

## **IAM LS -- Moving Data Between S3 and EC2 Instances**

### **Pre-Requisite**

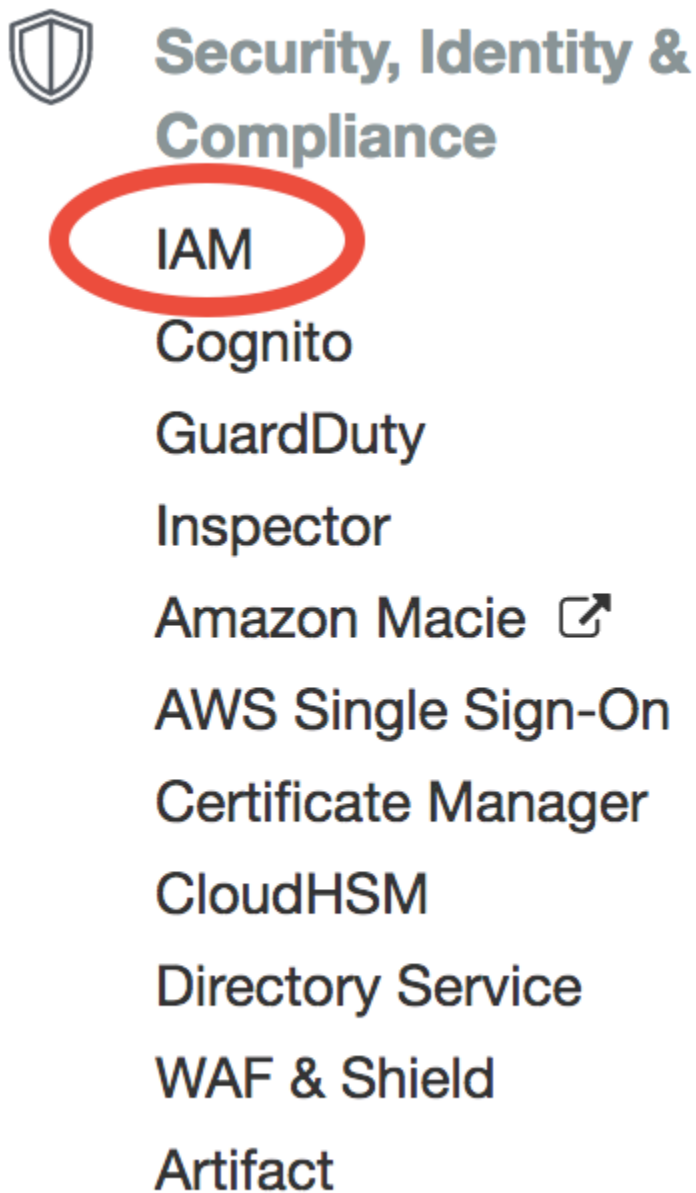
- 1. Create an IAM role with S3 read and write access.**
- 2. Create an EC2 instance with the above role**
- 3. Access the data in the S3 from EC2.**

## 1. Create an IAM role with S3 read and write access.

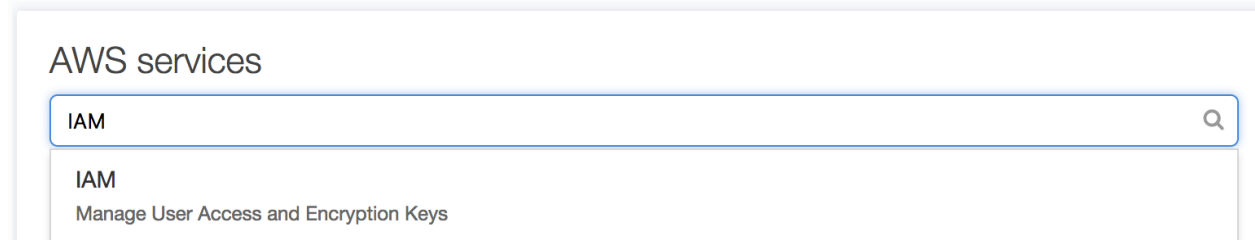
### Grant S3 permission to EC2

Create a new IAM role

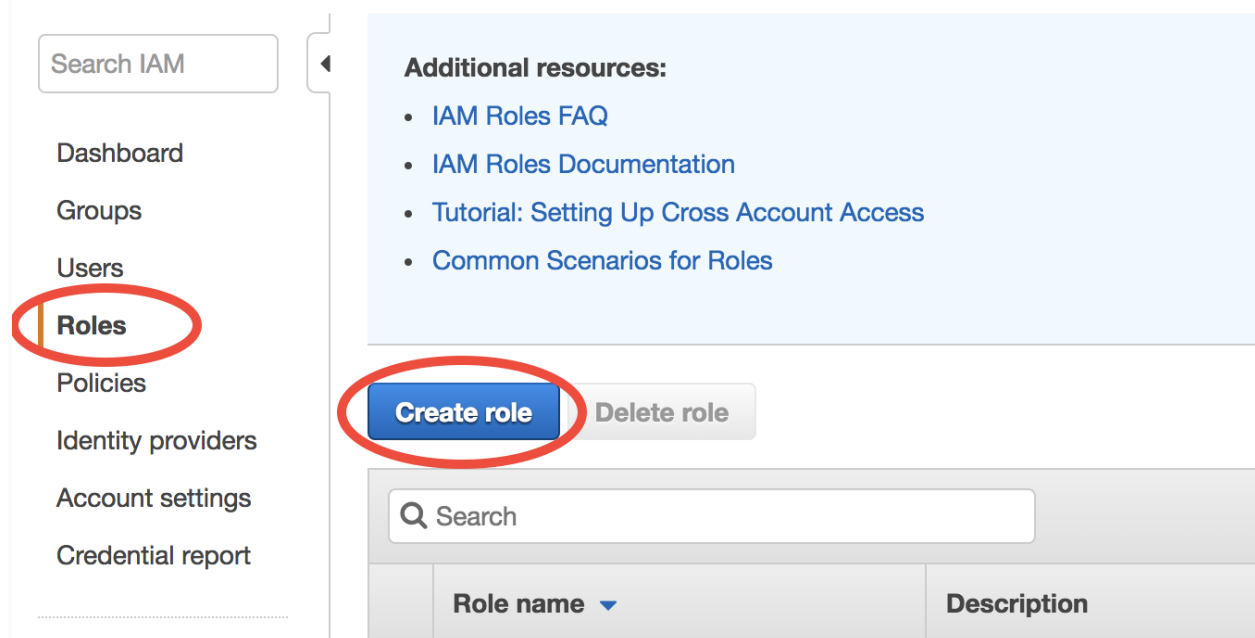
Choose “IAM” in the AWS main console:



It can also be searched from the top search bar, so you don't have to look through hundreds of AWS services:



Then choose “Roles” in the IAM console and click on “Create role”:





The first step is to choose “X” (which will be allowed to access “Y”). AWS calls it “trusted entity”. Select EC2, of course.


Create role


123

Select type of trusted entity

 **AWS service**  
EC2, Lambda and others

 **Another AWS account**  
Belonging to you or 3rd party

 **Web identity**  
Cognito or any OpenID provider

 **SAML 2.0 federation**  
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

**EC2**  
Allows EC2 instances to call AWS services on your behalf.

**Lambda**  
Allows Lambda functions to call AWS services on your behalf.

The second step is to choose “Y”. Search for “S3” and then select “AmazonS3FullAccess”:

Create role

123

Attach permissions policies





Choose one or more policies to attach to your new role.

Create policy

Refresh

Filter: Policy type

Showing 4 results

	Policy name	Attachments	Description
<input type="checkbox"/>	 AmazonDMSRedshiftS3Role	0	Provides access to manage S3 settings for Redshift endpoin...
<input checked="" type="checkbox"/>	 AmazonS3FullAccess	0	Provides full access to all buckets via the AWS Management...
<input type="checkbox"/>	 AmazonS3ReadOnlyAccess	0	Provides read only access to all buckets via the AWS Manag...
<input type="checkbox"/>	 QuickSightAccessForS3StorageManagement...	0	Policy used by QuickSight team to access customer data pr...

Finally, give this role a descriptive name. Here I use “full\_S3\_access\_from\_EC2”. (For the “Role description”, enter whatever you like or just keep default.)

### Create role

1

2

3

#### Review

Provide the required information below and review this role before you create it.

**Role name\***

full\_S3\_access\_from\_EC2

Use alphanumeric and '+=, @-\_' characters. Maximum 64 characters.

**Role description**

Allows EC2 instances to have full control on S3 resources on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=, @-\_' characters.

**Trusted entities**

AWS service: ec2.amazonaws.com

**Policies**



AmazonS3FullAccess



Now a new IAM role is created. This only needs to be done once.

### Assign that role to EC2

Whenever you launch a new EC2 instance, in “Step 3: Configure Instance Details”, select the IAM role you created previously for the “IAM role” option.

## 2. Create an EC2 instance with the above role

The screenshot shows the 'Step 3: Configure Instance Details' page in the AWS Management Console. The page has a progress bar at the top with steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance (active), 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. Below the progress bar, the title 'Step 3: Configure Instance Details' is followed by a description: 'Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage more.' The form contains several sections: 'Number of instances' (set to 1) with a 'Launch into Auto Scaling Group' link; 'Purchasing option' (radio button for 'Request Spot instances' is unchecked); 'Network' (dropdown set to 'vpc-d5c6d2b3 (default)' with a 'Create new VPC' link); 'Subnet' (dropdown set to 'No preference (default subnet in any Availability Zone)' with a 'Create new subnet' link); 'Auto-assign Public IP' (dropdown set to 'Use subnet setting (Enable)'); and 'IAM role' (dropdown set to 'full\_S3\_access\_from\_EC2' with a 'Create new IAM role' link). The 'IAM role' dropdown is circled in red.

No need to touch other options on this page and just launch as usual. On this EC2 instance, **you don't need to run** `aws configure`,

and commands like `aws s3 ls` will just work (as long as AWSCLI is installed). .

This is actually a better practice since you never type your security credentials on this server (which might be stolen if your server gets hacked).

```
[root@ip-172-31-26-222 ec2-user]# aws s3 cp s3://b15-bucket001/Index.html index.html
download: s3://b15-bucket001/Index.html to ./index.html
[root@ip-172-31-26-222 ec2-user]# ls
file1  fold1  index.html
```

The above command is to download the file from S3 bucket

```
[root@ip-172-31-26-222 ec2-user]# aws s3 cp file1 s3://b15-bucket001
upload: ./file1 to s3://b15-bucket001/file1
```

```
$ aws s3 cp <local filename> s3://<<bucketname>>
```

This is to upload the file to s3 bucket.