Advanced IAM

If you are studying for AWS Developer Associate Exam, this guide will help you with quick revision before the exam. it can use as study notes for your preparation.

Dashboard | Other Certification Notes

Advanced IAM

Authorization Model Evaluation of Policies

1. If there is an explicit DENY condition in the policy, end decision and DENY access
2. If there is an ALLOW condition, end decision with ALLOW access
3. Else DENY

- If there is both an explicit DENY and explicit ALLOW condition, DENY wins because it gets executed first

IAM Policies and S3 Bucket Policies

- IAM Policies are attached to users, roles and groups
- S3 Bucket policies are attached to buckets
- When the evaluations happens, if an IAM Principal can perform an operation on a bucket, the union of its assigned IAM Policies and S3 Bucket Policies will be evaluated
- Example1:
  - IAM Role attached to EC2 instance, authorizes RW on “my_bucket”
  - No S3 Bucket Policy attached
  - EC2 instance can read and write to “my_bucket” because of the attached IAM Role
- Example2:
  - IAM Role attached to EC2 instance, authorizes RW on “my_bucket”
  - S3 Bucket Policy explicitly denies the access from the IAM Role
  - EC2 can not read and write from the bucket because explicit deny has higher priority then the explicit allow
- Example3:
  - IAM Role attached to EC2 instance, no S3 bucket permissions
  - S3 Bucket Policy explicitly allows RW to the IAM Role
  - EC2 instance can read and write to the bucket, union policy has the read write access

Dynamic Policies with IAM

- How do we assign each user a `/home/<user>` folder in S3 bucket?
- Option 1:
  - Create policies for each user, every time we create an user we create a policy (DOES NOT SCALE!)
- Option 2:
  - Create one dynamic policy with IAM
  - Leverage the special policy variable **${aws:username}**

Inline and Managed Policies

AWS Managed Policies

- Maintained by AWS
- Good for power users and administrators
- Updated in case new services are launched or new API calls are added
- Examples: AmazonReadOnlyAccess, AmazonS3FullAccess, AmazonDynamoDBFullAccess, AWSLambdaExecute, ...

- IAM Role attached to EC2 instance, no S3 bucket permissions
  - S3 Bucket Policy explicitly allows RW to the IAM Role
  - EC2 instance can read and write to the bucket, union policy has the read write access

Dynamic Policies with IAM

- How do we assign each user a `/home/<user>` folder in S3 bucket?
- Option 1:

    - Create policies for each user, every time we create an user we create a policy (DOES NOT SCALE!)
- Option 2:
    - Create one dynamic policy with IAM
    - Leverage the special policy variable **${aws:username}**

Inline and Managed Policies

    - IAM Role attached to EC2 instance, no S3 bucket permissions
    - S3 Bucket Policy explicitly allows RW to the IAM Role
    - EC2 instance can read and write to the bucket, union policy has the read write access

Dynamic Policies with IAM

- How do we assign each user a `/home/<user>` folder in S3 bucket?
- Option 1:
    - Create policies for each user, every time we create an user we create a policy (DOES NOT SCALE!)
- Option 2:
    - Create one dynamic policy with IAM
    - Leverage the special policy variable **${aws:username}**

Inline and Managed Policies

AWS Managed Policies

- Maintained by AWS
- Good for power users and administrators