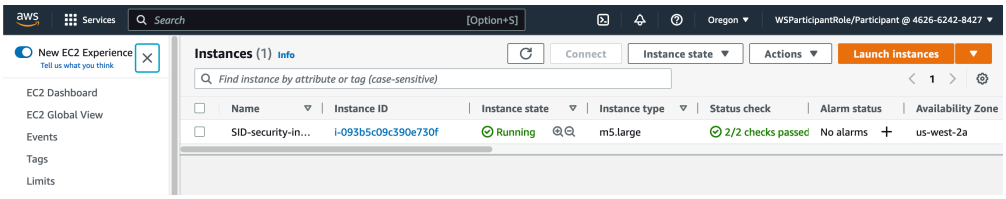
# Testing GuardDuty Malware with an object.

Now that we have GuardDuty configured with our S3 bucket, we will create an object and test whether GuardDuty tags the object correctly.

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

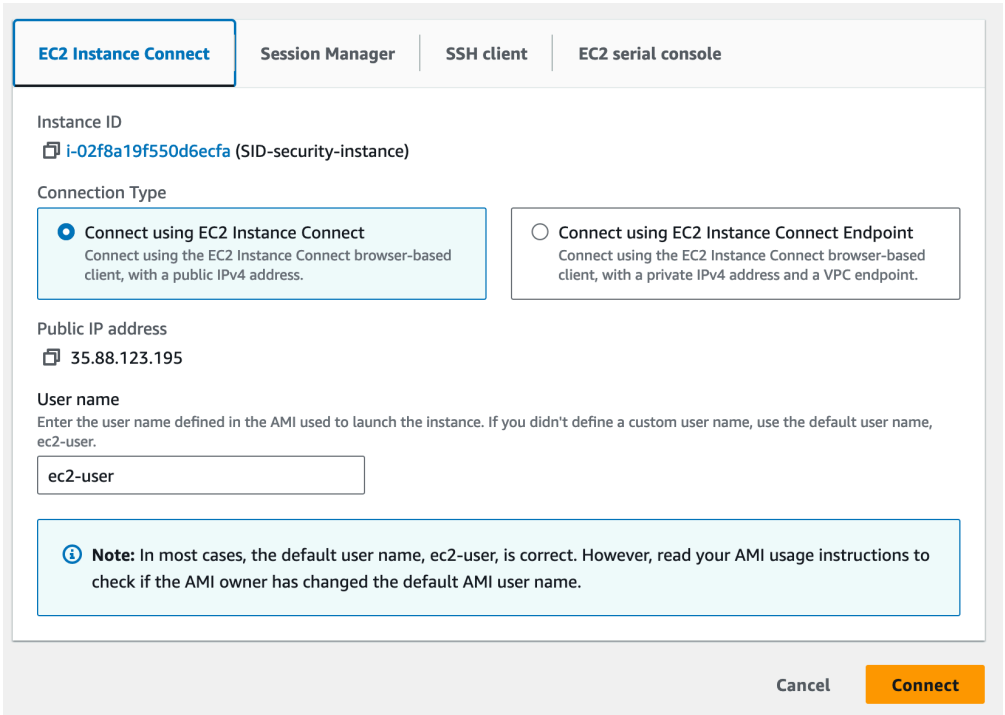
## Connect to the EC2 Instance using EC2 Instance Connect



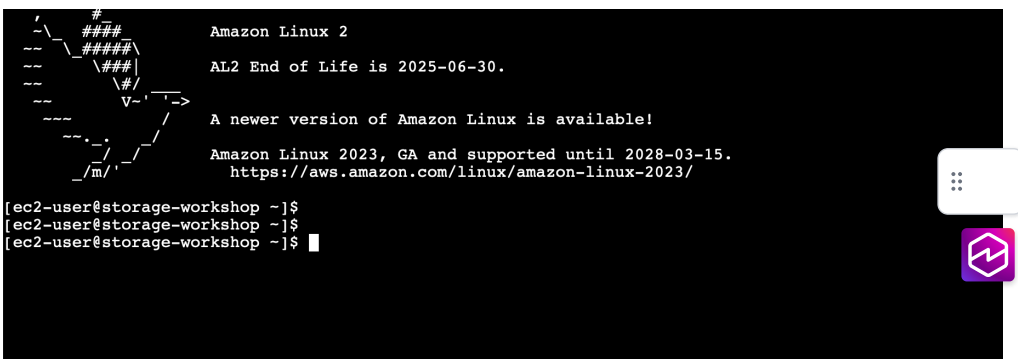

Right click the `SID-security-instance` and click `connect`.

Select the `EC2 Instance Connect` (browser-based SSH connection).

Set the User name to `ec2-user` if not already. It should look like the following:




If your screen looks correct, click `Connect`. Your screen should look similar to the following:



This is where we will create two test objects:

- Let's create a test object by using the following code:

```
echo 'This is a test object with text.' >> testobject.txt
```

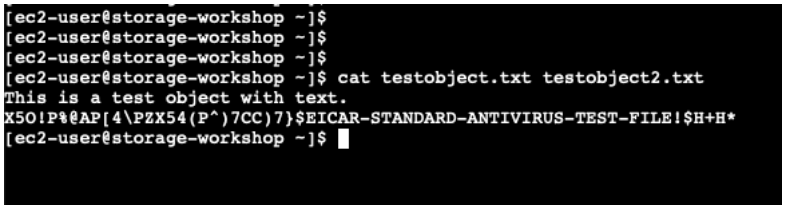
- Now let's create another test object but this time we will use a string:

```
echo 'X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*' >> testob 2.
```

- Let's ensure those two files were created correctly, as we will use them for our test.

```
cat testobject.txt testobject2.txt
```

- Your screen should have two that corrispond to each file, like this:




---

Now we can create a test by uploading each of those files to S3. *Note* Make sure to change the name of the s3 bucket to the one in your account.

```
aws s3 cp testobject.txt s3://${bucket}
aws s3 cp testobject2.txt s3://${bucket}
```

---

Let's check whether the object gets tagged appropriately:

- First we can check the testobject.txt:

```
aws s3api get-object-tagging --key testobject.txt --bucket ${bucket}
```

- Then the testobject2.txt:

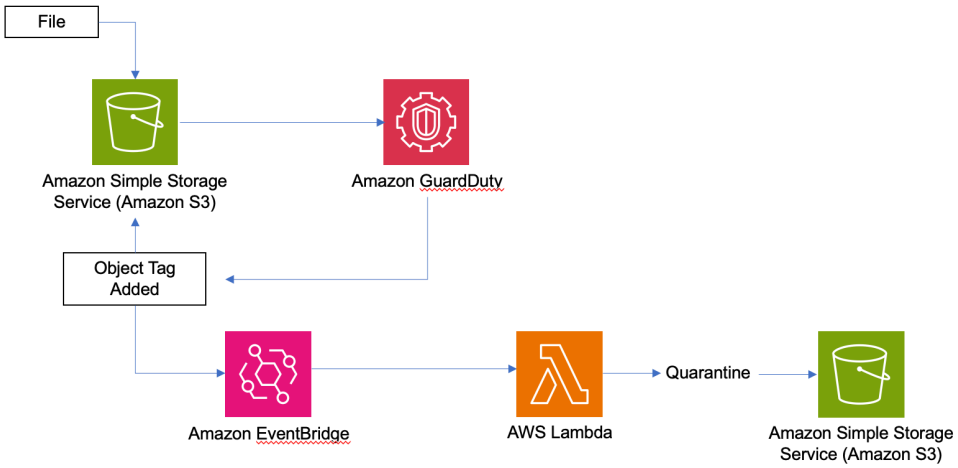
```
aws s3api get-object-tagging --key testobject2.txt --bucket ${bucket}
```

Your screen should look something like this:


Take note of how the test file we created with the fake malware signature was tagged appropriately but the other object was not.

- Using the tags on the object is a great way to take action on the objects that are tagged as a threat and quarantine them or delete them, depending on the environment and use case. For example you

could do something like:




**Lab complete**
Congratulations you have completed the GuardDuty Malware Protection for S3 lab. In this lab, you learned how to configure GuardDuty Malware Protection to detect the presence of threats within S3 buckets.

Previous Next