Cloudfront - II

Origin Access Identity

To restrict access to content that you serve from Amazon S3 buckets, follow these steps:

- Create a special CloudFront user called an origin access identity (OAI) and associate it with your distribution.
- Configure your S3 bucket permissions so that CloudFront can use the OAI to access the files in your bucket and serve them to your users. Make sure that users can’t use a direct URL to the S3 bucket to access a file there.
- After you take these steps, users can only access your files through CloudFront, not directly from the S3 bucket.
- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html

Signed URL vs Signed Cookies

Many companies that distribute content over the internet want to restrict access to documents, business data, media streams, or content that is intended for selected users, for example, users who have paid a fee. To securely serve this private content by using CloudFront, you can do the following:

- Require that your users access your private content by using special CloudFront signed URLs or signed cookies.
- Require that your users access your content by using CloudFront URLs, not URLs that access content directly on the origin server (for example, Amazon S3 or a private HTTP server). Requiring CloudFront URLs isn't necessary, but we recommend it to prevent users from bypassing the restrictions that you specify in signed URLs or signed cookies.

Signed URL vs Signed Cookies

CloudFront signed URLs and signed cookies provide the same basic functionality: they allow you to control who can access your content.

Use signed URLs in the following cases:

- You want to use an RTMP distribution. Signed cookies aren't supported for RTMP distributions.
- You want to restrict access to individual files, for example, an installation download for your application.
- Your users are using a client (for example, a custom HTTP client) that doesn't support cookies.

Use signed cookies in the following cases:

- You want to provide access to multiple restricted files, for example, all of the files for a video in HLS format or all of the files in the subscribers' area of website.
- You don't want to change your current URLs.

Signed URL vs Signed Cookies

- If you use both signed URLs and signed cookies to control access to the same files and a viewer uses a signed URL to request a file, CloudFront determines whether to return the file to the viewer based only on the signed URL.
- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/CFPrivateDistJavaDevelopment.html

Query String Parameters

- Some web applications use query strings to send information to the origin. A query string is the part of a web request that appears after a ? character; the string can contain one or more parameters, separated by & characters. In the following example, the query string includes two parameters, color=red and size=large:

http://d111111abcdef8.cloudfront.net/images/image.jpg?color=red&size=large

Query String Parameters

- For web distributions, you can choose if you want CloudFront to forward query strings to your origin and whether to cache your content based on all parameters or on selected parameters.
- Suppose that your website is available in five languages. The directory structure and file names for all five versions of the website are identical. As a user views your website, requests that are forwarded to CloudFront include a language query string parameter based on the language that the user chose. You can configure CloudFront to forward query strings to the origin and to cache based on the language parameter. If you configure your web server to return the version of a given page that corresponds with the selected language, CloudFront caches each language version separately, based on the value of the language query string parameter.

Query String Parameters

http://d111111abcdef8.cloudfront.net/main.html?language=de

http://d111111abcdef8.cloudfront.net/main.html?language=en

http://d111111abcdef8.cloudfront.net/main.html?language=es

http://d111111abcdef8.cloudfront.net/main.html?language=fr

http://d111111abcdef8.cloudfront.net/main.html?language=jp

Query String Parameters

You can configure CloudFront do one of the following:

- Don't forward query strings to the origin at all. If you don't forward query strings, CloudFront doesn't cache based on query string parameters.
- Forward query strings to the origin, and cache based on all parameters in the query string.
- Forward query strings to the origin, and cache based on specified parameters in the query string.

Optimizing Caching

- **Cache Based Only on Parameters for Which Your Origin Returns Different Versions of an Object**
- **Always List Parameters in the Same Order**
- **Always Use the Same Case for Parameter Names and Values – All being lowercase**
- **Don't Use Parameter Names that Conflict with Signed URLs – Expires, Key-Pair-Id, Policy & Signature**