AWS

Identify & Access Management (IAM)

what is it?

Allows you to securely control individual and group access to your resources. Users by default have no access until you assign them a role.

users

If you are setting up an AWS account for the first time you will begin with the root user and full administrative rights. Your first step should be creating a new user rather than using the root user for day to day activities.

After that you can create user accounts for anyone else who needs access to your account.

Users can have any combination of credentials:

- AWS access key
- X.509 certificate
- SSH key
- Password for web app logins
- MFA device

Default limits:

- 5000 per account
- 50 tags per user
- 5 SSH keys per user

AWS

Identify & Access Management (IAM)

groups

Groups are a collection of users. This could be a group of marketing users who need access to campaign data, finance users who need more sensitive data or customer service users who need access to customer data.

Default limits:

- 300 per account
- An IAM user can be a member of 10 groups

roles

This is what defines the set of permissions your users and services have. This where you decide if the 'marketing' role needs to be able to read/write to an S3 bucket, read/write to the RDS, and nothing else.

Default limits:

- 1000 per account
- 50 tags per role

policies

When they are first created users have no permissions. These are added by creating and attaching policies.

- **Managed Policies** - fixed policies provided by AWS
- **Customer Managed Policies** - policies created by the customer
- **Inline Policies** - policies which are directly attached to a user

AWS

Identify & Access Management (IAM)

creating policies

Policies can be created either using the UI or by writing JSON with what you need.

Default limits:

- 1500 customer-managed policies
- 10 policies attached to a user or role

policy example

There are three parts to the policy at its most basic level:

- **Version** - the current version of the policy language.
- **Action** - in this case to Create and Delete buckets
- **Effect** - in this case to 'Allow'. This is by default set to 'deny' in the same way that users have no permissions by default when they are created.
- **Resource** - the syntax here is used to determine the Amazon Resource Name (ARN). In this case my_new_bucket in S3.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   Action": [
    "s3:CreateBucket",
    "s3:DeleteBucket"
   ],
   "Effect": "Allow",
   "Resource": "arn:aws:s3:::my_new_bucket"
  }
 ]
}
```