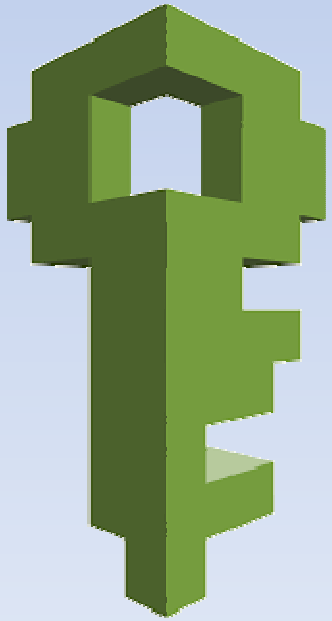
AWS Certified Solutions Architect - Associate

Module 3
AWS Identity and Access Management



Agenda

- What is AWS IAM
- Features
- Identities
- User Types
- How to Access AWS
- Policies Structure
- Role to EC2 Instance
- Request Flow
- Limitations
- Hands-On

What is IAM??

- AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resources for your users.

- You can use IAM to control who can use your AWS resources (authentication) and what resources they can use and in what ways (authorization).

IAM Features

- Shared access to AWS Account
- Identity federation
- Granular permissions
- Identity information for assurance
- Secure access to AWS Resources
- Eventually Consistent
- Mutli-Factor authentication (MFA)
- Free to use

IAM : Identities

Users

Group

Roles

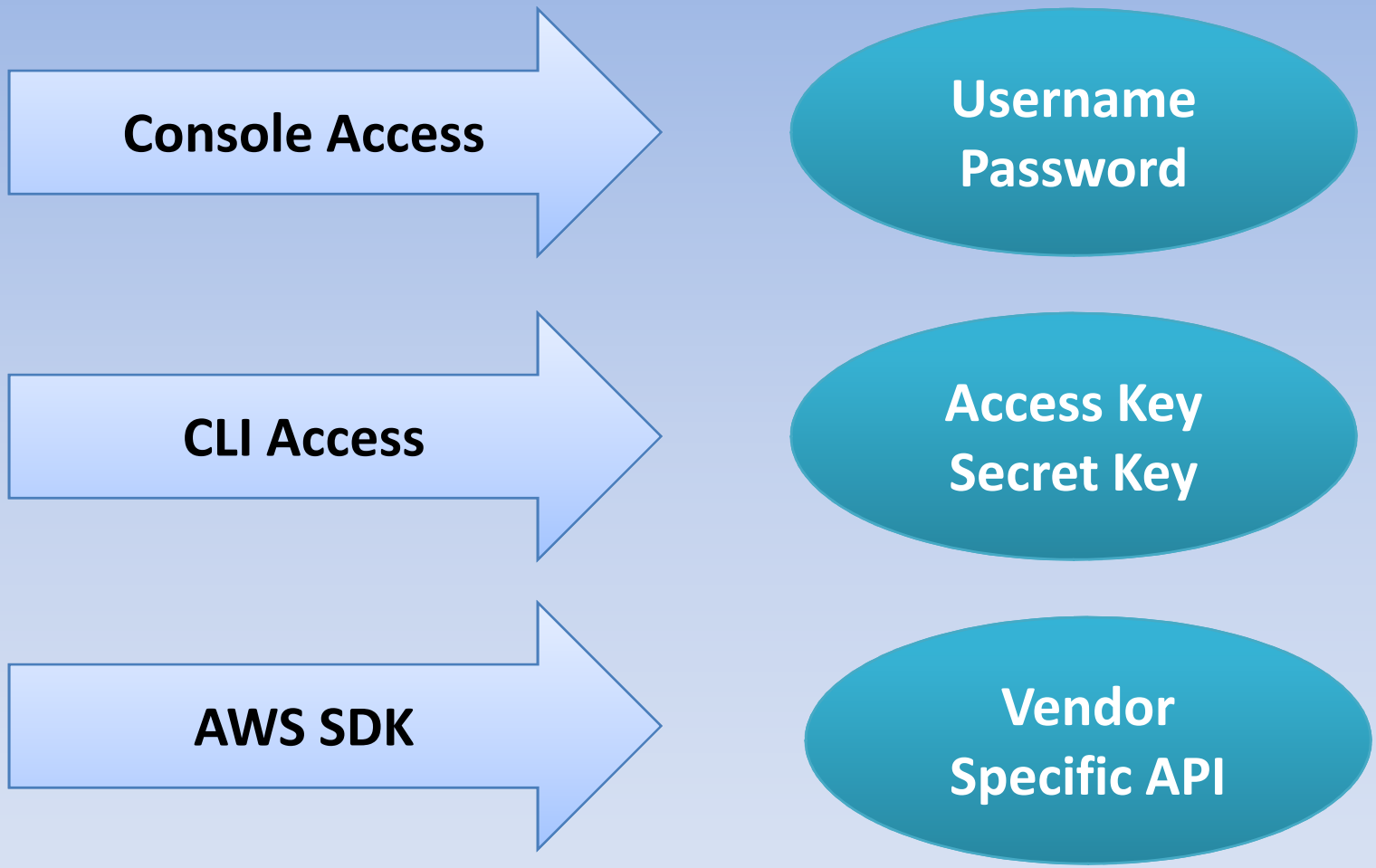
IAM: User types

- **Root User**
  - When you create an AWS account, you create an AWS account root user identity—that is, the email.
  - When you use your root user credentials, you have complete, unrestricted access to all resources in your AWS account.

- **IAM User**
  - IAM users are not separate accounts; they are users within your account.
  - Each user can have its own password for access to the AWS Management Console.
  - An IAM user doesn't have to represent an actual person; you can create an IAM user in order to generate an access key for an application.

- **Federating Existing Users**
  - If your users already have a way to be authenticated—for example, by signing in to your corporate network—you can federate those user identities into AWS.

IAM: Access AWS Account



IAM: Policies Structure

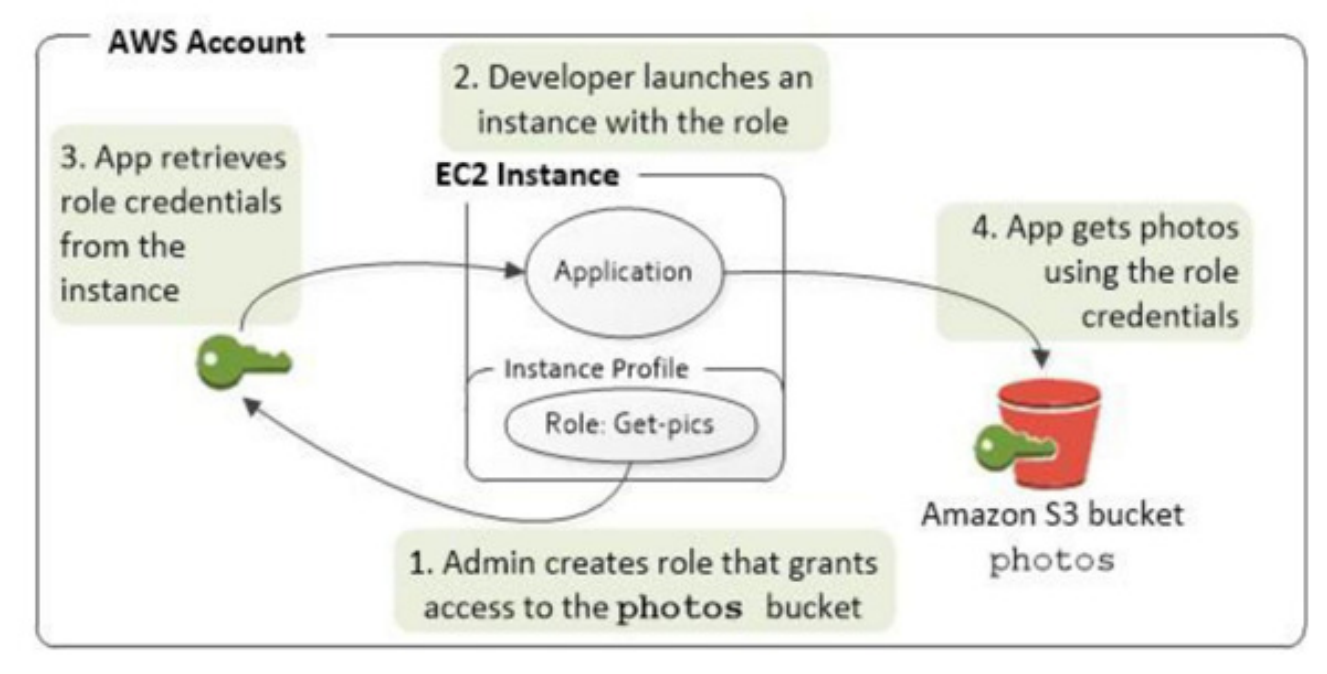
- Each policy is a JSON Document.
- A policy is a document that formally states one or more Permissions
- The policy document includes the following elements:
  - Effect
  - Action
  - Resource
  - Condition (Optional)

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "<SERVICE-NAME>:<ACTION-NAME>",
    "Resource": "*",
    "Condition": {
      "DateGreaterThan": {"aws:CurrentTime": "2017-07-01T00:00:00Z"},
      "DateLessThan": {"aws:CurrentTime": "2017-12-31T23:59:59Z"}
    }
  }
}
```

IAM Role to EC2 Instance

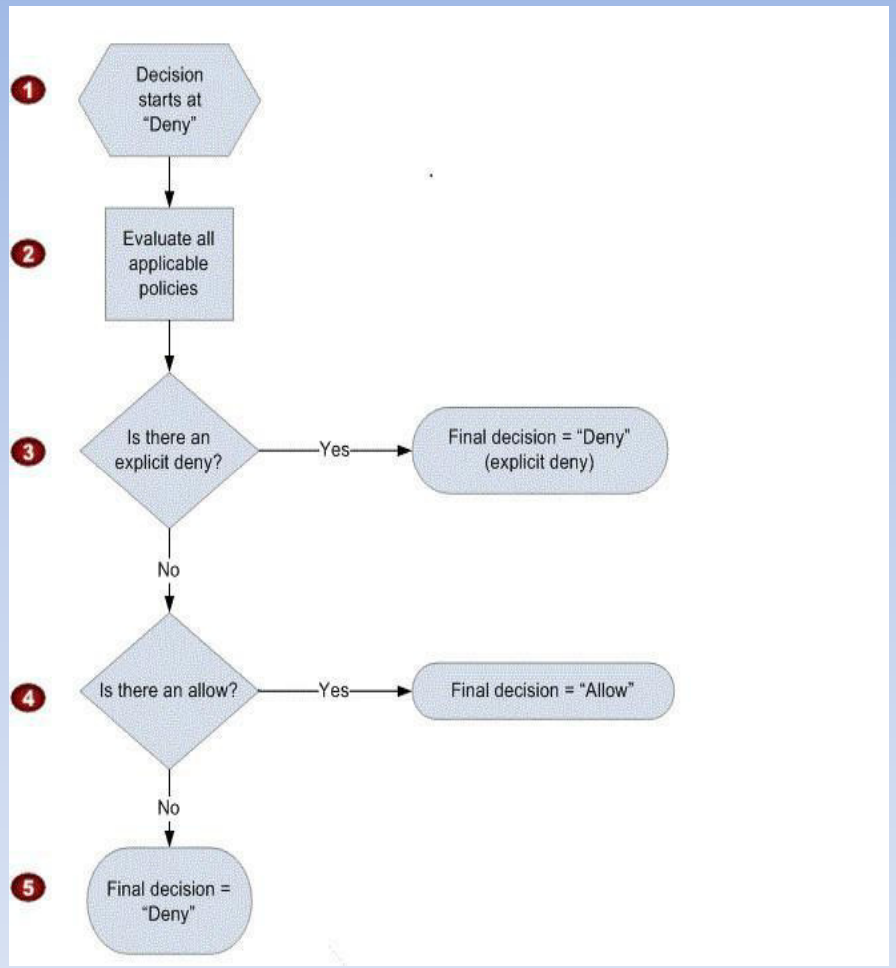
Use an IAM role to manage *temporary credentials* for applications that run on an EC2 instance

The role supplies temporary permissions that applications can use when they make calls to other AWS resources



IAM : Request Flow

- When a request is made, the AWS service decides whether a given request should be allowed or denied.
- The evaluation logic follows these rules:
  - By default, all requests are denied.
  - An explicit allow overrides this default.
  - An explicit deny overrides any allows.



IAM Limitation

Resource	Default Limit
Users in an AWS account	5000
Groups in an AWS account	1000
Roles in an AWS account	300
MFA devices in use by an IAM user	1
Access Keys assigned to an IAM User	2
Aliases for an AWS account	1
Groups an IAM user can be a member of	10
Managed policies attached to an IAM user	10
Managed policies attached to an IAM group	10
Managed policies attached to an IAM role	10