



Infrastructure as Code with CloudFormation



Mohammed Furqanuddin

Resources (16)						
Logical ID	Physical ID	Type	Status	Module		
CodeArtifactDomainDomainnextwork	arn:aws:codeartifact:ap-south-1:866795125560:domain/nextwork	AWS::CodeArtifact::Domain	CREATE_COMPLETE	-		
CodeArtifactRepositoryRepositorynextworkmavencentralstore	arn:aws:codeartifact:ap-south-1:866795125560:repository/nextwork/maven-central-store	AWS::CodeArtifact::Repository	CREATE_COMPLETE	-		
CodeArtifactRepositoryRepositorynextworknextworkdevopscid	arn:aws:codeartifact:ap-south-1:866795125560:repository/nextwork/nextwork-devops-cid	AWS::CodeArtifact::Repository	CREATE_COMPLETE	-		
CodeBuild00nextworkwebcloudformati0n00	nextwork-devops-cid	AWS::CodeBuild::Project	CREATE_COMPLETE	-		
CodeDeployApplicationNextworkdevopscid	nextwork-devops-cid	AWS::CodeDeploy::Application	CREATE_COMPLETE	-		
CodeDeployDeploymentGroup00nextworkwebdeploygroupcloudformation00	nextwork-devops-cid-deploymentgroup	AWS::CodeDeploy::DeploymentGroup	CREATE_COMPLETE	-		
CodeStarConnectionsConnectionConne	arn:aws:codestar-connections:ap-south-1:866795125560:connection/77209	AWS::CodeStarConnections::Connect	CREATE_COMPLETE	-		



Mohammed Furqanud...

NextWork Student

nextwork.org

Introducing Today's Project!

In this project, I will demonstrate how to build a CI/CD pipeline on AWS. I'm doing this project to learn CI/CD practically, understand deployment automation, and gain real-world DevOps experience

Key tools and concepts

In this project, I worked with services such as AWS CloudFormation, CodeBuild, CodeDeploy, CodeStar Connections, EC2, S3, IAM, and CodeArtifact to build a complete CI/CD pipeline. Through this, I learned key concepts like Infrastructure as Code, managing resource dependencies with DependsOn, troubleshooting CloudFormation errors and rollbacks, resolving IAM circular dependencies, using parameters to make templates reusable, and understanding how region-specific resources affect deployments.

Project reflection

This project took me approximately 3-4 hours to complete. The most challenging part was troubleshooting CloudFormation errors, especially resolving IAM dependency and circular reference issues. The most rewarding part was successfully deploying the CI/CD infrastructure using a reusable CloudFormation template and understanding how all the AWS services worked together end to end.



Mohammed Furqanud...

NextWork Student

nextwork.org

This project is part six of a series of DevOps projects where I'm building a CI/CD pipeline. I'll be working on the next project soon, where I'll continue expanding the pipeline and deepen my understanding of advanced DevOps concepts and AWS services.

Mohammed Furqanud...

NextWork Student

nextwork.org

Generating a CloudFormation Template

The IaC Generator is an AWS tool that automatically converts existing AWS resources into a CloudFormation template. # It works in three simple steps: # Scans your current resources # Generates an IaC template Lets you review and reuse it to deploy infrastructure quickly and consistently

A CloudFormation template is a text file (YAML or JSON) that defines AWS infrastructure as code. It tells AWS what resources to create and how they should be configured. The resources that I could add to my template include EC2 instances, IAM roles, S3 buckets, CodeBuild, CodeDeploy, security groups, and networking components.

The resources I couldn't add to my template were IAM instance profiles and roles that were already managed by another CloudFormation stack, because the IaC Generator does not allow importing resources that are already controlled by an existing stack to avoid conflicts.



Mohammed Furqanud...

NextWork Student

nextwork.org

The screenshot shows the AWS CloudFormation IAM Policy Generator interface. The top navigation bar includes 'CloudFormation', 'IAM generator', and 'nextwork-devops-clcd-1'. Below the navigation are buttons for 'YAML' (selected), 'Download', 'Copy template', and 'Import to stack'. A warning message states: '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.' It also includes links for 'View warning details' and 'Import edited template'. The main area is titled 'Template' and contains a code editor with the following YAML template:

```
1  ...
2  Metadata:
3    AWS::Metrics:
4      Iac Generator: "arn:aws:cloudformation:ap-south-1:866795125560:generatedTemplate/de54933-d548-417f-ac9b-5bf478ab0372"
5  Resources:
6    IAMManagedPolicyPolicyServiceRoleCodeBuildBasePolicynextworkdevopsclcdapsouth:
7      Type: "AWS::IAM::ManagedPolicy"
8      DeleteOnPolicyDelete: "Delete"
9      Description:
10        - ManagedPolicyName: "CodeBuildBasePolicy-nextwork-devops-clcd-ap-south-1"
11        - Path: "/service-role/"
12        - Description: "Policy used in trust relationship with CodeBuild"
13        - Groups: []
14        - PolicyDocument:
15          Version: "2012-10-17"
16          Statement:
17            - Resource:
```

Mohammed Furqanud...

NextWork Student

nextwork.org

Template Testing

Before testing my template, I deleted the existing CI/CD resources from my AWS account, because removing them ensures there are no conflicts and allows me to confirm that the CloudFormation template can successfully recreate the infrastructure from scratch.

I tested my template by deploying it using CloudFormation with new resources. The first deployment resulted in a CREATE_FAILED error due to two issues: a region mismatch caused by a hardcoded CodeStar Connection HostArn pointing to us-west-2 while deploying in ap-south-1, and an IAM dependency issue where CloudFormation tried to attach policies to the CodeBuild service role before the role was fully created. After removing the hardcoded HostArn, the stack was able to proceed correctly.

CloudFormation > Stacks > NextWorkDevOpsProject1					
Timestamp	Resource Name	Status	Progress	Failure Reason	Details
2026-01-20 23:57:46 UTC+0530	CodeArtifactDomainDomainName	CREATE_IN_PROGRESS	-	CONFIGURATION_COMPLETE	Eventual consistency check initiated
2026-01-20 23:57:46 UTC+0530	CodeDeployApplicationNextWorkDevOpsProject	CREATE_COMPLETE	-	-	-
2026-01-20 23:57:46 UTC+0530	IAMManagedPolicyPolicyServiceRoleCodeBuildCloudWatchLogsPolicyNextWorkDevOpsProjectap-south-1	CREATE_FAILED	-	Likely root cause	Resource handler returned message: "The role with name codebuild-nextwork-devops-cicd-service-role cannot be found. (Service: iam, Status Code: 404, Request ID: fa538b6-a451-4bb9-bf07-1fb27529e067) (SDK Attempt Count: 1)" (RequestToken: 3e16bd6e-905f-f5e0-4cb5-1121808ef7b5, HandlerErrorCode: NotFound)
2026-01-20 23:57:45 UTC+0530	IAMManagedPolicyPolicyCodeArtifactNextWorkComsumerPolicy	CREATE_IN_PROGRESS	-	-	Resource creation Initiated



Mohammed Furqanud...

NextWork Student

nextwork.org

DependsOn

To resolve the error, I added the DependsOn attribute to the IAM policy resources, ensuring that the CodeBuild service role was created first. The DependsOn attribute means CloudFormation waits for the specified resource to finish creating before starting the dependent resource, preventing timing and dependency errors.

The DependsOn line was added to four IAM managed policies: the CodeBuild base policy, CloudWatch logs policy, CodeConnections policy, and the CodeArtifact consumer policy. This ensures the CodeBuild service role is created first before any policies are attached.

```
1  ---
2  Metadata:
3  | AWSToolsMetrics:
4  |   Iac_Generator: "arn:aws:cloudformation:ap-south-1:866795125560:generatedTemplate/de549333-d548-417f-ac9b-5bf470ab0372"
5  Resources:
6  | IAMManagedPolicyPolicyserviceceroleCodeBuildBasePolicynextworkdevopscicdapsouth1:
7  |   UpdateReplacePolicy: "Delete"
8  |   Type: "AWS::IAM::ManagedPolicy"
9  |   DeletionPolicy: "Delete"
10 |   DependsOn: "IAMRoleCodebuildnextworkdevopscicdservicerole"
11 |   Properties:
12 |     ManagedPolicyName: "CodeBuildBasePolicy-nextwork-devops-cicd-ap-south-1"
13 |     Path: "/service-role/"
```

Mohammed Furqanud...

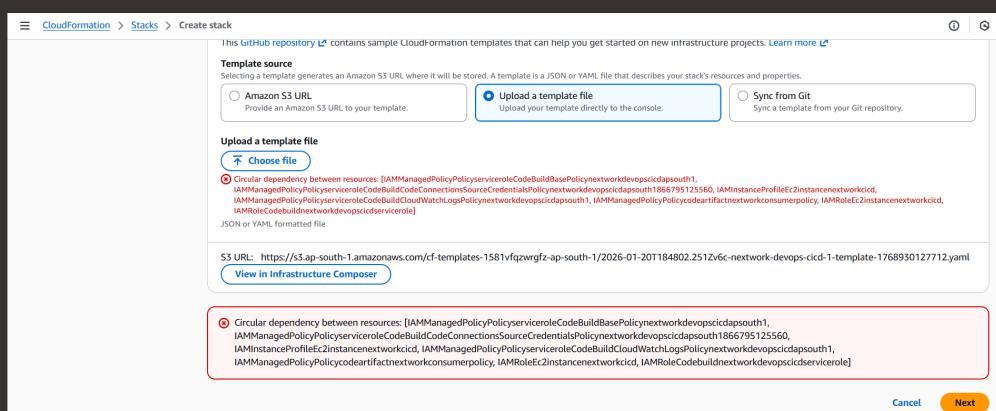
NextWork Student

nextwork.org

Circular Dependencies

I gave my CloudFormation template another test, but this time I ran into a circular dependency error. This happened because multiple IAM roles, policies, and instance profiles were configured to depend on each other, creating a loop that CloudFormation could not resolve during resource creation.

I fixed my CloudFormation template by removing the IAM policy references from the ManagedPolicyArns section of the CodeBuild IAM role, which eliminated the circular dependency and allowed CloudFormation to create the resources successfully





Mohammed Furqanud...

NextWork Student

nextwork.org

Manual Additions

In a project extension, I manually defined two additional resources in my CloudFormation template: A CodeBuild Project – to build the application artifacts. A CodeDeploy Deployment Group – to deploy the application to EC2 instances.

Before saving the template, I replaced all placeholder values with the actual logical resource IDs from my CloudFormation template. This included updating the references for the CodeBuild service role, S3 bucket, CodeDeploy role, and CodeDeploy application, ensuring that all resources correctly point to existing definitions and the stack can deploy without errors.

Parameters are inputs you provide when deploying a CloudFormation template. They make the template flexible and reusable, so values like the GitHub repo owner and name can be changed without editing the code.

```
655     - name:
656       # CodeBuild Project
657       Codebuild100nextworkwebcloudformation00:
658       Type: AWS::CodeBuild::Project
659       DependsOn:
660         - "ServiceRoleCodebuild100nextworkdevopsclifurqan"
661         - "S3BucketNextworkdevopsclifurqan"
662       Properties:
663         Name: nextwork-devops-cld
664         Description: Build project for NextWork web application
665         Source:
666           Type: GITHUB
667           Location: Sub "https://github.com/${githubRepoOwner}/${githubRepo}"
668           BuildSpec: buildspec.yml
669         Artifacts:
670           Type: S3
671           Name: nextwork-web-build.zip
672           Packaging: ZIP
673           Location: !Ref csBUCKETNextworkdevopsclifurqan
674             Path: /builds
675         Environment:
676           Type: LINUX_CONTAINER
677           ComputeType: BUILD_GENERAL1_SMALL
678           Image: aws/codebuild/amazonlinux-x86_64-standard:corretto8
679           ServiceRole: !GetAtt IAMRoleCodebuild100nextworkdevopsclifurqan.Arn
680         LogConfig:
681           CloudWatchLogs:
682             LogStreamName: /aws/codebuild/nextwork-devops-cld
683             Status: ENABLED
684             StreamName: webapp
685
686
```

Mohammed Furqanud...

NextWork Student

nextwork.org

Success!

I could verify all the deployed resources by visiting the Resources tab in the CloudFormation stack, where AWS lists every resource created as part of the deployment along with their status.

Resources (16)					
Logical ID	Physical ID	Type	Status	Module	
CodeArtifactDomainDomainnextwork	arn:aws:codeartifact:ap-south-1:866795125560:domain/nextwork	AWS::CodeArtifact::Domain	CREATE_COMPLETE	-	
CodeArtifactRepositoryRepositorynextworkmavencentralstore	arn:aws:codeartifact:ap-south-1:866795125560:repository/nextwork/maven-central-store	AWS::CodeArtifact::Repository	CREATE_COMPLETE	-	
CodeArtifactRepositoryRepositorynextworknextworkdevopsccid	arn:aws:codeartifact:ap-south-1:866795125560:repository/nextwork/nextwork-devops-ccid	AWS::CodeArtifact::Repository	CREATE_COMPLETE	-	
CodeBuild00nextworkwebcloudformationon00	nextwork-devops-ccid	AWS::CodeBuild::Project	CREATE_COMPLETE	-	
CodeDeployApplicationNextworkdevopsccid	nextwork-devops-ccid	AWS::CodeDeploy::Application	CREATE_COMPLETE	-	
CodeDeployDeploymentGroup00nextworkwebdeploygroupcloudformation00	nextwork-devops-ccid-deploymentgroup	AWS::CodeDeploy::DeploymentGroup	CREATE_COMPLETE	-	
CodeStarConnectionsConnectionConne	arn:aws:codestar-connections:ap-south-1:866795125560:connection/77ec07	AWS::CodeStarConnections::Connect	CREATE_COMPLETE	-	



nextwork.org

The place to learn & showcase your skills

Check out nextwork.org for more projects

