amazon web services

Como fornecer acesso a um bucket do Amazon S3

João Paulo Santana
Enterprise Solutions Architect

Amazon S3

Como fornecer acesso a um bucket do Amazon S3

João Paulo (JP) Santana – AWS Enterprise Solutions Architect

Agosto 2016

Índice

Como fornecer acesso a um bucket do Amazon S3

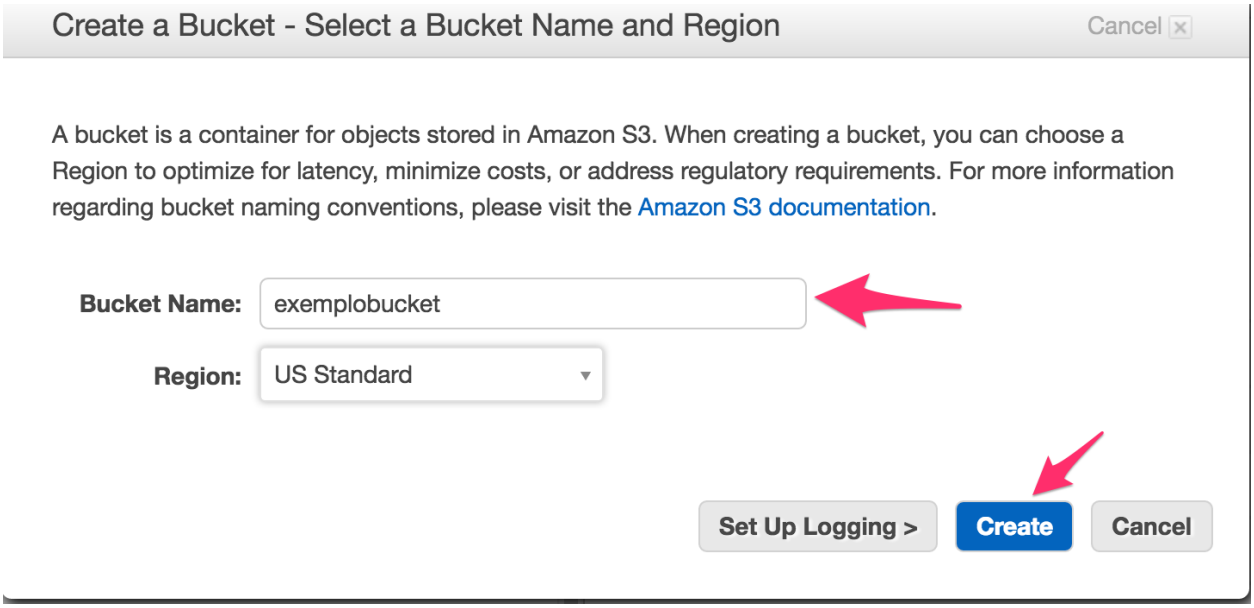
Introdução

Uma pergunta bastante recorrente é a seguinte: “Como dou acesso, a um usuário da minha conta AWS, para um bucket do Amazon S3?”. Os casos de uso para isto são os mais variados. Alguns usuários desejam criar uma área comum para compartilhamento de arquivos, outros para substituir se serviço de FTP, outros para preparar uma área para backup de arquivos e outros ainda para criar uma área que será utilizada por uma aplicação. Vamos responder a essa pergunta demostrando como fornecer acesso para leitura e escrita à um bucket do Amazon S3 para um grupo do AWS Identity and Access Management (IAM) da sua conta AWS, chamado *grupobucket*, contendo um usuário do IAM chamado usuario*bucket*.

Neste exemplo criaremos um bucket do Amazon S3 chamado exemplobucket.

Criação do Bucket

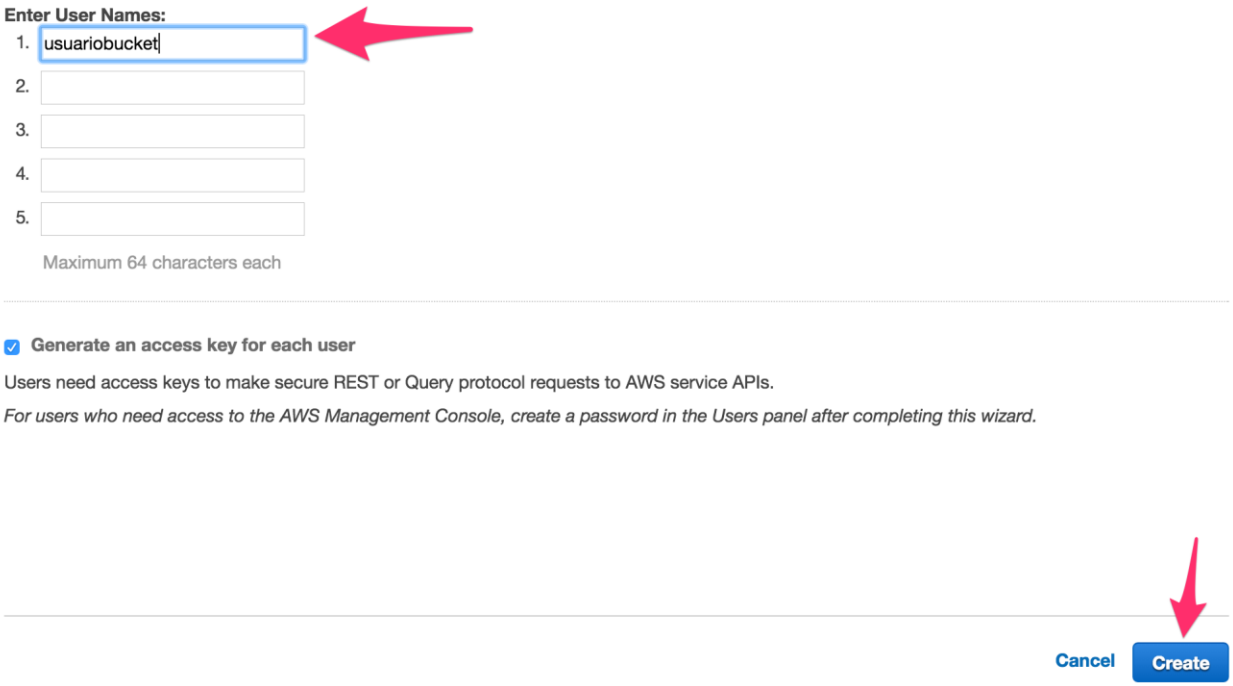
1. Acesse a console AWS, clique em **Services, Storage & Content Delivery** e selecione **S3**;
2. Clique no botão **Create Bucket**, atribua um nome ao bucket (lembrando que nomes de buckets S3 precisam ser únicos globalmente), escolha a região de preferência e clique em **Create Bucket**;



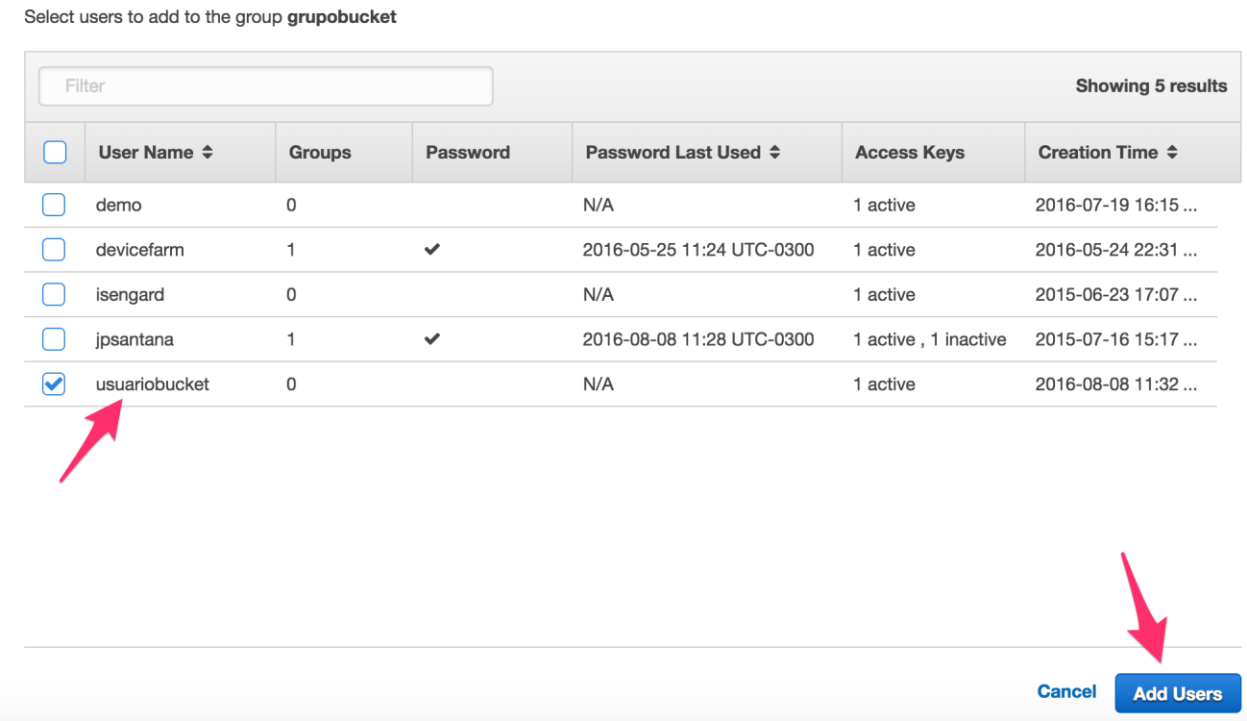
Agora vamos criar o usuário e grupo do IAM e adicionar o usuário ao grupo.

Criação do Grupo e Usuário do IAM e Adição de Usuário

1. Acesse a console AWS, clique em **Services, Security & Identity** e selecione **IAM**;
2. Na console do IAM, clique em **Users**, **Create New User**, atribua um nome ao usuário e clique **Create**;



3. Faça download ou tome nota das credenciais de Access Key e Secret Access Key. Estas credenciais serão utilizadas posteriormente para realizar chamadas API aos serviços AWS;
4. Selecione o usuário criado, clique **Manage Password** e atribua um password para o usuário. Existe também a opção de gerar um usuário automaticamente e requerer que o usuário mude a senha no primeiro logon;
5. De volta à console do IAM, clique **Groups**, **Create New Group**, atribua um nome ao grupo, clique **Next Step**, não atribua nenhuma política ao grupo neste momento, clique **Next Step** novamente e finalmente clique **Create Group**;
6. De volta à console do IAM mais uma vez, clique **Groups**, selecione o grupo criado, e selecione **Add Users to Group** no botão **Group Actions**. Selecione o usuário criado e clique **Add Users**;



Agora vamos criar a política de acesso que será associada ao grupo e proverá o acesso desejado ao bucket do Amazon S3.

Criação da Política de Acesso ao bucket do Amazon S3

1. De volta ao dashboard do AWS IAM, clique em **Policies**, **Create Policy**, **Create Your Own Policy**, atribua um nome e descrição, caso desejar e adicione a politica em formato JSON.

Para a criação da política de acesso, podemos pensar em diversos tipos de acesso que podemos fornecer a nossos usuários, dependendo do caso de uso. Podemos fornecer acessos para um usuário que deseja interagir com seu bucket do Amazon S3 através da console AWS. Outro tipo de acesso é mais programático, seja através da ferramenta de linha de comando AWS (AWSCLI), de uma ferramenta de terceiros como por exemplo CyberDuck, S3 Browser ou TNTDrive ou ainda de acesso realizados por uma aplicação, por exemplo uma aplicação que escreve ou lê dados adicionados à um bucket do Amazon S3 por um website.

Para o caso de acessos interativos ao bucket, através da console, devemos utilizar uma política que inclua permissões para que o usuário possa listar todos os buckets da conta AWS. Para listar buckets o usuário precisará que as ações *GetBucketLocation* e *ListAllMyBuckets* estejam presentes.

A seguinte política exemplo fornece permissão para este tipo de acesso à um bucket. Chamarei esse bucket exemplo de "*exemplobucket*".

```
"Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::exemplobucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
```

```
      ],
      "Resource": ["arn:aws:s3:::exemplobucket/*"]
    }
  ]
}
```

As ações *GetBucketLocation* e *ListAllMyBuckets* permitem que usuários possam visualizar o bucket usando a console. Sem essas permissões o acesso seria negado à console do Amazon S3. No entanto, mesmo podendo listar todos os buckets os usuários estariam restritos a visualizar o somente o conteúdo do bucket *exemplobucket.* As permissões de leitura e escrita estão especificadas somente para *exemplobucket,* se o usuário tentar acessar outro bucket, o acesso será negado.

Para acessos do tipo programático, as permissões *GetBucketLocation* e *ListAllMyBuckets* não são necessárias.

O mesmo exemplo de política para acesso programático de leitura e escrita ao bucket *exemplobucket,* ficaria da seguinte forma:

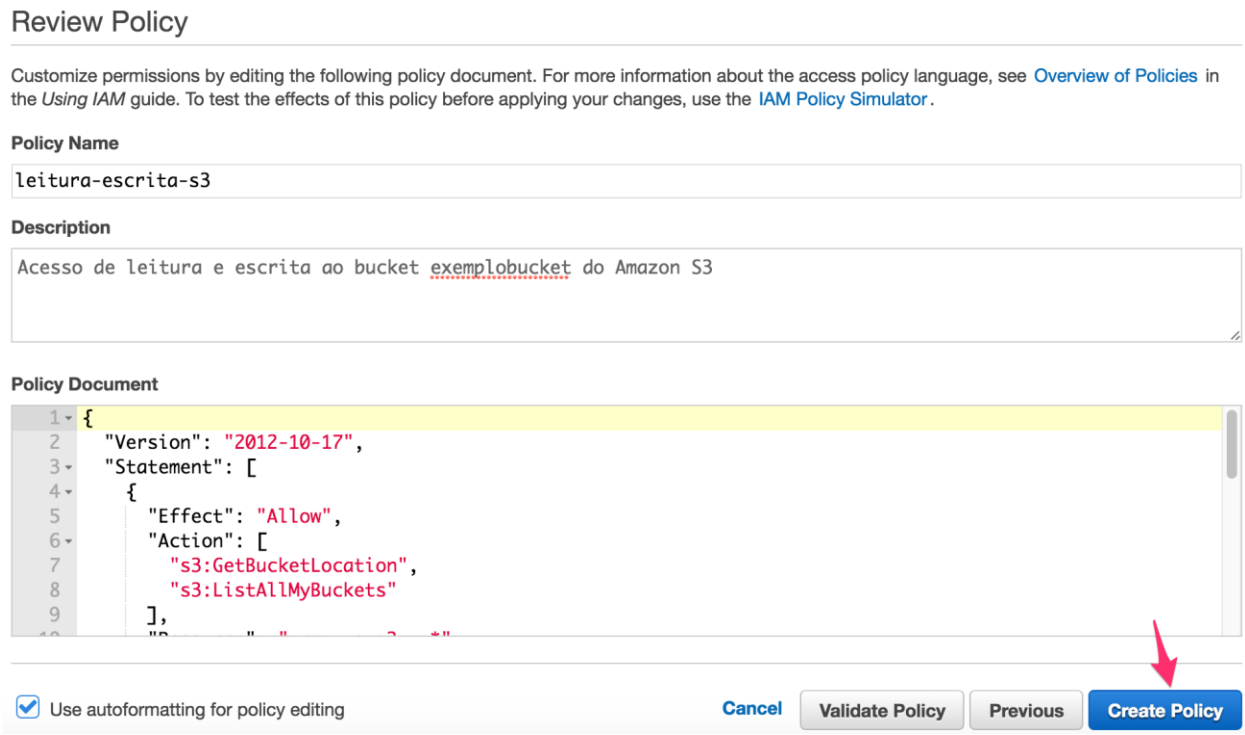
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::exemplobucket"]
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::exemplobucket/*"]
    }
  ]
}
```

Note-se que ambas políticas acima possuem duas partes. Isto acontece porque as ações normalmente requerem acesso em objetos dentro do bucket porém a ação ListBucket especificamente requer acesso ao bucket em si. Esta é a razão de estarmos utilizando o elemento Resurce especificando *arn:aws:s3::: exemplobucket* para a ação *ListBucket* enquanto que para as demais ações utilizamos *arn:aws:s3::: exemplobucket /**.

Se tivéssemos combinado os dois Amazon Resource Names (ARN's) utilizando * teríamos fornecido permissões para qualquer bucket e objeto que iniciasse com *exemplobucket,* o que não é o objetivo aqui.

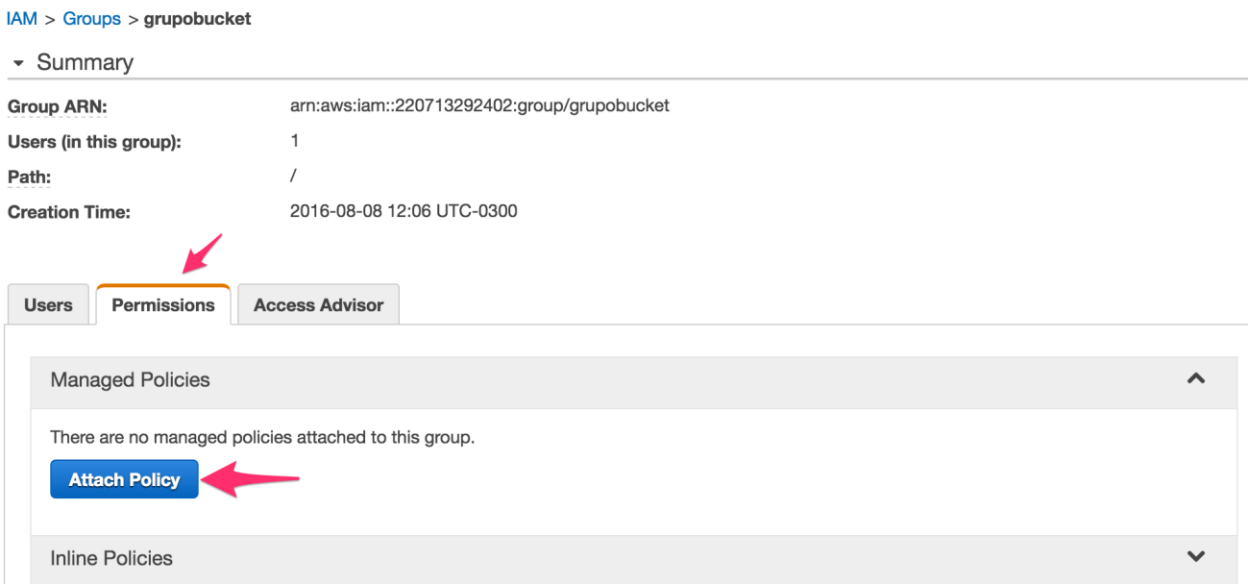
2. Uma vez tendo adicionado a política desejada, clique em **Create Policy**;



Uma vez tendo criado todos estes objetos. Vamos atribuir a política ao Grupo do AWS IAM.

Atribuindo Política ao Grupo do IAM

1. Clique em **Groups** e clique sobre o grupo para abrir as opções de configuração;
2. Selecione a aba **Permissions** e clique em **Attach Policy** na sessão **Managed Policies**;

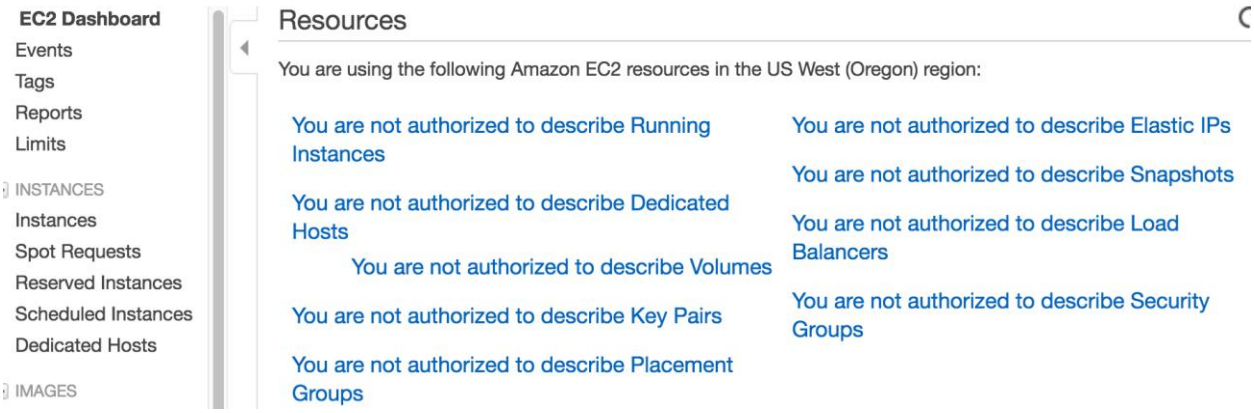


3. Selecione a política criada na sessão anterior e clique **Attach Policy**.

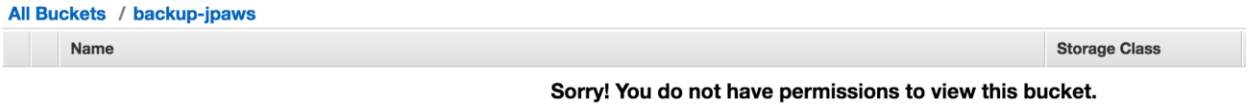
Todas as configurações foram efetuadas. Vamos agora tentar acessar o bucket com nosso usuário através da Console AWS.

Testando as Permissões

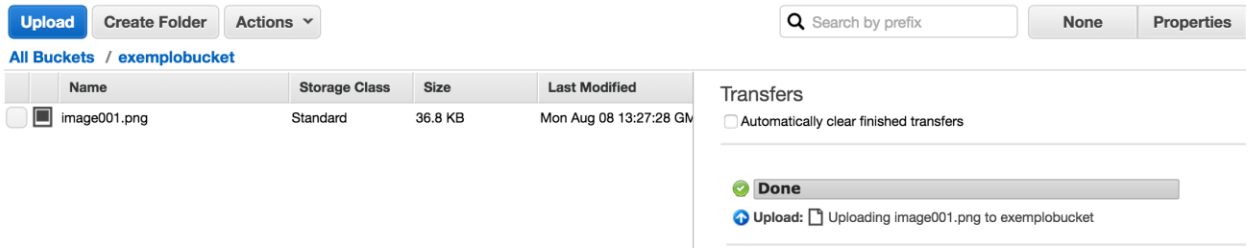
1. Efetue logon na console com o usuário recém-criado;
2. Uma vez na console AWS, tente acessar algum outro serviço para testar se as permissões estão efetivadas somente no Amazon S3. Tente acessar, por exemplo, o serviço Amazon EC2. Você deve visualizar uma imagem semelhante ao screenshot abaixo, demonstrando que você não possui acesso a este serviço;



3. Tente agora acessar o serviço Amazon S3. Você deve ser apto a listar todos os buckets.
4. Tente acessar um bucket que não seja o qual incluímos em nossa política, no meu caso o exemplobucket. Você deve visualizar uma mensagem semelhante à do screenshot abaixo, demonstrando que você não tem acesso ao bucket selecionado;



5. Acesse o bucket criado anteriormente, no meu caso *exemplobucket,* e tente fazer upload de um arquivo. Tente também remover o arquivo. Você deve ser apto a realizar todas essas ações no bucket.



Conclusão

Implementamos, em poucos minutos, uma política de acesso à um grupo do AWS IAM com para que seu usuário esteja apto a utilizar um bucket do Amazon S3. Através de práticas como esta você poderá implementar níveis de permissões que estejam de acordo com a tarefa necessária para cada usuário, evidando assim prover acessos desnecessários aos usuários, o que pode comprometer a segurança de seu ambiente na Nuvem AWS.