06

S3 Políticas de Bucket

Transcrição

Anteriormente, conseguimos trabalhar com políticas relacionadas aos grupos do IAM, ou seja, os grupos dos instrutores. Nesse vídeo iremos trabalhar com políticas de acesso ao *bucket*.

Acessando o *bucket* `alura-s3` como instrutor, abriremos o arquivo `testando2.txt`, usada em aulas passadas e, clicando em "Open", conseguimos visualizar seu conteúdo textual. Perceberemos que na sua URL existem diversos parâmetros de autenticação e outros, sem os quais não conseguiremos acessar o link. Isto indica que se as credenciais de segurança não forem passadas, o usuário não terá qualquer acesso a este determinado objeto, e isso é padrão do S3.

Os *buckets* e os objetos são privados por padrão. E, como já vimos nas primeiras aulas, se quiséssemos torná-los públicos, basta clicar em "Make public". No entanto, concordamos que isso começa a ficar bastante penoso à medida em que identificamos a ideia desse *bucket*, que é ter todos os seus arquivos visíveis ao público. Se um instrutor tiver que ficar marcando que um objeto é público a cada arquivo que for subir, uma hora ou outra ele pode se esquecer disto. Para melhorar, então, vamos tornar o *bucket* público.

Permitindo a leitura dos arquivos do *bucket*

Para realizarmos essa configuração, retornaremos ao *bucket*, para a aba chamada "Permissions" e nessa aba clicaremos no botão "Bucket Policy". Até então, estávamos trabalhando com políticas relacionadas a grupos de usuários, mas aqui nos encontramos do outro lado, temos uma visão diferente. Poderíamos escrever um JSON, naquele mesmo formato visto no IAM, mas utilizaremos um gerador, algo que nos facilite a vida, clicando em "Policy generator".

No passo 1, em "Select Type of Policy", selecionaremos o tipo de política que estamos gerando, em nosso caso "S3 Bucket Policy". No passo 2, em "Effect", escolheremos o efeito que queremos, de liberação do acesso de leitura a todo e qualquer usuário do mundo, de política de permissão ("Allow"). Em "Principal" informaremos quem sofrerá os efeitos, e como queremos permitir todos, basta usarmos o asterisco (`*`). Se fosse um usuário específico no nosso S3, poderíamos simplesmente colocar seu nome.

No campo "AWS Service" indicaremos o tipo de serviço, e como já selecionamos o S3 no tipo de política, ele é preenchido automaticamente. Em "Actions", é importante selecionarmos a correta para não permitirmos acesso total ao S3, para escrita, remoção e alteração. Queremos apenas dar acesso de leitura, portanto selecionaremos "GetObject".

E novamente, em "Amazon Resource Name (ARN)", colocaremos `arn:aws:s3:::alura-s3/`, ou seja, todos os objetos do *bucket* `alura-s3`. Clicaremos em "Add Statement" e desenvolveremos a política clicando em "Generate Policy", gerando um conteúdo JSON que deveremos copiar e colar no nosso *bucket*.

Clicaremos em "Save" para salvar, e a expectativa é que a partir desse momento, com essa política já salva, já tenhamos acesso ao arquivo `testando2.txt` sem a necessidade de passarmos parâmetros de autenticação. Ao acessar a URL, conseguiremos chegar ao arquivo - nesse e qualquer outro novo deste *bucket*.

Para conferir, poderemos subir um novo arquivo para o *bucket* `alura-s3`, e clicando em seu link veremos que conseguimos acessá-lo.

Nessa aula vimos que é possível aplicar políticas de acesso diretamente a um *bucket*, algo bastante útil quando queremos liberar o acesso público ao nosso *bucket*, ou estreitá-lo a determinados usuários e grupos. Então, há essas

duas visões de políticas possíveis. Já temos bastante ferramentas para liberar ou negar acesso a determinados serviços do S3.