Cloud Computing Exercise #16

Creating a user and an IAM policy for S3 access

A. Preparation

1. Sign in to your AWS account as the non-root admin user.

B. Create a new IAM user

1. Go to the IAM Dashboard (Identity and Access Management), select Access Management/Users on the left-hand side menu and click on “Add users”. Set the username to “jdoe” (for Jane Doe), give the user password-based access to the management console, and provide a custom password (e.g. janePW#1234). You can force the new user to change her password at her first login, but for this lab this is not necessary. Click through the rest of the steps with the default settings, and create the user. At this point, the new user has no permissions (cannot do anything), but we will change that later. Note the URL the new user can use to log into the AWS console on the “Success” page – you will need it to log in as this new user later. If you look at the list of users in your account again, you should see the new user in addition to yourself.

C. Create two buckets and upload files to them

1. Go to the S3 service, and create two buckets. Pick the bucket names such that one would have the words “read-write” in it, and the other would have the words “read-only”. Bucket names are global and must be unique, so the one you're attempting to use may already be taken. Consider trying a different name while including the suggested keywords for your reference I will refer to these buckets as “read-write” and “read-only” in this lab. Select the buckets, click on “Properties” and note the ARN for both buckets.
2. Create two text files on your local machine called “file01.txt” and “file02.txt” with some arbitrary content, e.g.

This is an example text file.

1. Upload file01.txt to the read-write bucket, and upload the file02.txt to the read-only bucket.

D. Create an IAM policy for the new user

1. Go back to the IAM service, select Access Management/Policies and click on “Create Policy”. You can use the visual editor, but I recommend that you click on the JSON tab and create the IAM policy as a JSON document. You can use the default IAM policy version ("2012-10-17"). Do not specify a principal – this is an identity-based IAM policy and will be attached to the new user, jdoe.
2. The bucket policy should have the following four statements:
   * The user should have permissions to list all buckets in the account by the management console. This requires allowing the “s3:GetBucketLocation” and “s3:ListAllMyBuckets” for all resources (use the wildcard character) in S3. Hint: you can specify multiple actions in the same statement by putting them in a JSON array.
   * The user should have permissions to list the bucket contents for both the read-only and the read-write S3 buckets. Go to <https://docs.aws.amazon.com/AmazonS3/latest/userguide/list_amazons3.html>, where the possible IAM policy actions are listed for S3, and find the appropriate action string from the list. Hint: listing the content of a bucket is “listing the bucket”. Do not forget to add the “s3:” service prefix to the S3 action strings. Here, the resource should be an array of the ARNs for the two buckets you created previously.
   * The user should have permissions to read and write objects from/to the read-write bucket. Again, find the appropriate action strings on the S3 IAM policy action list. Hint: writing is “putting an object”, while reading is “getting an object”. Here the resource should be all objects in the read-write bucket (and not the bucket itself).
   * The user should have permissions to read objects from the read-only bucket. This is similar to the previous one, but there is only one action allowed and the resource is all objects in the read-only bucket.

(If you need assistance with structuring the policy, you can check the modules section for guidance.)

1. Add a tag to the IAM policy with key “Name” and value “jdoe\_s3\_policy”. Then, give it the same name and select “Create Policy”. You should see the new policy in the list of your policies with the provided name.

E. Attach the IAM policy to the new user

1. Go to IAM/Access management/Users and select the user jdoe. On the “Permissions” tab select “Add Permissions”, then “Attach policies directly”. In the permissions policies, filter by type, “Customer managed” and “jdoe\_s3\_policy” should show up. Select it, and add these permissions to the user jdoe. The IAM policy should show up in the user’s “Permissions Policies” list.

F. Login as the new user and test the IAM policy

1. Log out of AWS (or start another web browser, e.g Firefox or Chrome) and log in as user jdoe using the login URL you saved and the password you provided.
2. Go to S3 (Services/S3/Buckets), and you should see the read-write and the read-only buckets on the list of buckets. Select the read-write bucket, and you should see the file01.txt in that bucket. Select the file file01.txt and download it. This shows that the read permissions work. Now modify the downloaded file (e.g. add another line: This is a second line.), save it and upload it to the read-write bucket. If you download the same file from the read-write bucket again, you should get the modified file (with the second line added). Thus, the write permission also works.
3. Now select the read-only bucket, look at its content and download the file02.txt file. This shows that the read permissions work on this bucket. Now try to upload the modified file01.txt to this bucket. The upload should fail, with a red banner on the top of the screen saying “Upload failed”. If you scroll down, you should see your file upload with status “Failed”. This shows that this user cannot upload files to the read-only bucket.
4. Log out of AWS as the user jdoe, and log back in as the non-root admin user.

G. Clean up after yourself

1. Go to the list of the account’s users (IAM/Access management/Users) and delete the user jdoe. Then, go to the IAM policy list (IAM/Access management/Policies) and delete the policy “jdoe\_s3\_policy”. Finally, go to the S3 bucket list (S3/Buckets), delete the files from the buckets, and then delete the buckets.
2. Log out of AWS.