Identity and Access Management (IAM)

- Global Service
- Root account - default, shouldn't be used or shared
- Users - people within organization, can be grouped.
- Groups can only contain users, not other groups.
- Users don't have to belong to a group & can be part of multiple groups

IAM: Permissions.

JSON Docs - Policies.

eg.

```
{"version": "2012-10-17",
"Statement": [
    {"Effect": Allow
     "Action": "ec2:Describe"
     "Resource": "*"
      :
      :
    }
]
}
```

Least Priviledge Principle: dont give more permissions than what a user needs.

Inline policy - only attached to a single user

Policy structure:

```
{
    "Version": "2012-10-17"          → policy language version
    "Id": "S3-Account-Permission"    → identifier (optional)
    "Statement": [
        {
            "Sid": "1"               → Statement id (optional)
            "Effect": "Allow"        → effect of policy, deny, Allow etc
            "Principal": {           → acc/user/role to which policy is applied to
                "AWS": ["arn:aws:iam:1234987:root"]
            }
            "Action": [              → list of actions policy allows or denies
                "S3:GetObject",
                "S3:PutObject"
                ],
            "Resource": ["arn:aws:iam: . . . :root"]
                                     → list of resource to which actions applied to
        }
    ]
}
```

Condition: condition for when policy is in effect (optional).

IAM - Password Policy:

- Strong passw = higher security.
- In AWS, you can set password policy -
  - Set a min pass. length
  - Require specific char types
  - Allow all IAM users to change their own passw
  - Require users to change passw after some time
  - Prevent passw re-use

IAM - Multifactor Authentication (MFA)

- MFA = password you know + security device you own
- You want to protect atleast your root accounts & IAM users.

MFA device options:-

1) Google Authenticator (phone only)
2) Authy (Multi-device) - support for multiple tokens on a single device

virtual MFA device

3) Universal 2nd factor (U2F) Security Key
   - physical device
   - eg - Yubikey by Yubico
   - supports multiple users & roots

Others:

- Hardware key fob MFA Device
- —u————————— for AWS GovCloud (US).

How users can access AWS? - 3 options

1) AWS Management Console (passw + MFA)
2) AWS CLI : protected by access keys
3) AWS SDK : for code : protected by access keys

Users manage their own access keys, just like passw, dont share.

* aws --version
* aws configure
  Access key ID :
  Secret Access key :
  Default region:
  default o/p format: enter.

* aws iam list-users : lists all users

AWS cloudshell: (not available in all regions).

aws iam list-users --region us-west-1

default is region u are currently in

- All files you create stay
- You can download/upload files.

IAM Roles for Services

- Some AWS service will need to perform action on your behalf.

- To do so, we will assign permission to AWS service with IAM Roles.

Common roles: EC2 Instance Roles, lambda fn roles, Roles for Cloudformation

IAM Security Tools:

IAM credential report: a report that lists all your account's users and status of their various credentials.

IAM Access advisor: - shows service permissions granted to a user & when they were last accessed.
- You can use this information to revise your policies.

Shared Responsibility Model for IAM:

AWS	You
- Infrastructure (global network security)	- Users, Groups, Roles, Policies management and monitoring
- Configuration & vulnerability analysis	- Enable MFA on all accounts
- Compliance validation	- Rotate keys
	- Use IAM tools to apply appropriate permissions
	- Analyze access patterns & review permissions.