

## Configuring Amazon S3 security settings and access controls

<

Attach IAM Role to EC2 Instance

Getting started at an AWS hosted workshop

- ▼ S3 Security Best Practices
  - ▼ Prepare Your Lab

## Attach IAM Role to EC2 Instance

Connect to the EC2 Instance
Bucket Name

- ▶ Lab 1 S3 Security Exercises
- ▶ Lab 2 S3 Access Grants
- ► Lab 3 Enabling Malware Protection for S3 by using GuardDuty
- ► Lab 4 S3 Access Control Lists Lab Summary

## Attach iAM Role to ECZ ilistance

## Attach an IAM Role to the Running EC2 Instance

IAM roles are designed so that your applications can securely make API requests from your instances, without requiring you to manage the security credentials that the applications use. Instead of creating and distributing your AWS credentials, you can delegate permission to make API requests using IAM roles.

Configuring Amazon S3 security settings and access controls > S3 Security Best Practices > Prepare Your Lab >

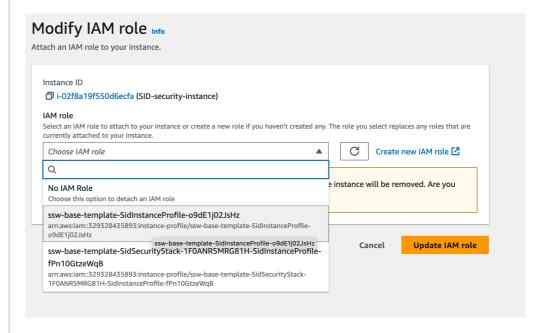
In this case the Role has already been created as part of the setup.

From the AWS console in the top search bar, search and select EC2.

- There should be an EC2 instance running called SID-security-instance.
- Click the check box next to the instance.
- Click Actions.
- Click Security.
- Click Modify IAM role.
- Select the role that begins with ssw-base-template-SidInstanceProfile- (it should have an alpha-numeric string at the end of it)

Keep in mind that the alpha-numeric string at the end of the role will be different for each person

After following the instructions your screen should look like the following:



Now click Update IAM role

In the following instructions we will connect to the EC2 instance that we assigned the role to.

