



# Automate with Cloud Formation



tiubenedict@gmail.com

NextWorkDevOpsProject2										
		Delete		Update		Stack actions ▾				
Stack info		Events		Resources		Template				
Outputs		Parameters		Change sets		Git sync				
<strong>Resources (10)</strong>										
<input type="text"/> Search resources										
Logical ID	Physical ID	Type	Status	Module						
CodeArtifactDomain00domainnextwork00xNjxb	arn:aws:codeartifact:ap-southeast-2:050752641312:domain/nextwork	AWS::CodeArtifact::Domain	<span>CREATE_COMPLETE</span>	-						
CodeArtifactRepository00repositorynextworkmavencentralstore00Jgrfu	arn:aws:codeartifact:ap-southeast-2:050752641312:repository/nextwork/maven-central-store	AWS::CodeArtifact::Repository	<span>CREATE_COMPLETE</span>	-						
CodeArtifactRepository00repositorynextworknextworkpackages00aqihP	arn:aws:codeartifact:ap-southeast-2:050752641312:repository/nextwork/nextwork-packages	AWS::CodeArtifact::Repository	<span>CREATE_COMPLETE</span>	-						
CodeBuildProject	nextwork-web-build	AWS::CodeBuild::Project	<span>CREATE_COMPLETE</span>	-						
CodeCommitRepository	a1ed7f31-db0e-4c2d-beba-29e4dd943773	AWS::CodeCommit::Repository	<span>CREATE_COMPLETE</span>	-						
IAMManagedPolicy00policycodeartifactnextworkconsumerpolicy008elvs	arn:aws:iam::050752641312:policy/codeartifact-nextwork-consumer-policy	AWS::IAM::ManagedPolicy	<span>CREATE_COMPLETE</span>	-						
IAMManagedPolicy00policeserviceroleCodeBuildbasePolicynextworkwebbuild	arn:aws:iam::050752641312:policy/service-role/CodeBuildBasePolicy	AWS::IAM::ManagedPolicy	<span>CREATE_COMPLETE</span>	-						



tiubenedict@gmail.com

NextWork Student

[NextWork.org](http://NextWork.org)

---

# Introducing today's project!

## What is AWS CloudFormation?

AWS CloudFormation is an Infrastructure as Code service, allowing you to create aws resource stacks programmatically from a text file template. It helps developers recreate stacks reliably.

## How I used CloudFormation in this project

We used CloudFormation's IaC generator to scan our account for resources that it can base the configs from, and we used CloudFormation to re-launch those same resources using a template.

## One thing I didn't expect in this project was...

I didn't think that a CloudFormation template would be a bit difficult to set-up without using the IaC generator.

## This project took me...

This project took me 60-90 minutes.



tiubenedict@gmail.com

NextWork Student

[NextWork.org](http://NextWork.org)

# CloudFormation templates

A CloudFormation template is a text file that contains the configurations necessary for creating a resource stack in AWS.

The screenshot shows a CloudFormation template named "NextWorkWebAppSetup".

**Template details:**

- Template generation status: Complete
- Template ID: arn:aws:cloudformation:ap-southeast-2:050752641312:generatedTemplate/2dd971b0-59f0-4cee-aa3a-fe471f982bbb
- Creation time: 2024-10-16 01:19:51 UTC+0900
- Updated time: 2024-10-16 01:20:07 UTC+0900

**Configurations:**

- Deletion policy: DELETE
- Update replace policy: DELETE

**Template definition:** (selected tab) | Template resources | AWS CDK

**Template:**

- YAML ▾
- Download
- Copy
- Import to stack (button)

⚠ Some optional properties were not included in the template. You can download the template and add the optional properties if they are configured for your resources [Learn more](#)

View warning details | Import edited template

Canvas | Template (selected)

```
1 Metadata:
2 | TemplateId: arn:aws:cloudformation:ap-southeast-2:050752641312:generatedTemplate/2dd971b0-59f0-4cee-aa3a-fe471f982bbb
3 Resources:
4 IAMManagedPolicy@0policyserviceroleCodeBuildCloudWatchLogsPolicynextworkwebbuildapsouteast200DBio2;
```



tiubenedict@gmail.com

NextWork Student

[NextWork.org](http://NextWork.org)

---

# IaC generator

I created a CloudFormation template using the IaC generator, which scans my account for resources that I can draw the configurations from.

## **Not all resources could be added to my template**

The resources I couldn't add to a template were the source core repository (setting up a CodeCommit repo) and CodeBuild project.

The resources that I could add to my template includes the S3 bucket, IAM roles and policies, and the CodeArtifact domain and associated repositories.



# Manually adding resources

After downloading the generated template, I manually defined two more resources: the CodeCommit repository and the CodeBuild project.

I had to manually define these because setting up a repo can be more complicated such as Git configs or user permissions, while configurations also need to be set for the build environment.

I also had to make sure the references were consistent in this template, so I made two edits: the S3 bucket for hosting the build artifact, and the specific IAM role amazon resource name for the CodeBuild project.

```
> benedict-t > Downloads > ! NextWorkWebAppSetup-template-1729009215157.yaml
Resources:
  CodeArtifactRepository@repositorynextworknextworkpackages@0AqIhp:
    Properties:
      DomainName:
        # CodeCommit Repository
        CodeCommitRepository:
          Type: AWS::CodeCommit::Repository
          Properties:
            RepositoryName: nextwork-web-project
            RepositoryDescription: A web application for the NextWork home page

  # CodeBuild Project
  CodeBuildProject:
    Type: AWS::CodeBuild::Project
    Properties:
      Name: nextwork-web-build
      Description: Build project for NextWork web application
      Source:
        Type: CODECOMMIT
        Location: !GetAtt CodeCommitRepository.CloneUrlHttp
        BuildSpec: buildspec.yml
      Artifacts:
        Type: S3
        Name: nextwork-web-build.zip
        Packaging: ZIP
        Location: !Ref S3Bucket@0nextworkbuildartifactsbene00jz02G
      Environment:
        Type: LINUX_CONTAINER
        ComputeType: BUILD_GENERAL1_SMALL
        Image: aws/codebuild/amazonlinux2-x86_64-standard:corretto8
        ServiceRole: !GetAtt IAMRole@0codebuildnextworkbuildservicerole00kYuh.Arn
      LogsConfig:
        CloudWatchLogs:
          GroupName: nextwork-build-logs
          Status: ENABLED
          StreamName: webapp
```



**tiubenedict@gmail.com**

NextWork Student

[NextWork.org](http://NextWork.org)

---

# Testing my template

Before testing my template, I deleted those same resources that were included in the template, so that there wouldn't be the redundant resources sharing the same name, which would prevent CloudFormation from creating them.

A stack is a collection of AWS resources, created together using the CloudFormation template.

The result of my first test was: an error from creating the IAM policies for CodeArtifact and CodeBuild.



tiubenedict@gmail.com

NextWork Student

[NextWork.org](http://NextWork.org)

# Unpacking the first error

My first template test failed because the necessary permission template was not available yet to attach to the IAM policy, as it was also just in the process of being created in this template.

The screenshot shows the CloudFormation Events page with 36 events listed. The events are categorized into two groups: 'CREATE\_FAILED' and 'Resource creation cancelled'. The first group contains five events, all of which occurred at approximately the same time (around 2024-10-14 17:28:14 UTC+0900). The second group contains three events, all of which occurred at approximately the same time (around 2024-10-14 17:28:14 UTC+0900). The events are as follows:

Event ID	Resource	Status	Detailed Status	Status Reason
7:39	CodeArtifactRepository0	CREATE_FAILED	-	Internal Failure
7:38	S3Bucket0onetworkbuild	CREATE_FAILED	-	Resource creation cancelled
7:38	CodeArtifactDomain0od	CREATE_FAILED	-	Resource creation cancelled
7:38	IAMManagedPolicy0opd	CREATE_FAILED	-	Resource handler returned message: "The role with name codebuild-newnetwork-web-build-service-role cannot be found. (Service: iam, Status Code: 404, Request ID: 65ee22d6-0f21-4870-a60f-5e90e187beb2)" (RequestToken: 48c039da-d0e5-7878-cd74-faa3279965fb, HandlerErrorCode: NotFound)
7:38	IAMManagedPolicy0opd	CREATE_FAILED	-	Resource handler returned message: "The role with name codebuild-newnetwork-web-build-service-role cannot be found. (Service: iam, Status Code: 404, Request ID: a19a17e4-456e-45ea-be11-e82a4e8b7007" (RequestToken: 0bae4343-b6d4-eb8b-2af0-ec1fe3aa1c, HandlerErrorCode: NotFound)
7:38	IAMManagedPolicy0opd	CREATE_FAILED	-	Resource handler returned message: "The role with name codebuild-newnetwork-web-build-service-role cannot be found. (Service: iam, Status Code: 404, Request ID: bdb15464-0fba-4f76-9406-8e2925c537d7)" (RequestToken: 2c52de78-aec08-f70-8786-cec1f512867f, HandlerErrorCode: NotFound)

## To fix this error, I edited my CloudFormation template.

I added the line DependsOn: IAMRole so that that role gets created first before the IAM managed policies, which need that role, are created.



# Fixing the first error

The DependsOn attribute means that this resource has a dependency on another resource, so it must wait for that dependency to be created first to prevent errors.

The DependsOn line was added to four different parts of my template: the 3 IAM policies (1 for CodeArtifact, 2 for CodeBuild), and another for the CodeBuild project itself.

```
127 # IAM Policy for CodeArtifact
128 IAMManagedPolicy0@policycodeartifactnextworkconsumerpolicy008elws:
129   UpdateReplacePolicy: "Delete"
130   Type: "AWS::IAM::ManagedPolicy"
131   DeletionPolicy: "Delete"
132   DependsOn: "IAMRole0@codebuildnextworkwebbuildservicerole00DkYuh"
133   Properties:
134     ManagedPolicyName: "codeartifact-nextwork-consumer-policy"
135     Path: "/"
136     Description: "Provides permissions to read from CodeArtifact"
137     Groups: []
138     PolicyDocument:
139       Version: "2012-10-17"
140       Statement:
141         - Resource: "*"
142           Action:
143             - "codeartifact:GetAuthorizationToken"
144             - "codeartifact:GetRepositoryEndpoint"
145             - "codeartifact:ReadFromRepository"
146           Effect: "Allow"
147         - Condition:
148           StringEquals:
149             | sts:AWSServiceName: "codeartifact.amazonaws.com"
150             Resource: "*"
151             Action: "sts:GetServiceBearerToken"
152             Effect: "Allow"
153             Roles:
154               - "codebuild-nextwork-web-build-service-role"
155             Users: []
156 # IAM Role for CodeBuild
157 IAMRole0@codebuildnextworkwebbuildservicerole00DkYuh:
```



# Second template test

I gave my CloudFormation template another test! But this time, I couldn't create the stack because of an error. This is known as a Circular Dependency.

This error means two or more resources reference each other in the config, so CloudFormation doesn't know which one needs to be created first. Here, the necessary role was needed for the policies, but role creation also references the policies.

To fix this error, I removed the reference to the policies from the role creation section.

The screenshot shows the 'Specify template' page in the AWS CloudFormation console. The 'Upload a template file' section is selected, and a file named 'CloudFormationTemplate.yaml' is uploaded. A red box highlights the error message: 'Circular dependency between resources: [IAMManagedPolicy0policysericeroleCodeBuildCloudWatchLogsPolicynextworkwebbuildapsoutheast200DBi02, IAMManagedPolicy0policysericeroleCodeBuildBasePolicynextworkwebbuildapsoutheast200LeIT3, CodeBuildProject, IAMManagedPolicy0policyodanitafactnextworkconsumerpolicy008elws, IAMRole0codebuildnextworkwebbuildservicerole00DkYuh]'. Below the error message, there is a link to 'View in Infrastructure Composer'.



tiubenedict@gmail.com  
NextWork Student

[NextWork.org](http://NextWork.org)

# My final template test ☐

In my final test, creating the new stack was a great success

I could verify all the deployed resources by visiting the resources tab from within the CloudFormation stack.

Not all the resources in the list had a shortcut URL, because they were deployed to a specific region, not universally to my IAM account.

Resources (10)						
Logical ID	Physical ID	Type	Status	Module		
CodeArtifactDomain00do mainnextwork0xNjb	arn:aws:codeartifact: southeast- 205075264131:domain/ nextwork	AWS::CodeArtifact:Doma in	CREATE_COMPLETE	-		
CodeArtifactRepository0 Repositorynextworkmav encentralstore0Jgrfu	arn:aws:codeartifact: southeast- 205075264131:repo/ nextwork/maven- central-store	AWS::CodeArtifact:Repos itory	CREATE_COMPLETE	-		
CodeArtifactRepository0 Repositorynextworkne workpackages0AqjHP	arn:aws:codeartifact: southeast- 205075264131:repo/ nextwork/network- packages	AWS::CodeArtifact:Repos itory	CREATE_COMPLETE	-		
CodeBuildProject	nextwork-web-build	AWS::CodeBuild:Projec t	CREATE_COMPLETE	-		
CodeCommitRepository	aTed7f51-db0e-4c2d- beba-294d46943773	AWS::CodeCommit:Repo sitory	CREATE_COMPLETE	-		
IAMManagedPolicy00poli cycodeartifactnextwork consumerpolicy00dews	arn:aws:iam:050752641 312:policy/codeartifact- nextwork-consumer- policy	AWS::IAM::ManagedPolic y	CREATE_COMPLETE	-		
IAMManagedPolicy00poli cycodeartifactnextwork servicepolicyCodeBuildBa sePolicynextworkwebfull	arn:aws:iam:050752641 312:policy/service- role/CodeBuildBasePolicy nextworkwebfull	AWS::IAM::ManagedPolic y	CREATE_COMPLETE	-		



NextWork.org

# Everyone should be in a job they love.

Check out nextwork.org for  
more projects

