Contents

[IAM 2](#_Toc517092697)

[What does IAM give you? 2](#_Toc517092698)

[Critical terms 2](#_Toc517092699)

[IAM summary 2](#_Toc517092700)

[S3 3](#_Toc517092701)

[S3 basics: 3](#_Toc517092702)

[S3 objects consists of: 3](#_Toc517092703)

[S3-Storage Tiers/Classes: 3](#_Toc517092704)

[S3 charges: 3](#_Toc517092705)

[Cross region replication 3](#_Toc517092706)

[Lifecycle management: 4](#_Toc517092707)

[CloudFront(CDN) 4](#_Toc517092708)

[Security: 4](#_Toc517092709)

[Encryption: 4](#_Toc517092710)

[Storage Gateway 5](#_Toc517092711)

[CLI: 5](#_Toc517092712)

# IAM

*Essentially, IAM allows you to manage users and their level of access to the AWS console.*

## What does IAM give you?

* Centralized control of your AWS account
* Shared access to your AWS account
* Granular permissions
* Identity Federation (including Active directory, Facebook, Linkedin etc)
* Multifactor Authentication
* Provide temporarily accessfor users/devices and services where necessary
* Allows you to set up your own password rotation policy
* Integrates with many different WAS services
* Suppoorts PCI DSS Compliance

Critical terms***:***

{“Version”:”2012-10-17”,

”Statement”:

[{“Effect”:”Allow”,

”Action”:”\*”,

”Resource”:”\*”}]

}

* Users – end users (think people)
* Groups – a collection of users under one set of permissions
* Roles – you create roles and can then assign to AWS resources
* Policies – a document that defines one or more permissions

IAM summary***:***

IAM is universal – does not apply to regions

- Root account is the account during the account setup and has admin privileges

- New users have no permissions when first created

- New users assigned Access Key ID and Secret Access keys

- Key ID and Secret Access keys cannot be used for login but for access using API

And CLI. You will view them once, if loose, need to be recreated.

- Always setup MFA (Multifactor authentication) on root acc.

- You can create and customize your own password rotation policies.

# S3

*S3 provides developers and IT teams with secure, durable, highly scalable object storage. Amazon S3 is easy to use, with a simple web services interface to store and retrieve any amount of data from anywhere on the web*

## S3 basics:

* Object-based – i.e. allows you to upload files.
* Files can be from 0 bytes to 5TB
* There is unlimited storage
* Files are stored in Buckets
* S3 is universal namespace. Names must be unique globally.
* https://s3-**eu-west2**.amazonaws.com/**karalov**
* When you upload a file to S3, you will receive a HTTP 200 code if the upload was successful
* Read after Write consistency for PUTS of new Objects
* Eventual consistency for overwrite PUTS and DELETES (can take some time to propagate)
* S3 is a simple Key-value store, object based

## S3 objects consists of:

* Key (name of the object)
* Value (data made from bytes)
* Version ID
* Metadata (data about data you storing)
* Sub resources: Access Control Lists, Torrent

## S3-Storage Tiers/Classes:

99.99999999% durability for all classes

1. **S3 Standard**: 99.99% availability, stored redundantly across multiple devices in multiple facilities, and is designed to sustain the loss of 2 facilities concurrently.

2**. S3 – IA**: (Infrequently Acessed): for data that is accessed less frequently, but requires rapid access when needed, Lower fee than S3, but you’re charged retrieval fee. Avail. 99.9%,

3. **S3 One Zone** – IA: a lower cost optionfor infrequently accessed data, but do not require the multiple Availability Zone data residence. Availability 99.5%

4. **Glacie**r: very cheap, but used for archival only. Expedited, standard or bulk. A standard retrieval time takes 3-5 hours.

## S3 charges:

* Storage
* Requests
* Storage management pricing
* Data transfer pricing

Cross region replication**:**

*Cross-region replication is a bucket-level configuration that enables automatic, asynchronous copying of objects across buckets in different AWS Regions.*

* Versioning must me enabled on both the source and destination buckets
* Regions must be unique
* Files in an existing bucket are not replicated automatically. All subsequent updated files will be replicated automatically.
* You cannot replicate to multiple buckets or use daisy chaining
* Delete markers are replicated
* Deleting individual versions or delete markers will be not replicated.

## Lifecycle management:

* Can be used in conjunction with versioning.
* Can be applied to current versions and previous versions.
* Following actions can be done:
* Transition to standard IS storage class (128kb and 30 days after the creation date)
* Archive to Glacier (30 days after IA)
* Permanently delete

## CloudFront(CDN)

Amazon CloudFront is a global content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to your viewers with low latency and high transfer speeds. CloudFront is integrated with AWS – including physical locations that are directly connected to the AWS global infrastructure

* Edge location – location where contant will be cached. This is separate to an AWS region/AZ. Not read only, they are writable
* Origin – origin of all files, that the CDN will distribute. Thi scan be either as S3 bucket, an EC2 instance, Elastic Load balancer or Route53
* Distribution – a collection of Edge locations.
* Web distribution – used for websites
* RTMP – used for media streaming
* Objects are cached for the life of TTL (Time to Live)
* You can clear cached objects, but you will be charged.

## Security:

* All newly created buckets are PRIVATE by default
* You can setup access control to your buckets using:
* Bucket policies
* Access control lists
* S3 buckets can be configured to create access logs which log requests made to the S3 bucket. This can be done to another bucket.

## Encryption:

* In transit (SSL/TLS)
* AT Rest:
* Server side encryption:
  + S3 managed keys – **SSE-S3**
  + AWS key management service, managed keys – **SSE-KMS**
  + With customer provided keys – **SSE-C**
* Client side encryption

## Storage Gateway

*AWS Storage Gateway is a hybrid storage service that enables your on-premises applications to seamlessly use AWS cloud storage. You can use the service for backup and archiving, disaster recovery, cloud bursting, storage tiering, and migration. Your applications connect to the service through a gateway appliance using standard storage protocols, such as NFS and iSCSI.*

* File gateway – for flat files, stored directly on S3
* Volume gateway:
* Stored volumes – entire dataset is stored on site and is asynchronously backed up to S3
* Cached volumes – entire dataset is stored on S3 and the most frequently accessed data is cached on site
* Gateway Virtual tape library (VTL)
* Used for backup and uses popular backup applications like NetBackup, Backup Exec, Veeam etc.

## S3 transfer acceleration

Utilizes the CloudFront edge network to accelerate uploads to S3. Instead of uploading directly to S3 bucket, you can use a distinct URL to upload directly to an edge location which will then transfer that file to S3.

## S3 static websites

* You can use S3 to host static websites
* Serverless
* Very cheap, scales automatically
* Statis only, cannot host dynamic sites

## CLI:

>aws configure

>aws s3 ls

>aws s3 cp –recursive s3://karalov/myfolder .