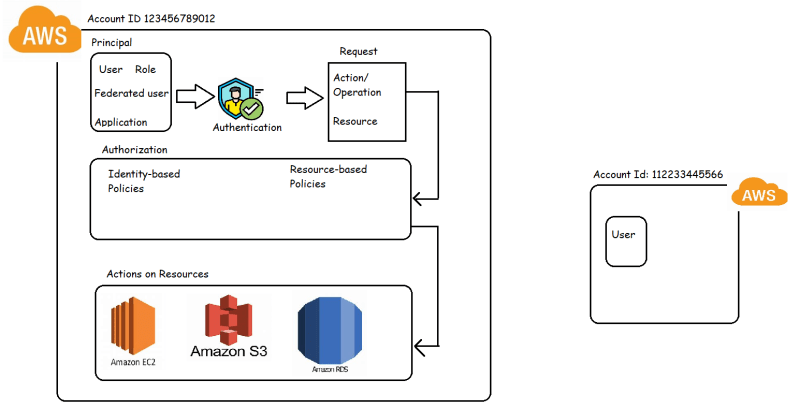
**Understanding How IAM Works**

Basic Workflow 

Terms

* IAM Resources: The user, group, role, policy, identity provider
* IAM Identities: The IAM resource objects used to identify user or group (user,group, roles)
* IAM Entities: IAM users and roles

Principal:

* A principal is a person or application that can make a request for an action on an AWS Resource.
* Principal is authenticated as AWS account root user or IAM Entity to make request to AWS.
* Federated users are also supported to make request for access to AWS Resource.

Request: When a prinicipal tries to use AWS, then a request is sent to AWS with the following information

* Actions or operations
* Resources
* Principal

**IAM Policy Structure**

<https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_grammar.html>

Basic Syntax

{

"Version" : ("2008-10-17" | "2012-10-17"),

"Id": "<policy id>",

"Statement" : [

{

"Sid": "<statement id>,

"Principal": "",

"Effect": "<Allow/Deny>",

"Action": [] // list of actions to be allowed or denied,

"Resource": [] //list of resources on which the Actions are to be allowed /denied

}

]

}

How to get actions on AWS Resources?

<https://docs.aws.amazon.com/service-authorization/latest/reference/reference_policies_actions-resources-contextkeys.html>

In AWS when we create any resource it will have ARN (Amazon Resource Name)

The default effect is Deny for all the actions and resources not covered in IAM policy

In IAM whenever there is conflict between Allow and Deny, Deny always wins

{

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

"Statement": [

{

"Effect": "Allow",

"Action": "s3:\*",

"Resource": "\*"

},

{

"Effect": "Deny",

"Action": "s3:\*",

"Resource": "\*"

}

]

}

If we apply above policy to a user, his s3 access is denied

To write Policies, we need to

know about actions

know about resource ids

Scenario1:

I have an s3 bucket qtlearningiam

I want to give access to qa team to do everything on qtlearningiam apart from delete

Solution to Scenario 1:

Lets find the ARN for s3 bucket <https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazons3.html#amazons3-resources-for-iam-policies>

ARN: arn:aws:s3:::qtlearningiam

Lets try to create a policy based on AWS S3 Read only access

{

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

"Statement": [

{

"Effect": "Allow",

"Action": [

"s3:Get\*",

"s3:List\*"

],

"Resource": "\*"

}

]

}

To find actions <https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazons3.html#amazons3-actions-as-permissions>

We have concluded the following should be the policy

{

"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",

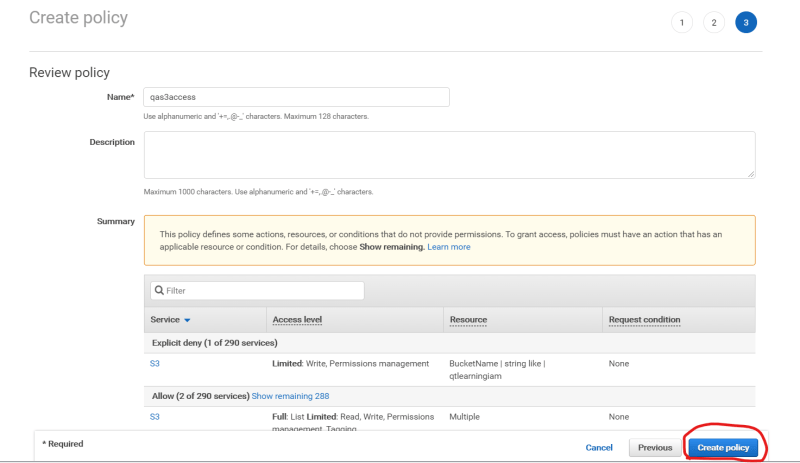
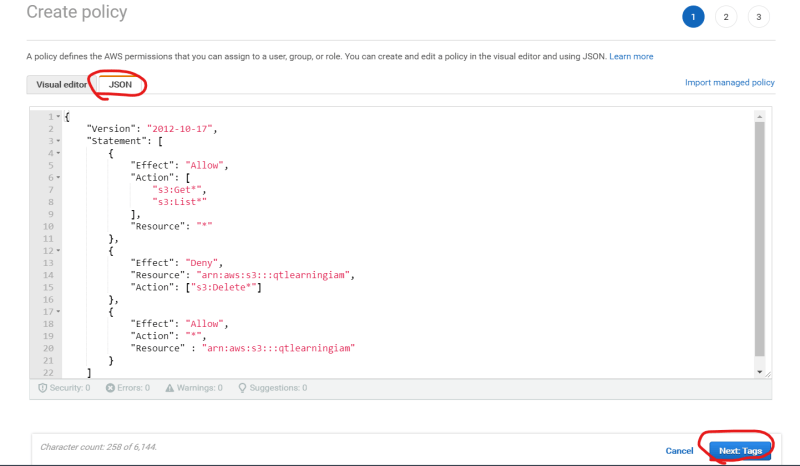
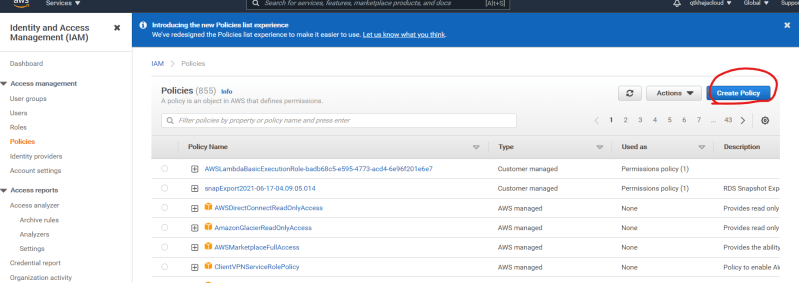
"Action": "\*",

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

}

]

}

Now lets create an IAM Policy 

Let’s assign this policy to qa group and verify how it works

We have observed bucket actions on s3 bucket qtlearningiam are ok but we are not able to perform some actions which we expect to work

To deal with this kind of issues, we would be policy simulator from next session.