Create AWS S3 Upload and List Objects Policy without Delete Action

By **Josphat Mutai** - July 19, 2020

You can support us by downloading this article as PDF from the Link below. Download the guide as PDF

In this walkthrough, we'll look at how to use user permissions with Amazon S3. We will create a bucket and AWS Identity and Access Management user on our AWS account with specific permissions. My use case for this was having IAM user that can upload files to AWS S3 buckets only, without the permission to delete objects.

Create a Test bucket:

Use aws command with `s3` option to create a bucket:

```
$ aws s3 mb s3://backupsonly
make_bucket: backupsonly
```

Create an IAM user

The following create-user command creates an IAM user named `uploadonly` in the current account:

```
$ aws iam create-user --user-name uploadonly
```

Output:

```
{
    "User": {
        "Path": "/",
        "UserName": "uploadonly",
        "UserId": "AIDAJII2GMOH3OAFWCIGK",
        "Arn": "arn:aws:iam::104530196855:user/uploadonly",
        "CreateDate": "2018-08-07T08:51:23.600Z"
    }
}
```

Create AWS User and Policy

Next, we need to create a policy that will be associated with the created AWS user account.

This is the **json** file that we'll use for the policy:

```
$ cat aws-s3-policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:Get*",
                "s3:List*",
                "s3:Put*"
            ],
            "Resource": "*"
        }
    ]
}
```

We specified the actions for:

- List all bucket contents
- Get a list of all buckets on S3
- Upload files to S3 buckets

The following command creates a user managed policy named *upload-only-policy*:

```
$ aws iam create-policy --policy-name upload-only-policy \
--policy-document file://aws-s3-policy.json
```

You should get output like below:

```
{
    "Policy": {
        "PolicyName": "upload-only-policy",
        "PolicyId": "ANPAZYBH8BTU6NFCTTR46",
        "Arn": "arn:aws:iam::104530196855:policy/upload-only-policy",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "IsAttachable": true,
        "CreateDate": "2018-08-07T09:02:13.013Z",
        "UpdateDate": "2018-08-07T09:02:13.013Z"
    }
}
```

The policy used is a JSON document in the current folder that grants read/write access to all Amazon S3 buckets.

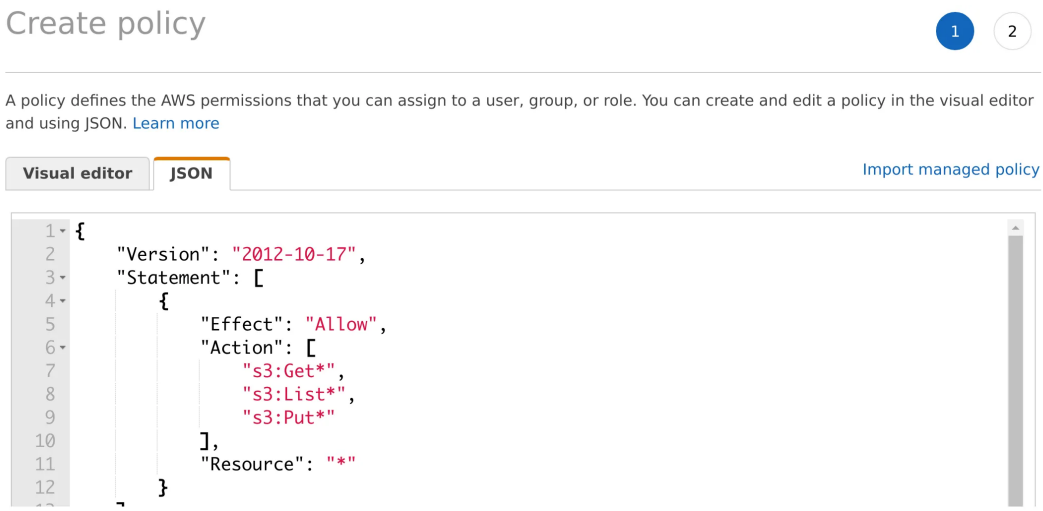
You can also limit this to a specific bucket by changing resource section. Example:

```
"Resource": [
       "arn:aws:s3:::bucket-name/*"
]
```

Or to a specific folder inside a bucket:

```
"Resource": [
      "arn:aws:s3:::bucket-name/folder1/*"
]
```

You can also do the same from AWS IAM web interface:



Assign AWS Policy to IAM User

The following `attach-user-policy` command attaches the AWS managed policy named `upload-only-policy` to the IAM user named `uploadonly` :

```
$ aws iam attach-user-policy --policy-arn \
arn:aws:iam::104530196855:policy/upload-only-policy --user-name uploadonly
```

There is no output for this command

You can now create an access key for an IAM user to test:

```
$ aws iam create-access-key --user-name uploadonly
```

Store the secret access key in a secure location. If it is lost, it cannot be recovered, and you must create a new access key.

From UI go to **IAM > Users > Add Permissions > Attach existing policies directly**

Configure your AWS CLI and test:

```
$ sudo pip install awscli
$ aws configure
```

Provide:

- AWS Access Key ID
- AWS Secret Access Key

Test file upload:

```
$ aws s3 cp test-demo.yml s3://backupsonly/
upload: ./test-demo.yml to s3://backupsonly/test-demo.yml
```

Try delete:

```
$ aws s3 rm s3://backupsonly/test-demo.yml
```

You should get an error message:

```
delete failed: s3://backupsonly/test-demo.yml
An error occurred (AccessDenied) when calling the DeleteObject operation: Access Denied
```

Let me know through comments section if you encounter an error message.

AWS Recommended courses:

Other AWS articles available in our blog are:

How to reset / change IAM user password on AWS

How to extend EBS boot disk on AWS without an instance reboot

Create AWS S3 Upload and List Objects Policy without Delete Action

How to Configure Cpanel Backups to S3 Object Store

How to Install and Use AWS CLI on Linux – Ubuntu / Debian / CentOS

How to Reset RDS Master User Password on AWS

**Your support is our everlasting motivation,
that cup of coffee is what keeps us going!**

As we continue to grow, we would wish to reach and impact more people who visit and take advantage of the guides we have on our blog. This is a big task for us and we are so far extremely grateful for the kind people who have shown amazing support for our work over the time we have been online.

Thank You for your support as we work to give you the best of guides and articles. Click below to buy us a coffee.

Josphat Mutai

https://computingforgeeks.com/

Founder of Computingforgeeks. Expertise in Virtualization, Cloud, Linux/UNIX Administration, Automation,Storage Systems, Containers, Server Clustering e.t.c.