CloudFront – AWS – PoC (Proof of Concept)

Este é mais um arquivo que desenvolvi como uma prova de conceito do produto AWS CloudFront com OAI (origin access identity), farei a introdução do serviço e como desenvolvi um ambiente básico para testar a aplicação.

O que é CloudFront?

O Amazon CloudFront é uma rede de entrega de conteúdo (CDN) que acelera a entrega de conteúdo estático e dinâmico da Web para usuários finais. O CloudFront distribui o conteúdo por meio de uma rede global de datacenters denominados locais da borda.

Bora lá?

Primeiramente quero apresentar a ideia da arquitetura e design pattern que foi idealizado nesta postagem.

Uma imagem contendo Diagrama

Descrição gerada automaticamente

Nesta imagem temos um usuário acessando o nosso serviço de entrega de conteúdo para buscar uma imagem especifica em nosso ambiente, o usuário procura uma imagem que utilizamos e ao acessar a nossa distribuição ela conseguirá localizar o nosso conteúdo.

A ideia inicial desta arquitetura é trazer segurança para nosso Bucket, não permitindo acessar diretamente o nosso Bucket.

Política que asseguro o acesso apenas pelo nosso CDN

{

"Version": "2008-10-17",

"Id": "PolicyForCloudFrontPrivateContent",

"Statement": [

{

"Sid": "1",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity E2H6T0U0OY0QAS"

},

"Action": "s3:GetObject",

"Resource": "arn:aws:s3:::webfrontcdn2/\*"

},

{

"Sid": "2",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity E2H6T0U0OY0QAS"

},

"Action": "s3:GetObject",

"Resource": "arn:aws:s3:::webfrontcdn2/\*"

},

{

"Sid": "3",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity E3HHEFE7U3BM0G"

},

"Action": "s3:GetObject",

"Resource": "arn:aws:s3:::webfrontcdn2/\*"

},

{

"Sid": "4",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity E3HHEFE7U3BM0G"

},

"Action": "s3:GetObject",

"Resource": "arn:aws:s3:::webfrontcdn2/\*"

},

{

"Sid": "5",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity E3HHEFE7U3BM0G"

},

"Action": "s3:GetObject",

"Resource": "arn:aws:s3:::webfrontcdn2/\*"

}

]

}

PoC - Proof of Concept

Vamos colocar a arquitetura a prova?

Acessando inicialmente o nosso CDN para buscar a imagem bike.jpg

Tela de computador mostrando aplicativo de jogo sendo usado

Descrição gerada automaticamente com confiança média

Agora nosso usuário irá tentar localizar outra foto que está em nosso segundo Bucket

Tela de computador

Descrição gerada automaticamente

E agora digamos que um usuário com má impressão consiga localizar nosso bucket e tente por meio direto do link abrir os dados que possuímos no bucket, o que acontecerá?

Tela de computador

Descrição gerada automaticamente

Está configuração de segurança só é possível pelas configuração de OAI que restringe o acesso diretamente em nosso bucket, este tipo de acesso permite blindar o nosso bucket de acessos indevidos e vazamento de informações.

Com isso conseguimos concluir com sucesso nossa prova de conceito.

Referências:

[Restringir o acesso ao conteúdo do Amazon S3 - Amazon CloudFront](https://docs.aws.amazon.com/pt_br/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3.html)

[Conceitos básicos de um site estático seguro - Amazon CloudFront](https://docs.aws.amazon.com/pt_br/AmazonCloudFront/latest/DeveloperGuide/getting-started-secure-static-website-cloudformation-template.html)