**AWS IAM CLI Lesson:**

**Create a new user:**

$ aws iam create-user --user-name myCLIuser

**Create access-keys for that user:**

$ aws iam create-access-keys --user-name myCLIuser

**configure access keys with new credentials**

**$** aws configure -- profile myCLIuser

**Try to list S3 buckets**

$ aws s3 ls - - profile myCLIuser

You can’t access cause there’s no access

**List all the policies:**

$ aws iam list-policies

**Copy the s3 read-only-access:**

arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess

**Attach S3 policy to the user:**

aws iam  attach-user-policy --policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess --user-name myCLIuser

**Now try listing buckets:**

$aws s3 ls - -profile myCLIuser

**Now Let’s detach the policy we attached earlier or we can’t delete the user:**

$ aws iam detach-user-policy --user-name myCLIuser --policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess

**Delete the access keys for that user:**

Note that not everyone may delete the access keys therefore having the default profile with admin access is useful.

aws iam delete-access-key --user-name myCLIuser --access-key-id AKIAJ4JWEBIUBPSEJ4XZFQ

**Delete the user:**

aws iam delete-user --user-name sauravCLI

**We can also do a lot more things**

Check out the documentation here: http://docs.aws.amazon.com/cli/latest/reference/iam/index.html

See you in the next lab!