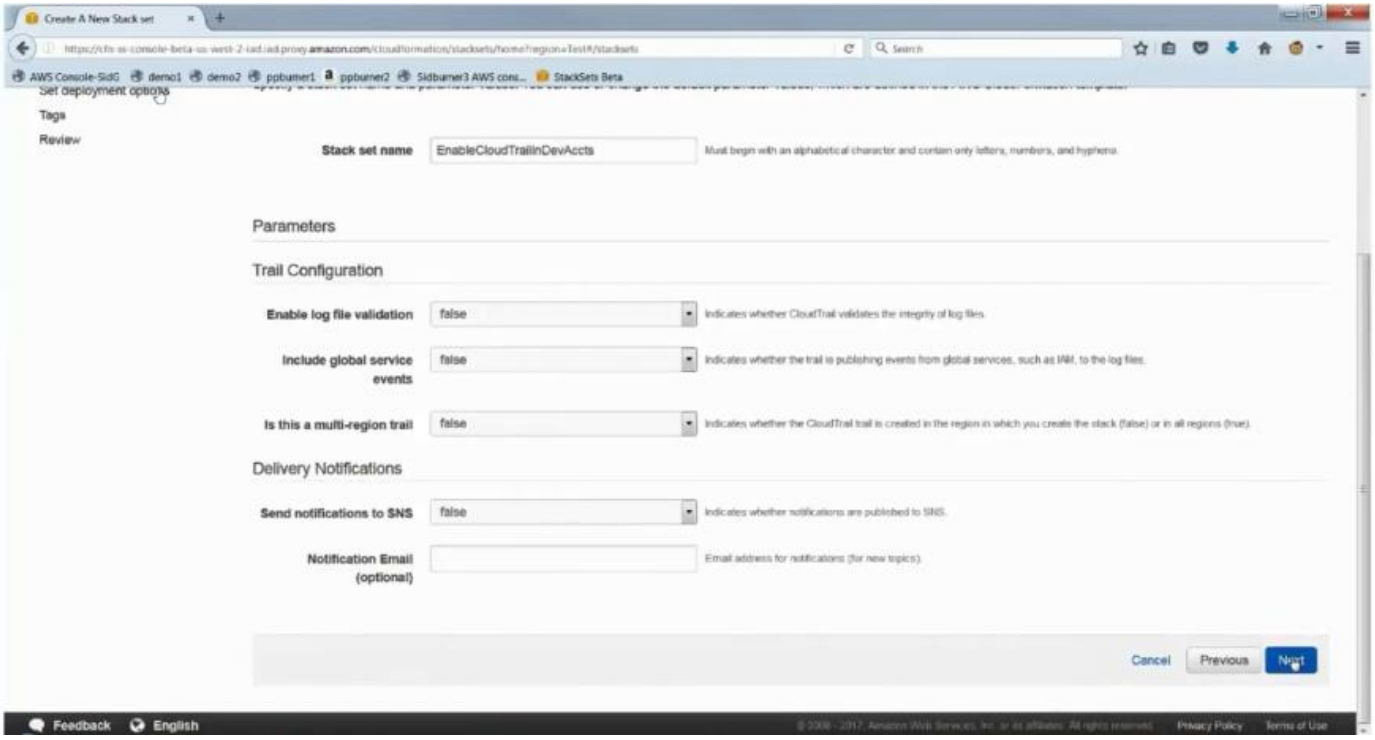
**- Aater Suleman, CEO, Flux7**

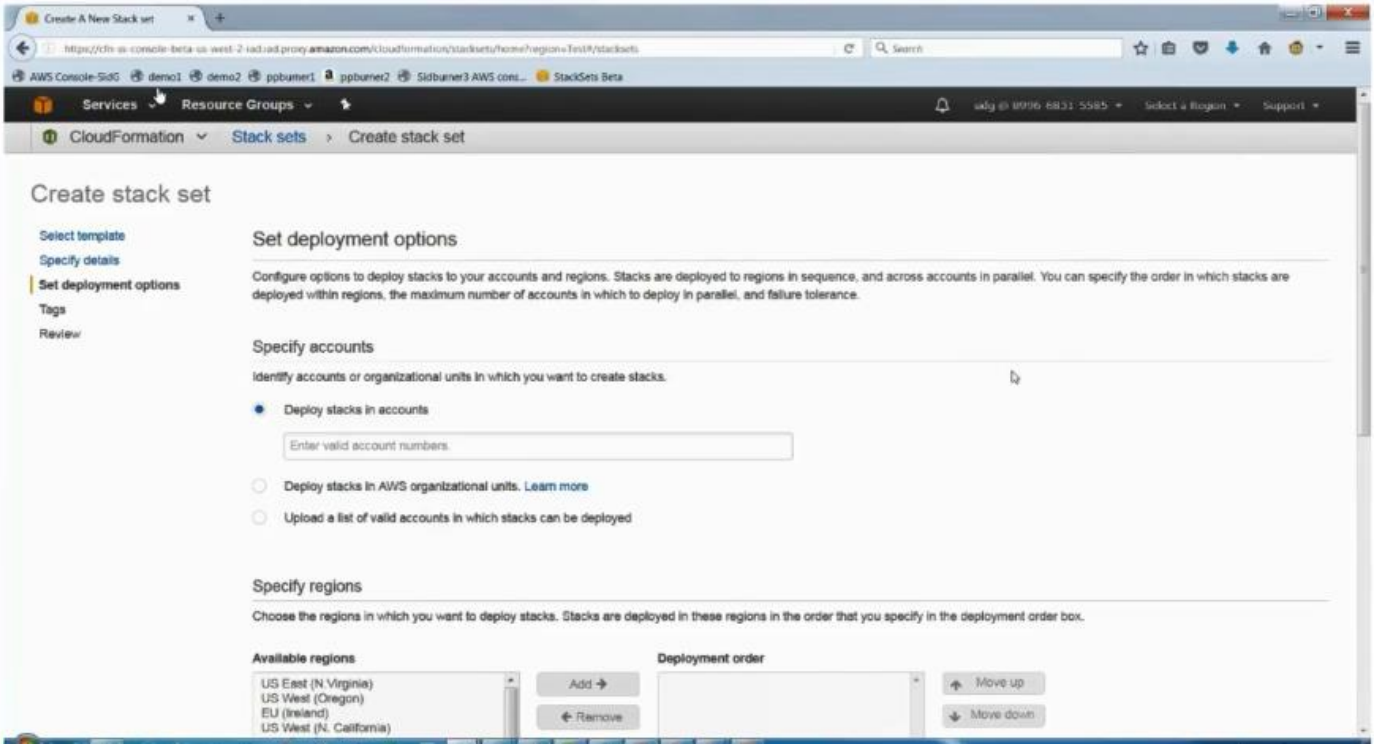
# STACKSETS DEMO

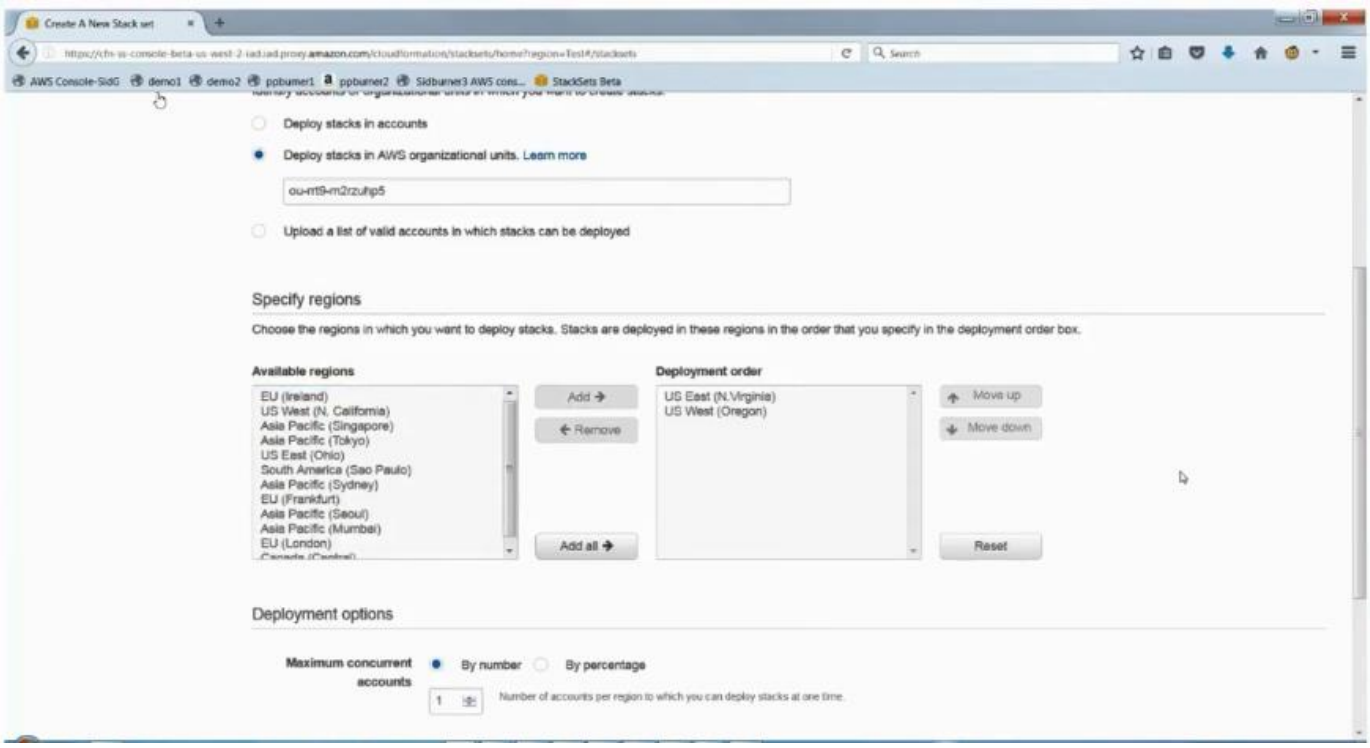


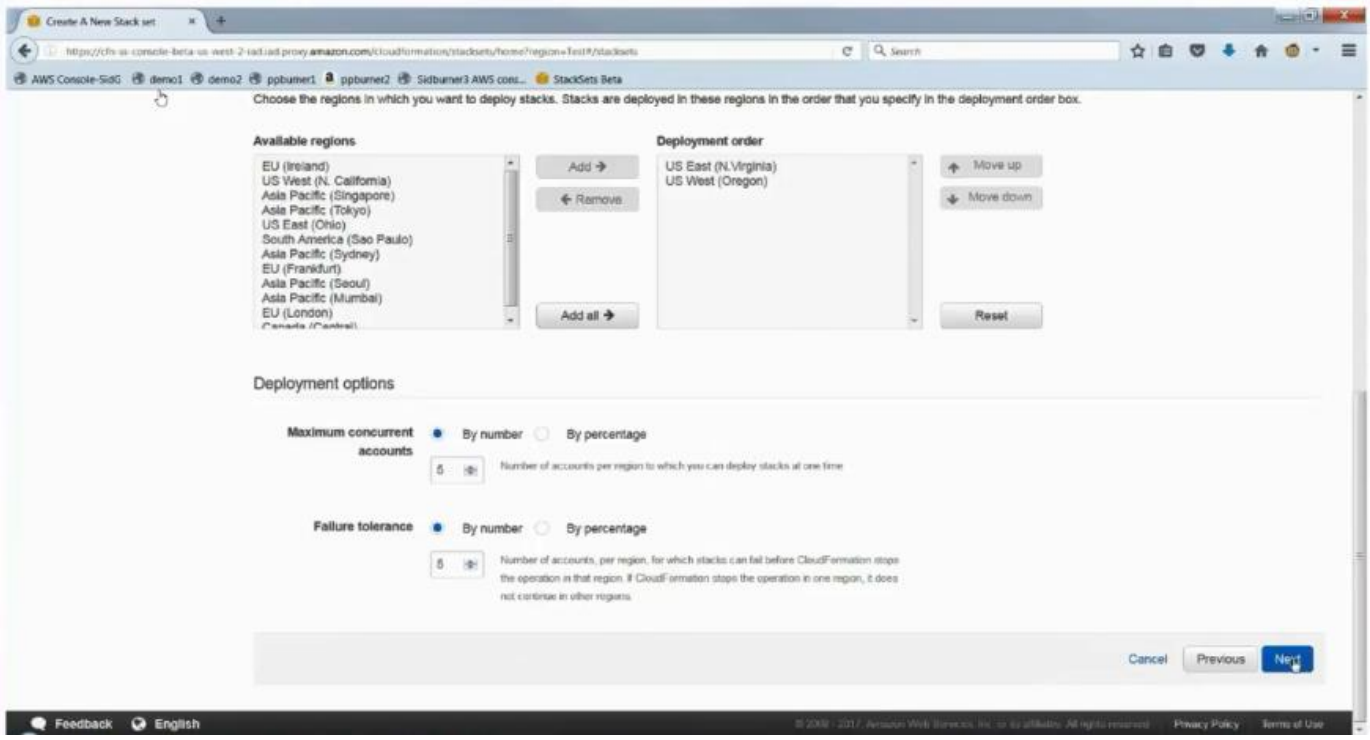

Create A New Stack set
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Services
Resource Groups
CloudFormation
Stack sets
Create stack set
Create stack set
Select template
Specify details
Set deployment options
Tags
Review
Select template
A stack set is a container 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-ena...
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.
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).
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.

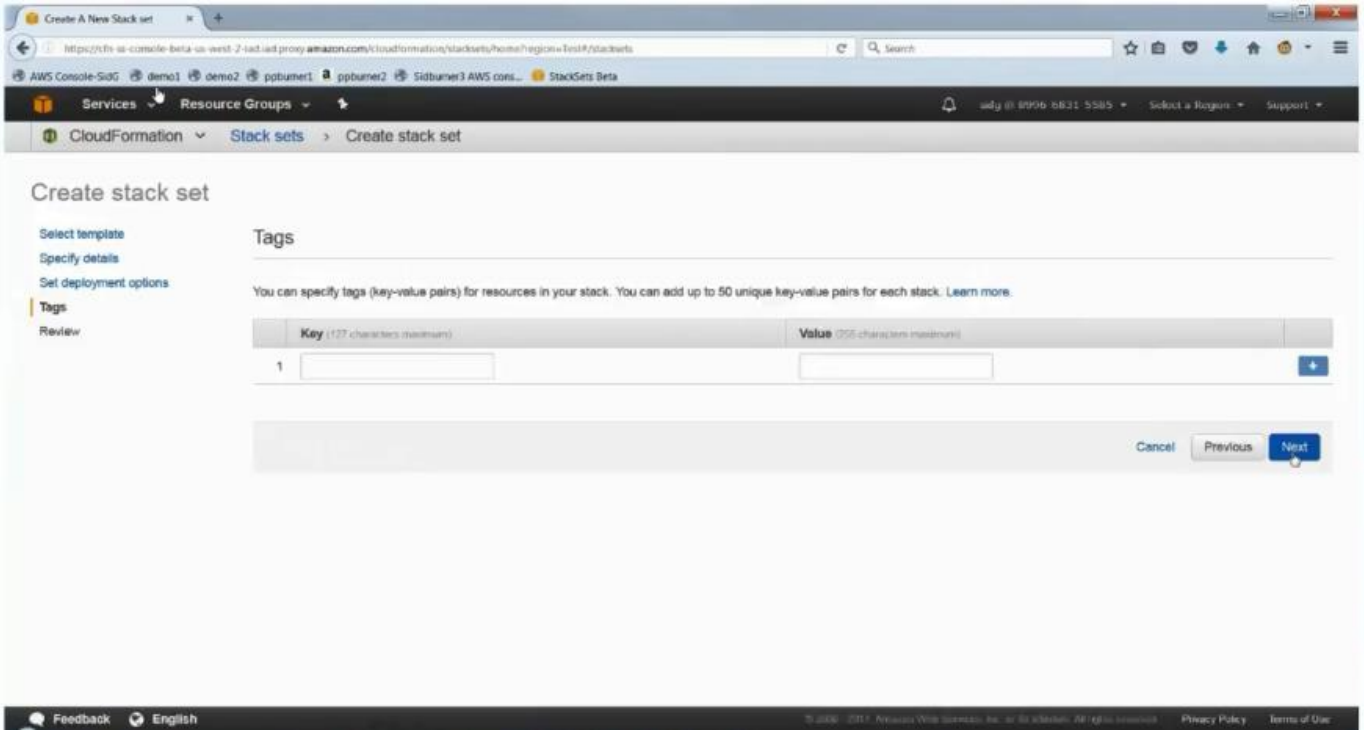

Create A New Stack set
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Set deployment options
Tags
Review
A stack set is a container for a set of AWS CloudFormation stacks across multiple AWS accounts and regions. Choose the template that describes the stack sets 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-ena...
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.
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).
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.
Cancel
Next

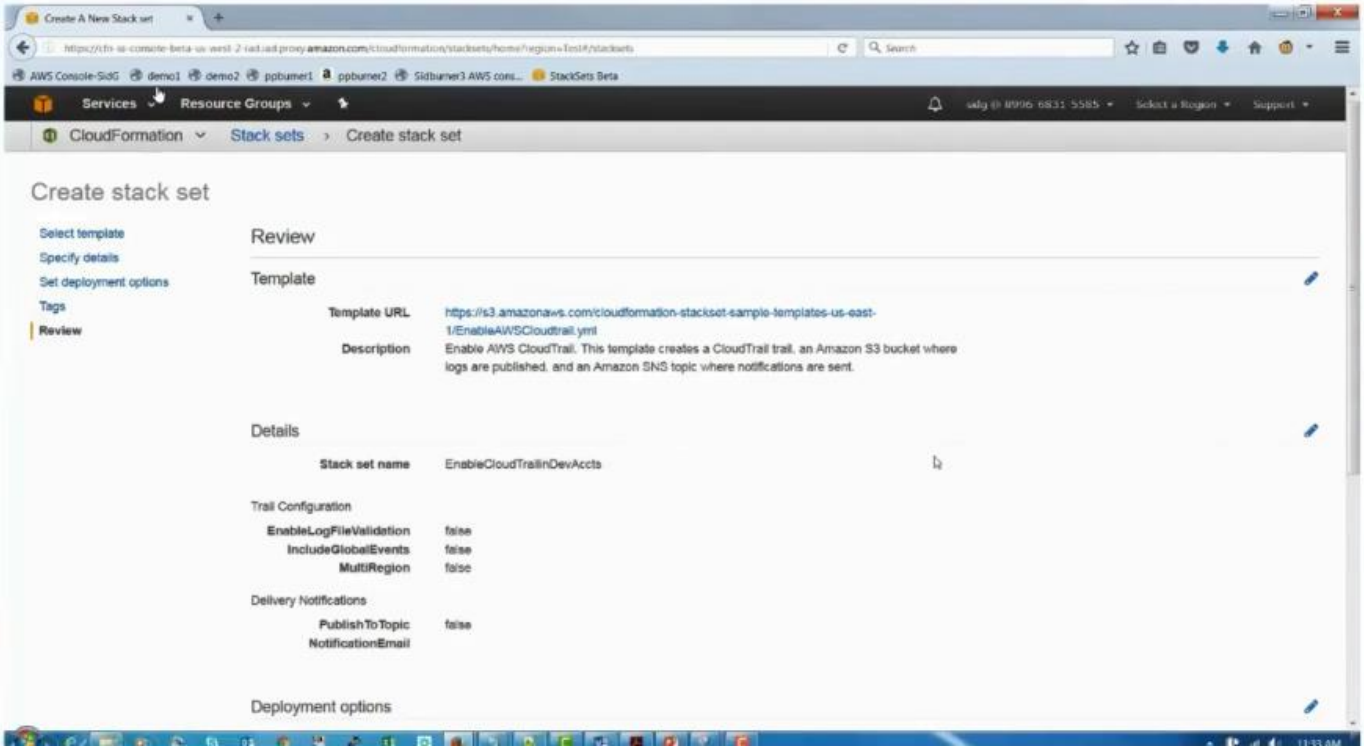

Create A New Stack set
Set deployment options
Tags
Review
Stack set name
EnableCloudTrailinDevAccts
Must begin with an alphabetical character and contain only letters, numbers, and hyphens.
Parameters
Trail Configuration
Enable log file validation
false
Indicates whether CloudTrail validates the integrity of log files.
Include global service events
false
Indicates whether the trail is publishing events from global services, such as IAM, to the log files.
Is this a multi-region trail
false
Indicates whether the CloudTrail trail is created in the region in which you create the stack (false) or in all regions (true).
Delivery Notifications
Send notifications to SNS
false
Indicates whether notifications are published to SNS.
Notification Email (optional)
Email address for notifications (for new topics).
Cancel
Previous
Next
Feedback
English
Privacy Policy
Terms of Use

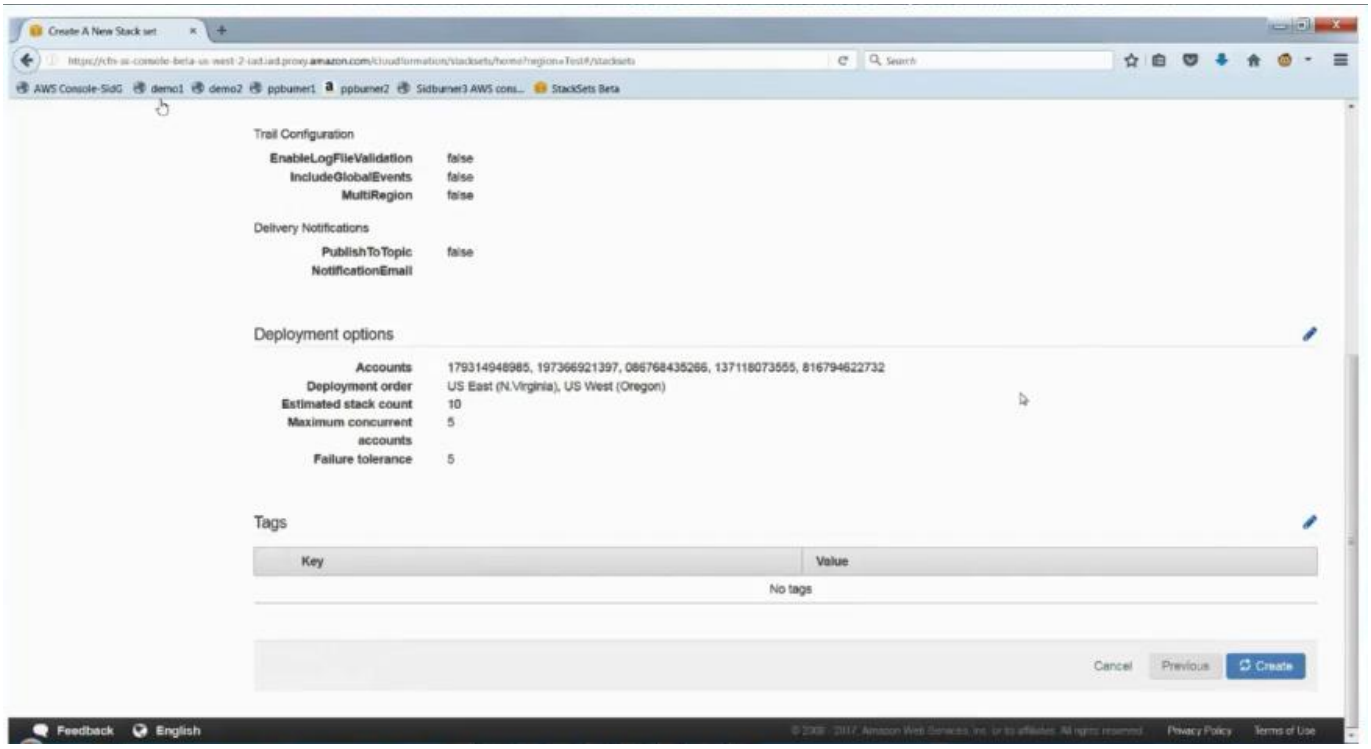

Services
Resource Groups
CloudFormation
Stack sets
Create stack set
Create stack set
Select template
Specify details
Set deployment options
Tags
Review
Set deployment options
Configure options to deploy stacks to your accounts and regions. Stacks are deployed to regions in sequence, and across accounts 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.
Specify accounts
Identify accounts or organizational units in which you want to create stacks.
Deploy stacks in accounts
Enter valid account numbers
Deploy stacks in AWS organizational units. Learn more
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
US East (N.Virginia)
US West (Oregon)
EU (Ireland)
US West (N. California)
Add
Remove
Deployment order
Move up
Move down

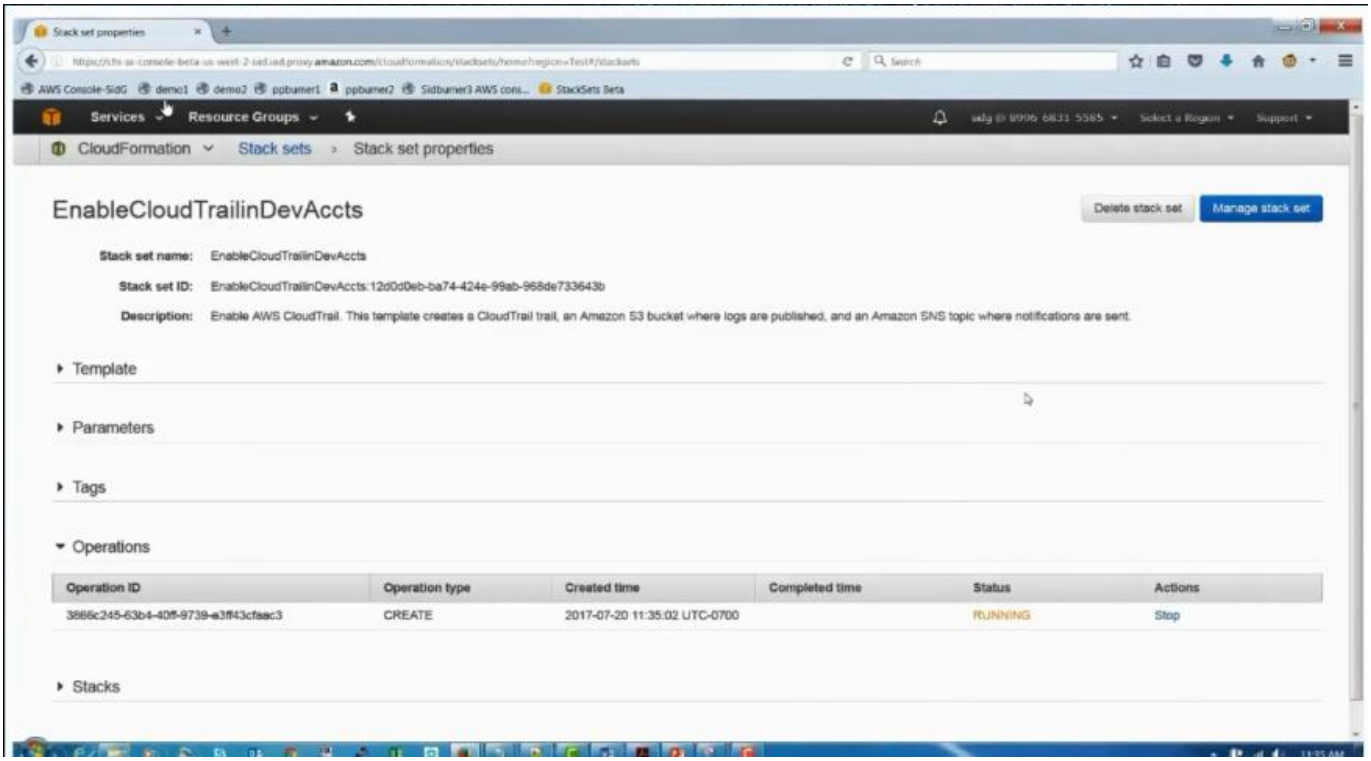

Create A New Stack set
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Deploy stacks in accounts
Deploy stacks in AWS organizational units. Learn more
ou-rrt9-m2rzuhip5
Upload a list of valid accounts in which stacks can be deployed
Specify regions
Choose the regions 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)
Add
Remove
Add all
Deployment order
US East (N.Virginia)
US West (Oregon)
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.

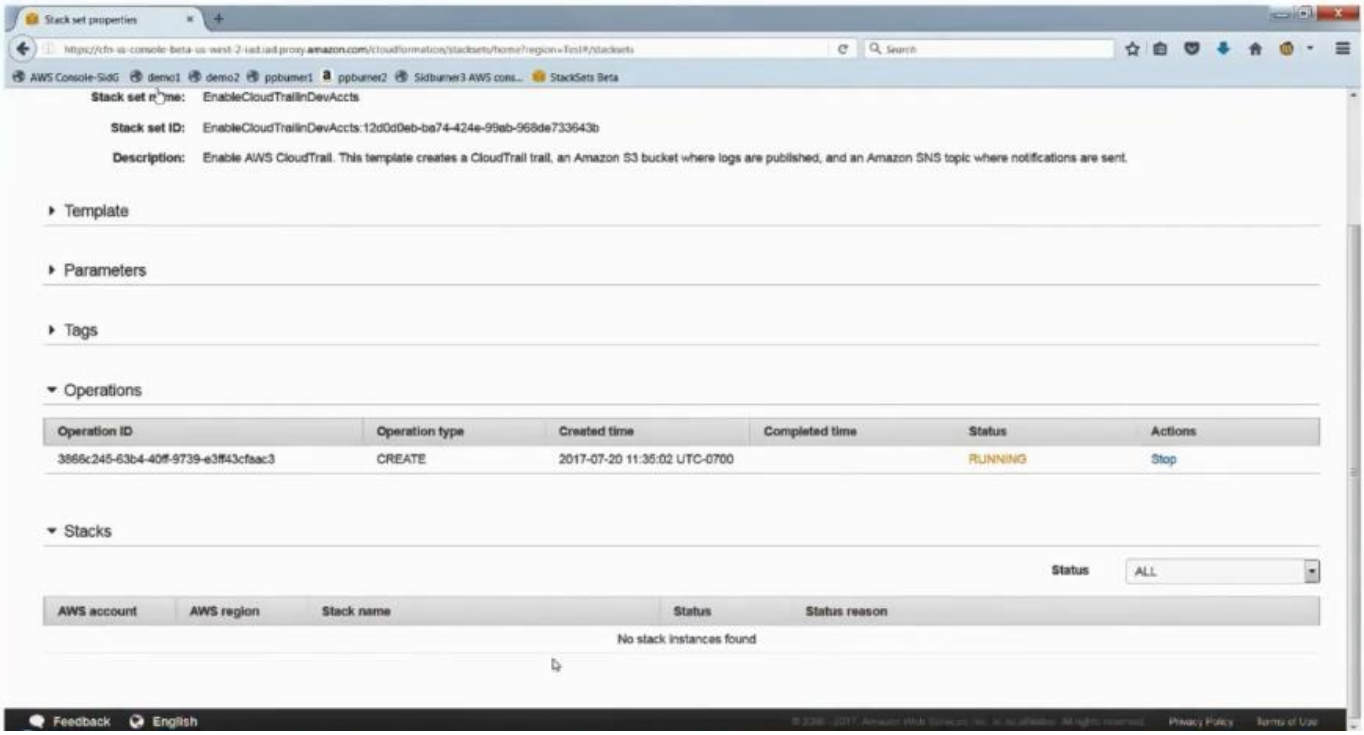

Create A New Stack set
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Choose the regions in which you want to deploy stacks. Stacks are deployed in these regions in the order that you specify in the deployment order box.
Available regions
EU (Ireland)
US West (N. 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)
Add
Remove
Add all
Deployment order
US East (N.Virginia)
US West (Oregon)
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
0
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
Feedback
English
Privacy Policy
Terms of Use

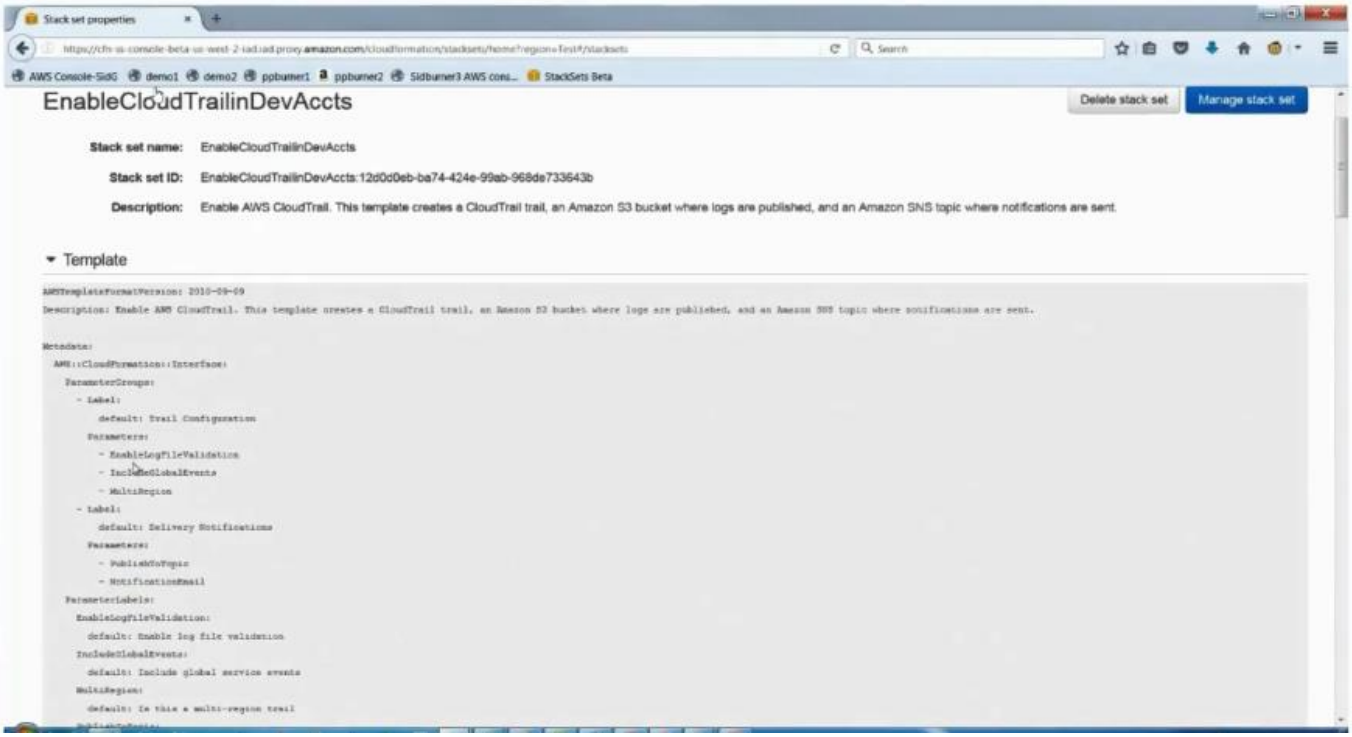

Create A New Stack set
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Services
Resource Groups
CloudFormation
Stack sets
Create stack set
Create stack set
Select template
Specify details
Set deployment options
Tags
Review
Tags
You can specify tags (key-value pairs) for resources in your stack. You can add up to 50 unique key-value pairs for each stack. Learn more.
Key
Value
1
Cancel
Previous
Next
Feedback
English
Privacy Policy
Terms of Use

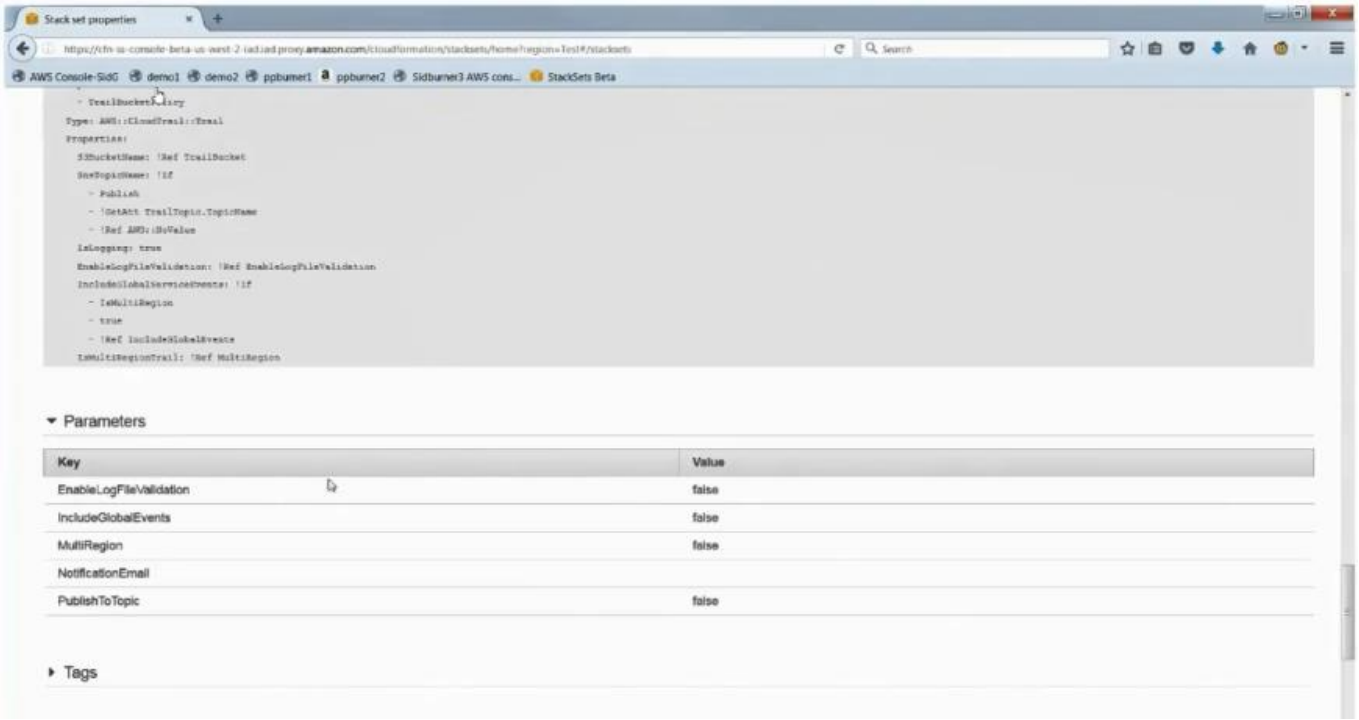

Create A New Stack set
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Services
Resource Groups
CloudFormation
Stack sets
Create stack set
Create stack set
Select template
Specify details
Set deployment options
Tags
Review
Review
Template
Template URL
https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/EnableAWSCloudtrail.yml
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.
Details
Stack set name
EnableCloudTrailinDevAccts
Trail Configuration
EnableLogFileValidation
false
IncludeGlobalEvents
false
MultiRegion
false
Delivery Notifications
PublishToTopic
false
NotificationEmail
Deployment options

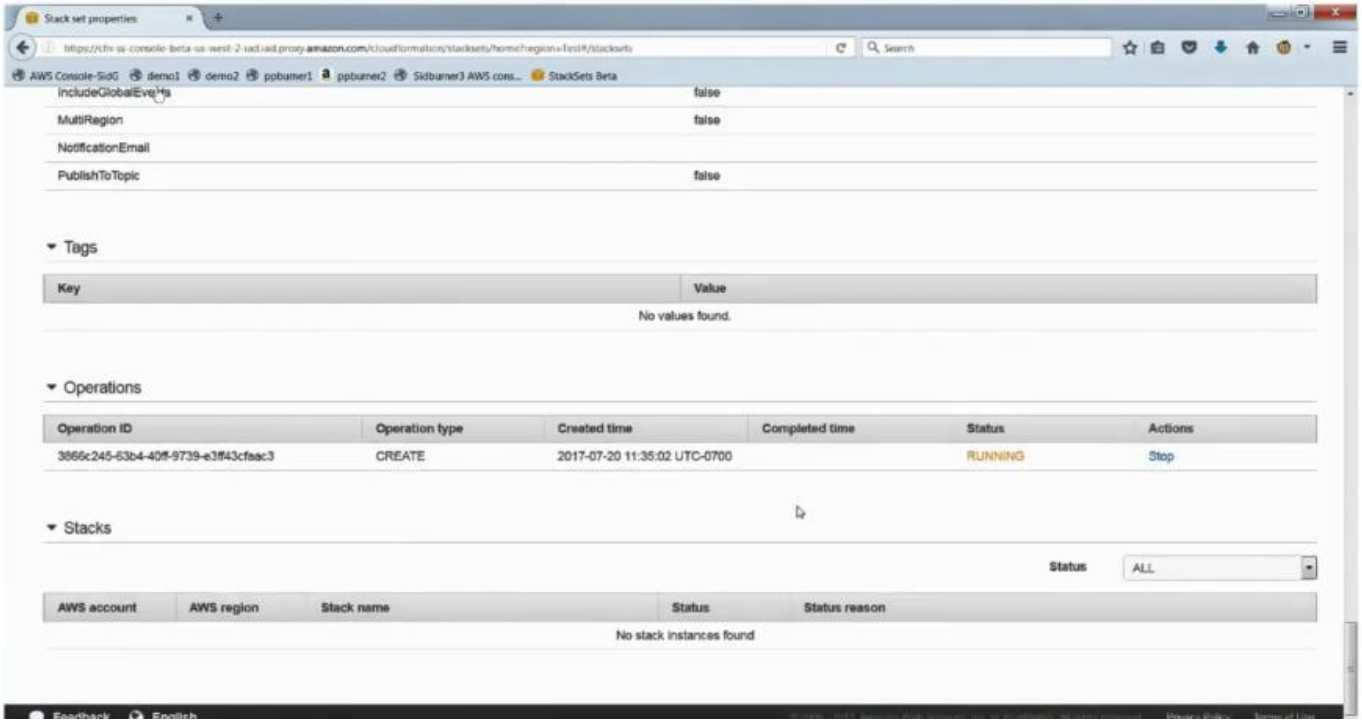

Create A New Stack set
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Trail Configuration
EnableLogFileValidation false
IncludeGlobalEvents false
MultiRegion false
Delivery Notifications
PublishToTopic false
NotificationEmail
Deployment options
Accounts 179314946985, 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
Privacy Policy
Terms of Use

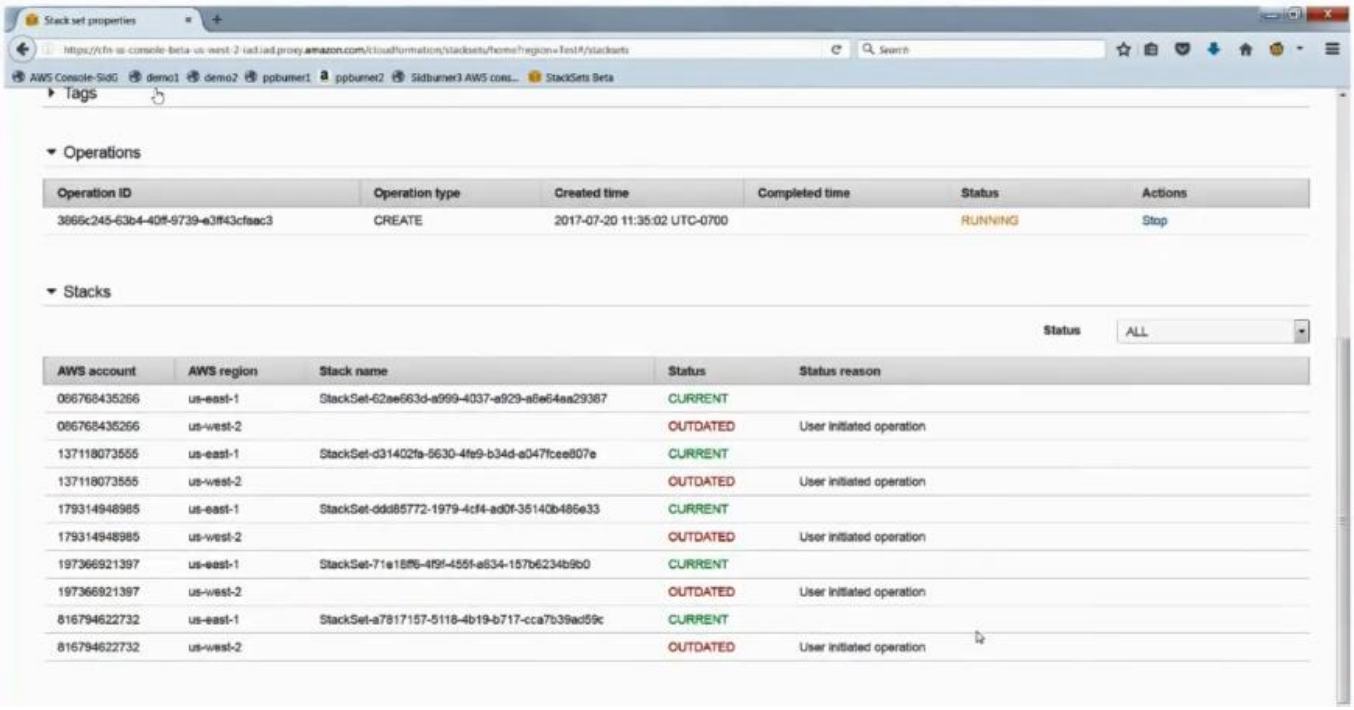

Stack set properties
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Services
Resource Groups
Select a Region
Support
CloudFormation
Stack sets
Stack set properties
EnableCloudTrailinDevAccts
Delete stack set
Manage stack set
Stack set name: EnableCloudTrailinDevAccts
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
RUNNING
Stop
Stacks

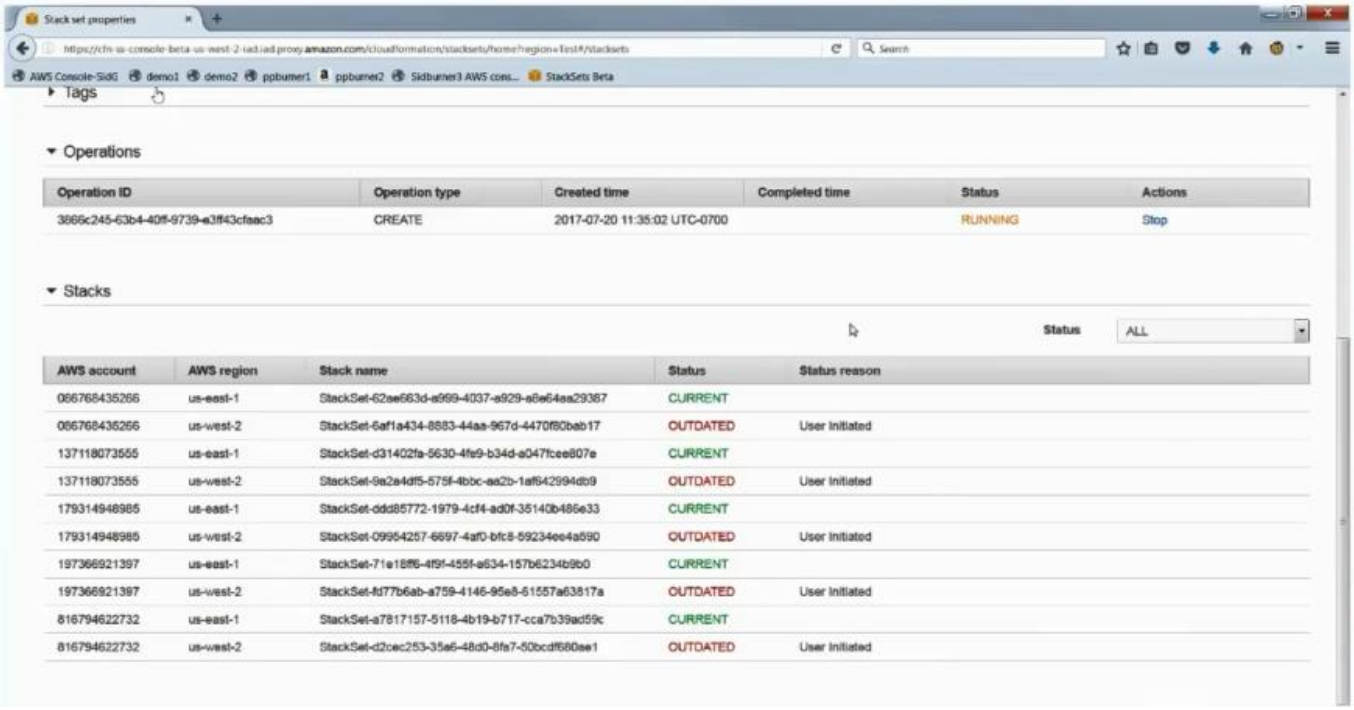

Stack set properties
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Stack set name: EnableCloudTrailinDevAccts
Stack set ID: EnableCloudTrailinDevAccts:12d0d0eb-ba74-424e-99ab-968de733643b
Description: Enable AWS CloudTrail. This template creates a CloudTrail trail, 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
RUNNING
Stop
Stacks
Status
ALL
AWS account
AWS region
Stack name
Status
Status reason
No stack instances found
Feedback
English
Privacy Policy
Terms of Use

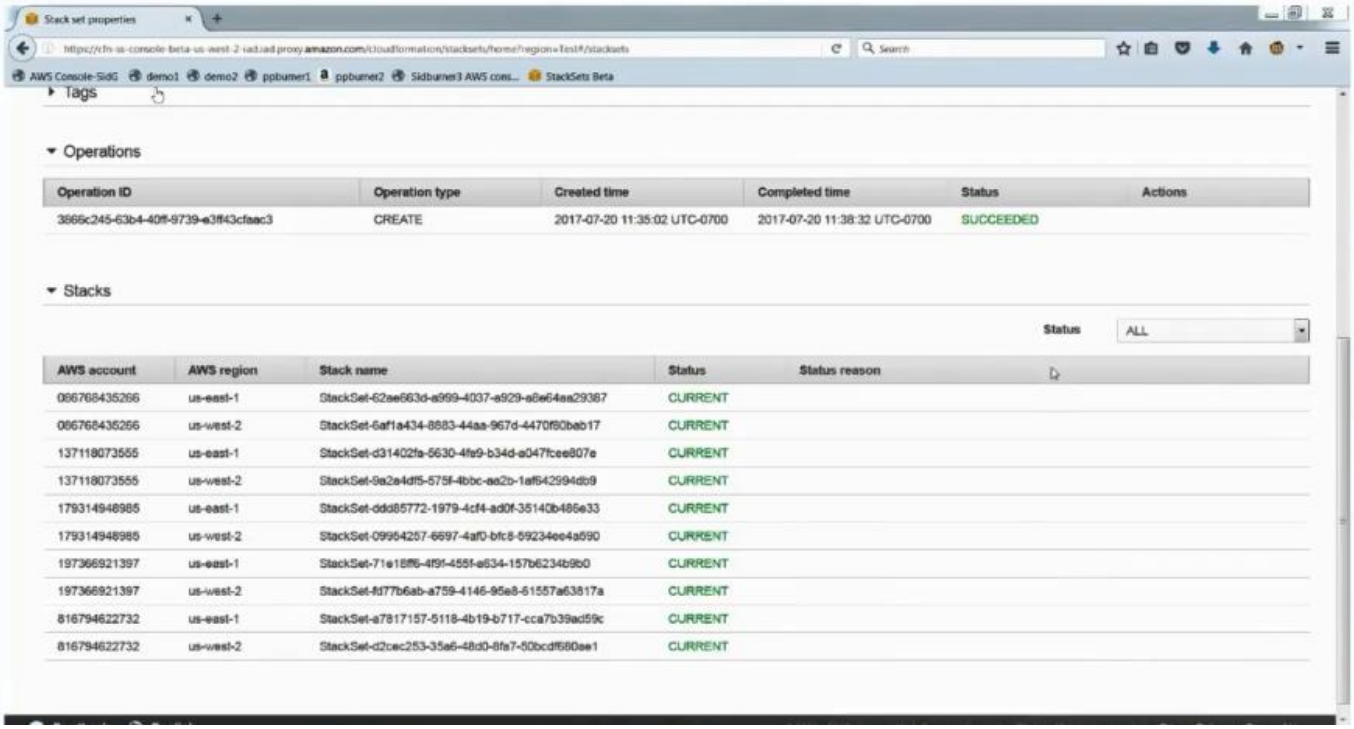

Stack set properties
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
EnableCloudTrailinDevAccts
Delete stack set
Manage stack set
Stack set name: EnableCloudTrailinDevAccts
Stack set ID: EnableCloudTrailinDevAccts:12d0d0eb-ba74-424e-99ab-968de733643b
Description: 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
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:
- Label:
default: Trail Configuration
Parameters:
- EnableLogFileValidation
- IncludeGlobalEvents
- MultiRegion
- Label:
default: Delivery Notifications
Parameters:
- PublishSnsTopic
- NotificationEmail
ParameterLabels:
EnableLogFileValidation:
default: Enable log file validation
IncludeGlobalEvents:
default: Include global service events
MultiRegion:
default: Is this a multi-region trail

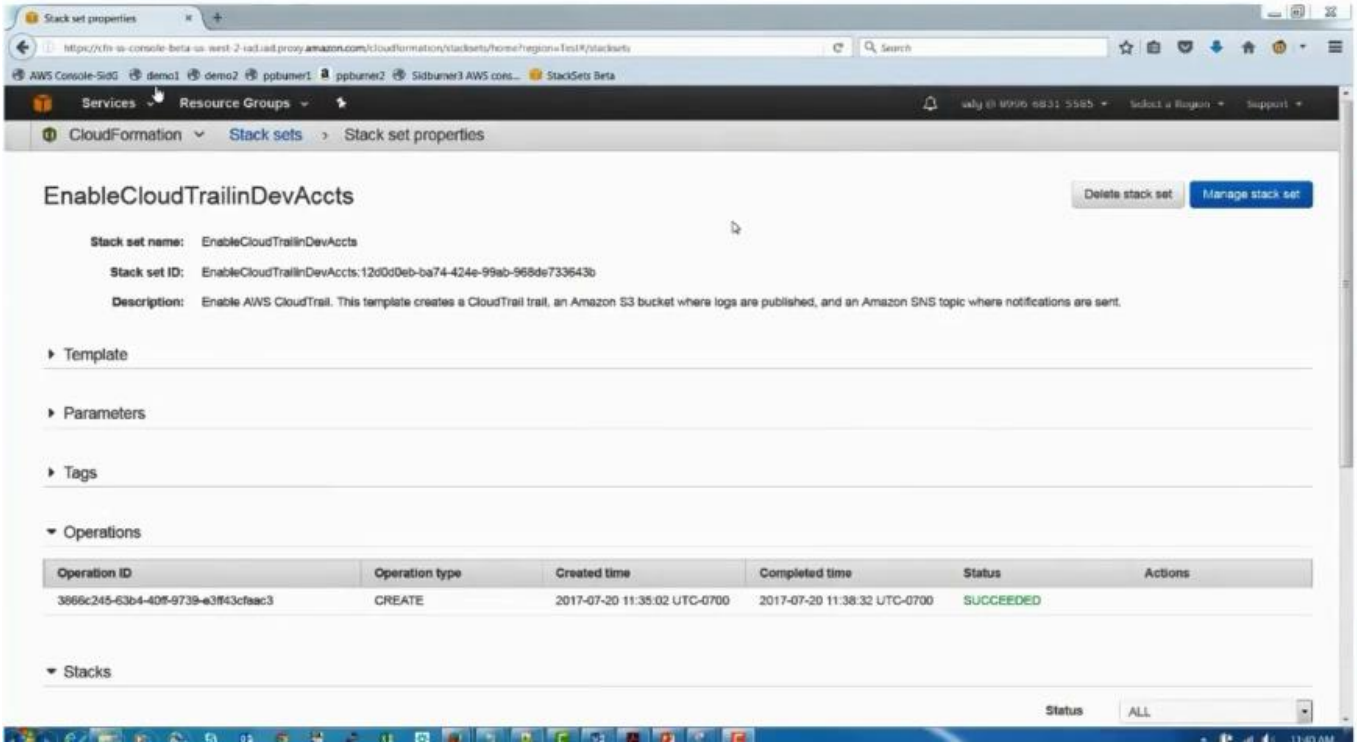

Stack set properties
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Parameters
Key
Value
EnableLogFileValidation
false
IncludeGlobalEvents
false
MultiRegion
false
NotificationEmail
PublishToTopic
false
Tags

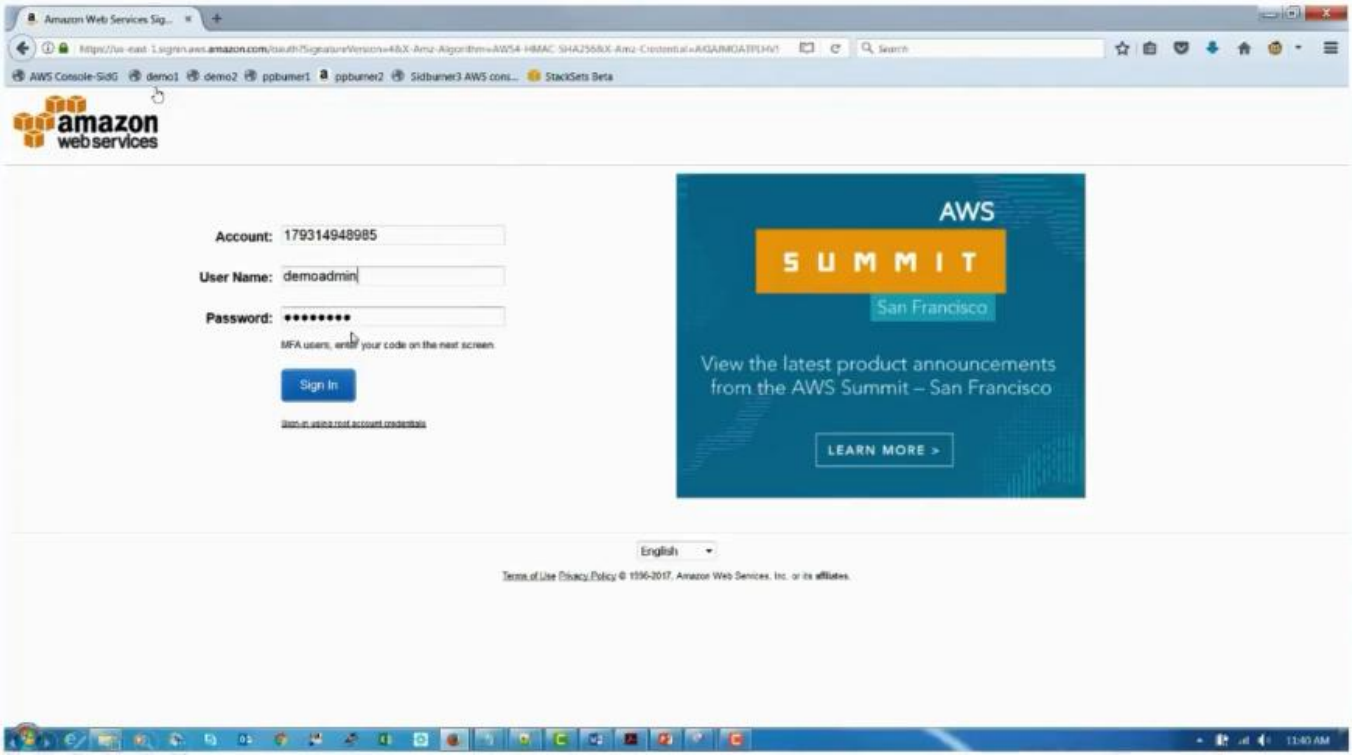

Stack set properties
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
MultiRegion
false
NotificationEmail
PublishToTopic
false
Tags
Key
Value
No values found.
Operations
Operation ID
Operation type
Created time
Completed time
Status
Actions
3866c245-63b4-40ff-9739-e3ff43cfaac3
CREATE
2017-07-20 11:35:02 UTC-0700
RUNNING
Stop
Stacks
Status
ALL
AWS account
AWS region
Stack name
Status
Status reason
No stack instances found
Feedback
English

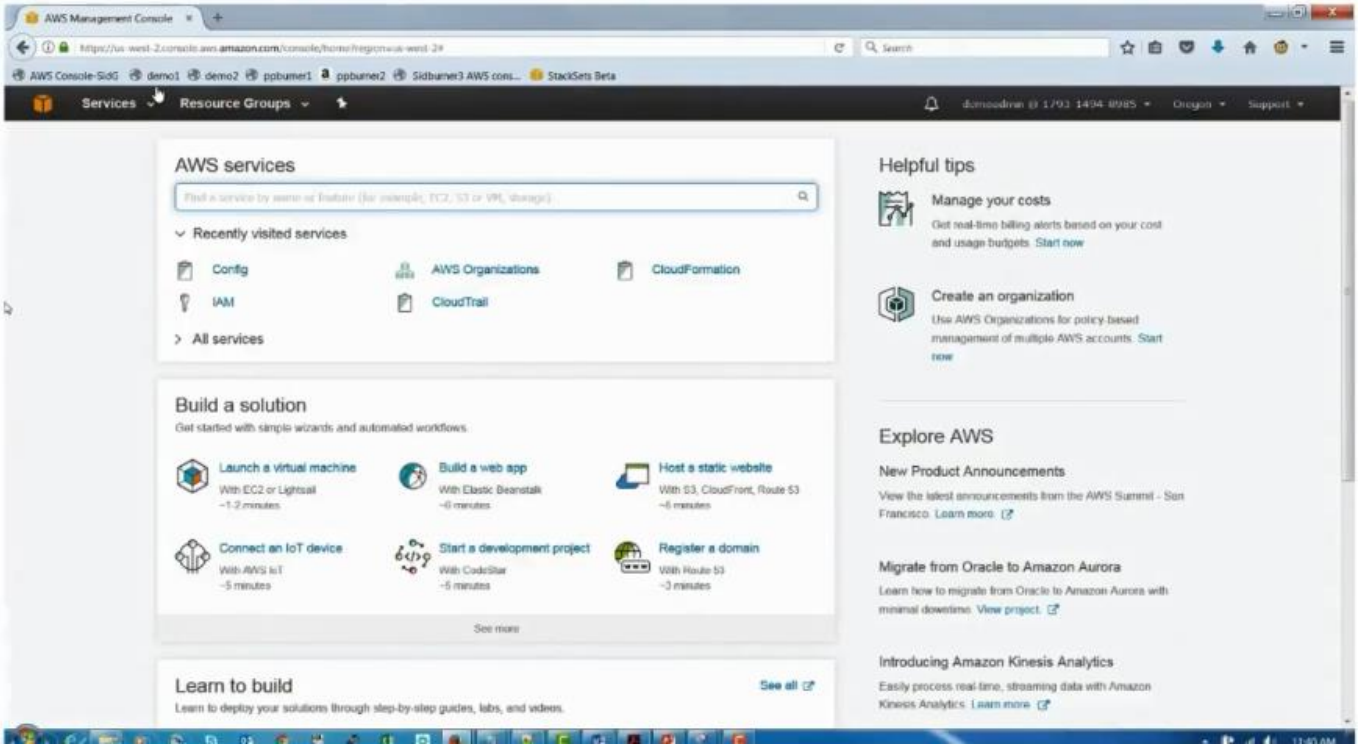

Stack set properties
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Tags
Operations
Operation ID
Operation type
Created time
Completed time
Status
Actions
3866c245-63b4-40ff-9739-e3ff43cfaac3
CREATE
2017-07-20 11:35:02 UTC-0700
RUNNING
Stop
Stacks
Status
ALL
AWS account
AWS region
Stack name
Status
Status reason
066768435266 us-east-1 StackSet-62ae663d-a999-4037-a929-a6e64ea29367 CURRENT
066768435266 us-west-2 OUTDATED User initiated operation
137118073555 us-east-1 StackSet-d31402fa-5630-4fe9-b34d-a047fcee807e CURRENT
137118073555 us-west-2 OUTDATED User initiated operation
179314948985 us-east-1 StackSet-ddd85772-1979-4cf4-ad0f-35140b486e33 CURRENT
179314948985 us-west-2 OUTDATED User initiated operation
197366921397 us-east-1 StackSet-71e18ff6-4f9f-455f-a634-157b6234b9b0 CURRENT
197366921397 us-west-2 OUTDATED User initiated operation
816794622732 us-east-1 StackSet-a7817157-5118-4b19-b717-cca7b39ad59c CURRENT
816794622732 us-west-2 OUTDATED User initiated operation

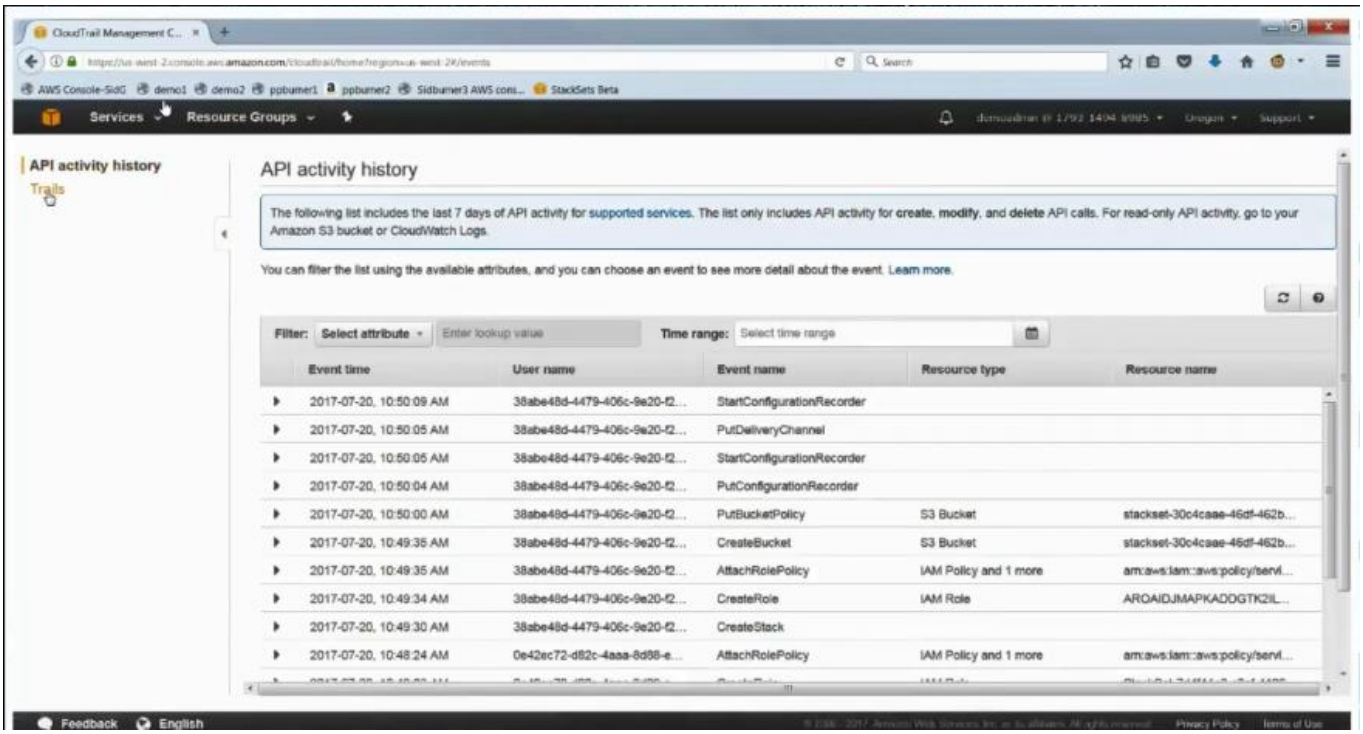

Stack set properties
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Tags
Operations
Operation ID
Operation type
Created time
Completed time
Status
Actions
3866c245-63b4-40ff-9739-e3ff43cfaac3
CREATE
2017-07-20 11:35:02 UTC-0700
RUNNING
Stop
Stacks
Status
ALL
AWS account
AWS region
Stack name
Status
Status reason
066768435266 us-east-1 StackSet-62ae663d-a999-4037-a929-a6e64ea29367 CURRENT
066768435266 us-west-2 StackSet-6af1a434-8883-44aa-967d-4470f60bab17 OUTDATED User initiated
137118073555 us-east-1 StackSet-d31402fa-5630-4fe9-b34d-a047fcee807e CURRENT
137118073555 us-west-2 StackSet-9a2a4df5-575f-4bbc-aa2b-1af642994db9 OUTDATED User initiated
179314948985 us-east-1 StackSet-ddd85772-1979-4cf4-ad0f-35140b486e33 CURRENT
179314948985 us-west-2 StackSet-09954257-6697-4af0-bfc8-59234ee4a590 OUTDATED User initiated
197366921397 us-east-1 StackSet-71e18ff6-4f9f-455f-a634-157b6234b9b0 CURRENT
197366921397 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-d2cec253-35a6-48d0-8fa7-50bcdf680ae1 OUTDATED User initiated

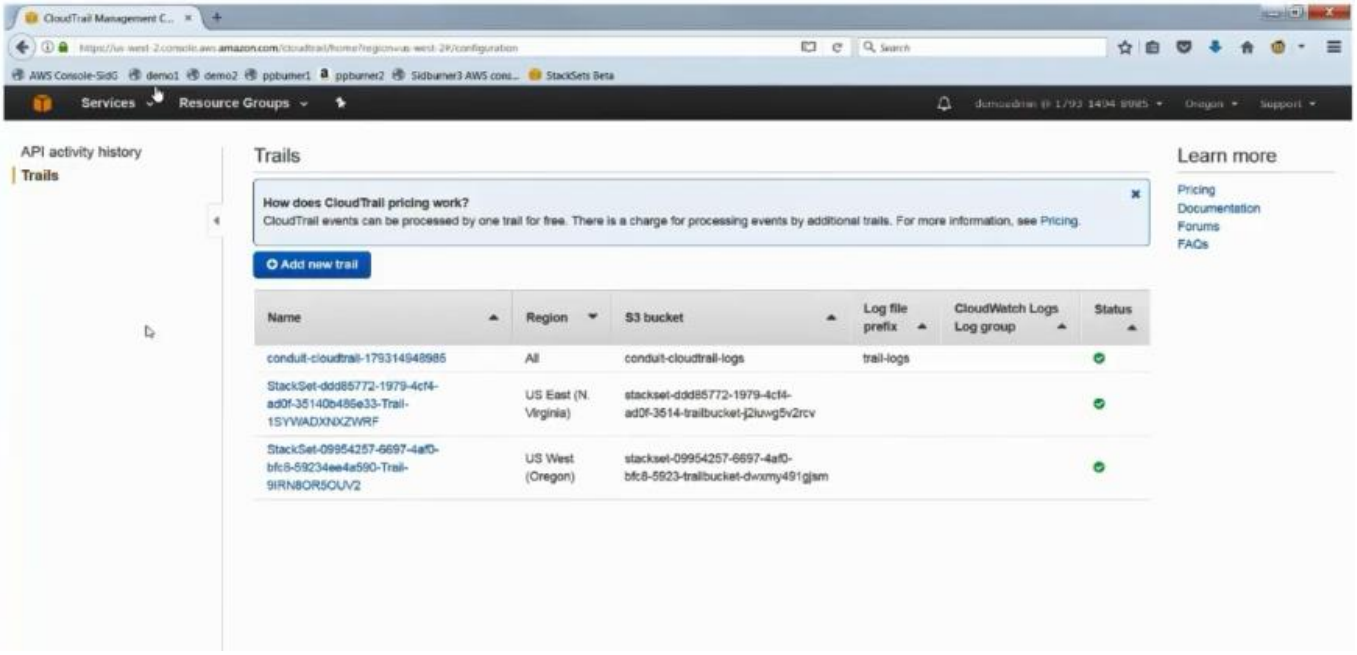

Stack set properties
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Tags
Operations
Operation ID
Operation type
Created time
Completed time
Status
Actions
3866c245-63b4-40ff-9739-e3ff43cfaac3
CREATE
2017-07-20 11:35:02 UTC-0700
2017-07-20 11:38:32 UTC-0700
SUCCEEDED
Stacks
Status
ALL
AWS account
AWS region
Stack name
Status
Status reason
066768435266 us-east-1 StackSet-62ae663d-a999-4037-a929-a8e64aa29387 CURRENT
066768435266 us-west-2 StackSet-6af1a434-8883-44aa-967d-4470f80bab17 CURRENT
137118073555 us-east-1 StackSet-d31402fa-5630-4fe9-b34d-a047fcee807e CURRENT
137118073555 us-west-2 StackSet-9a2a4df5-575f-4bbc-aa2b-1af642994db9 CURRENT
179314948985 us-east-1 StackSet-ddd85772-1979-4cf4-ad0f-35140b486e33 CURRENT
179314948985 us-west-2 StackSet-09954257-6697-4af0-bfc8-59234ee4a590 CURRENT
197366921397 us-east-1 StackSet-71e18ff6-4f9f-455f-a634-157b6234b9b0 CURRENT
197366921397 us-west-2 StackSet-fd77b6ab-a759-4146-95a8-51557a63817a CURRENT
816794622732 us-east-1 StackSet-a7817157-5118-4b19-b717-cca7b39ad59c CURRENT
816794622732 us-west-2 StackSet-d2cac253-35a6-48d0-8fa7-50bcdf68bae1 CURRENT

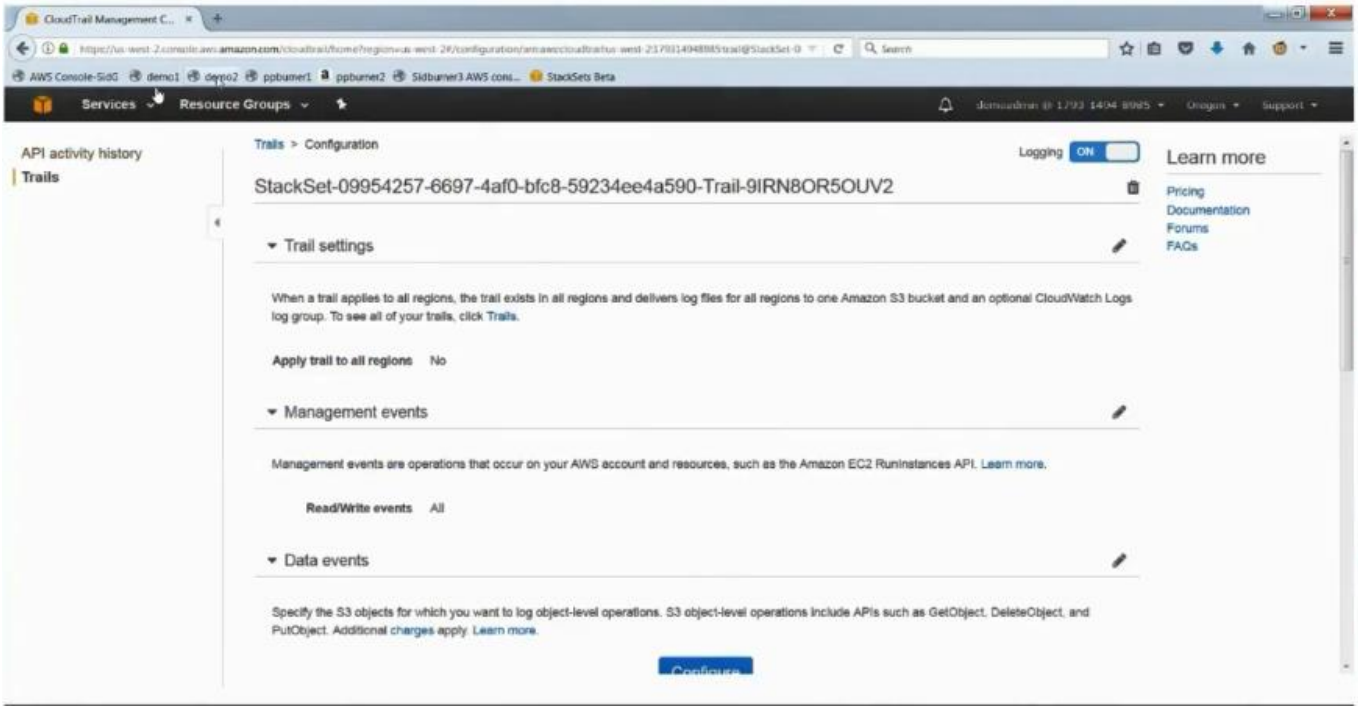

Stack set properties
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Services
Resource Groups
CloudFormation
Stack sets
Stack set properties
EnableCloudTrailinDevAccts
Delete stack set
Manage stack set
Stack set name: EnableCloudTrailinDevAccts
Stack set ID: EnableCloudTrailinDevAccts:12d0d0eb-ba74-424e-99ab-968de733643b
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

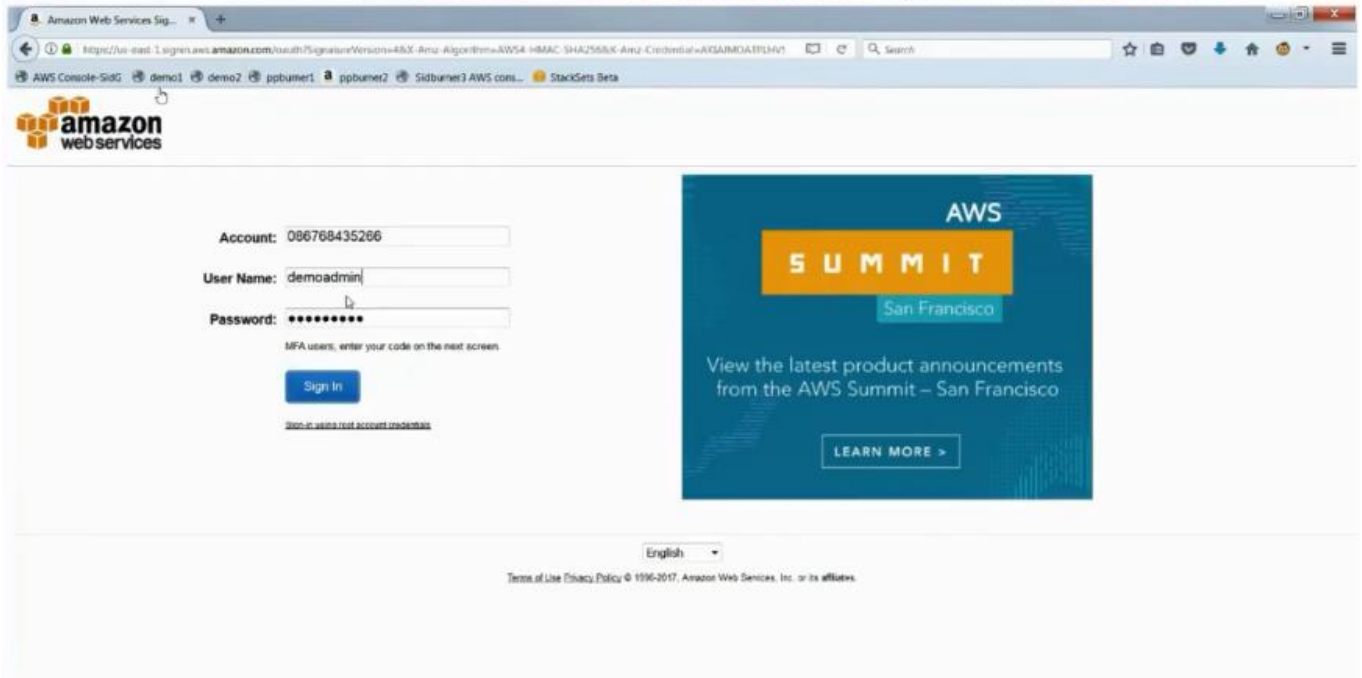

Amazon Web Services Sig...
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
amazon web services
Account: 179314948985
User Name: demoadmin
Password:
MFA users, enter your code on the next screen.
Sign In
Sign in using root account credentials
AWS
SUMMIT
San Francisco
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.

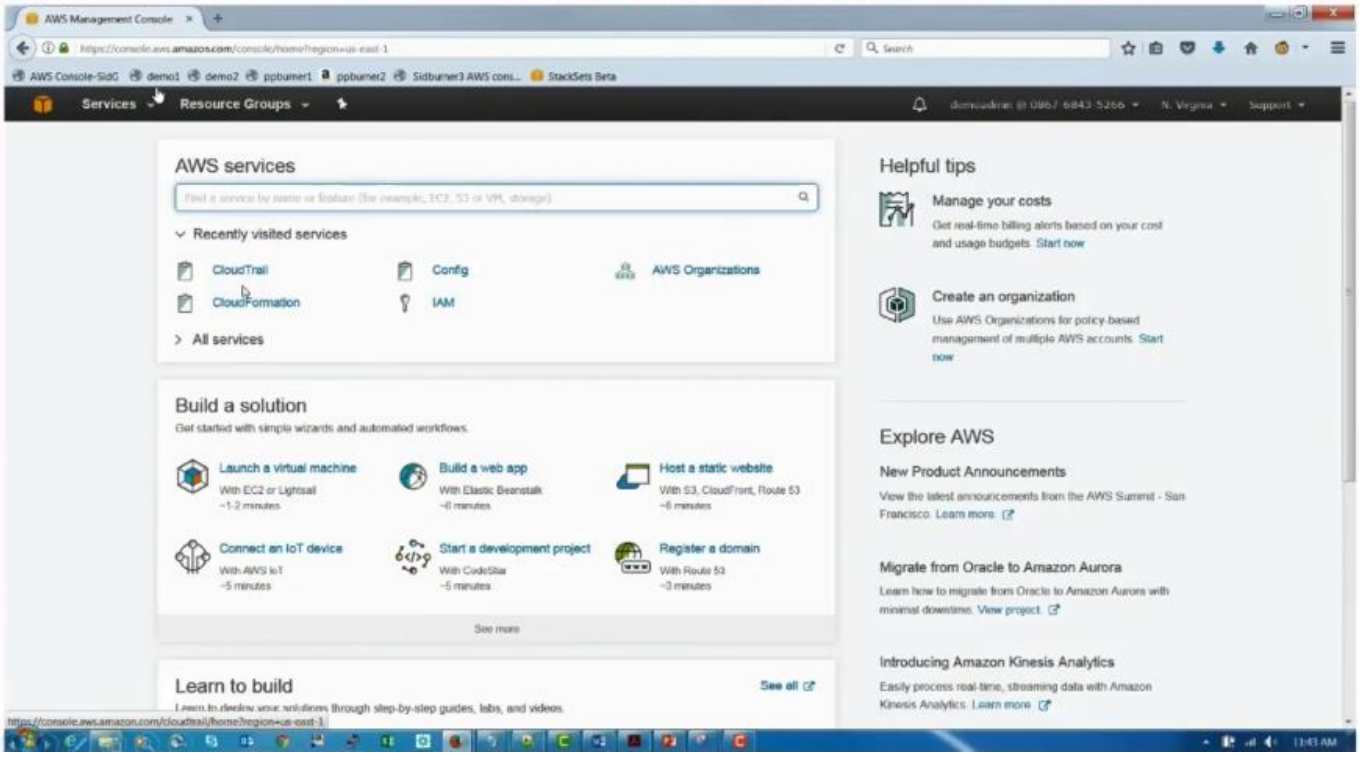

AWS Management Console
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Services
Resource Groups
Oregon
Support
AWS services
Recently visited services
Config
AWS Organizations
CloudFormation
IAM
CloudTrail
All services
Build a solution
Get started with simple wizards and automated workflows.
Launch a virtual machine
With EC2 or Lightsail
Build a web app
With Elastic Beanstalk
Host a static website
With S3, CloudFront, Route 53
Connect an IoT device
With AWS IoT
Start a development project
With CodeStar
Register a domain
With Route 53
See more
Learn to build
See all
Learn to deploy your solutions through step-by-step guides, labs, and videos.
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.

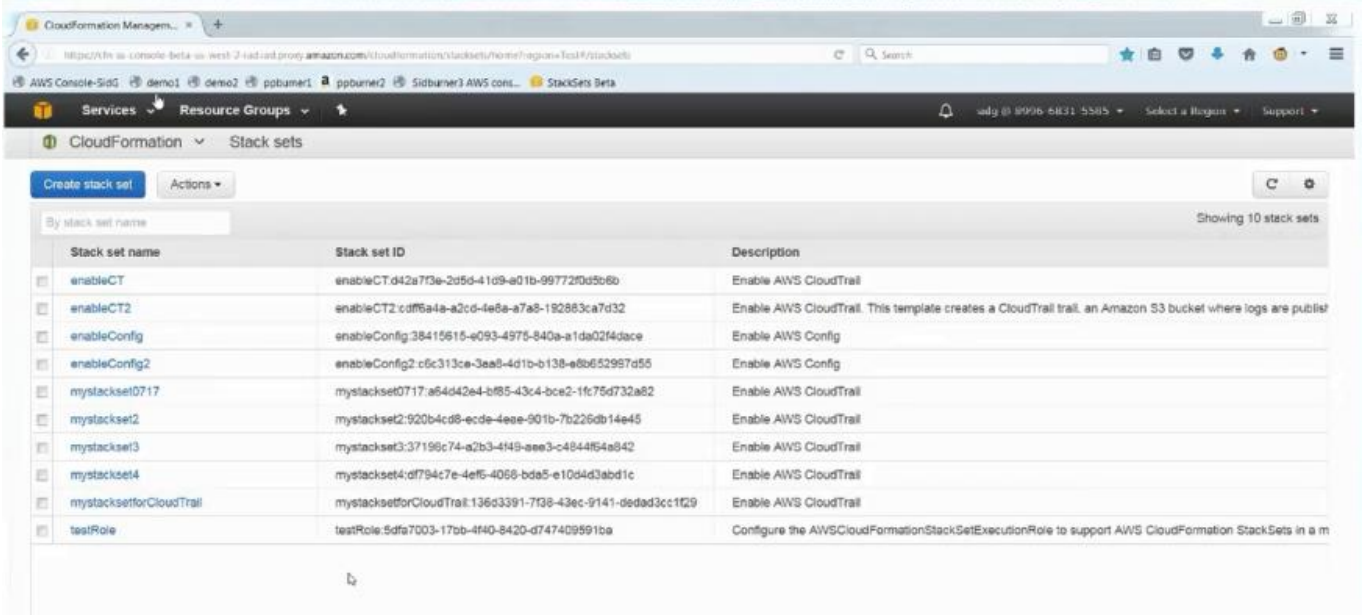

CloudTrail Management C...
Services
Resource Groups
API activity history
Trails
API activity history
The following list includes the last 7 days of API activity for supported services. The list only includes API activity for create, modify, and delete API calls. For read-only API activity, go to your 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-30c4caae-46df-462b...
2017-07-20, 10:49:35 AM 38abe48d-4479-406c-9e20-f2... CreateBucket S3 Bucket stackset-30c4caae-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/servi...
2017-07-20, 10:49:34 AM 38abe48d-4479-406c-9e20-f2... CreateRole IAM Role AROAIDJMAPKADOGTK2IL...
2017-07-20, 10:49:30 AM 38abe48d-4479-406c-9e20-f2... CreateStack
2017-07-20, 10:48:24 AM 0e42ec72-d82c-4aaa-8d86-e... AttachRolePolicy IAM Policy and 1 more arn:aws:iam::aws:policy/servi...
Feedback
English


CloudTrail Management C...
Services
Resource Groups
API activity history
Trails
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
StackSet-ddd85772-1979-4cf4-ad0f-35140b486e33-Trail-1SYWADXNXZWRF US East (N. Virginia) stackset-ddd85772-1979-4cf4-ad0f-3514-trailbucket-j2luwg5v2rcv
StackSet-09954257-6697-4af0-bfc8-59234ee4a590-Trail-9IRN8OR5OUV2 US West (Oregon) stackset-09954257-6697-4af0-bfc8-5923-trailbucket-dwxmy491gjsm
Learn more
Pricing
Documentation
Forums
FAQs

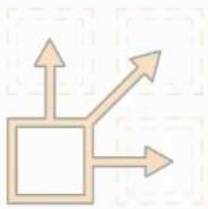

CloudTrail Management C...
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
Services
Resource Groups
Oregon
Support
API activity history
Trails
Trails > Configuration
Logging
ON
StackSet-09954257-6697-4af0-bfc8-59234ee4a590-Trail-9IRN8OR5OUV2
Learn more
Pricing
Documentation
Forums
FAQs
Trail settings
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
Management events are operations that occur on your AWS account and resources, such as the Amazon EC2 RunInstances API. Learn more.
Read/Write events All
Data events
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.


Amazon Web Services Sig...
AWS Console-SidG
demo1
demo2
ppburner1
ppburner2
Sidburner3 AWS cons...
StackSets Beta
amazon web services
Account: 086768435266
User Name: demoadmin
Password: ••••••••••
MFA users, enter your code on the next screen.
Sign In
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.




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

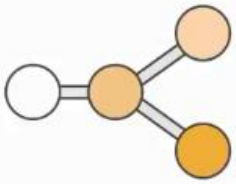
Keep track of what you are validating

- 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

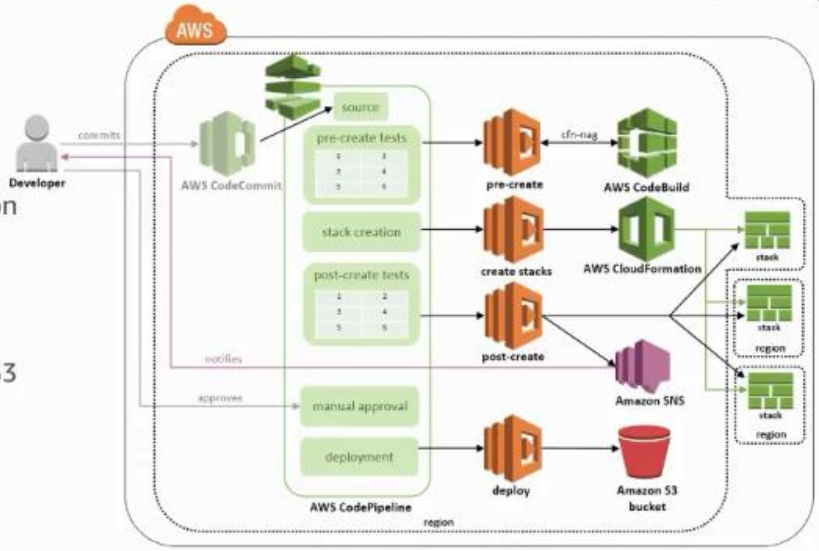
http://docs.aws.amazon.com/solutions/latest/aws-cloudformation-validation-pipeline/

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

# REFERENCE IMPLEMENTATION

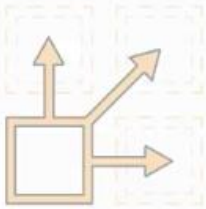
Triggered by a commit on your repo

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



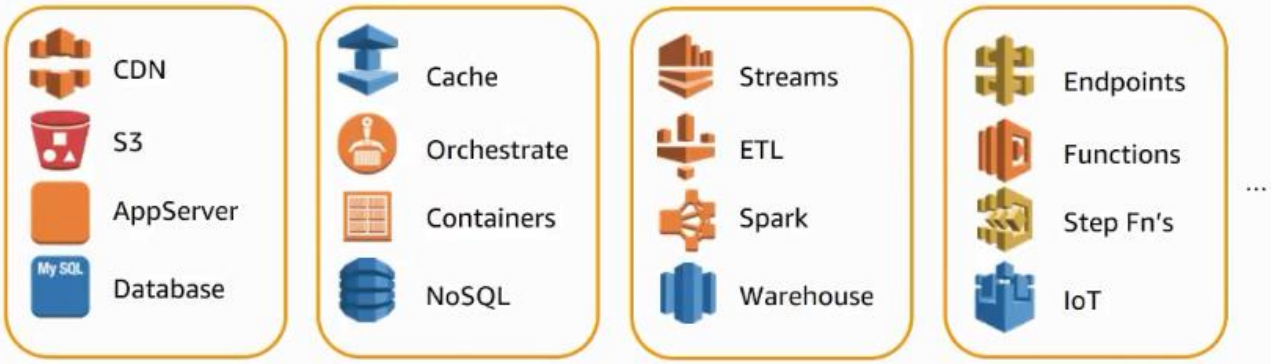
System Admins:
Provisioning at scale

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)

Serverless
Transactional
(Lambda, APIs, IoT)

aws re:Invent
© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
aws

## 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

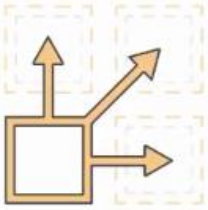
SERVERLESS

APEX
serverless architecture

SPARTA

| | |
|---|---|
| Apex | Lambada |
| Up | Lambdoku |
| Chalice | Shep |
| ClaudiaJS | Sparta |
| DEEP | Turtle |
| Gordon | Zappa |
| Gestalt | Lambdify |
| Iron Functions | Squeezer |
| 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 | http://amzn.to/2y8KbjV |
| Stack Policies | http://amzn.to/28JmWkT |
| Deletion Policy | http://amzn.to/1qtkrkq |
| IAM Policy | http://amzn.to/2e345Tp |
| AWS Config | https://aws.amazon.com/config/ |
| Rollback Triggers | http://amzn.to/2zDV3GR |
| StackSets | http://amzn.to/2zK0nGi |
| Validation Pipeline | http://amzn.to/2hrz8rM |

DEV317

**Deep Dive on AWS CloudFormation**

# Remember to complete your evaluations! ☺

Anil Kumar – aanik@amazon.com @anilsdomain
Luis Colon – licolon@amazon.com @luiscolon1

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