LAB: Access S3 via CLI from EC2 with IAM Roles and Policies

You need:

- An AWS Account
- An S3 Bucket with Static Hosting Enabled

Duration of the Lab: 30 Minutes.

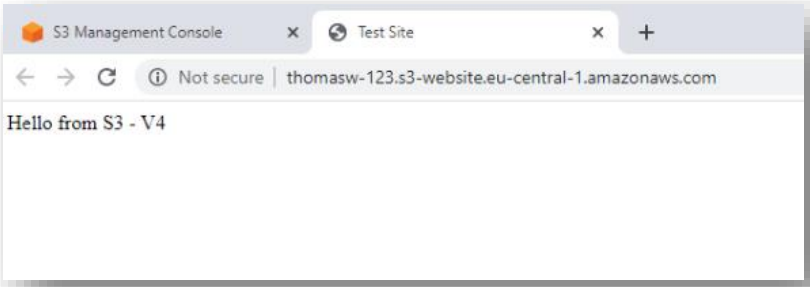
Difficulty: medium

Contents

S3 CLI

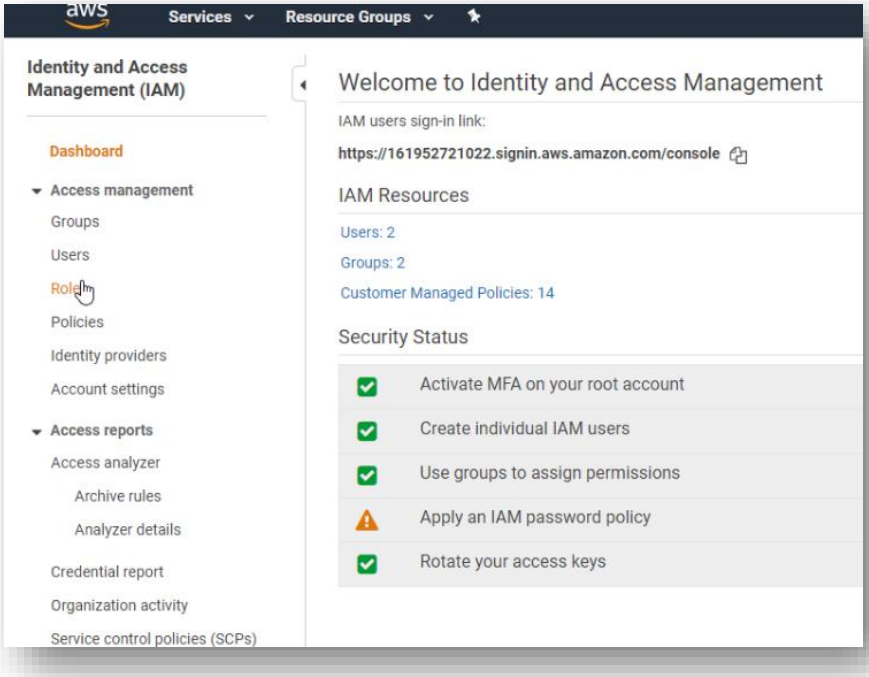
We will use an EC2 Instance with IAM permissions to access your S3 Bucket.

Make sure the S3 statically hosted Website is still here:

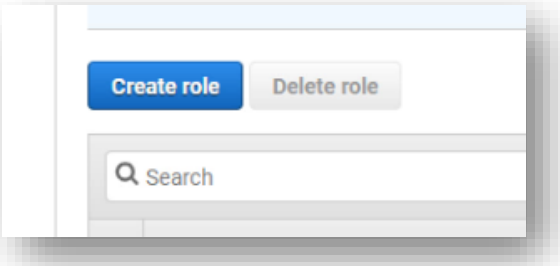


Create a new Role

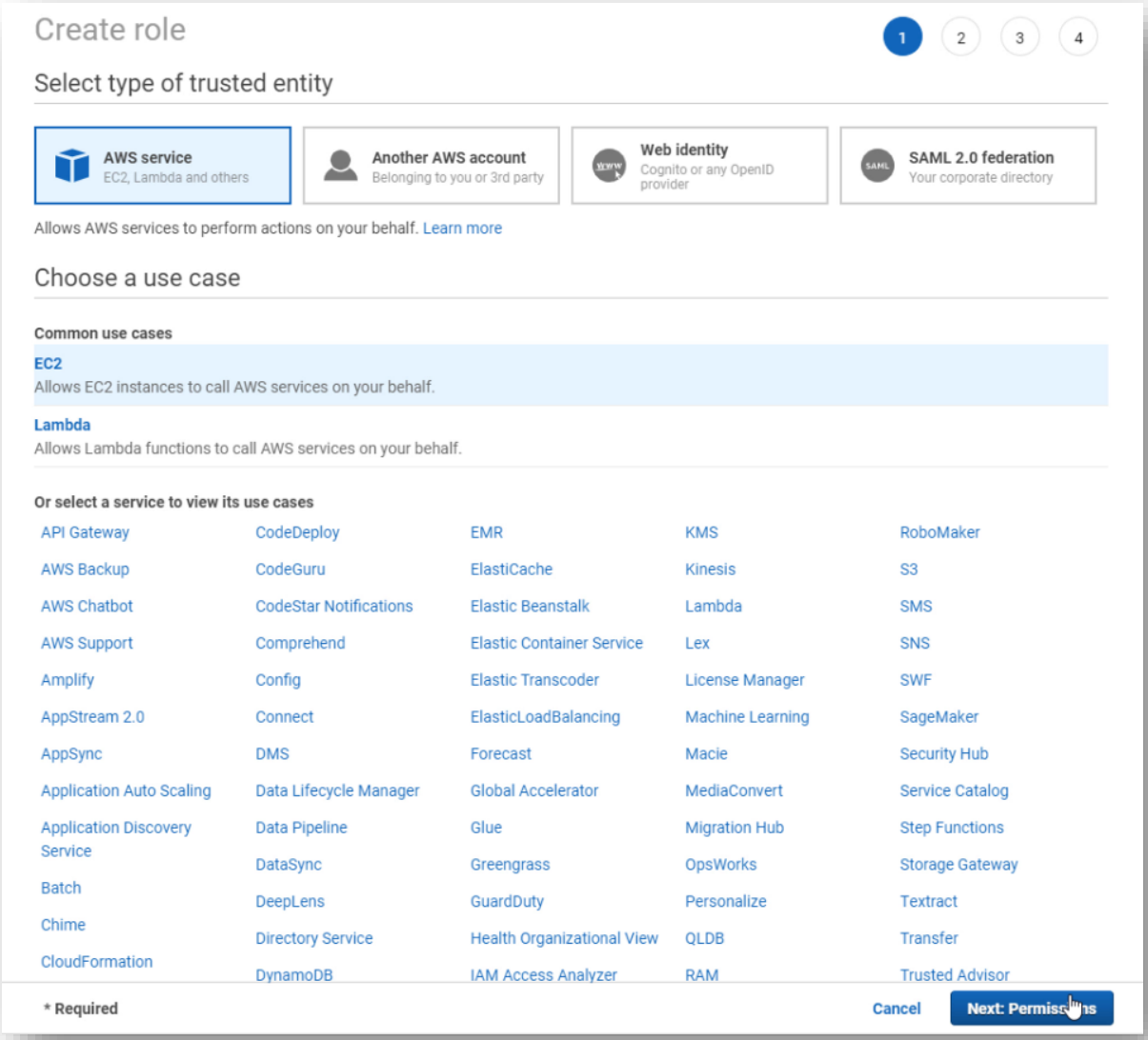
First, let's create a new IAM Role. Go to the IAM Dashboard -> Roles:



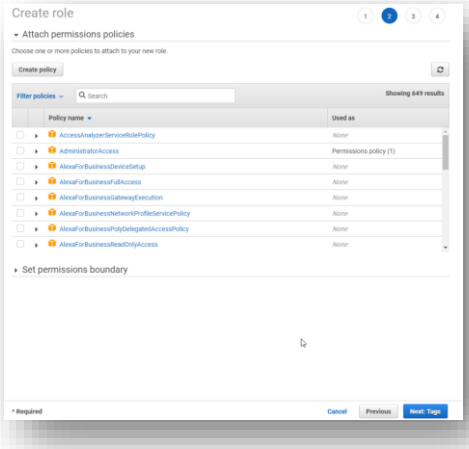
Create a new role:

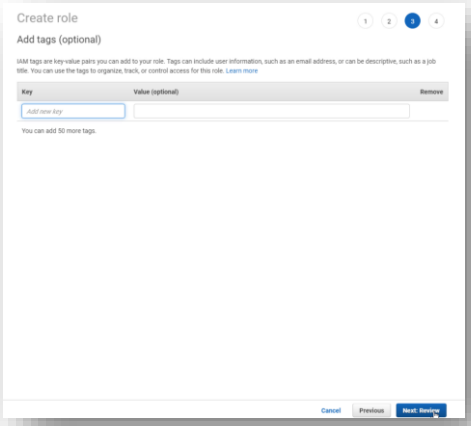


Choose AWS-Service and EC2 Role:

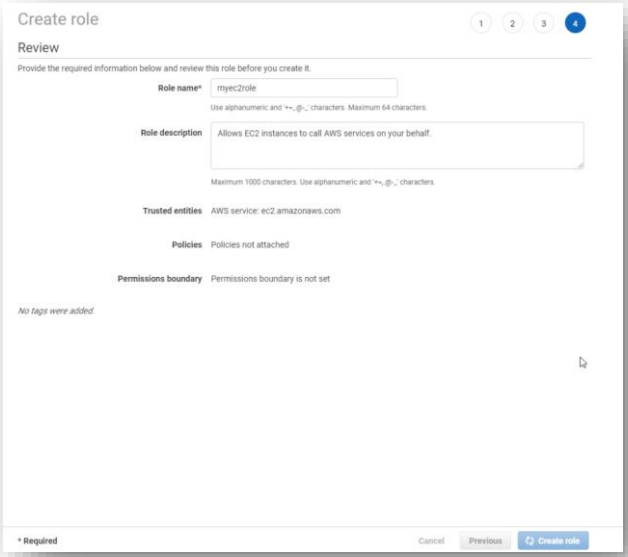


Don't attach any policy or tags:

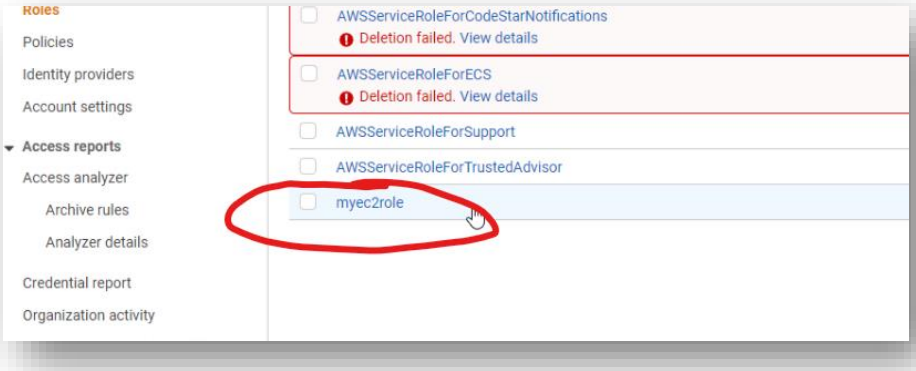




Give the Role a name:

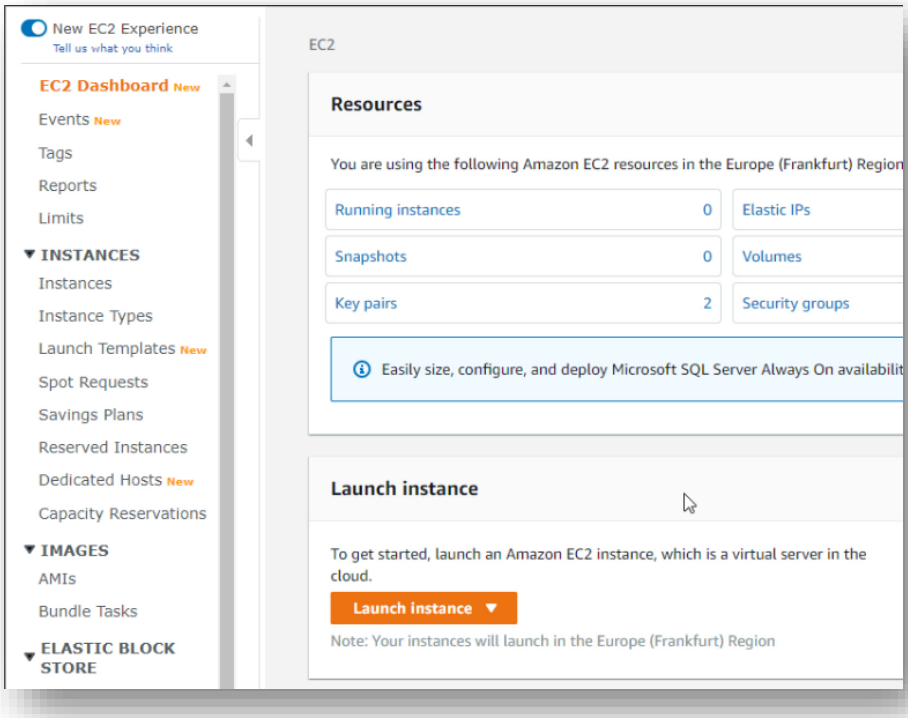


Open the new role:

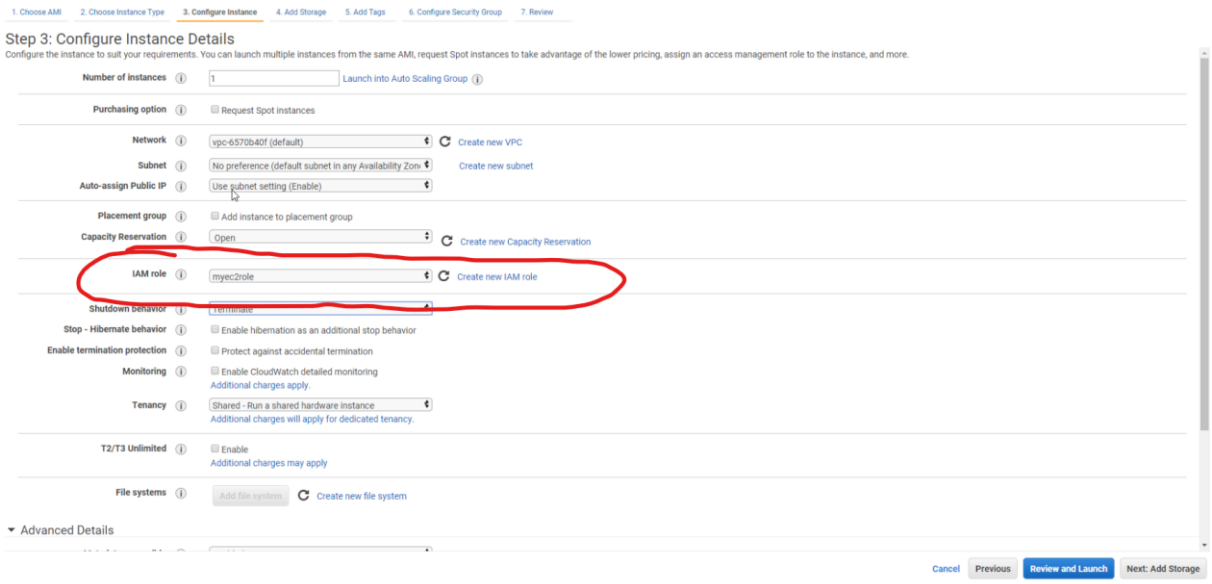


Launch an EC2 Instance

Before we add a new permission (an inline policy), let's see if we can get access to the S3 Bucket like this. Head over to the EC2 Dashboard and launch a new EC2 Instance.



Launch a new instance, choose Amazon Linux 2 AMI and t2.micro instance, but configure the instance to use the new role you created:



Launch the instance and then ssh into the instance:

```
Course 14 - Understanding Docker with AWS ECS and Fargate> ssh -i "my-keypair.pem" ec2-user@ec2-3-126-208-162.eu-central
-1.compute.amazonaws.com
The authenticity of host 'ec2-3-126-208-162.eu-central-1.compute.amazonaws.com (3.126.208.162)' can't be established.
ECDSA key fingerprint is SHA256:AOgYP2X5g1q0kfNiIpbj8qUUnsO51ZVk2tfg2v4r97I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-3-126-208-162.eu-central-1.compute.amazonaws.com,3.126.208.162' (ECDSA) to the list of k
nown hosts.

       __|  __|_  )
       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
1 package(s) needed for security, out of 7 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-41-159 ~]$ aws
usage: aws [options] <command> <subcommand> [<subcommand> ...] [parameters]
To see help text, you can run:

  aws help
  aws <command> help
  aws <command> <subcommand> help
aws: error: too few arguments
[ec2-user@ip-172-31-41-159 ~]$
```

Add an Inline Policy

Now try to run the following command:

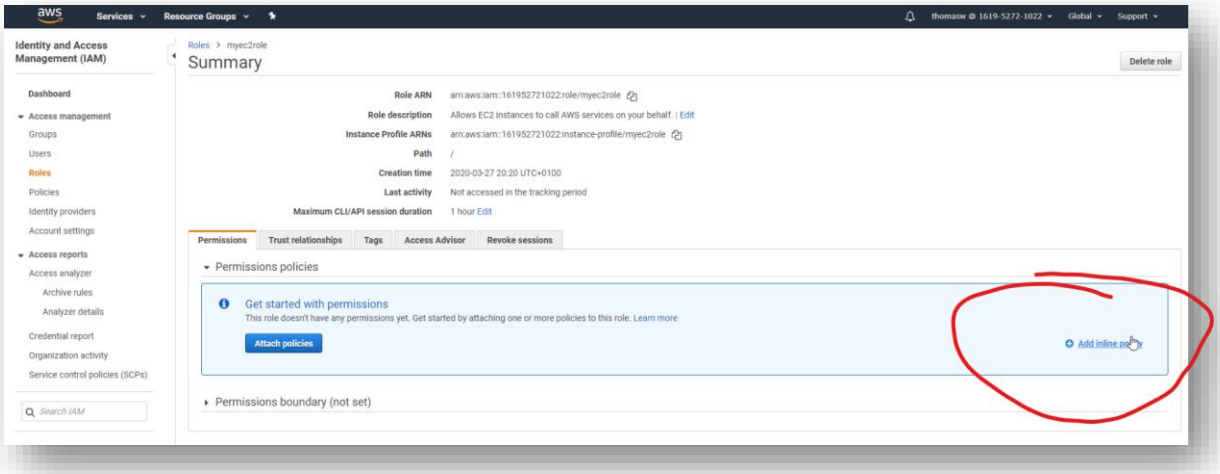
```
aws s3 ls
```

It will fail, because it doesn't have the right permissions:

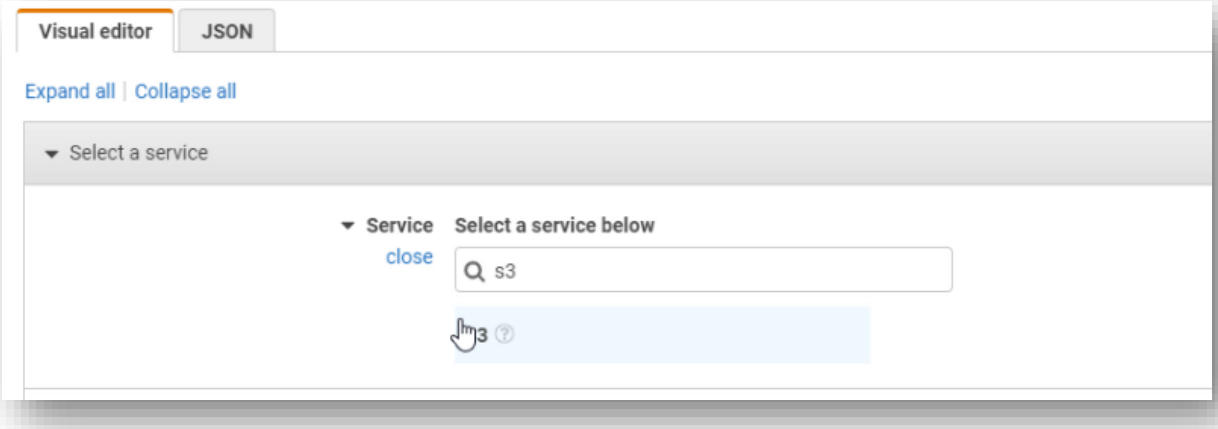
```
aws: error: too few arguments
[ec2-user@ip-172-31-41-159 ~]$ aws s3 ls

An error occurred (AccessDenied) when calling the ListBuckets operation: Access Denied
[ec2-user@ip-172-31-41-159 ~]$
```

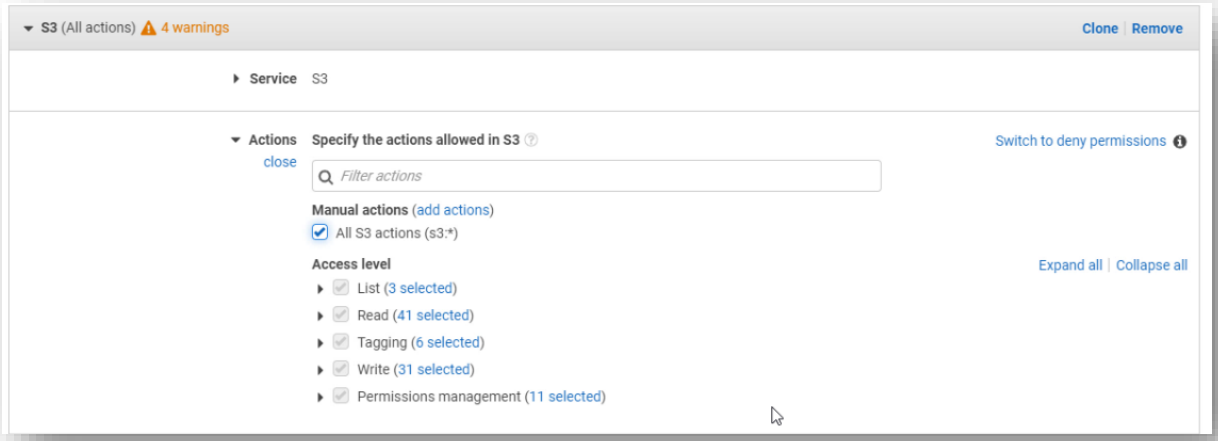
Go back to the IAM Dashboard -> roles and open the role your created. Let's add an inline policy:



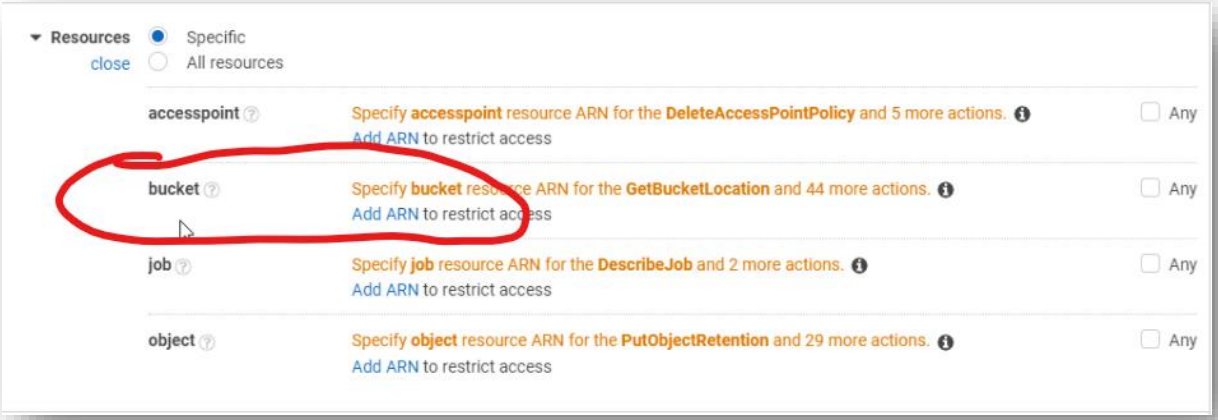
Service choose "S3":

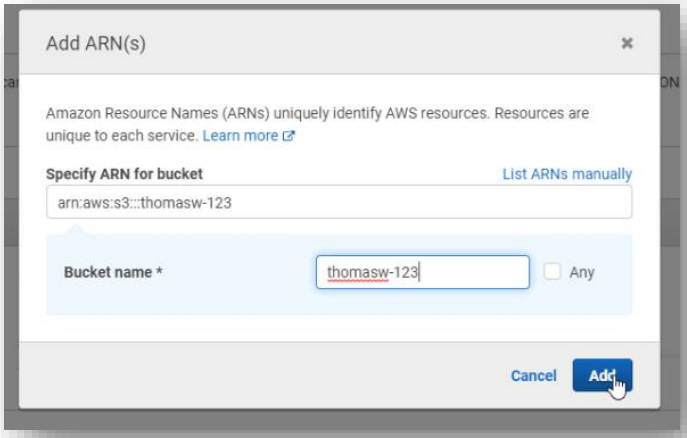


Choose all S3 actions:

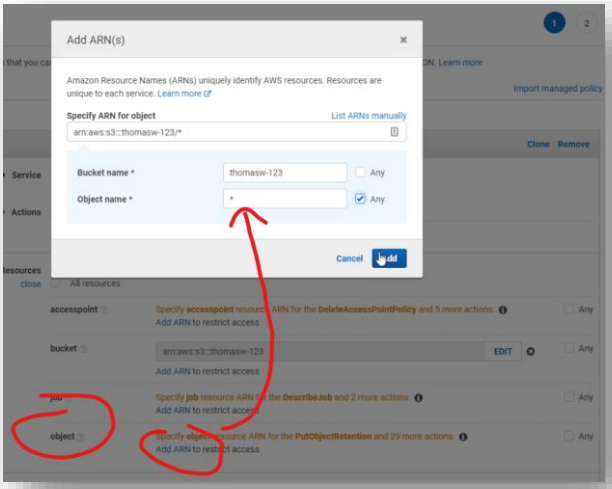


For Bucket name choose the bucket name you created earlier:

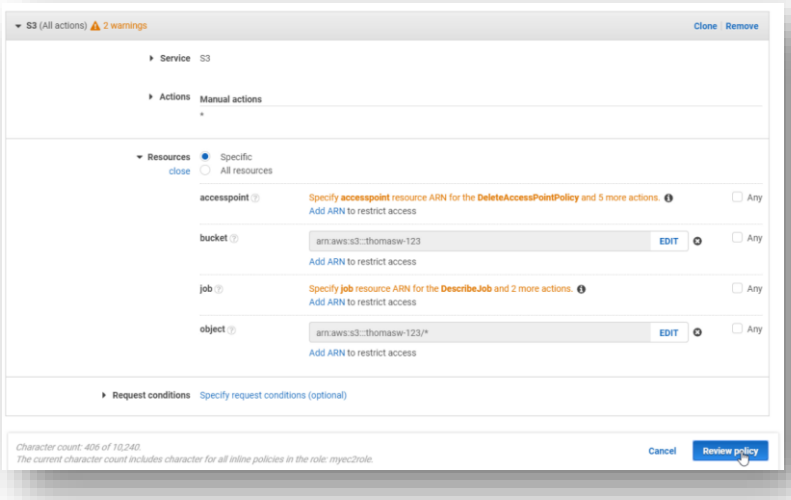




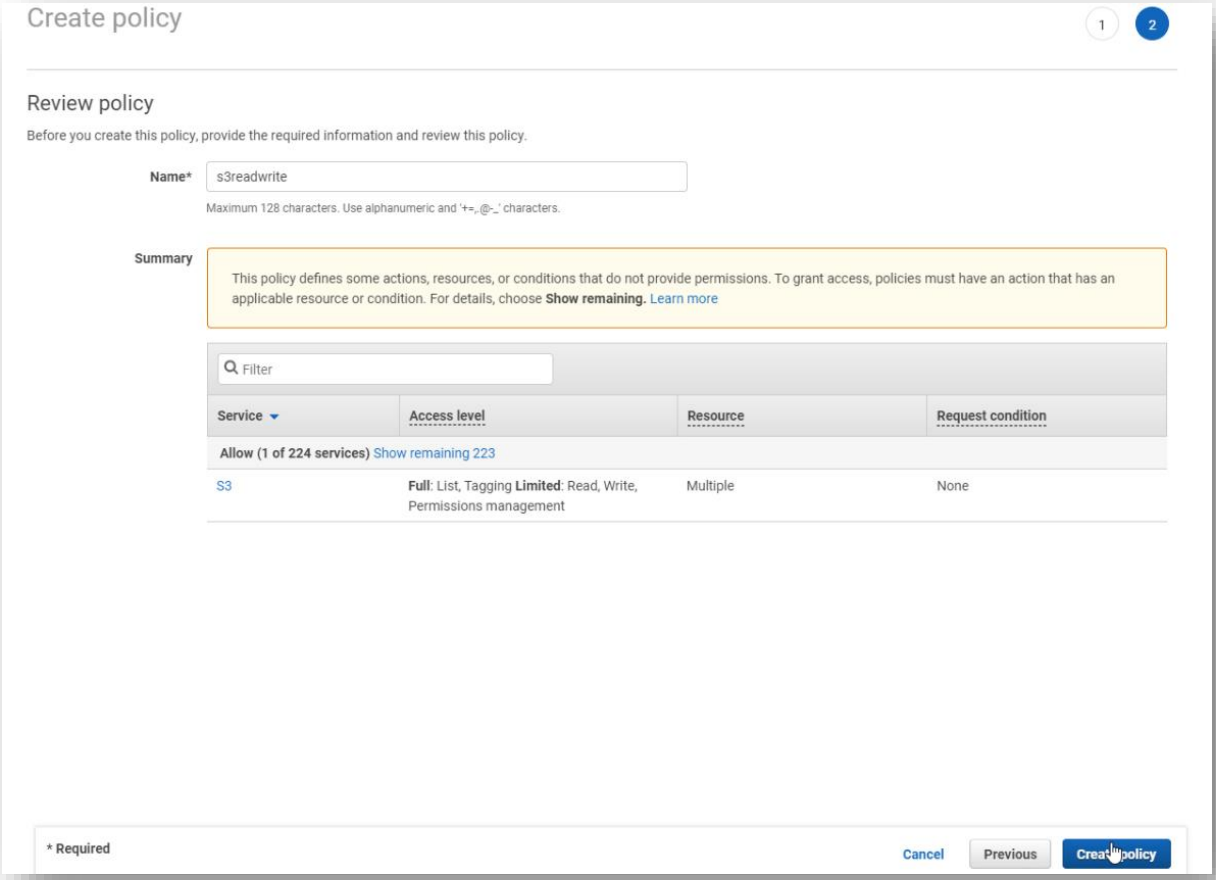
For Object name choose “any” in the bucket you created earlier:



Review your policy:

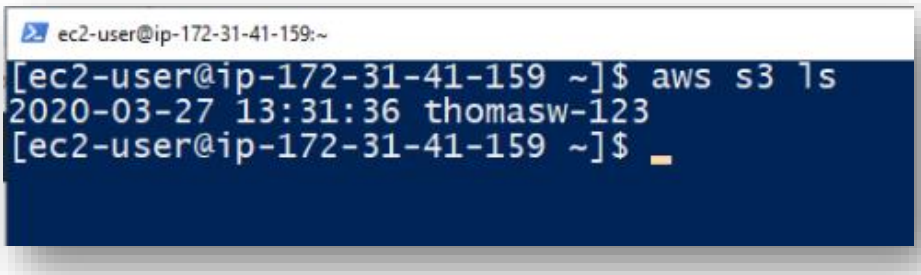


Give your policy a name:

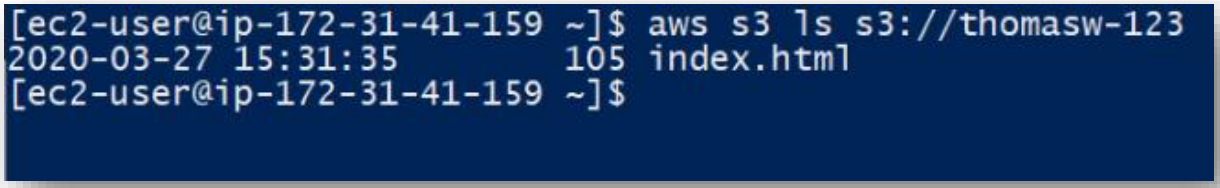


S3 CLI with inline Policy

When you try to list the buckets now from your EC2 Instance then it should work:



You can also list the contents of the bucket:



```
aws s3 ls s3://bucket-name
```

or download files:

```
[ec2-user@ip-172-31-41-159 ~]$ aws s3 cp s3://thomasw-123/index.html .
download: s3://thomasw-123/index.html to ./index.html
[ec2-user@ip-172-31-41-159 ~]$
```

```
aws s3 cp s3://bucket-name/index.html .
```

Then edit the file with nano and write some text between the body-tags:

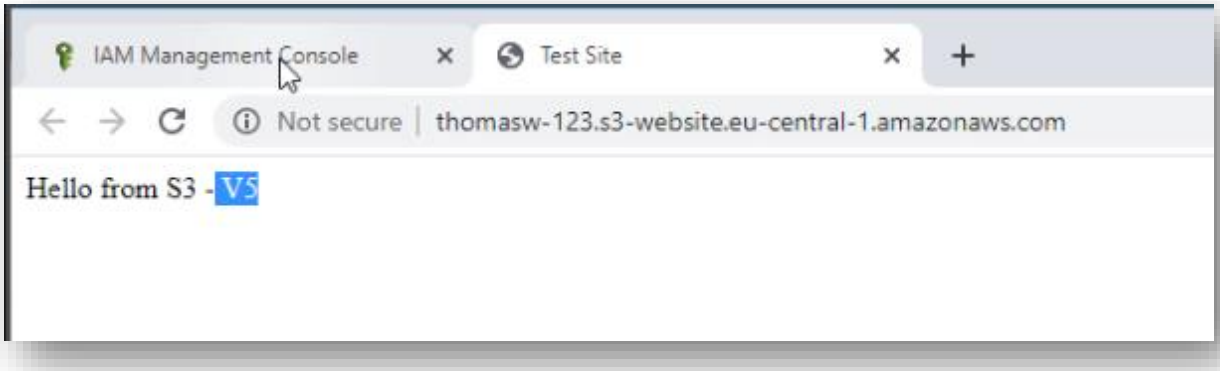
```
nano index.html
```

Note: Exit with Ctrl+x, you will be asked to save, hit return to save.

And re-upload the file:

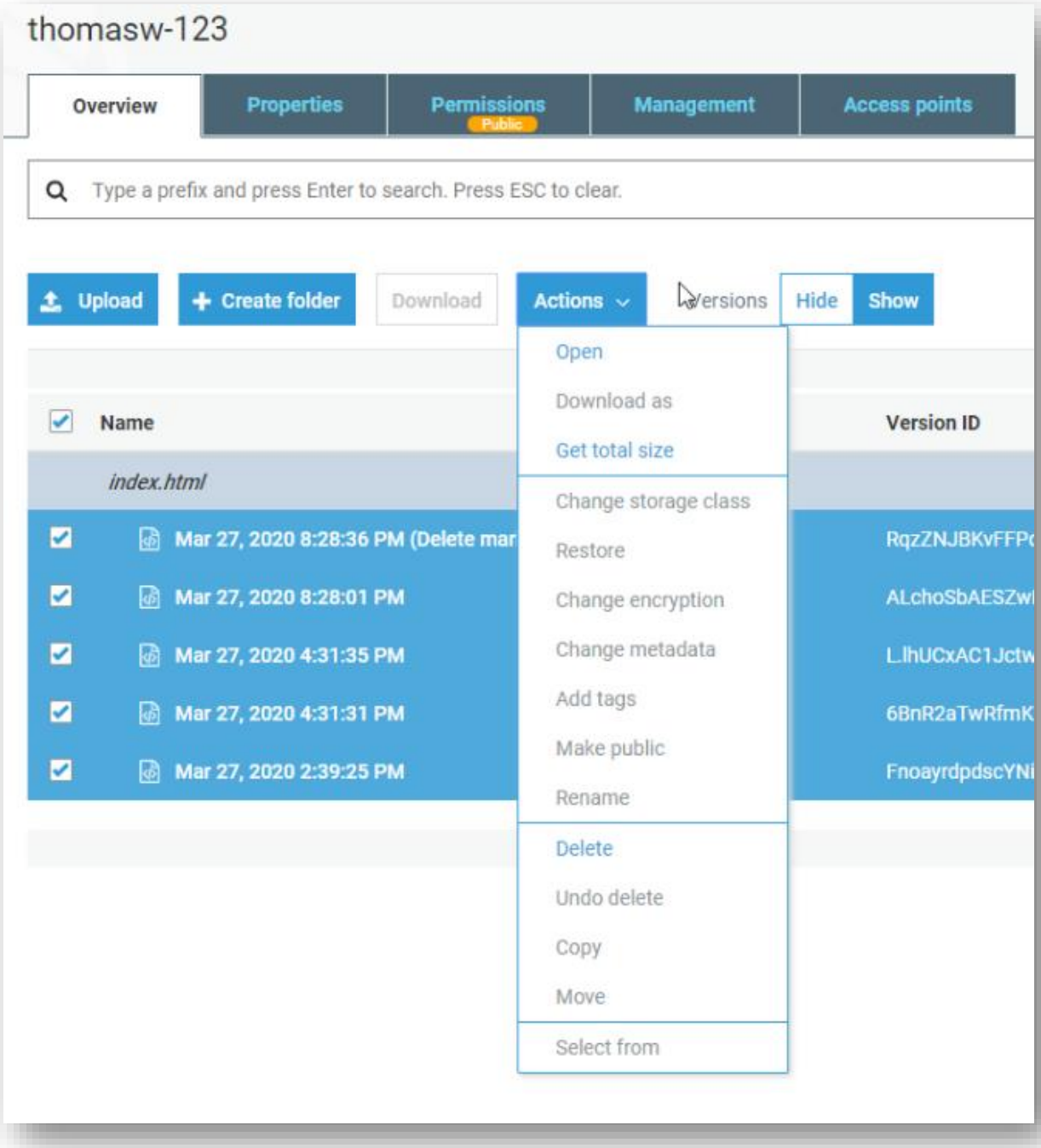
```
[ec2-user@ip-172-31-41-159 ~]$ cat index.html
<!DOCTYPE html>
<head>
    <title>Test Site</title>
</head>
<body>
    Hello from S3 - V4
</body>
[ec2-user@ip-172-31-41-159 ~]$ nano index.html
[ec2-user@ip-172-31-41-159 ~]$ cat index.html
<!DOCTYPE html>
<head>
    <title>Test Site</title>
</head>
<body>
    Hello from S3 - V5
</body>
[ec2-user@ip-172-31-41-159 ~]$ aws s3 cp index.html s3://thomasw-123/index.html
upload: ./index.html to s3://thomasw-123/index.html
[ec2-user@ip-172-31-41-159 ~]$
```

If you reload the website if should be updated immediately:



Cleanup

Delete all the versions in your S3 Bucket, otherwise you can't delete the bucket:



Then type in

```
aws s3 rb s3://bucket-name
```

```
[ec2-user@ip-172-31-41-159 ~]$ aws s3 rb s3://thomasw-123
remove_bucket: thomasw-123
[ec2-user@ip-172-31-41-159 ~]$
```

And terminate your EC2 instance, as well as remove the role you created.

Lab End
