**IAM continued**

* Fix for unable to upload objects is to add the arn to allow it

{

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

"Statement":[

{

"Effect":"Allow",

"Action":[

"s3:Get\*",

"s3:List\*"

],

"Resource":"\*"

},

{

"Effect":"Deny",

"Resource":"arn:aws:s3:::qtlearningiam",

"Action":[

"s3:Delete\*"

]

},

{

"Effect":"Allow",

"Action":"\*",

"Resource":[

"arn:aws:s3:::qtlearningiam",

"arn:aws:s3:::qtlearningiam/\*"

]

}

]

}

* Note:
* Installing necessary softwares on Windows <https://www.youtube.com/watch?v=mRILfUNbsIo&list=PLuVH8Jaq3mLud3sVDvJ-gJ__0zd15wGDd&index=14>
* Install Windows Terminal <https://www.youtube.com/watch?v=qLVn2EvPsYc&list=PLuVH8Jaq3mLud3sVDvJ-gJ__0zd15wGDd&index=11>

**Scenario-2**

* Lets give permission for developers to start or stop any ec2 instances but not any other activities. They should be able to view all ec2 (read only)
* Note: <https://www.youtube.com/watch?v=me2s3mTNwGo&list=PLuVH8Jaq3mLszrC7lv68a0VcrDripW-HK&index=2> to create an ec2 instance
* Lets create an ec2 instance from root account

{

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

"Statement": [

{

"Effect": "Allow",

"Action": "ec2:Describe\*",

"Resource": "\*"

},

{

"Effect": "Allow",

"Action": "elasticloadbalancing:Describe\*",

"Resource": "\*"

},

{

"Effect": "Allow",

"Action": [

"cloudwatch:ListMetrics",

"cloudwatch:GetMetricStatistics",

"cloudwatch:Describe\*"

],

"Resource": "\*"

},

{

"Effect": "Allow",

"Action": "autoscaling:Describe\*",

"Resource": "\*"

},

{

"Effect": "Allow",

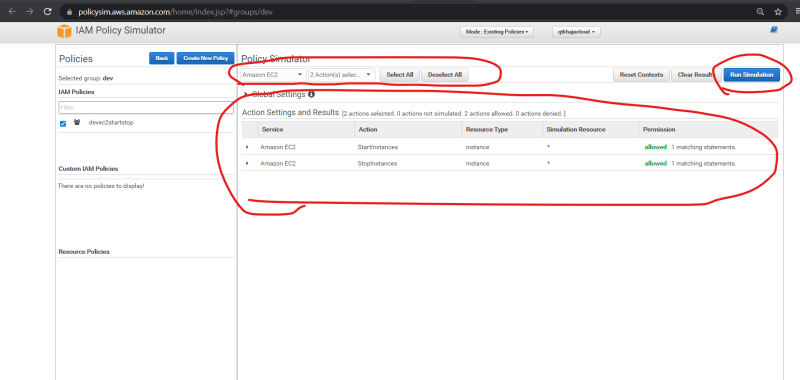
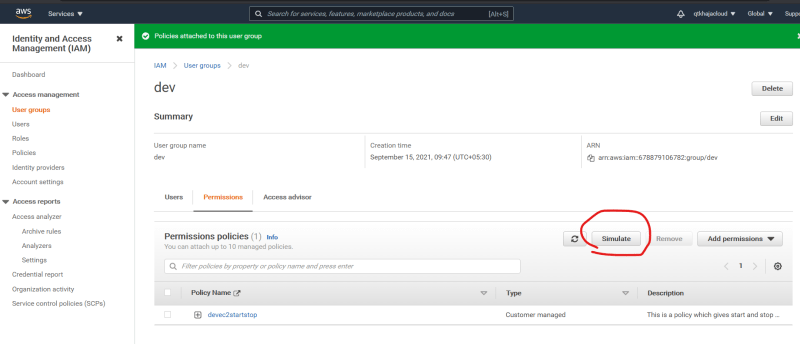
"Action": ["ec2:StartInstances","ec2:StopInstances"],

"Resource": "\*"

}

]

}

* Create a policy and attach it to the developers group 

**Scenario 3**

* In addition to the policy create above Give Permission to Developers to be able to Terminate Instances only if they are in mumbai region. In other regions permission should be denied
* To do this we need to specify conditons in policy <https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_elements_condition.html>
* <https://github.com/asquarezone/awsadministration/commit/b6b3b1cd8e5eb56dc79b8fd4bc3c080a5895e566> for the solution

**Scenario 4:**

* Remove all the policies for QA group
* Create an iam policy for QA group which allows to read all ec2 and start and stop the ec2 instance if the instance type is t2.\*
* Also try evaluating with policy simulator.