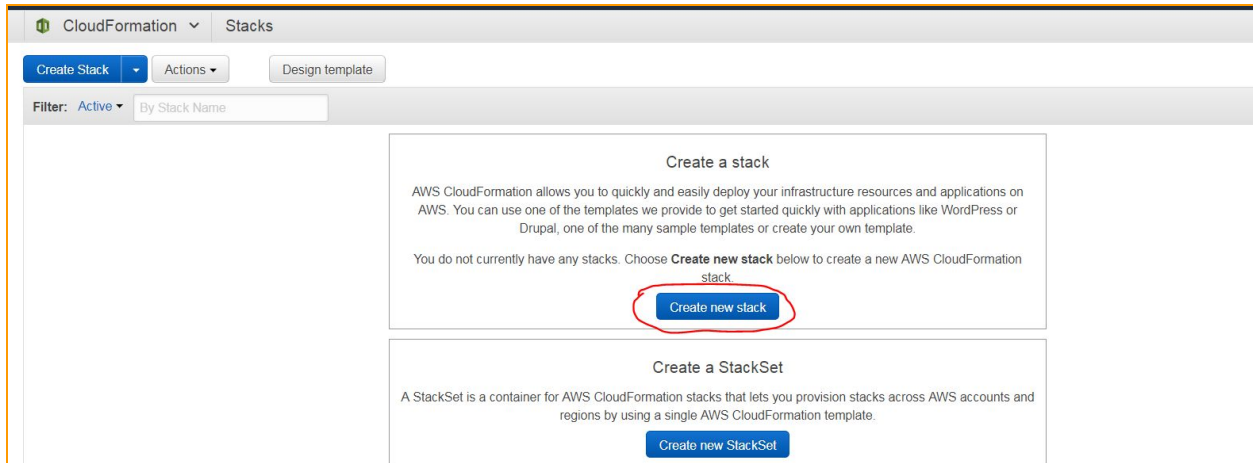
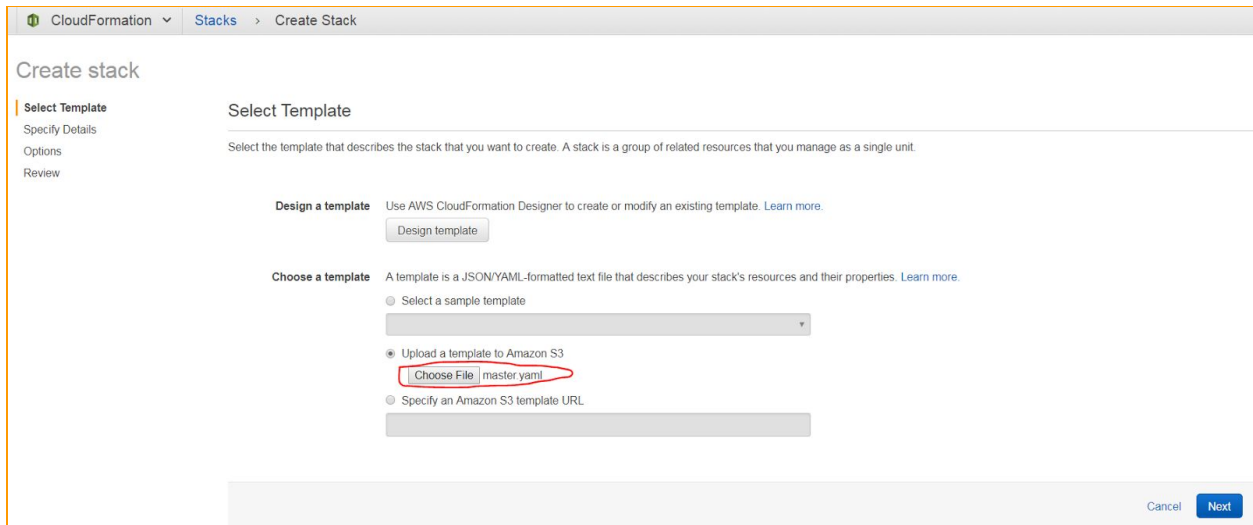


This cloudformation Templates will create a one S3 bucket with buckets policy and two IAM roles, the first roles will have an full access for S3 buckets and the 2nd roles will have read-write on the S3 . I made nested stack. We can write ansible playbook similar to this tasks :)

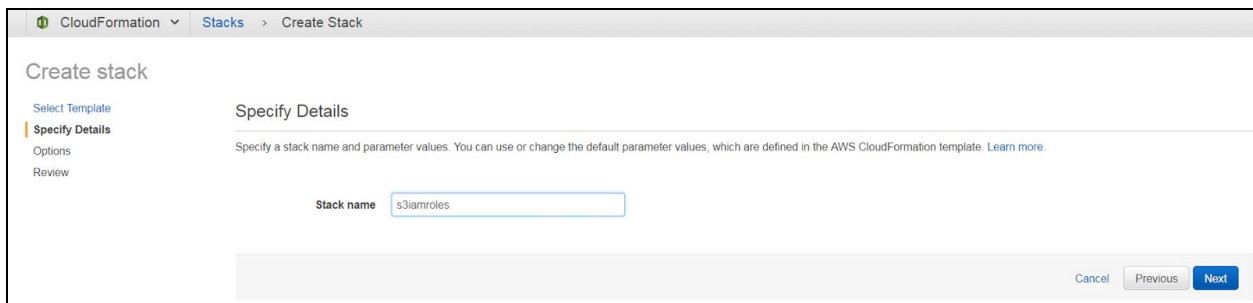
Click on “Create new stack”



Select the master.yml files



provide the name of the stacks



Just click “Next”

The screenshot shows the 'Create Stack' page in the AWS CloudFormation console, specifically the 'Options' tab. The left sidebar has 'Options' selected. The main area is titled 'Options' and contains sections for 'Tags', 'Permissions', and 'Advanced'. The 'Tags' section has a table with columns 'Key' and 'Value'. The 'Permissions' section has a dropdown for 'IAM Role' and a text input for 'Enter role arn'. The 'Advanced' section is collapsed. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons.

CloudFormation > Stacks > Create Stack

Create stack

Select Template
Specify Details
Options
Review

Options

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 (127 characters maximum)	Value (255 characters maximum)
1	

+

Permissions

You can choose an IAM role that CloudFormation uses to create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses the permissions defined in your account. [Learn more.](#)

IAM Role Choose a role (optional)
Enter role arn

Advanced

You can set additional options for your stack, like notification options and a stack policy. [Learn more.](#)

Cancel Previous **Next**

Check the “acknowledgement” and Click “Create”

The screenshot shows the 'Create Stack' page in the AWS CloudFormation console, specifically the 'Review' tab. The left sidebar has 'Review' selected. The main area is titled 'Review' and contains sections for 'Template', 'Details', 'Options', 'Advanced', 'Capabilities', and 'Quick Create Stack'. The 'Capabilities' section has a blue box with a warning icon and text about IAM resources. At the bottom right are 'Cancel', 'Previous', and 'Create' buttons.

CloudFormation > Stacks > Create Stack

Create stack

Select Template
Specify Details
Options
Review

Review

Template

Template URL: <https://s3-us-east-1.amazonaws.com/stack-templates-us-east-1/20160908/01-v1-stack.yaml>
Description: This template deploys S3 buckets and roles with policies for CSS Test csa-assignment Last Modified: 22nd September 2016 Author: Samal Dimdung <dmdung@gmail.com>
Estimate cost: Cost

Details

Stack name: s3iamroles

Options

Tags

No tags provided

Advanced

Notification: Disabled
Termination Protection: Disabled
Timeout: none
Rollback on failure: Yes

Capabilities

The following resource(s) require capabilities: [AWS::CloudFormation::Stack]
This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more.](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Quick Create Stack (Create stacks similar to this one, with most details auto-populated)

Cancel Previous **Create**

You will see below screen

The screenshot shows the 'Stacks' page in the AWS CloudFormation console. At the top, there are buttons for 'Create Stack', 'Actions', and 'Design template'. Below is a table of stacks with columns 'Stack Name', 'Created Time', 'Status', and 'Description'. The 'Events' tab is selected, showing a log of events for the 's3iamroles' stack.

CloudFormation > Stacks

Create Stack Actions Design template

Filter: Active By Stack Name

Stack Name	Created Time	Status	Description
s3iamroles-s3test-11YAX13Z...	2018-01-08 13:39:47 UTC-0500	CREATE_IN_PROGRE...	Stack for creating S3Bucket for CSS Test S3
s3iamroles-rolestest-15ELUJR...	2018-01-08 13:39:47 UTC-0500	CREATE_IN_PROGRE...	Stack for IAM Roles with for to access S3
s3iamroles	2018-01-08 13:39:42 UTC-0500	CREATE_IN_PROGRE...	This template deploys S3 buckets and roles with policies for CSS Test csa-assignment Last Modified: 22nd September 2016 Author: Samal Dimdung <dmdung@gmail.com>

Overview Outputs Resources **Events** Template Parameters Tags Stack Policy Change Sets

2018-01-08	Status	Type	Logical ID	Status Reason
13:39:48 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	s3test	Resource creation Initiated
13:39:47 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	rolestest	Resource creation Initiated
13:39:46 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	rolestest	
13:39:46 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	s3test	
13:39:42 UTC-0500	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	s3iamroles	User Initiated

Once its complete you will see below screen (three cloudformation stack for master, s3 buckets and roles.

Stack Name	Created Time	Status	Description
s3iamroles-s3test-11YAX13Z...	2018-01-08 13:39:47 UTC-0500	CREATE_COMPLETE	Stack for creating S3Bucket for CSS Test S3
s3iamroles-rolestest-15ELU3R...	2018-01-08 13:39:47 UTC-0500	CREATE_COMPLETE	Stack for IAM Roles with for to access S3
s3iamroles	2018-01-08 13:39:42 UTC-0500	CREATE_COMPLETE	This template deploys S3 buckets and roles with policies for CSS Test css-assignment Last Modified: 22nd September 2016 Author: Samal Dindung <dmdung@gmail.com>

The S3 bucket created with policy what you have defined in cf templates

Amazon S3 > css-assignment-11100

Overview Properties Permissions Management

Access Control List Bucket Policy CORS configuration

Bucket policy editor ARN: arn:aws:s3::css-assignment-11100

Type to add a new policy or edit an existing policy in the text area below.

```

1 {
2   "Version": "2008-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "AWS": "arn:aws:iam::309815942436:role/TaskRole2"
8       },
9       "Action": [
10        "s3:ListBucket",
11        "s3:GetBucketLocation",
12        "s3:ListBucketMultipartUploads",
13        "s3:ListBucketVersions"
14      ],
15       "Resource": "arn:aws:s3::css-assignment-11100",
16       "Condition": {
17        "StringEquals": {
18          "aws:sourceVpc": "vpc-e1a2b3c4d"
19        }
20      }
21    },
22    {
23       "Effect": "Allow",
24       "Principal": {
25         "AWS": "arn:aws:iam::309815942436:role/TaskRole1"
26       },
27       "Action": [

```

Roles Section, you can see two roles TaskRole1 and TaskRoles2

Role name	Description	Trusted entities
TaskRole1		AWS service: ec2
TaskRole2		AWS service: ec2

TaskRoles1 have full access of S3 buckets

Search IAM

Dashboard Groups Users Roles Policies Identity providers Account settings Credential report Encryption keys

Roles > TaskRole1

Summary

Role ARN: arn:aws:iam::309815942436:role/TaskRole1

Role description: /

Instance Profile ARNs: /

Path: /

Creation time: 2018-01-08 13:39 EST

Permissions Trust relationships Access Advisor Revoke sessions

Attach policy Attached policies: 1

Policy name	Policy type
AmazonS3FullAccess	AWS managed policy

Add inline policy

TaskRoles2 have a list/read/write access on S3 bucket

Search IAM

Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report

Encryption keys

Roles > TaskRoles2

Summary

Role ARN: arn:aws:iam::304555555555:role/TaskRoles2

Role description

Instance Profile ARNs

Path: /

Creation time: 2018-01-08 13:39 EST

Permissions Trust relationships Access Advisor Revoke sessions

Attach policy Attached policies: 2

Policy name	Policy type
vpflowlogs	Managed policy
IAMPolicyName-2	Inline policy

Policy summary Edit policy Simulate policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Action": "s3:ListBucket",  
6       "Resource": "arn:aws:s3:::csss-assignment-11100",  
7       "Effect": "Allow"  
8     },  
9     {  
10      "Action": "s3:PutObject",  
11      "Resource": "arn:aws:s3:::csss-assignment-11100/*",  
12      "Effect": "Allow"  
13    },  
14    {  
15      "Action": "s3:GetObject",  
16      "Resource": "arn:aws:s3:::csss-assignment-11100/*",  
17      "Effect": "Allow"  
18    }  
19  ]  
20 }
```