CDP specific Roles

## admin-role – Deny Billing and CloudTrail

A ‘role’ to be defined that will be used to allow the ‘owner’ of the account to administer all resources within the CDP AWS Account. The ‘role’ may have following policies attached to it. The ‘policy’ will ‘allow’:

* \*
* <Other areas To be confirmed>

The ‘policy’ will ‘deny’:

* Disable Cloud Trail
* Change Billing / Payment Method
* <Other areas To be confirmed>

## 

## productowner-role

A ‘role’ to be defined that will be used to allow the product owner to configure the ‘policies’ within the AWS ‘Non-Production’ Account for resources associated to CDP. The ‘role’ may have following policies attached to it.

The ‘policy’ will ‘allow’:

* Amend existing IAM policies associated to CDP
* View CostExplorer
* View TrustedAdvisor
* <Other areas To be confirmed>

The ‘policy’ will ‘deny’:

* Ability to view / create / modify any other AWS Services (such as Billing, S3, EC2, VPC etc)
* <Other areas To be confirmed>

## 

## leaddeveloper-role/Data-Admin Role

A ‘role’ will be defined that will be used to allow the lead developer to administer AWS resources (EC2 instances, S3 buckets etc) within the AWS ‘Non-Production’ Account for CDP. The ‘role’ may have following policies attached to it.

The ‘policy’ will ‘allow’:

* View / create / modify / delete AWS Resources (EC2 instances etc)
* <Other areas To be confirmed>

The ‘policy’ will ‘deny’:

* Ability to view / create / modify any other AWS Services (such as IAM, VPC, CloudTrail, Billing etc)
* <Other areas To be confirmed>

## 

## developer-role/Data-Engineer Role

A ‘role’ will be defined that will be used to allow the developer to list / modify AWS resources (EC2 instances, S3 buckets etc) within the AWS ‘Non-Production’ Account for CDP. The ‘role’ may have following policies attached to it.

The ‘policy’ will ‘allow’:

* View / modify AWS Resources (EC2 instances etc)
* <Other areas To be confirmed>

The ‘policy’ will ‘deny’:

* Ability to view / create / modify any other AWS Services (such as IAM, VPC, CloudTrail, Billing etc)
* <Other areas To be confirmed>

## tester-role

A ‘role’ will be defined that will be used to allow the tester to utilise (view metric, test scaling) on AWS resources (EC2 instances, S3 buckets etc) within the AWS ‘Non-Production’ Account for CDP. The ‘role’ may have following policies attached to it.

The ‘policy’ will ‘allow’:

* <Other areas To be confirmed>

The ‘policy’ will ‘deny’:

* Ability to view / create / modify any other AWS Services (such as IAM, VPC, CloudTrail, Billing etc)
* <Other areas To be confirmed>

## 

## ops-role

Could be PRODUCTION only.

A ‘role’ will be defined that will be used to allow users to manage the product / service / application in the AWS ‘Production’ Account for CDP. The access will be limited, but will allow view access to the logs, list the AWS resources being used, perform some remedial actions.

The ‘role’ may have following policies attached to it.

The ‘policy’ will ‘allow’:

* <Other areas To be confirmed>

The ‘policy’ will ‘deny’:

* Ability to view / create / modify any other AWS Services (such as IAM, VPC, CloudTrail, Billing etc)
* <Other areas To be confirmed>

## 

## cicd-role

A ‘role’ will be defined that will be used to allow automated deployment of product(s) in the AWS Accounts for CDP. The ‘role’ may have following policies attached to it.

The ‘policy’ will ‘allow’:

* Manage/create/delete the CI/CD services/artifacts

The ‘policy’ will ‘deny’:

* Ability to view / create / modify any other AWS Services (such as IAM, VPC, CloudTrail, Billing etc)
* <Other areas To be confirmed>