S3

- main building block of AWS
- 'infinitely scaling' storage

- used as a backbone for many websites, in integration too
- EBS snapshots are also stored in S3

S3 Use cases -

- Backup and storage
- Disaster Recovery
- Archive
- Hybrid cloud Storage
- App hosting
- Media hosting
- Data lakes & big data analytics
- Software delivery
- Static website

Buckets - Files (objects) are stored in 'buckets' (dictionaries).

- buckets must have globally unique name
- S3 looks like a global service but buckets are created in a region.
- Naming convention -
  1) no uppercase
  2) no underscore
  3) 3-63 chars long
  4) not an IP
  5) must start with lowercase or number

what can u store

- object (files) have a key
- key is full path.
  prefix + object name.

- There is 'no' concept of directories within buckets.
- just keys with very long names that contain '/'

- max size 5TB = 5000GB
- If uploading >5GB, multipart upload use.

Metadata

tags - (Unicode key/Val pair - up to 10) - used ~~for~~ security/lifecycle

- Version ID.

Create a bucket
- add objects.

Note - if you open object, using object actions you will have a presigned url with ur AWS creds so it opens.
but if u try using public url it will deny access unless you provide public acess.

S3 Security - Bucket Policy.
1) User based: IAM policies - which API calls should be allowed for a specific user from IAM console

2) Resource based -
- Bucket Policies :- bucket wide rules from S3 console - allows cross account.
- Object Access control list - finer grain.
- Bucket Access control list - less common

Note - an IAM user can access S3 if
IAM permissions allow it OR resource policy allows it
AND there is no explicit deny.

3) Encryption : encrypt objects in Amazon S3 using encryption keys

S3 Bucket Policies -
- Json based policies

S3 bucket settings - were created to prevent company data leak

* Use policy generator to add policies
First disable all public access settings.