AWS Solution Architect Training

Module 03
Identity and Access Management (IAM)

Instructor: Tim Platt, Cloud Solution Architect

Identity and Access Management (IAM)

Identity – Authentication and Authorization

Key Points

- Authentication – prove WHO you are.
- Authorization – WHAT are you allowed to do?

IAM Identities

IAM identities can have permissions attached to them – which allows them to take ACTIONs against RESOURCES – such as launching an EC2 instance, deleting an S3 bucket, etc.

IAM User

Users are human beings
(or should be)

IAM Group (of Users)

We can put Users with similar needs in a Group (of Users)

IAM Roles

Roles are **temporary** credentials
These can be utilized by Users
or Services / Resources / Servers

IAM Policy Example

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowEC2Actions",
            "Effect": "Allow",
            "Action": [
                "ec2:TerminateInstances",
                "ec2:StartInstances",
                "ec2:RunInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

What does this allow someone to do?

It allows them to create (”Run”), start, stop, and delete any EC2 instance in the account

IAM Roles

IAM Role

Key Points

- An IAM Role is an Identity
- It can be given permissions to do things
- The role can be used by:
  - Human beings (IAM Users)
  - AWS Services (Such as AWS Lambda, EC2, etc.)
  - By our application code (Python, JavaScript, C#, Java programs that we write
  - Used in ”Identity Federation” scenarios (Single Sign On)
  - Can be used to access resources in different AWS accounts (Cross-Account access)

SUPERPOWER: The Role provides a set of TEMPORARY credentials – they expire in a very short amount of time – and security teams LOVE this

Links

- AWS IAM User Guide: https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html
- IAM Best Practices (Know these for the exam!): https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html
- Identities (User, Role, User Group): https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html
- IAM Policy Examples: https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_examples.html