OAI vs OAC: Entendendo os Mecanismos de Controle de Acesso no CloudFront.

O OAI (Identidade de acesso à origem) é o sistema legado de segurança da Cloudfront, a sua principal função é forçar que o acesso a qualquer arquivo, nos Buckets S3 da Amazon, passe pelo CloudFront, impedindo seu acesso direto, apenas pelo endereço DNS ou link de acesso. Neste mecanismo, é criada uma identidade no CloudFront e certas políticas ligadas a ela, que permitem o acesso a um conteúdo dos Buckets S3, exclusivamente através do Cloufront. Sua origem não possui uma data específica, porém, é o primeiro mecanismo de segurança ligado ao CloudFront e possui documentação desde 2018.

Já o OAC (Controle de acesso à origem), é uma evolução do OAI, neste caso, em vez da criação de uma identidade, é criada uma série de políticas e controle de acesso, com o mesmo objetivo da OAI, acesso ao conteúdo de Buckets S3, exclusivamente através do CloudFront e suas distribuições para os chamados pontos de borda. A OAI está sendo substituída, em suas funções pela OAC e, atualmente, a AWS recomenda sempre a utilização desta última, em detrimento da primeira. A criação da OAC no CloudFront pelo usuário, se baseia no serviço principal de controle de login, autenticação e segurança da AWS, o IAM. Conforme as políticas de uso configuradas, somente o CloudFront pode assumir uma identidade e acessar o Bucket S3. Enquanto a OAI usa uma identidade virtual, a OAC utiliza o mecanismo de autenticação do IAM.

Algumas diferenças técnicas:

O OAI não suporta S3 com SSE-KMS (Server-Side Encryption com AWS KMS), o padrão de criptografia mais recente do S3, suporta apenas métodos de leitura (GET e READ) e pode ter problemas com regiões S3 mais recentes.

Algumas vantagens:

O padrão de segurança do OAC, ligado ao IAM é mais robusto que a criação da identidade pelo OAI, que não é completamente alinhado aos padrões do ecossistema do IAM. A criptografia, usando chaves KMS gerenciadas pelo cliente atende a quesitos de conformidade mais rigorosos, A OAC permite que o CloudFront utilize tanto escrita quanto leitura, possibilitando tanto o upload e exclusão quanto os downloads nos Buckets S3, enquanto o OAI apenas trabalha com leitura, permitindo o acesso e download do conteúdo. A OAC também vai permitir o acesso aos métodos HTTP dinâmicos, o que não se consegue com o OAI.

Desta forma, naturalmente, até por se tratar de uma evolução da OAI, a OAC se mostra como uma solução mais moderna, flexível e segura, integrando com o ecossistema IAM nativamente, adotando o protocolo SigV4, que possibilita maior integração com os sistemas de encriptação do S3.

O OAI deve ser, então, utilizado em sistemas de acesso mais antigos, porém, deve ser programada sua migração para o OAC, que possui total compatibilidade com os sistemas atuais.

Ambos possuem a função de proteção do Bucket S3, através de acesso controlado, utilizando o CloudFront.