# Cross Account Access

* Identify our account numbers
* Login to AWS Console (**Dev Account**)
* Create a user in IAM
  + Username is John
  + Provide AWS console access
  + Attach AdministratorAccess policy
* Note down your account number
* Sign out
* Login to **Production account**
* Create new S3 Bucket
  + Mysharedbucket
  + Developer is able to see the buckets in Production and will be able to upload or delete the assets/files to shared bucket
* Go to IAM 🡪 Create policy
  + Choose Create your own policy
  + Policy name - “read-write-app-bucket”
  + Description – This allows to write from Developer account
  + Policy Document

{

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

"Statement": [

{

"Effect": "Allow",

"Action": "s3:ListAllMyBuckets",

"Resource": "arn:aws:s3:::\*"

},

{

"Effect": "Allow",

"Action": [

"s3:ListBucket",

"s3:GetBucketLocation"

],

"Resource": "arn:aws:s3:::productionapp"

},

{

"Effect": "Allow",

"Action": [

"s3:GetObject",

"s3:PutObject",

"s3:DeleteObject"

],

"Resource": "arn:aws:s3:::productionapp/\*"

}

]

}

Update Resource to the ARN of the bucket (Replace productionapp with bucket name)

* Click on the Role
* Create the new Role
  + myDevelopersAccess
  + Role Type is Cross Account Access (Access to Another Account)
  + Select AWS Accounts that you own
  + Enter the Account ID of the Developer Account
  + Attach policy - read-write-app-bucket
* Logout of Production Account
* Login to the Developer Account
* Go to Users 🡪 Select user you created
  + Click on permissions
  + Add inline policy
  + Select custom policy

{

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

"Statement": {

"Effect": "Allow",

"Action": "sts:AssumeRole",

"Resource": "arn:aws:iam::PRODUCTION-ACCOUNT-ID:role/myDevelopersAccess"

}

}

* + Replace Production Account ID with the ID of your Production Account
  + Verify the Role Name MyDevelopersAccess
  + Policy Name – allow-assume-s3-role-in-production
* Logout
* Login as User we created (For ex: John) from the user URL
* Click on user at Top right and click on Switch Roles tehn Switch Role
  + Account – Production Account ID
  + Role – MyDevelopersAccess
  + Select Color
  + Click on Switch Role
  + Watch the User section at Top right it will show as user@Production account
* Click on S3
  + Can see list of buckets
  + Upload files to sharedbucket
  + Try to upload to other bucket (it should have failed)
* Switch back to Developer account by going to user section at Top right