|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Service | IAM Role Type | Account | IAM Role Name (used for this post) | IAM Role Policy (required for this post) | IAM Role Permissions |
| AWS CodePipeline | Service role | Dev (111111111111) and Prod (222222222222) | *cicd\_codepipeline\_service\_role*  Select Another AWS Account and use this account as the account ID to create the role.  Later update the trust as follows: “Principal”: {“Service”: “codepipeline.amazonaws.com”}, | Use the permissions in the template cicd\_codepipeline\_service\_policy.json to create the policy for this role. | This CodePipeline service role has appropriate permissions to the following services in a local account:   * Manage CodeCommit repos * Initiate build via CodeBuild * Create deployments via CodeDeploy * Assume cross-account CodeDeploy role in prod account to deploy the application |
| AWS CodePipeline | IAM role | Dev (111111111111) | *cicd\_codepipeline\_trigger\_cwe\_role*  Select Another AWS Account and use this account as the account ID to create the role.  Later update the trust as follows: “Principal”: {“Service”: “events.amazonaws.com”}, | Use the permissions in the template cicd\_codepipeline\_trigger\_cwe\_policy.json to create the policy for this role. | CodePipeline uses this role to set a CloudWatch event to trigger the pipeline when there is a change or commit made to the code repository. |
| AWS CodePipeline | IAM role | Prod (222222222222) | *cicd\_codepipeline\_cross\_ac\_role*  Choose Another AWS Account and use the dev account as the trusted account ID to create the role. | Use the permissions in the template cicd\_codepipeline\_cross\_ac\_policy.json to create the policy for this role. | This role is created in the prod account and has permissions to use CodeDeploy and fetch from Amazon S3. The role is assumed by CodePipeline from the dev account to deploy the app in the prod account. Make sure to set up trust with the dev account for this IAM role on the Trust relationships tab. |
| AWS CodeBuild | Service role | Dev (111111111111) | *cicd\_codebuild\_service\_role*  Choose CodeBuild as the use case to create the role. | Use the permissions in the template cicd\_codebuild\_service\_policy.json to create the policy for this role. | This CodeBuild service role has appropriate permissions to:   * The S3 bucket to store artefacts * Stream logs to CloudWatch Logs * Pull code from CodeCommit * Get the SSM parameter for CodeBuild * Miscellaneous Amazon EC2 permissions |
| AWS CodeDeploy | Service role | Dev (111111111111) and Prod (222222222222) | *cicd\_codedeploy\_service\_role*  Choose CodeDeploy as the use case to create the role. | Use the built-in AWS managed policy *AWSCodeDeployRole* for this role. | This CodeDeploy service role has appropriate permissions to:   * Miscellaneous Amazon EC2 Auto Scaling * Miscellaneous Amazon EC2 * Publish Amazon SNS topic * AWS CloudWatch metrics * Elastic Load Balancing |
| EC2 Instance | Service role for EC2 instance profile | Dev (111111111111) and Prod (222222222222) | *cicd\_ec2\_instance\_profile*  Choose EC2 as the use case to create the role. | Use the permissions in the template cicd\_ec2\_instance\_profile\_policy.json to create the policy for this role. | This is set as the EC2 instance profile for the EC2 instances where the app is deployed. It has appropriate permissions to fetch artefacts from Amazon S3 and decrypt contents using the KMS key.  You must update this role later with the actual KMS key and S3 bucket name created as part of the deployment process. |