Origin Access Identity and Origin Access Control

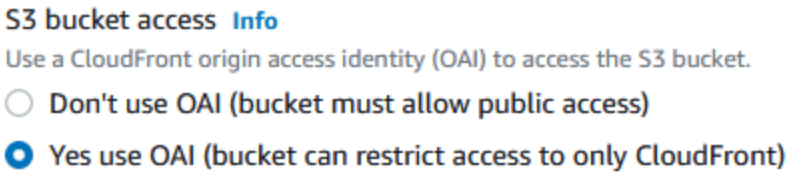
When using S3 with CloudFront, a setup often used when serving static webpages and application files, having an additional layer of security would not hurt. Well, AWS provides us with two methods of restricting access to an Amazon S3 distribution: Origin Access Identity (OAI) and Origin Access Control (OAC).

Origin Access Identity (OAI): A feature of the CloudFront service, it allows us to serve the content of a S3 Bucket without granting public access to the bucket. This restricts any unauthorized user from accessing the S3 files through its direct URL and forces them to use the CloudFront distribution URL instead.

Origin Access Control (OAC): A relatively recent addition to the AWS feature lineup, it performs the same function as OAI, that of permitting access to a select group of S3 buckets, but it uses IAM principals to authenticate with the S3 bucket origin. As mentioned before, IAM is Amazon's proprietary access control and management service suite and AWS considers it a best practice to use it for the security of AWS resources.

However, OAC, unlike OAI is not exclusive to CloudFront, and can also be applied to other types of endpoints such as custom origins or origins hosted on EC2 instances. This makes it a much wider offering than OAI, and its reliance on IAM also makes it a much better integrated part of the AWS ecosystem (IAM and its features will be covered in more depth in future sections).

Refocusing back to OAI, it is worth remembering that OAI is not enabled by default and that it must be configured in the S3 bucket access settings, as shown in the image below:



Additionally, a brief description of how Origin Access Identity works is given in the infographic below: