IAAS ACADEMY

IAM Authorization & Policies

Amazon Web Services

IAM Components

Authorization

Authorization is process of specifying privileges in *policies* which determine what actions a principal can or cannot perform on the AWS environment.

Policies

Policies are basically permissions to enable you to perform specific task on the AWS platform, either interactively or using API actions. Policies attached to users, groups or roles to grant or deny them the required level of access.

Policy Documents are created in JavaScript Object Notation (JSON). This is a key value pair of an attribute with an associate value.

- Note that Values can be nested.

IAM Components

Policy Document Components

Policy documents contain one or more permissions and each permission defines:

- Effect – Allow or Deny
- Service – Applying the permission to a specific service
- Resource – specify the Amazon Resource Name (ARN) of particular AWS infrastructure for which this permission applies. Format of ARN is usually:
    - “arn:aws:service:region:account-id:[resourcetype:]resource”
        - E.g. arn:aws:S3:us-west-1:589658964521:my_business_proposals/”
- Action – specify the exact action that the permission allows or denies. Note you can list out all the actions in a list or use wildcards
- Condition (Optional) – Define one or more conditions that limit the action by the permissions. For example, you can grant the permission to write files to an S3 bucket, but limit this action so that it is restricted to a particular source IP Address

IAM Components

Example Policy

Amazon S3 ReadOnlyAccess

```
        {
           "Version": "2012-10-17",
           "Statement": [
                {
                   "Effect": "Allow",
                   "Action": [
                                        "s3:Get*",
                                         "s3:List*"
              ],
              "Resource": "*"
            }
          ]
}
```

IAM Components

Creating Policies

- Copy an AWS Managed Policy and customize
  - Start with an AWS Managed Policy, then customize it to fit your needs.
- Policy Generator
  - Use the policy generator to select services and actions from a list and create your own policy
- Create Your Own Policy
  - Use the policy editor to type or paste in your own policy.

IAM Components

Policy Grammar

Policy Validator automatically examines your existing IAM access control policies to ensure that they comply with the IAM policy grammar.
A policy is a JSON document written using the IAM policy grammar. It defines access permissions for the AWS user, group, or role you attach the policy to. If the Policy Validator determines that a policy is not in compliance with the grammar, it prompts you to fix the policy. Policy Validator is only available if you have non-compliant policies

Note:

- You cannot save any new or updated policies that do not comply with the policy syntax
- The policy validator only checks JSON policy syntax and grammar. It does not validate that your ARNs, action names, or condition keys are correct.

IAM Components

Multiple Permissions

Like many Identity and Access management services it is possible that multiple permissions can be granted to a principal for access to a given resource or service. Sometimes this will create conflicting permissions and AWS resolves these as follows:

- Initially all requests are denied
- All policies are analysed – Deny will always override an Allow
- If there are no specific Deny and there is a specific 'Allow', then the request is allowed
- If there are no specify Allow or Deny, then by default the request is denied

IAAS ACADEMY

Next Video

Hands-On-Labs – IAM Policies

Amazon Web Services