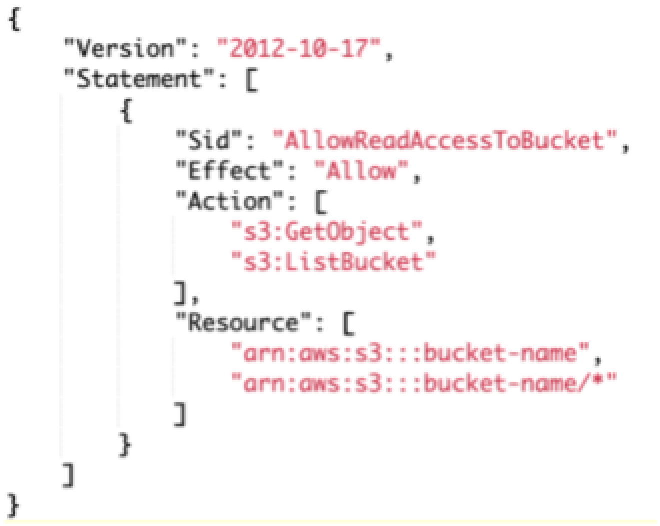
IAM Policies

- IAM permissions are granted via "policies"
- A policy defines who can access a resource and what actions are allowed on that resource
- Each IAM policy is composed of actions, resources, and principals
  - principal => either an IAM user or a role
  - actions => what the principal can / can't do
  - resources => where can the principal perform these actions
- There are three types of IAM policies:
  - "Built-in" policies provided by AWS
  - "Custom" policies created by AWS users
  - "Inline" policies



```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowReadAccessToBucket",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

NEXT