**CodeDeploy With S3**

**Description:**

CodeDeploy with S3 Continuous Deploy process, we should create required prerequisite IAM Roles for the service communication.

From Amazon Document sharing the steps here. For more details, please refer the below given URL.

<https://docs.aws.amazon.com/codedeploy/latest/userguide/getting-started-codedeploy.html>

**Prerequisites:**

We need 2 IAM roles: a **Service Role** and an **Instance Profile Role**.

**Service Role**: Service Role access will be granted to AWS CodeDeploy to read through your EC2 instance tags. For auto-scaled instances, it looks for your autoscaling name tags. Service Role Policy is as following:

**Create a Service Role:**

1. Go to **IAM** Dashboard.
2. In the navigation pane, choose **Roles**, and then choose Create role.
3. On the Create role page, choose **AWS service**, and from the Choose the service that will use this role list, choose **CodeDeploy**.
4. From Select your use case, choose **CodeDeploy**.
5. Choose Next: **Permissions**.
6. On the **Attached permissions** policy page, if there is a box next to **AWSCodeDeployRole**, select it, and then choose Next: **Review**.

The AWSCodeDeployRole policy provides the permissions required for your service role to:

* Read the tags on your instances or identify your Amazon EC2 instances by Auto Scaling group names.
* Publish information to Amazon SNS topics.
* Retrieve information about CloudWatch alarms.
* Retrieve information about Elastic Load Balancing.

1. On the Review page, in Role name, type a name for the service role (for example **CodeDeployServiceRole**), and then choose Create role.
2. If you want this service role to have permission to access all currently supported endpoints, you are finished with this procedure.

If you want to restrict this service role from access to some endpoints, in the list of roles, browse to and choose the role you just created, and continue to the next step.

1. On the Trust relationships tab, choose Edit trust relationship.
2. You should see the following policy, which provides the service role permission to access all supported endpoints:

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "",

"Effect": "Allow",

"Principal": {

"Service": "codedeploy.amazonaws.com"

},

"Action": "sts:AssumeRole"

}

]

}

1. Service Role created successfully.

**Get the Service Role ARN**

* Go to **IAM** Dashboard
* In the navigation pane, choose **Roles**.
* In the Filter box, type **CodeDeployServiceRole (Created Service Role)**, and then press Enter.
* Choose **CodeDeployServiceRole**.
* Make a note of the value of the **Role ARN** field.

arn:aws:iam::208825294701:role/deploy

**Create an IAM Instance Profile for Your Amazon EC2 Instances**

* Your Amazon **EC2 instances** need permission to access the Amazon **S3 buckets** or **GitHub** repositories where the applications that will be deployed by AWS CodeDeploy are stored.
* To launch Amazon EC2 instances that are compatible with AWS **CodeDeploy**, you must create an additional I**AM role, an instance profile.**
* This role gives AWS CodeDeploy permission to access the Amazon S3 buckets or GitHub repositories where your applications are stored.

**Steps:**

1. Sign in to the AWS Management Console and open the IAM console at [**https://console.aws.amazon.com/iam/**](https://console.aws.amazon.com/iam/)
2. In the IAM console, in the navigation pane, choose Policies, and then choose Create policy. (If a Get Started button appears, choose it, and then choose Create Policy.)
3. On the Create policy page, paste the following in the JSON tab:

{

"Version": "2012-10-17",

"Statement": [

{

"Action": [

"s3:Get\*",

"s3:List\*"

],

"Effect": "Allow",

"Resource": "\*"

}

]

}

1. Choose **Review** policy.
2. On the Create policy page, type CodeDeployDemo-EC2-Permissions in the Policy Name box.
3. (Optional) For Description, type a description for the policy.
4. Choose Create Policy.
5. In the navigation pane, choose Roles, and then choose Create role.
6. On the Create role page, choose AWS service, and from the Choose the service that will use this role list, choose EC2.
7. From the Select your use case list, choose EC2.
8. Choose Next: Permissions.
9. On the Attached permissions policy page, if there is a box next to CodeDeployDemo-EC2-Permissions, select it, and then choose Next: Review.
10. On the Review page, in Role name, type a name for the service role (for example CodeDeployDemo-EC2-Instance-Profile), and then choose Create role.
11. You can also type a description for this service role in the Role description box.
12. You've now created an IAM instance profile to attach to your Amazon EC2 instances.