AWS S3

Nguyễn Hàn Duy

handuy1992@gmail.com

S3 Bucket policy

Bucket policy

- Tương tự IAM policy, nhưng gắn với bucket
- Gồm các ALLOW/DENY rules áp dụng trong same/different account
- Nếu ALLOW và DENY rule cùng tác động đến 1 resource: DENY rule sẽ được áp dụng high priority
- Áp dụng cho cả anonymous principal (user không thuộc AWS).

IAM policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

Principa: cho ai đc truy cập

S3 bucket policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicRead",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
        }
    ]
}
```

Bucket policy use cases

- Cấu hình static web hosting
- Cross-account access
- Tham khảo:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/example-bucket-policies.html

Static web hosting on S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicRead",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
            ]
        }
    ]
}
```

Give cross-account access

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccount",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::ACCOUNT-ID:root"
                ]
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        }
    ]
}
```

Allow all except one bucket

https://sample-bucket-policy-515462467908.s3.ap-southeast-1.amazonaws.com/sample.json