Core AWS Services

2019年2月7日 星期四　　下午11:00

1.Identity & Access Management

What is IAM?

- **IAM** (**I**dentity & **A**ccess **M**anagement) is the service where AWS user accounts and their access to various AWS services is managed.

- The common use of **IAM** is to manage:
  - ***Users***
  - ***Groups***
  - ***Access Policies***
  - ***Roles***
  - ***User Credentials***
  - ***User password policies***
  - ***Multi-Factor Authentication (MFA)***
  - ***API keys for programmatic (CLI) access***

- By default, any new user created in an AWS account is created ***without*** access to any AWS services (only the ability to log in).

- For a user to access an AWS service, permission must be granted to that user. Which is managed in/by IAM.

IAM Users:

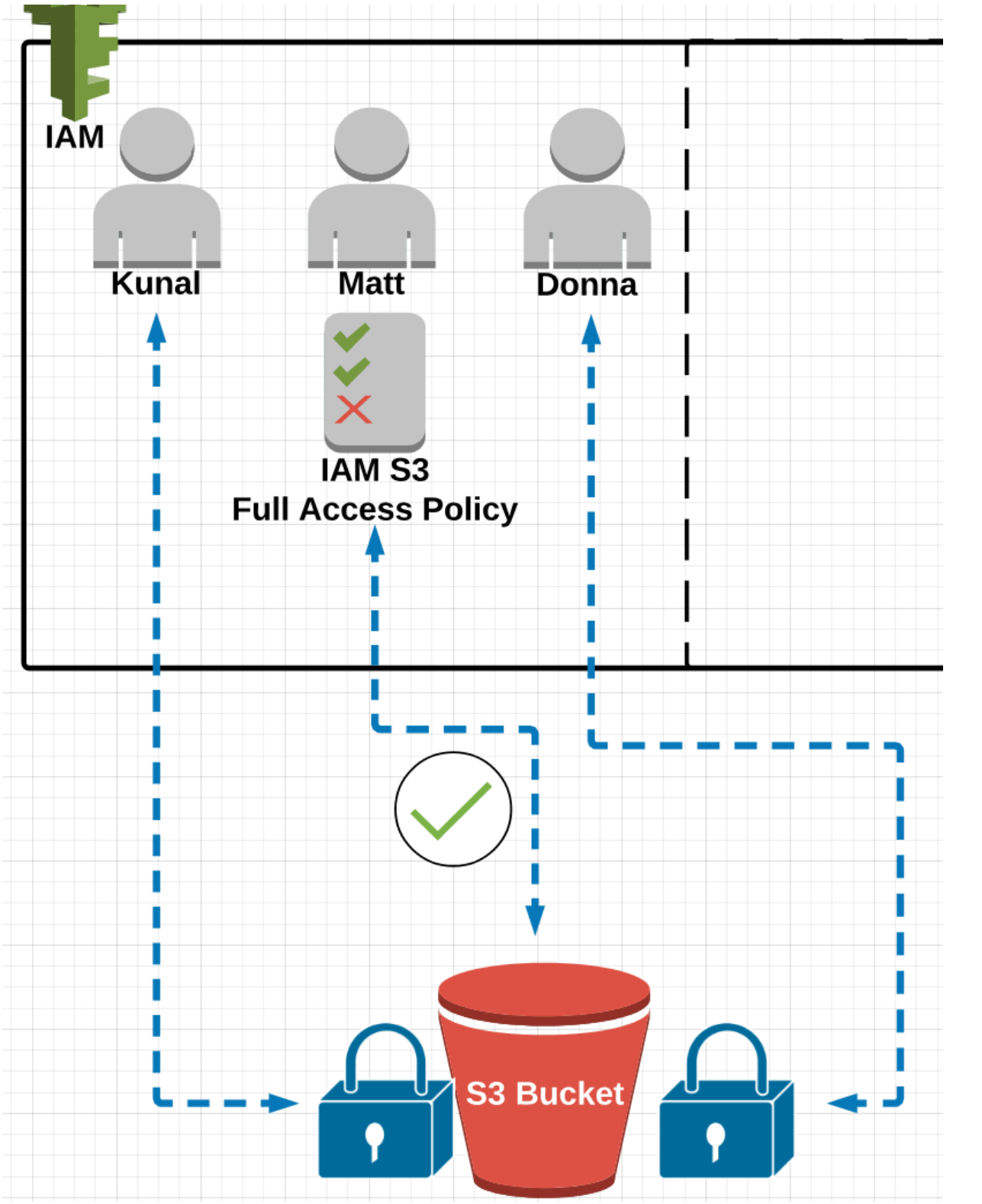
- ***IAM users*** are individuals who have been granted access to an AWS account. For example, if your company gives you access to their AWS account, then you are an IAM user (probably one of many the company has setup).

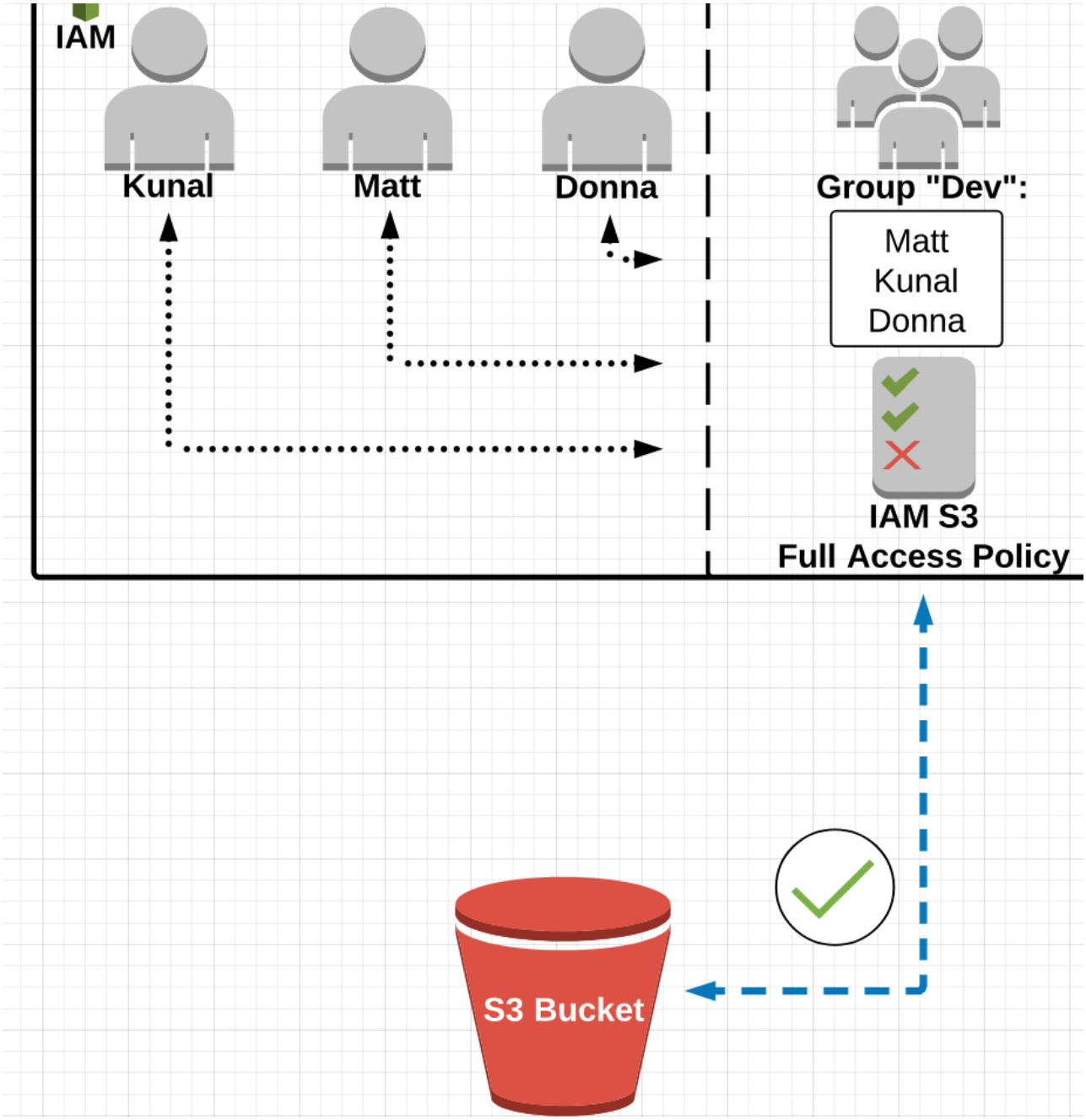
- Each IAM user has three main components:
  - ***A user-name***
  - ***A password***
  - ***Permissions to access various AWS services***

- Without permissions being explicitly granted to an IAM user, that user will not able to access any AWS services.

- Generally, a companies I.T. department will be responsible for "attaching" what are called ***IAM permission policies*** to an IAM user based on what that user needs access to (in order to do their job).

So what are IAM permission policies and how do they work?


IAM
Kunal
Matt
Donna
IAM S3
Full Access Policy
S3 Bucket



Other Uses/Benefits of IAM:

- The common use of **IAM** is to manage:
  - ~~***Users***~~
  - ~~***Groups***~~
  - ~~***Access Policies***~~
  - ***Roles***
  - ***User Credentials***
  - ***User password policies***

- ***Multi-Factor Authentication (MFA)***
- ***API keys for programmatic (CLI) access***

- ***Roles:***
  - How different AWS services, such as EC2 and S3, are granted permission to communicate and share data.

- ***User Credentials:***
  - IAM user's user-name and password for logging into AWS.

- ***User Password Policies:***
  - IAM user password format requirements (i.e. a password must be a minimum of 8 characters and include 1 number).

- ***Multi-Factor Authentication (MFA):***
  - A two-layer form of log-in verification that requires an additional (rotating) code number.

- ***API Keys for Programmatic (CLI) Access:***
  - Special credentials required for accessing AWS resources via the Command Line Interface (CLI).

2.Storage Services(S3)

S3 Defined:

Simple Definition:
An online, bulk storage service that you can access from almost any device.

AWS Definition:
"Amazon S3 has a simple web services interface that you can use to ***store and retrieve any amount of data, at any time, from anywhere on the web***. It gives any user access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of web sites. The service aims to maximize benefits of scale and to pass those benefits on to users."

AWS S3

S3 Basics:

Components and Structure

Basics:

(1) S3 = Simple Storage Service
(2) It is AWS's primary storage service.
(3) You can store any type of file in S3.

Buckets:

(1) Root level "Folders" you create in S3 are referred to as ***buckets***.
(2) Any "subfolder" you create in a bucket is referred to as a ***folder***.

S3 Folder

Objects:

(1) Files stored in a bucket are referred to as ***objects***.

S3 Object

Regions:

(1) When you create a bucket, you must select a specific region for it to exist in. This means that ***any data you upload to the S3 bucket will be physically located in a data center in that region***.

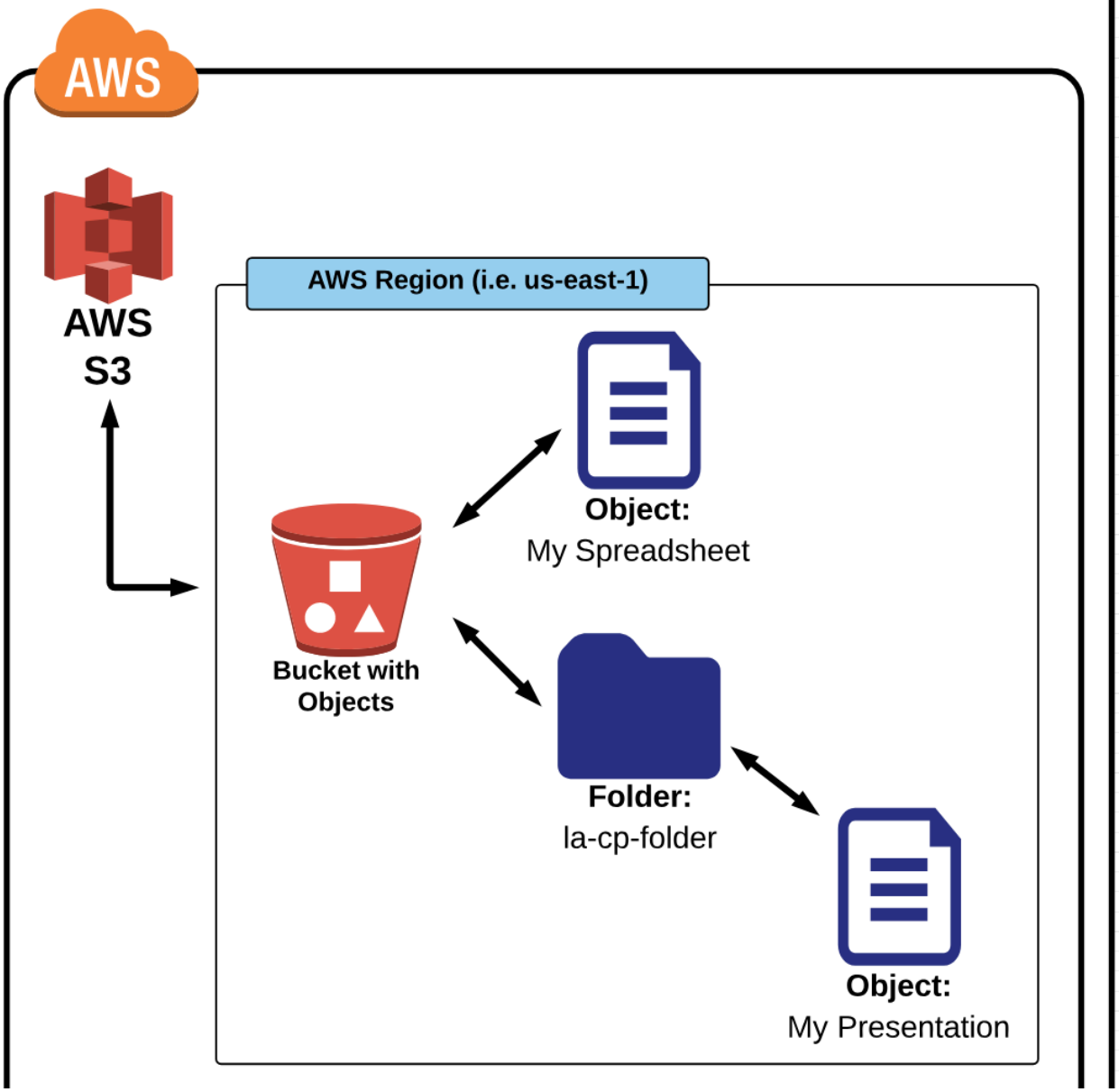
(2) ***Best practice*** is to select the region that is physically ***closest to you*** (to ***reduce transfer latency***).

OR

(3) If you are serving files to a ***customer*** based in a certain area of the world, ***create the bucket in a region closest to your customers*** (to reduce latency for your customers).

S3 Basics:

Components and Structure (visualized)



Buckets and Folders:

Creating an S3 Bucket:

(1) Choose a bucket name:

Bucket names must follow a set of rules:
-Bucket names must be unique across ALL of AWS.
-Bucket names must be 3 to 63 characters in length.
-Bucket names can only contain lowercase letters, numbers and hyphens.
-Bucket names must not be formatted as an IP address (e.g., 192.168.5.4).

(2) Select a region

NOTE: There are more “advanced” rules that allow for some varying formats, which can be found here:
http://docs.aws.amazon.com/AmazonS3/latest/dev/BucketRestrictions.html

Uploading (Import) an Object to a Bucket:

(1) Navigate into a bucket
(2) Select “upload”
(3) Select a file to upload
(4) Click “Start Upload”

Creating a Folder in a Bucket:

(1) Navigate into a bucket
(2) Click on ”Create Folder"
(3) Give the folder a name

NOTE: Uploading an object directly into folder is the same process, just navigate into the folder first.

S3 Storage Classes:

S3 Storage Classes:

What is a storage class?

(1) A ***storage class*** represents the "classification" assigned to each Object in S3.

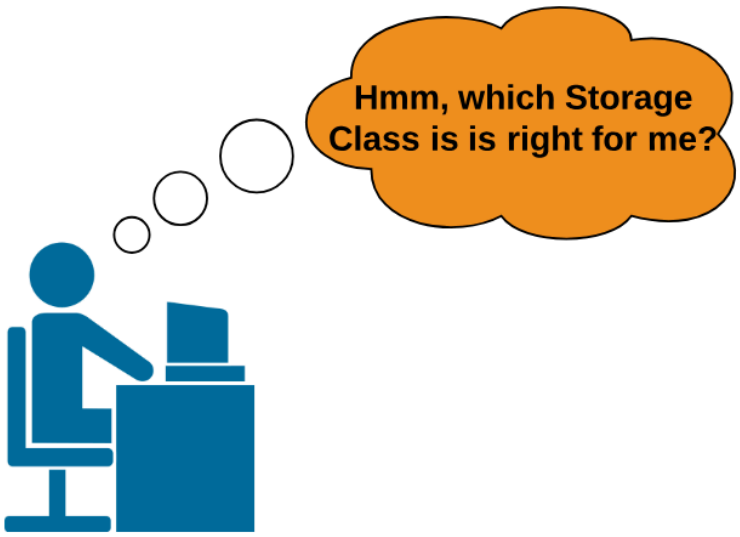
Available storage classes include:
-Standard
-Standard-IA (Infrequent Access)
-One Zone-IA (Infrequent Access)
-Intelligent-Tiering
-Glacier

(2) Each ***storage class*** has varying attributes that dictate things like:

-Storage cost
-Object ***availability***
-Object ***durability***
-Frequency of access (to the object)

(3) Each object must be assigned a storage class ("standard" is the default class)

(4) You can change the ***storage class*** of an object at any time (***for the most part***).



S3 Storage Classes:

Standard:
(1) Designed for general, all-purpose storage.
(2) Is the default storage option.
(3) ***99.999999999% object durability*** (“eleven nines”).
(4) ***99.99% object availability***

(4) ***99.99% object availability.***
(5) Is the most expensive storage class.

Standard-IA (Infrequent Access):
(1) Designed for objects that you do not access frequently, but must be immediately available when accessed. (uses multiple Availability Zones)
(2) ***99.999999999% object durability***.
(3) ***99.90% object availability.***
(4) Is less expensive than the standard storage class.

One Zone-IA (Infrequent Access):
(1) Designed for objects that you do not access frequently, but must be immediately available when accessed. (only uses 1 Availability Zone)
(2) ***99.99% object durability***.
(3) ***99.50% object availability***.
(4) Is ~20% less expensive than the standard-IA storage class

Intelligent-Tiering:
(1) Designed to optimize costs by automatically moving data to the most cost-effective tier based on your usage.
(2) ***99.999999999% object durability*** (“eleven nines”).
(3) ***99.90% object availability.***
(4) Pricing depends on the assigned storage class.

Glacier:
(1) Designed for long-term archival storage.
(2) May take several hours for objects stored in Glacier to be retrieved.
(3) ***99.999999999% object durability***
(4) Is the cheapest S3 storage class (very low cost)

Detailed S3 pricing based on storage class:
https://aws.amazon.com/s3/pricing/