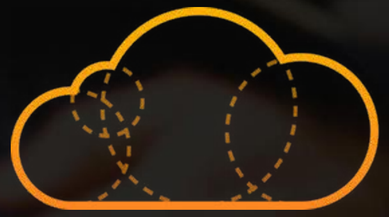
Identity Access Management 101 - Summary



A CLOUD GURU

What have we learned so far?

A CLOUD GURU

- IAM consists of the following:
- Users
- Groups (A way to group our users and apply polices to them collectively)
- Roles
- Policy Documents

```
{"Version": "2012-10-17",
  "Statement":
  [
    {"Effect": "Allow",
      "Action": "*",
      "Resource": "*"}
  ]
}
```

What have we learned so far?

A CLOUD GURU

- **IAM is universal.** It does not apply to regions at this time.
- The “root account” is simply the account created when first setup your AWS account. It has complete Admin access.
- New Users have **NO permissions** when first created.
- New Users are assigned **Access Key ID & Secret Access Keys** when first created.
- These are not the same as a password, and you cannot use the Access key ID & Secret Access Key to Login in to the AWS Management Console.
- You can use this to access AWS via the APIs and Command Line, however.

What have we learned so far?

A CLOUD GURU

- You only get to view Access key ID & Secret Access Key once. If you lose them, you have to regenerate them. So, save them in a secure location.
- Always setup Multifactor Authentication (MFA) on your root account.
- You can create and customise your own password rotation policies.