Steps to create Production Environment for Mechanical Turk and Developer environment

Reference: IAM Policy Elements, Grammar and Evaluation Logic specifications <https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies.html>

1. Create a Mechanical Turk policy in AWS Console
   1. Go to AWS Console
   2. Login and select IAM Management Console from Services dropdown
   3. Click on Policies from left hand side pane
   4. Click on Create Policy
   5. From next step during create Policy select service as MechanicalTurk
   6. At this point, full permissions are granted to this Policy to use Mechanical Turk
   7. This is sufficient for creating a script to create HIT, Qualification test, qualify workers, approve/reject HITs, pay workers, create a HIT batches, re-assign workers, create custom qualification based on previous HITs and Qualification test made etc.
   8. Click create and submit
2. Create an IAM Group
   1. Go to AWS Console
   2. Login and select IAM Management Console from Services dropdown
   3. Click on Groups from left hand side pane
   4. Create Group and assign Programming permissions (do not select AWS Console)
   5. Attach MechanicalTurk policy we created in Step 1
   6. At this time, group has MTurk full access
   7. Click submit
3. Create an IAM User for developer/programming access
   1. Go to AWS Console
   2. Login and select IAM Management Console from Services dropdown
   3. Click on Users from left hand side pane
   4. Create User and assign Programming permissions (do not select AWS Console)
   5. Select Group created in Step 2
   6. Click Submit
   7. This user is now created and assigned to group created in step 2 and has permissions to MTurk.
4. Create AWS S3 Storage Bucket
   1. Go to AWS Console
   2. Login and select S3 in Storage section from Services dropdown
   3. Remove Block Public Policy since we will be using custom policies on S3 storage.
   4. Create a Bucket Policy as follows, here the policy states the root user and IAM user we created has permission to add Access control lists, Put objects to S3 buckets and to put objects to ACL i.e. to grant read, write and other advanced permissions to a list of email ids.

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Sid": "AddCannedAcl",  "Effect": "Allow",  "Principal": {  "AWS": [  "arn:aws:iam::119077787221:root",  "arn:aws:iam::119077787221:user/iam-mturk-user"  ]  },  "Action": [  "s3:PutObject",  "s3:PutObjectAcl"  ],  "Resource": "arn:aws:s3:::mturk-s3-cg/\*",  "Condition": {  "StringEquals": {  "s3:x-amz-acl": "public-read"  }  }  }  ]  } |

* 1. Now add CORS (Cross Origin resource sharing to allow S3 urls to be access, authenticated to user access. Example: to allow GET, PUT, POST and DELET Http protocol requests.

|  |
| --- |
| [  {  "AllowedHeaders": [  "\*"  ],  "AllowedMethods": [  "PUT",  "POST",  "DELETE"  ],  "AllowedOrigins": [  "https://mturk-s3-cg.s3.amazonaws.com"  ],  "ExposeHeaders": []  },  {  "AllowedHeaders": [  "\*"  ],  "AllowedMethods": [  "PUT",  "POST",  "DELETE"  ],  "AllowedOrigins": [  "https://mturk-s3-cg.s3.amazonaws.com"  ],  "ExposeHeaders": []  },  {  "AllowedHeaders": [],  "AllowedMethods": [  "GET"  ],  "AllowedOrigins": [  "\*"  ],  "ExposeHeaders": []  }  ] |

* 1. At this point we have almost likely gave full permissions to object creators, root users that have accounts in AWS console.
  2. We can restrict object level access by providing authenticated permissions by editing Access control list at the time we “Put Objects” into S3 buckets.

1. Create a AWS S3 access policy in AWS Console
   1. Go to AWS Console
   2. Login and select IAM Management Console from Services dropdown
   3. Click on Policies from left hand side pane
   4. Click on Create Policy
   5. From next step during create Policy select service as S3
   6. Go to JSON tab and copy paste following. Note: We have already created an S3 Bucket and named it as “mturk-s3-cg”. So add following policy by replacing a bucket that you created

|  |
| --- |
| {  "Version": "2012-10-17",  "Statement": [  {  "Sid": "VisualEditor0",  "Effect": "Allow",  "Action": [  "s3:GetObject",  "s3:PutBucketAcl",  "s3:PutBucketPolicy",  "s3:PutAccessPointPolicy",  "s3:PutObjectAcl",  "s3:GetObjectVersion"  ],  "Resource": "arn:aws:s3:::mturk-s3-cg/\*"  },  {  "Sid": "ModifyBucketPolicy",  "Action": [  "s3:GetBucketPolicy",  "s3:PutBucketPolicy"  ],  "Effect": "Allow",  "Resource": "arn:aws:s3:::mturk-s3-cg"  },  {  "Sid": "AccessS3Console",  "Action": [  "s3:GetBucketLocation",  "s3:ListAllMyBuckets"  ],  "Effect": "Allow",  "Resource": "arn:aws:s3:::\*"  }  ]  } |

1. Create an IAM User