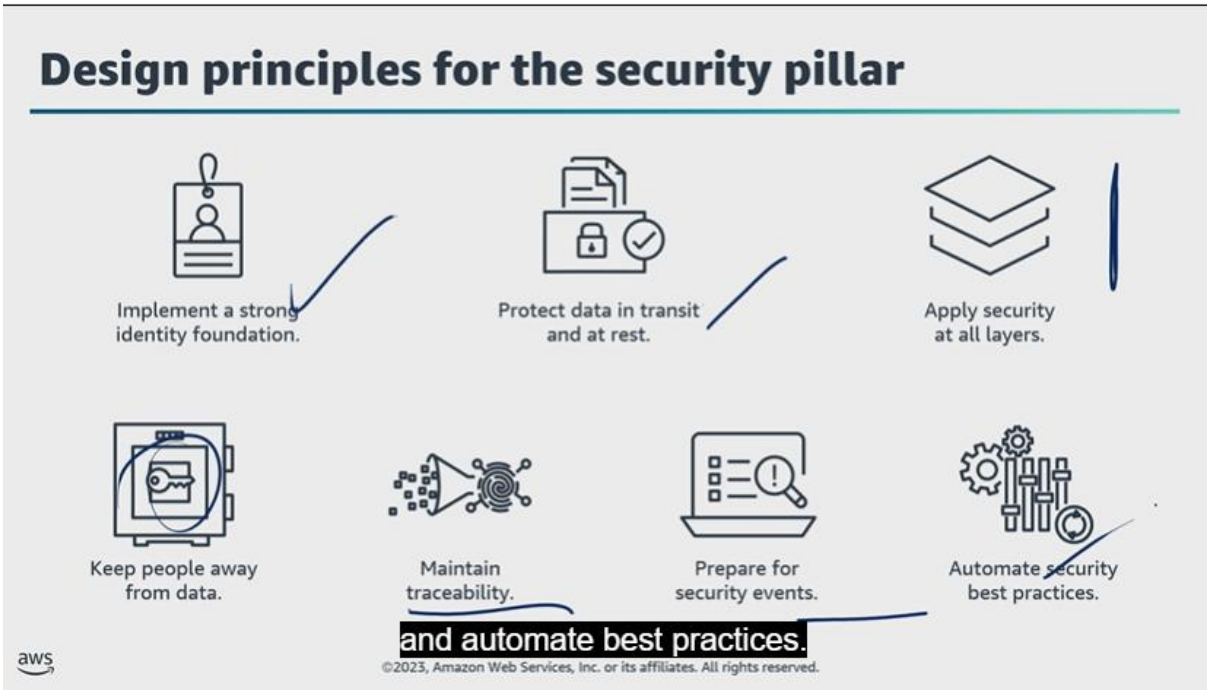
Securing Access

AWS = Security of the cloud

You = security in the cloud

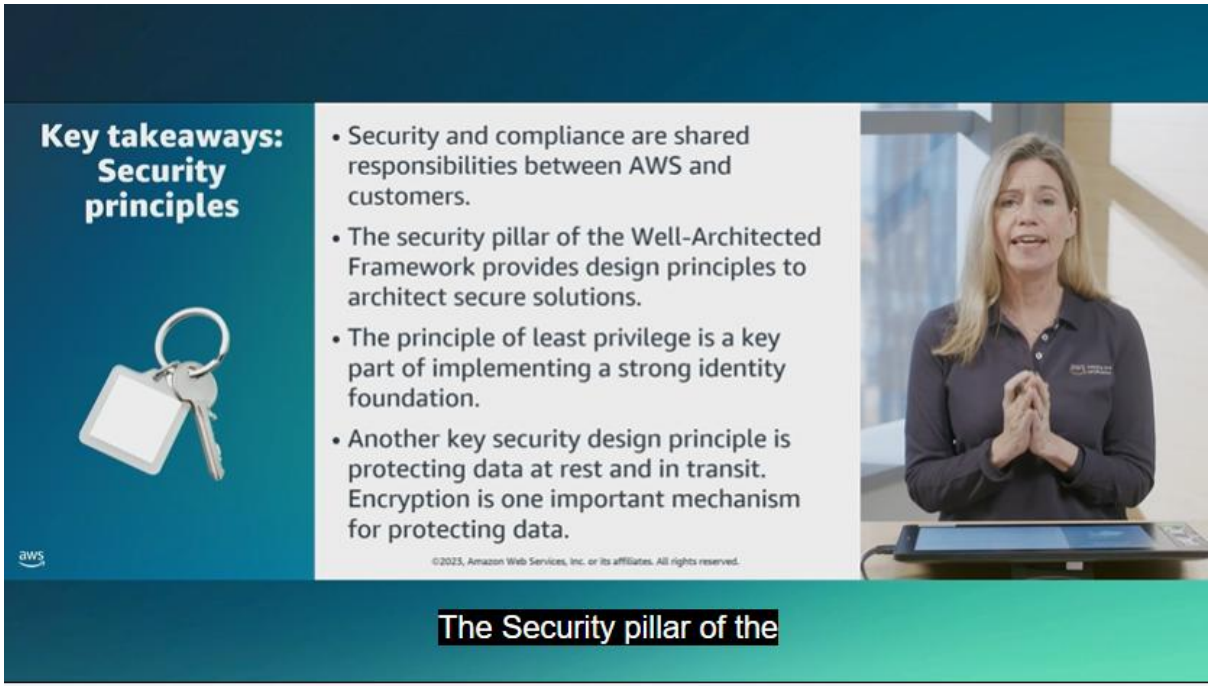
Security ada di 6 pilar yang lalu.



S3 Bucket = permission diberikan tergantung ke orangnya.

Cryptographic protocol.

Amazon S3 = yang bisa encryption.



Authenticating and securing access

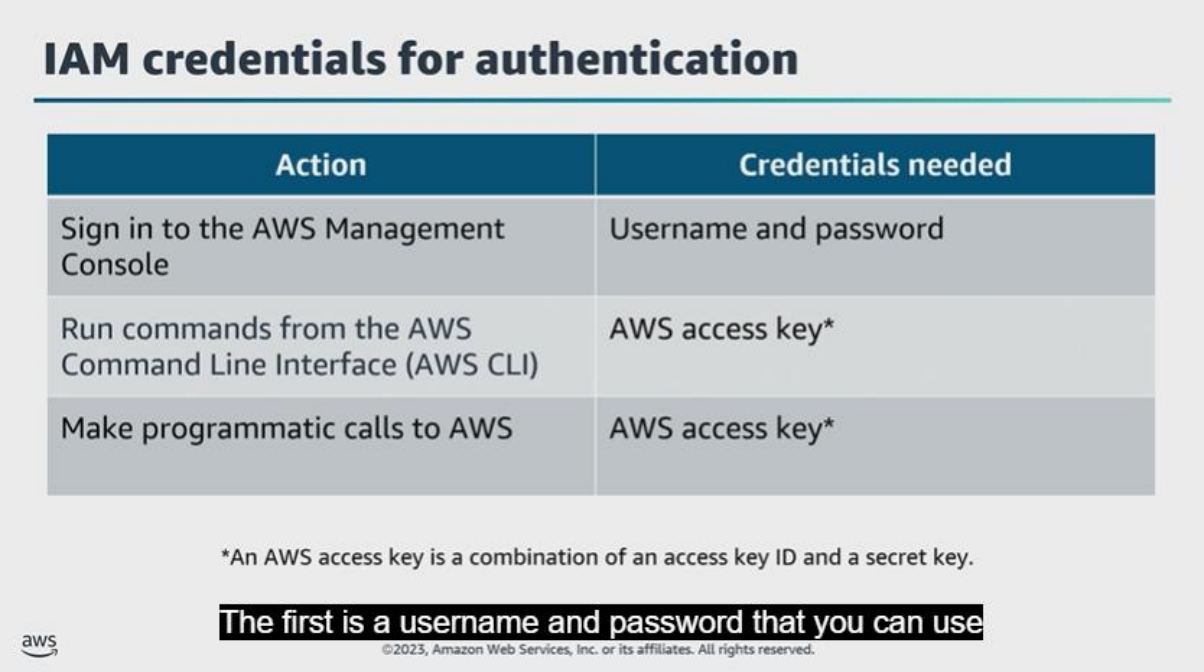
Authentication = memastikan siapa saja yang bisa masuk ke server.

Authorization = apa yang diizinkan ke user.

IAM resource = Things stored in IAM

IAM entity = Resource can used for authenticated

IAM identity = Can be authorized to do something



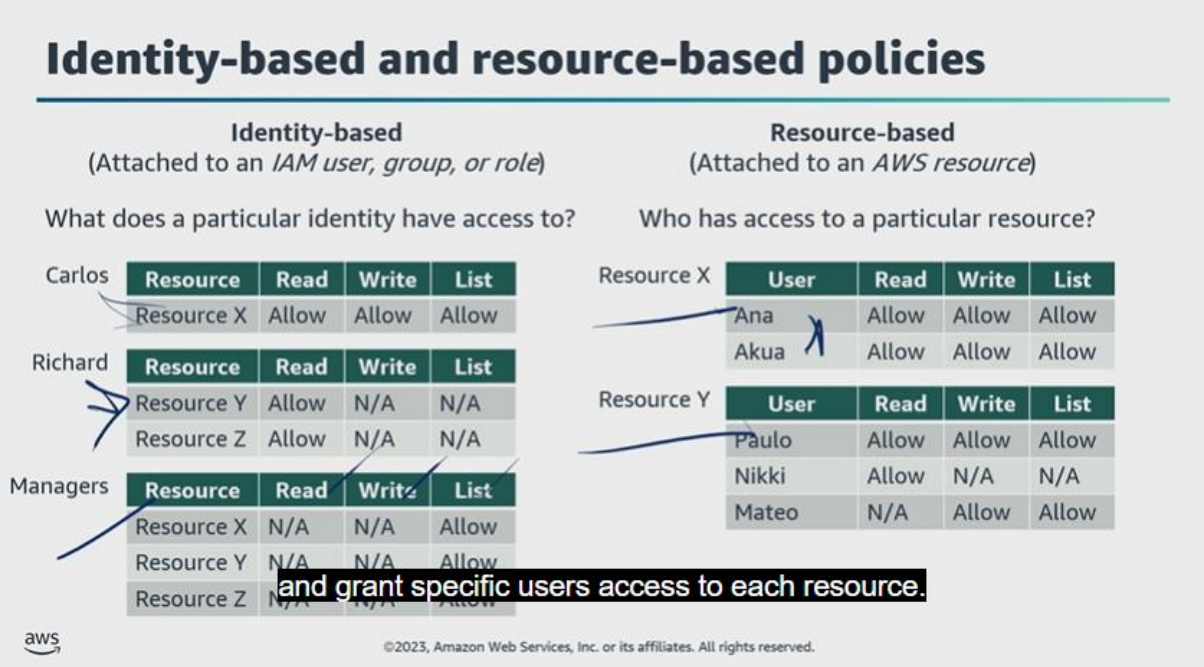
AWS access key = **Access key id** and **secret key id**

Protect root user (pakai root yang tidak bisa dipakai orang lain)

Authorizing Users

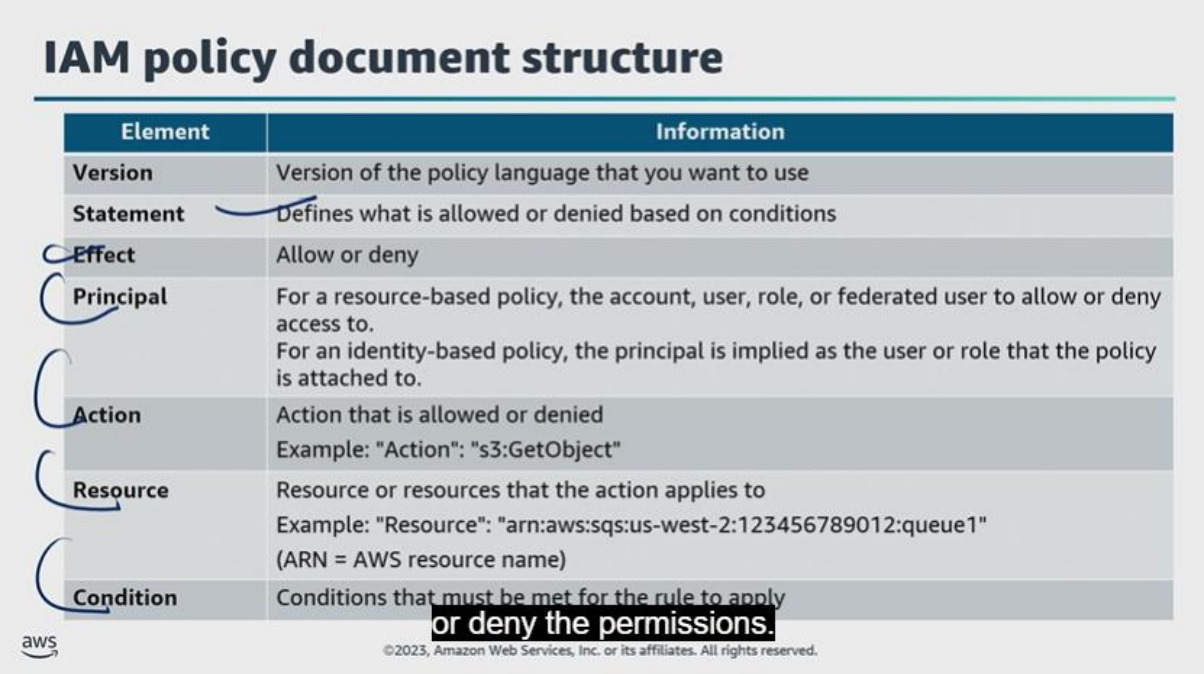
Policy defines the permissions (allowed/denied) default = denied

- Identity based (per user)
- Resource-based (per resource)

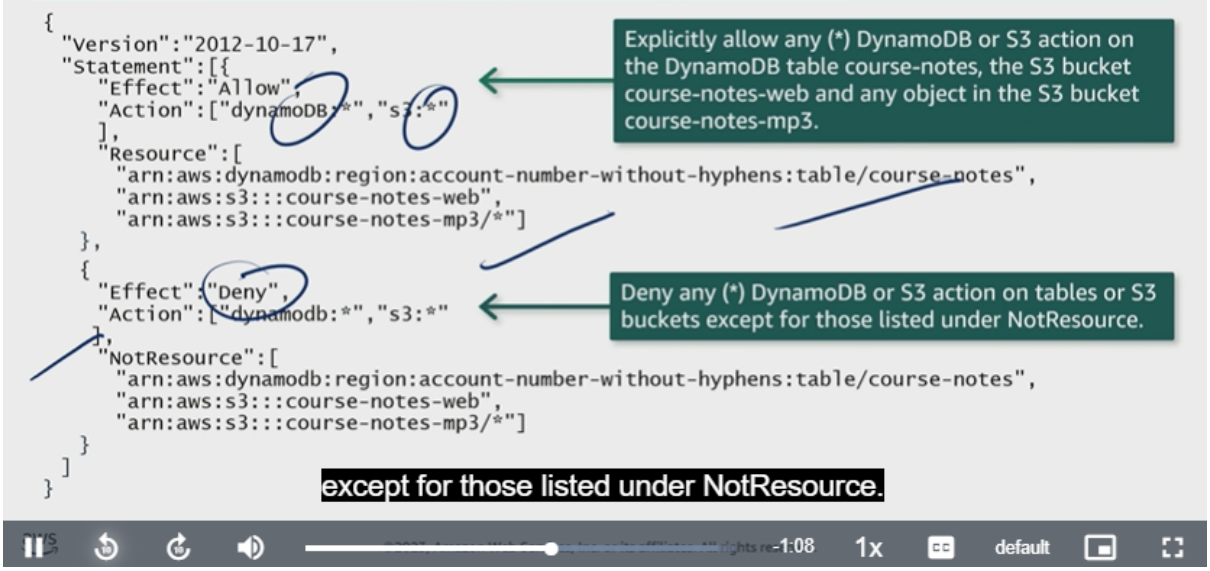


Policy: get, put, list / read, write, list

Parts of IAM Policy (stored in JSON documents) = effect, action, resources.



Example: resource-based policy



except for those listed under NotResource.

Example: Identity-based policy

```
{
 "Version":"2012-10-17",
 "Statement":[{
   "Effect":"Allow",
   "Action":[
     "iam:*LoginProfile",
        "iam:*AccessKey*",
        "iam:*SSHPublicKey*"
    ],
    "Resource":[
     "arn:aws:iam::account-id-without-hyphens:user/${aws:username}"
  }
}
```

The Action element lists all the actions that are allowed by the Effect: Allow.

The Resource element lists the AWS resources that the allowed actions can be performed on.

that might be attached to a user, group or role.

Example: Cross-account, resource-based policy

Policy created by account A

```
{
    "Version": "2012-10-17",
    "Statement": {
      "Sid": "AccountBAccess1",
        "Principal": {"AWS": "111122223333"},
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": [
            "arn:aws:s3:::DOC-EXAMPLE-BUCKET,
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*
        ]
    }
}
```

Account number of Account B

Allow account B to take any S3 action on the DOC-EXAMPLE-BUCKET.