Identity and Access Management (IAM)

Capacity Development Series by Chate Sat: Episode 3
18 August 2019
Seed Space, Yangon, Myanmar

Saw Winn Naung

#whoami

former system engineer

An information security engineer

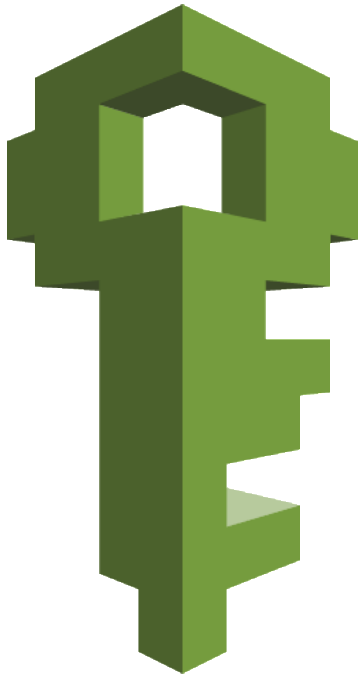
Devops enthusiastic

Identity and **A**ccess **M**anagement (IAM)

- AWS IAM is one of amazon service control who can control what resources
  - User swn can create ec2 instance
  - Instance i-**** can read blah blah s3 bucket

IAM Features

- Enhanced Security
- Granular Control
- Temporary Credential
- External identity system (Google , Open ID Connect)
- Integrated with many AWS services
- Multi-factor authentication (MFA)
- Free to use



Root User

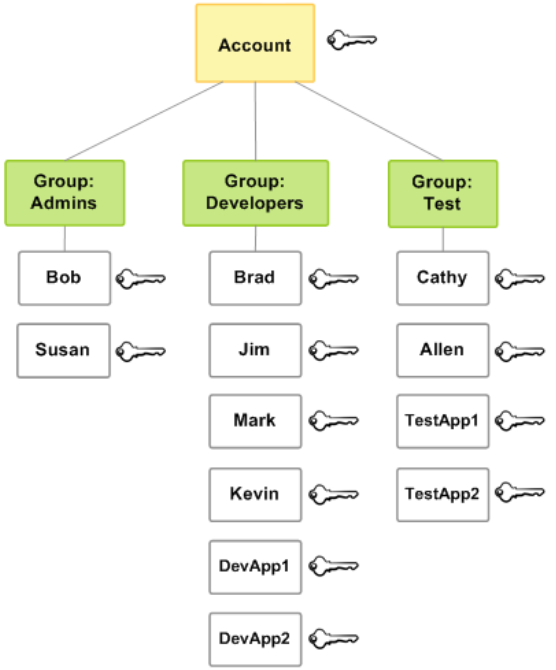
- The Identity used to login AWS account
- Full Access (root user)
- Do not use this account not for everyday tasks
- Enable MFA
- Do not use your amazon shopping account

User

- A person or application that uses it to interact with AWS
- Username and password for AWS console access
- Key-based access for programmatic access
- Have zero access at start

Group

- Collection of IAM Users
- Apply permission to entire users inside the group
- Example; Developer group and Admin group
- Users can be in multiple group



Roles

- 2nd user of AWS IAM, role is similar to an IAM user without credential
- Allow to delegate access to user or services
- For temporary security credential

Role vs User and Group

- Role
  - Short term access
  - Internal and external user
- User
  - Long term access
  - Internal

Policy

- AWS Permission for user , group and role
- Many predefined policy which can modified
- Can use json or visual editor
- Inline and Manage Policy

IAM Policy Structure

```
{
  "Statement":[{
    "Effect":"effect",
    "Principal":"Principal",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

Principal – The Entity that is allowed or denied

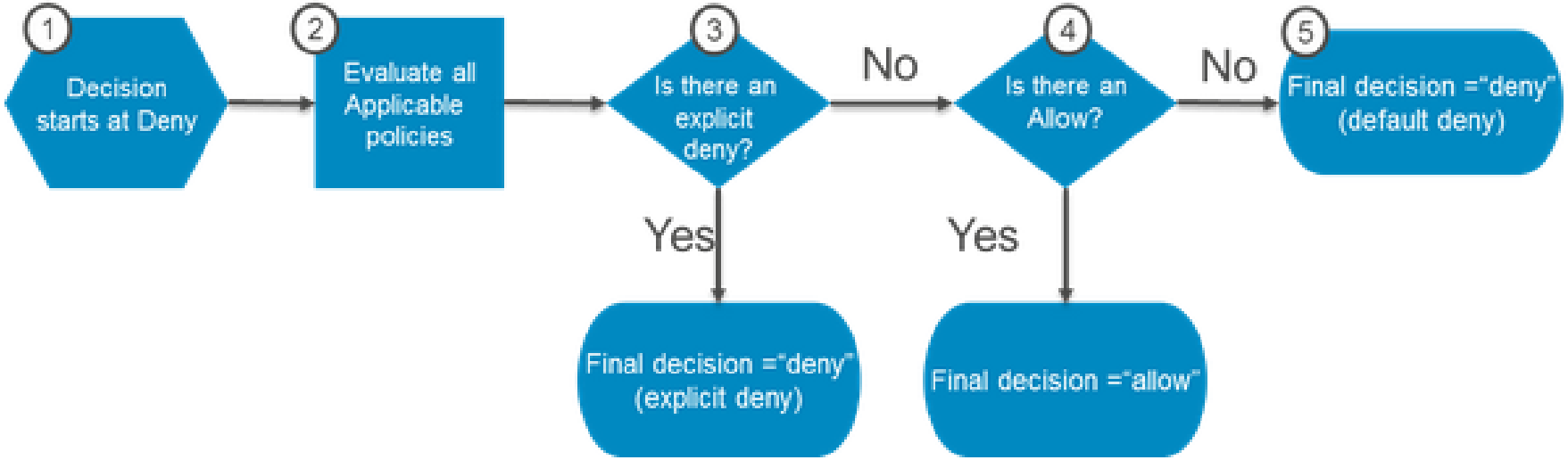
Action – Types of access that allow or deny

Resource – The Amazon Resource names

Condition – Optional conditions

Policy Evaluation

This diagram illustrates the authorization process.

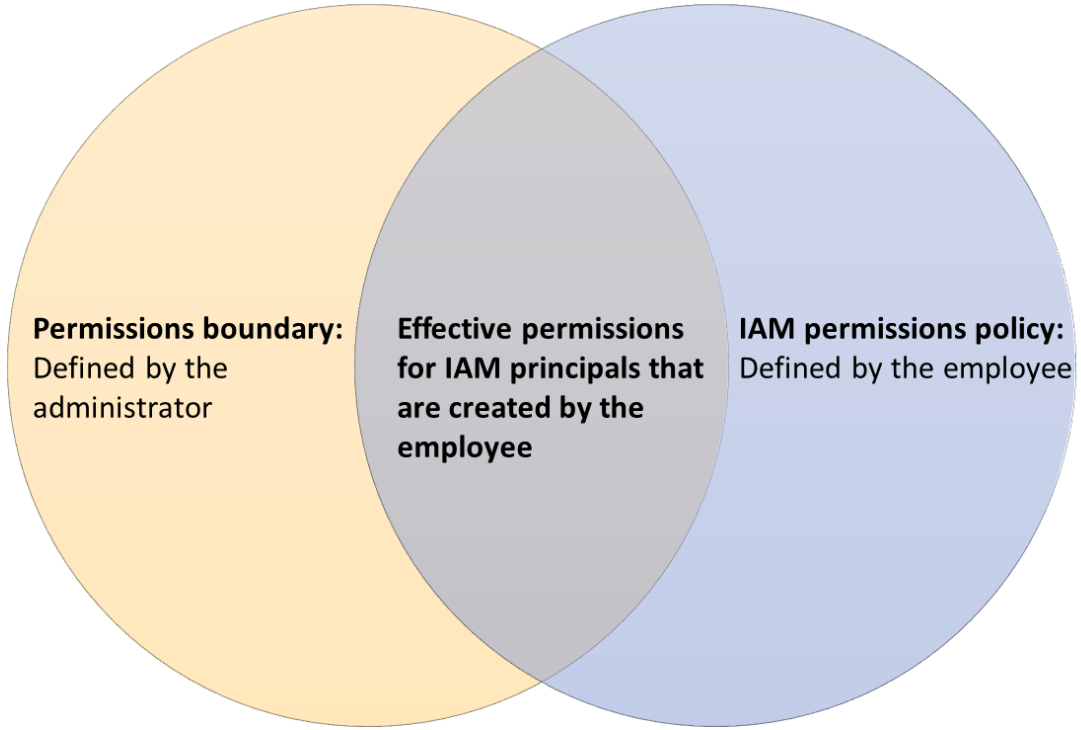


Policy Types and Use Case

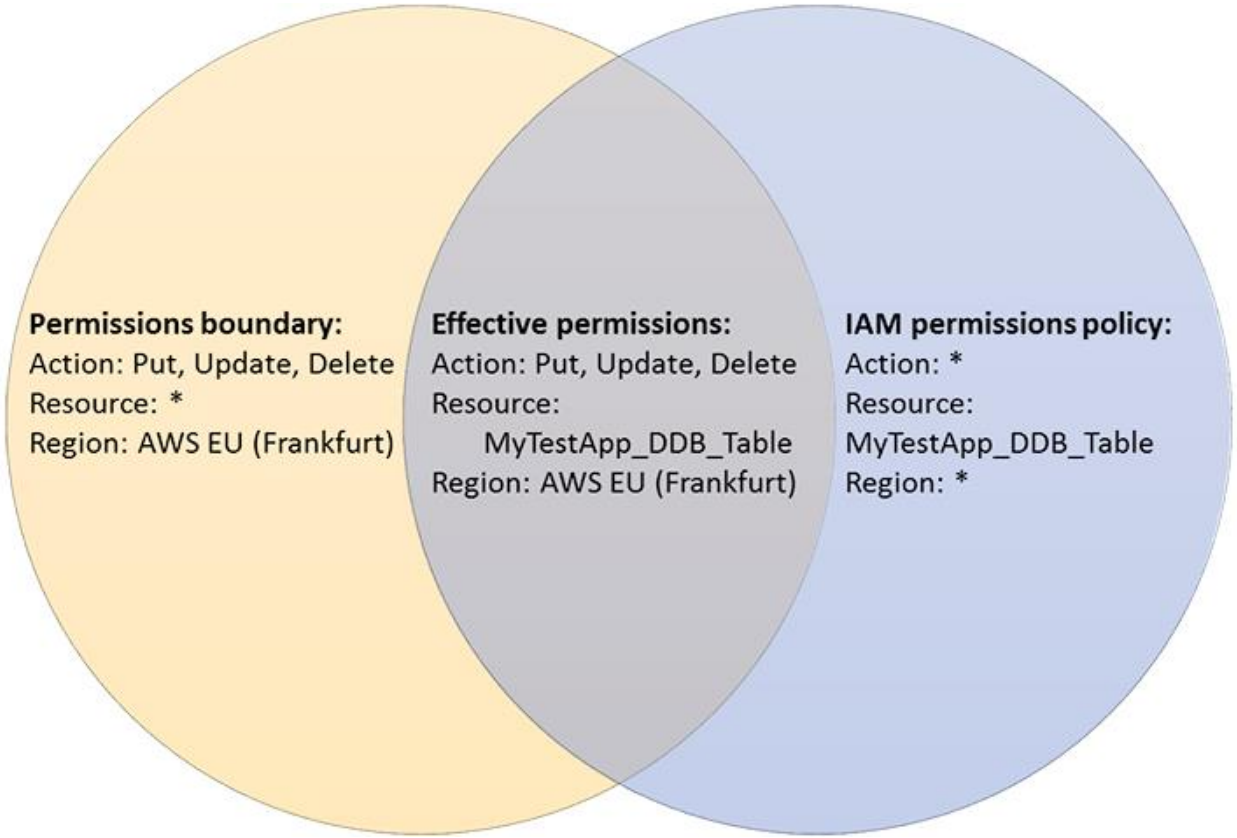
Service Control Policy(SCP)	AWS Organizations
Identity-based policy and Permission boundaries	AWS IAM inline policy and manage policy
AWS Security Token Service (AWS STS)	Reduce general shared permission
Resource based policy	Specific AWS Services
Endpoint Policies	VPC Endpoints

AWS Permission boundaries

- Control the maximum permissions of user can



Permission boundaries Example



Restrict resources creation in a region

```
{
  "Version" : "2012-10-17",
  "Statement" : [
  {
    "Effect": "Allow",
    "Action": [
                "dynamodb:PutItem",
                "dynamodb:UpdateItem",
                "dynamodb:DeleteItem"
     ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:RequestedRegion": "eu-central-1"
        }
    }
  }
]
}
```

Grant a user to perform S3 operations

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::AccountA-ID:user/Dave"
            },
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::examplebucket"
            ]
        },
        {
            "Sid": "statement2",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::AccountA-ID:user/Dave"
            },
            "Action": [
                 "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::examplebucket/*"
            ]
        }
    ]
}
```

Restrict access to services in production

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyServicesNotAccessed",
            "Effect": "Deny",
            "Action": [
                "groundstation:*",
                "gamelift:*"
            ],
            "Resource": []
        }
    ]
}
```


Any Questions?
And Thanks