**DevOps-Mlangles-SOP**

**INDEX**  
  
[**Introduction**](#Bookmark2)

[**Training Account IAM roles and Permissions**](#Bookmark1)

[**Digital Account IAM roles and Permissions**](#Bookmark3)

[**Code Commit Repo**](#Bookmark4)

[**Event Bridge rule in Digitalinfra Account**](#Bookmark5)

[**Event Bridge rule in Training Account**](#Bookmark8)

[**KMS key in Training Account**](#Bookmark10)

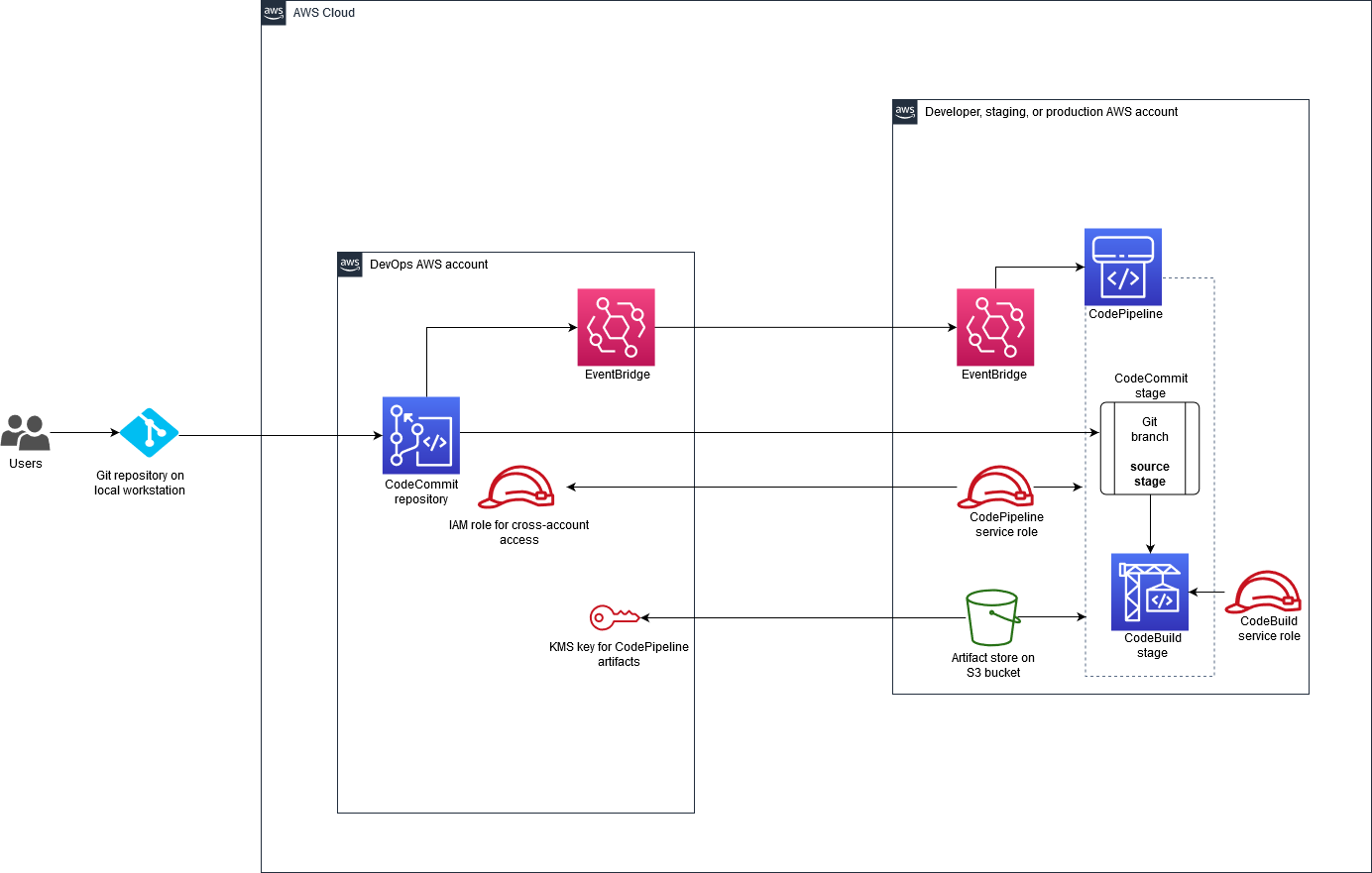
[**Create a Build Project**](#Bookmark11)

[**Create Pipeline in Training account**](#Bookmark12)

[**Create an S3 Bucket for Target**](#Bookmark13)

[**S3 bucket for artifacts**](#Bookmark14)

**Introduction**

* In this scenario we have two accounts –
  + DigitalInfra account (906424543471) - (Codecommit repo)
  + training account (268370550335) - (CodePipeline)
* In this setup we have a total of 4 polices (9 policies) in Training account and in Digital account we have 2 roles (4 policies)  
    
  

**Training Account IAM roles and Permissions**

First Create IAM roles in the training account with their policies.

* A role named **mlangles-dev-role** is attached to the Codepipeline(Trusted entities:Codepipeline) with the following Policies.

|  |
| --- |
| [AWSCodePipelineServiceRole-us-east-1-dummy](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3A268370550335%3Apolicy%2Fservice-role%2FAWSCodePipelineServiceRole-us-east-1-dummy) |
| {  "Statement": [  {  "Action": [  "iam:PassRole"  ],  "Resource": "\*",  "Effect": "Allow",  "Condition": {  "StringEqualsIfExists": {  "iam:PassedToService": [  "cloudformation.amazonaws.com",  "elasticbeanstalk.amazonaws.com",  "ec2.amazonaws.com",  "ecs-tasks.amazonaws.com"  ]  }  }  },  {  "Action": [  "codecommit:CancelUploadArchive",  "codecommit:GetBranch",  "codecommit:GetCommit",  "codecommit:GetRepository",  "codecommit:GetUploadArchiveStatus",  "codecommit:UploadArchive"  ],  "Resource": "\*",  "Effect": "Allow"  },  {  "Action": [  "codedeploy:CreateDeployment",  "codedeploy:GetApplication",  "codedeploy:GetApplicationRevision",  "codedeploy:GetDeployment",  "codedeploy:GetDeploymentConfig",  "codedeploy:RegisterApplicationRevision"  ],  "Resource": "\*",  "Effect": "Allow"  },  {  "Action": [  "codestar-connections:UseConnection"  ],  "Resource": "\*",  "Effect": "Allow"  },  {  "Action": [  "elasticbeanstalk:\*",  "ec2:\*",  "elasticloadbalancing:\*",  "autoscaling:\*",  "cloudwatch:\*",  "s3:\*",  "sns:\*",  "cloudformation:\*",  "rds:\*",  "sqs:\*",  "ecs:\*"  ],  "Resource": "\*",  "Effect": "Allow"  },  {  "Action": [  "lambda:InvokeFunction",  "lambda:ListFunctions"  ],  "Resource": "\*",  "Effect": "Allow"  },  {  "Action": [  "opsworks:CreateDeployment",  "opsworks:DescribeApps",  "opsworks:DescribeCommands",  "opsworks:DescribeDeployments",  "opsworks:DescribeInstances",  "opsworks:DescribeStacks",  "opsworks:UpdateApp",  "opsworks:UpdateStack"  ],  "Resource": "\*",  "Effect": "Allow"  },  {  "Action": [  "cloudformation:CreateStack",  "cloudformation:DeleteStack",  "cloudformation:DescribeStacks",  "cloudformation:UpdateStack",  "cloudformation:CreateChangeSet",  "cloudformation:DeleteChangeSet",  "cloudformation:DescribeChangeSet",  "cloudformation:ExecuteChangeSet",  "cloudformation:SetStackPolicy",  "cloudformation:ValidateTemplate"  ],  "Resource": "\*",  "Effect": "Allow"  },  {  "Action": [  "codebuild:BatchGetBuilds",  "codebuild:StartBuild",  "codebuild:BatchGetBuildBatches",  "codebuild:StartBuildBatch"  ],  "Resource": "\*",  "Effect": "Allow"  },  {  "Effect": "Allow",  "Action": [  "devicefarm:ListProjects",  "devicefarm:ListDevicePools",  "devicefarm:GetRun",  "devicefarm:GetUpload",  "devicefarm:CreateUpload",  "devicefarm:ScheduleRun"  ],  "Resource": "\*"  },  {  "Effect": "Allow",  "Action": [  "servicecatalog:ListProvisioningArtifacts",  "servicecatalog:CreateProvisioningArtifact",  "servicecatalog:DescribeProvisioningArtifact",  "servicecatalog:DeleteProvisioningArtifact",  "servicecatalog:UpdateProduct"  ],  "Resource": "\*"  },  {  "Effect": "Allow",  "Action": [  "cloudformation:ValidateTemplate"  ],  "Resource": "\*"  },  {  "Effect": "Allow",  "Action": [  "ecr:DescribeImages"  ],  "Resource": "\*"  },  {  "Effect": "Allow",  "Action": [  "states:DescribeExecution",  "states:DescribeStateMachine",  "states:StartExecution"  ],  "Resource": "\*"  },  {  "Effect": "Allow",  "Action": [  "appconfig:StartDeployment",  "appconfig:StopDeployment",  "appconfig:GetDeployment"  ],  "Resource": "\*"  }  ],  "Version": "2012-10-17"  } |

|  |
| --- |
| [mlangles-assume-policy](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3A268370550335%3Apolicy%2Fmlangles-assume-policy) |
| {  "Version": "2012-10-17",  "Statement": {  "Effect": "Allow",  "Action": "sts:AssumeRole",  "Resource": [  "arn:aws:iam::906424543471:role/mlangles-cross-acc-role"  ]  }  } |

* + [AWSKeyManagementServicePowerUser](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAWSKeyManagementServicePowerUser)
* A role named **cwe-role-us-east-1-mlangles-test** is attached to the Eventbridge (Trusted entities: events) with the following Policies.

|  |
| --- |
| [mlangles-test-2-invocation-pipeline](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/details/cwe-role-us-east-1-mlangles-test/editPolicy/mlangles-test-2-invocation-pipeline?step=addPermissions) |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Allow",  "Action": [  "codepipeline:StartPipelineExecution"  ],  "Resource": [  "arn:aws:codepipeline:us-east-1:268370550335:mlangles-test-2"  ]  }  ]  } |

* + [AmazonEventBridgeFullAccess](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEventBridgeFullAccess)
* A role named **cross-account-eventbridge** is attached to the Digital account(Trusted entities: 906424543471) with the following Policies.
  + [AmazonEventBridgeFullAccess](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEventBridgeFullAccess)
* A role named **codebuild-mlangles-build-service-role** is attached to the Digital account(Trusted entities: codebuild) with the following Policies.

|  |
| --- |
| [CodeBuildBasePolicy-mlangles-build-us-east-1](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3A268370550335%3Apolicy%2Fservice-role%2FCodeBuildBasePolicy-mlangles-build-us-east-1) |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Allow",  "Resource": [  "arn:aws:logs:us-east-1:268370550335:log-group:/aws/codebuild/mlangles-build",  "arn:aws:logs:us-east-1:268370550335:log-group:/aws/codebuild/mlangles-build:\*"  ],  "Action": [  "logs:CreateLogGroup",  "logs:CreateLogStream",  "logs:PutLogEvents"  ]  },  {  "Effect": "Allow",  "Resource": [  "arn:aws:s3:::codepipeline-us-east-1-\*"  ],  "Action": [  "s3:PutObject",  "s3:GetObject",  "s3:GetObjectVersion",  "s3:GetBucketAcl",  "s3:GetBucketLocation"  ]  },  {  "Effect": "Allow",  "Resource": [  "arn:aws:codecommit:us-east-1:268370550335:test"  ],  "Action": [  "codecommit:GitPull"  ]  },  {  "Effect": "Allow",  "Resource": [  "arn:aws:s3:::codepipeline-us-east-1-605621159220",  "arn:aws:s3:::codepipeline-us-east-1-605621159220/\*"  ],  "Action": [  "s3:PutObject",  "s3:GetBucketAcl",  "s3:GetBucketLocation"  ]  },  {  "Effect": "Allow",  "Action": [  "codebuild:CreateReportGroup",  "codebuild:CreateReport",  "codebuild:UpdateReport",  "codebuild:BatchPutTestCases",  "codebuild:BatchPutCodeCoverages"  ],  "Resource": [  "arn:aws:codebuild:us-east-1:268370550335:report-group/mlangles-build-\*"  ]  }  ]  } |

|  |
| --- |
| [CodeBuildCloudWatchLogsPolicy-mlangles-build-us-east-1](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3A268370550335%3Apolicy%2Fservice-role%2FCodeBuildCloudWatchLogsPolicy-mlangles-build-us-east-1) |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Allow",  "Resource": [  "arn:aws:logs:us-east-1:268370550335:log-group:mlangles-test-build",  "arn:aws:logs:us-east-1:268370550335:log-group:mlangles-test-build:\*"  ],  "Action": [  "logs:CreateLogGroup",  "logs:CreateLogStream",  "logs:PutLogEvents"  ]  }  ]  } |

* + [AWSKeyManagementServicePowerUser](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAWSKeyManagementServicePowerUser)

**Digital Account IAM roles and Permissions**

First Create IAM roles in the training account with their policies.

* A role named **mlangles-cross-acc-role** is attached to the account(Trusted entities: 268370550335) with the following Policies.

|  |
| --- |
| [mlangles-dev-kms-s3-policy](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3A906424543471%3Apolicy%2Fmlangles-dev-kms-s3-policy) |
| {  "Version": "2012-10-17",  "Statement": [  {  "Effect": "Allow",  "Action": [  "s3:GetObject\*",  "s3:PutObject",  "s3:PutObjectAcl",  "codecommit:ListBranches",  "codecommit:ListRepositories"  ],  "Resource": [  "arn:aws:s3:::codepipeline-us-east-1-605621159220/\*"  ]  },  {  "Effect": "Allow",  "Action": [  "kms:DescribeKey",  "kms:GenerateDataKey\*",  "kms:Encrypt",  "kms:ReEncrypt\*",  "kms:Decrypt"  ],  "Resource": [  "arn:aws:kms:us-east-1:268370550335:key/f7a063af-4666-4675-89d5-3c7773f44ff2",  "arn:aws:kms:us-east-1:268370550335:key/de09b69c-1af9-4f43-994c-8dd9fb9224ab"  ]  }  ]  } |

* + [AWSCodeCommitFullAccess](https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAWSCodeCommitFullAccess)
* A role named **cwe-role-us-east-1-mlops\_pipeline** is attached to the Evendbridge(Trusted entities: events) with the following Policies.
  + [AmazonEventBridgeFullAccess](https://us-east-1.console.aws.amazon.com/iamv2/home#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEventBridgeFullAccess)

|  |
| --- |
| [cross-account-eventbrige-role](https://us-east-1.console.aws.amazon.com/iamv2/home#/roles/details/cwe-role-us-east-1-mlops_pipeline/editPolicy/cross-account-eventbrige-role?step=addPermissions) |
| {  "Version": "2012-10-17",  "Statement": {  "Effect": "Allow",  "Action": "sts:AssumeRole",  "Resource": [  "arn:aws:iam::268370550335:role/cross-account-eventbridge"  ]  }  } |

**Code Commit Repo**  
Create a codecommit repo in Digitalinfra account with the name **mlangles-dev-repo** and configured the pipeline on dev branch.

**Event Bridge rule in Digitalinfra Account**  
Create an Eventbridge rule to transfer events to another (training) account eventbridge. In the target choose event bus in another account and paste the arn of that account.

|  |
| --- |
| Event Pattern |
| {  "source": ["aws.codecommit"],  "detail-type": ["CodeCommit Repository State Change"],  "resources": ["arn:aws:codecommit:us-east-1:906424543471:mlangles-dev-repo"],  "detail": {  "event": ["referenceCreated", "referenceUpdated"],  "referenceType": ["branch"],  "referenceName": ["dev"]  }  } |

Reference - [Use AWS CodeCommit and AWS CodePipeline to deploy a CI/CD pipeline in multiple AWS accounts - AWS Prescriptive Guidance (amazon.com)](https://docs.aws.amazon.com/prescriptive-guidance/latest/patterns/use-aws-codecommit-and-aws-codepipeline-to-deploy-a-ci-cd-pipeline-in-multiple-aws-accounts.html)

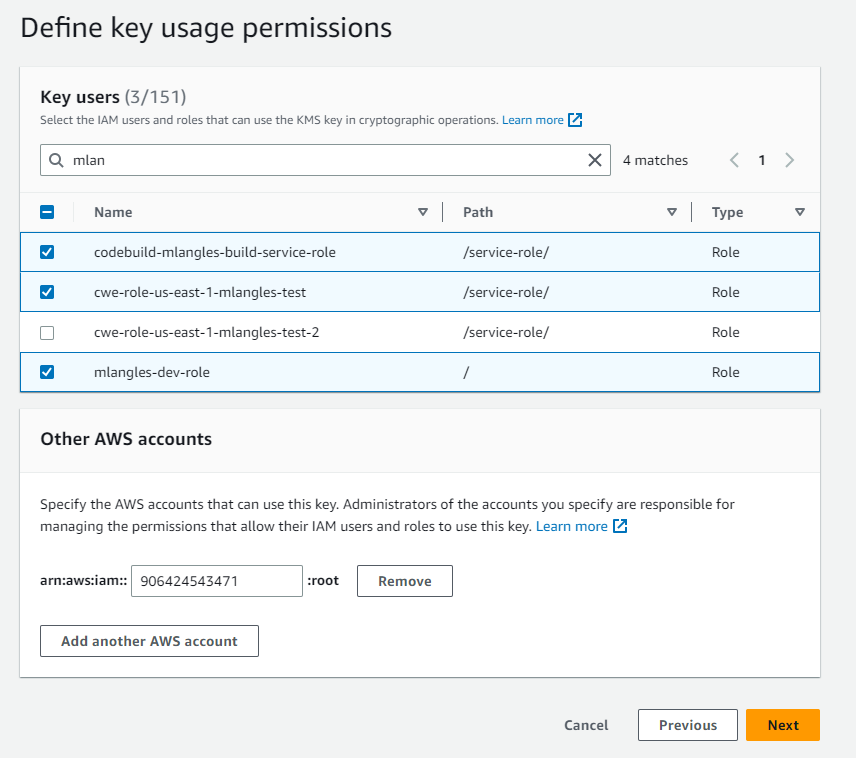
**Event Bridge rule in Training Account**

Create an Eventbridge rule to transfer events to another (training) account eventbridge. In the target choose the pipeline that you want to invocate (role – cwe-role-us-east-1-mlangles-test)

|  |
| --- |
| Event Pattern |
| {  "source": ["aws.codecommit"],  "detail-type": ["CodeCommit Repository State Change"],  "resources": ["arn:aws:codecommit:us-east-1:906424543471:mlangles-dev-repo"],  "detail": {  "event": ["referenceCreated", "referenceUpdated"],  "referenceType": ["branch"],  "referenceName": ["dev"]  }  } |

**KMS key in Training Account**

Create an KMS key in training account with

* administrator as some iam user (ex:root)
* Key users – select iam roles - mlangles-dev-role, cwe-role-us-east-1-mlangles-test, codebuild-mlangles-build-service-role
* Other AWS accounts – choose the account number in root  
    
  

**Create a Build Project**  
Before creating a pipeline make sure you have a buildproject that you are passing as argument in json.

**Create Pipeline in Training account**  
Create a Code Pipeline in Training Account with the following json file.

|  |
| --- |
| Mlangles.json |
| {  "pipeline": {  "name": "mlangles-test-2",  "roleArn": "arn:aws:iam::268370550335:role/mlangles-dev-role",  "artifactStore": {  "type": "S3",  "location": "codepipeline-us-east-1-605621159220",  "encryptionKey": {  "id": "arn:aws:kms:us-east-1:268370550335:key/de09b69c-1af9-4f43-994c-8dd9fb9224ab",  "type": "KMS"  }  },  "stages": [  {  "name": "Source",  "actions": [  {  "name": "Source",  "actionTypeId": {  "category": "Source",  "owner": "AWS",  "provider": "CodeCommit",  "version": "1"  },  "runOrder": 1,  "configuration": {  "BranchName": "dev",  "PollForSourceChanges": "false",  "RepositoryName": "mlangles-dev-repo"  },  "outputArtifacts": [  {  "name": "SourceArtifact"  }  ],  "inputArtifacts": [],  "roleArn": "arn:aws:iam::906424543471:role/mlangles-cross-acc-role"  }  ]  },  {  "name": "Build",  "actions": [  {  "name": "Build",  "actionTypeId": {  "category": "Build",  "owner": "AWS",  "provider": "CodeBuild",  "version": "1"  },  "runOrder": 1,  "configuration": {  "ProjectName": "mlangles-build"  },  "outputArtifacts": [  {  "name": "BuildArtifact"  }  ],  "inputArtifacts": [  {  "name": "SourceArtifact"  }  ],  "region": "us-east-1",  "namespace": "BuildVariables"  }  ]  },  {  "name": "deploy",  "actions": [  {  "name": "deployment-s3",  "actionTypeId": {  "category": "Deploy",  "owner": "AWS",  "provider": "S3",  "version": "1"  },  "runOrder": 1,  "configuration": {  "BucketName": "test.mlangles.com",  "Extract": "true"  },  "outputArtifacts": [],  "inputArtifacts": [  {  "name": "BuildArtifact"  }  ],  "region": "us-east-1"  }  ]  }  ],  "version": 5  },  "metadata": {  "pipelineArn": "arn:aws:codepipeline:us-east-1:268370550335:mlangles-test-2",  "created": "2023-06-27T14:50:33.760000+05:30",  "updated": "2023-06-28T14:58:26.166000+05:30"  }  } |

**Create an S3 Bucket for Target**

Create an s3 bucket for target in deployment stage. Allow ReadOnly access to the public.

**S3 bucket for artifacts**  
Make sure you have a policy that is similar to this that allows Digital infra access to training.

|  |
| --- |
| {  "Version": "2012-10-17",  "Id": "SSEAndSSLPolicy",  "Statement": [  {  "Sid": "DenyUnEncryptedObjectUploads",  "Effect": "Deny",  "Principal": "\*",  "Action": "s3:PutObject",  "Resource": "arn:aws:s3:::codepipeline-us-east-1-605621159220/\*",  "Condition": {  "StringNotEquals": {  "s3:x-amz-server-side-encryption": "aws:kms"  }  }  },  {  "Sid": "DenyInsecureConnections",  "Effect": "Deny",  "Principal": "\*",  "Action": "s3:\*",  "Resource": "arn:aws:s3:::codepipeline-us-east-1-605621159220/\*",  "Condition": {  "Bool": {  "aws:SecureTransport": "false"  }  }  },  {  "Sid": "",  "Effect": "Allow",  "Principal": {  "AWS": "arn:aws:iam::906424543471:root"  },  "Action": [  "s3:Get\*",  "s3:Put\*"  ],  "Resource": "arn:aws:s3:::codepipeline-us-east-1-605621159220/\*"  },  {  "Sid": "",  "Effect": "Allow",  "Principal": {  "AWS": "arn:aws:iam::906424543471:root"  },  "Action": "s3:ListBucket",  "Resource": "arn:aws:s3:::codepipeline-us-east-1-605621159220"  }  ]  } |

Reference - <https://prashant-48386.medium.com/cross-account-codepipeline-that-use-codecommit-from-another-aws-account-9d5ab4c892f6>