

Threat Defense Workshop Guide

Preparation Guide

September 2017

Table of Contents

[About this Document 3](#_Toc493780310)

[Amazon Login 3](#_Toc493780311)

[AWS Limit Increase 3](#_Toc493780312)

[Ubuntu Instance 5](#_Toc493780313)

[Creating DNS on Route 53 6](#_Toc493780314)

[Buying a New Domain 6](#_Toc493780315)

[S3 Bucket Creation 6](#_Toc493780316)

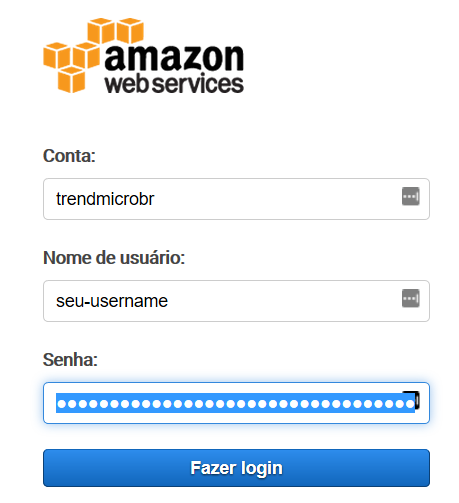
# About this Document

This guide explains how to prepare an AWS account to host a Threat Defense Workshop. This is a mandatory action that must be done once in a given AWS account to workshop work.

# Amazon Login

Access the following URL to enter AWS: <https://trendmicrobr.signin.aws.amazon.com/console>

**Note:** If you are not using Trend Micro Brazil AWS account, please use the provided URL.

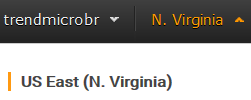


Account: trendmicrobr **or** the provided account

Username: **<your-username>**

Password: **<your-password>**

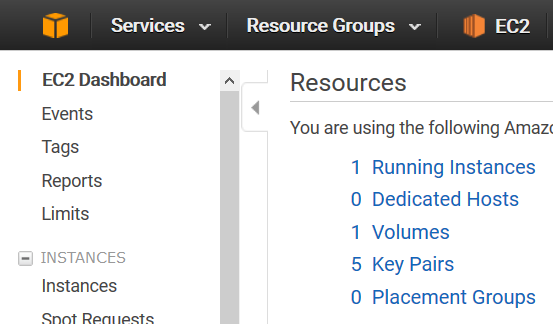
**Note:** After the login, make sure you stay at logged in “North Virginia” during all times, as the workshop must be run in this region.



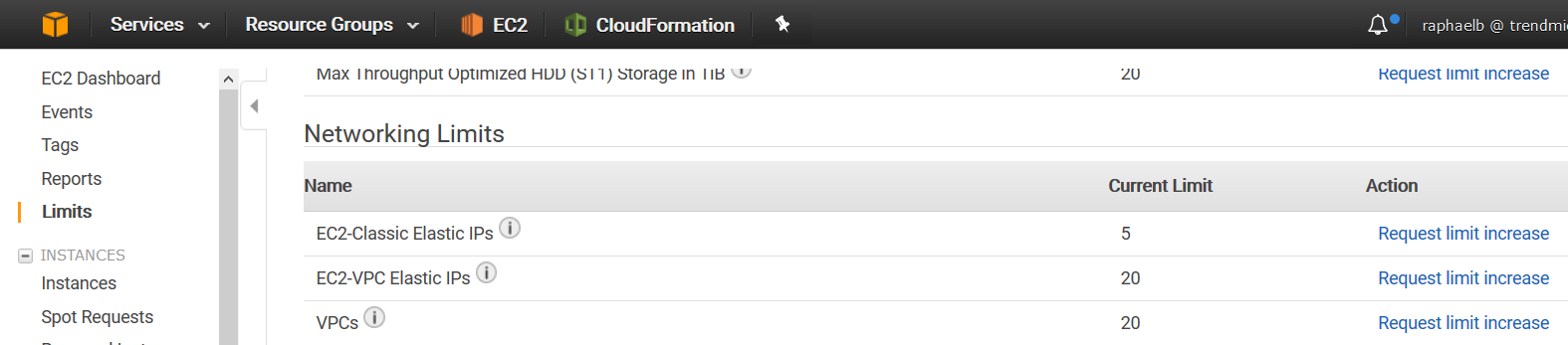
# AWS Limit Increase

By design, AWS has some limitations that must be lifted in order to run the Threat Defense Workshop. These limitations includes, but are not restricted to, number of t2.medium EC2 instances, EIP, etc.

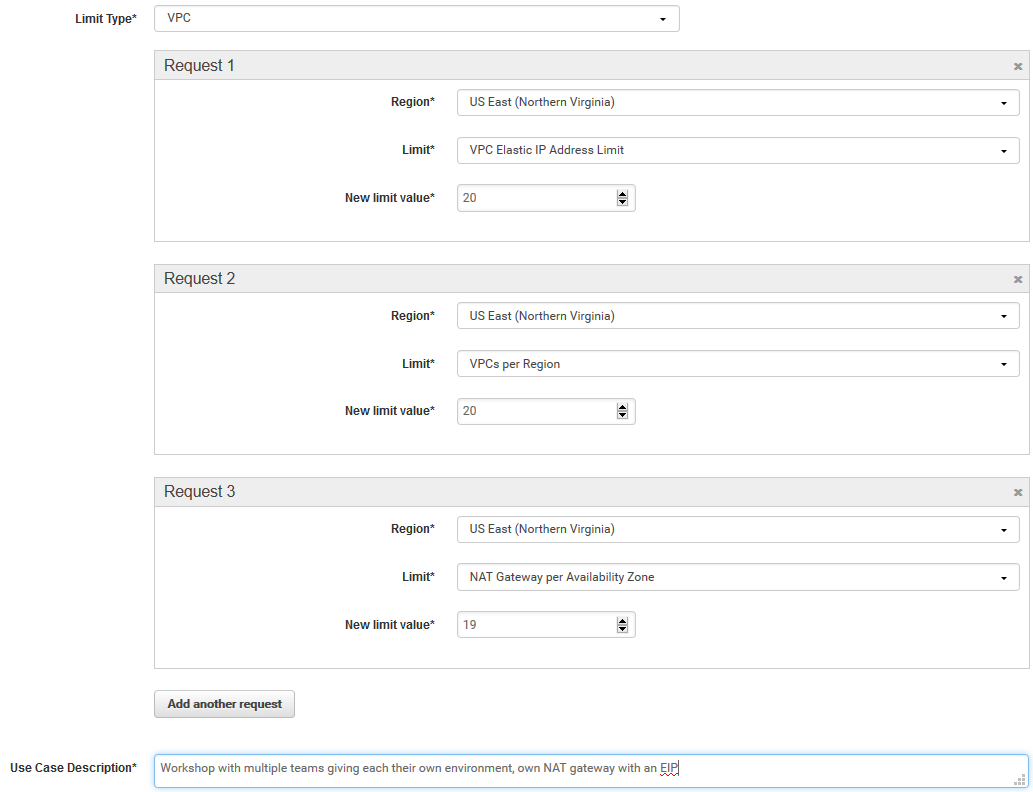
First, login to the AWS account and go to the EC2 service. On the left pane, click on “Limits”:



Click on “Request limit increase” next to “VPCs”:

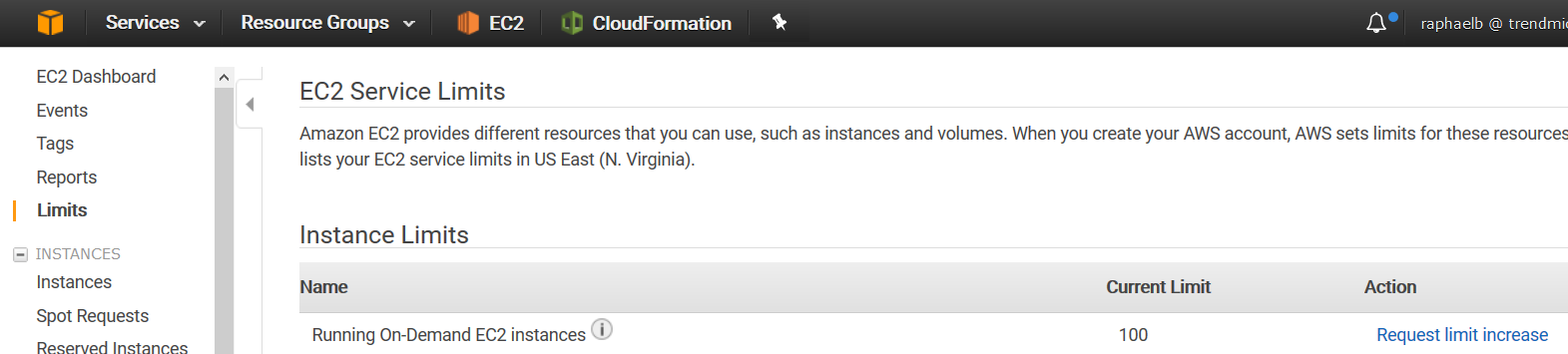


In the following screen, fill the form as below:

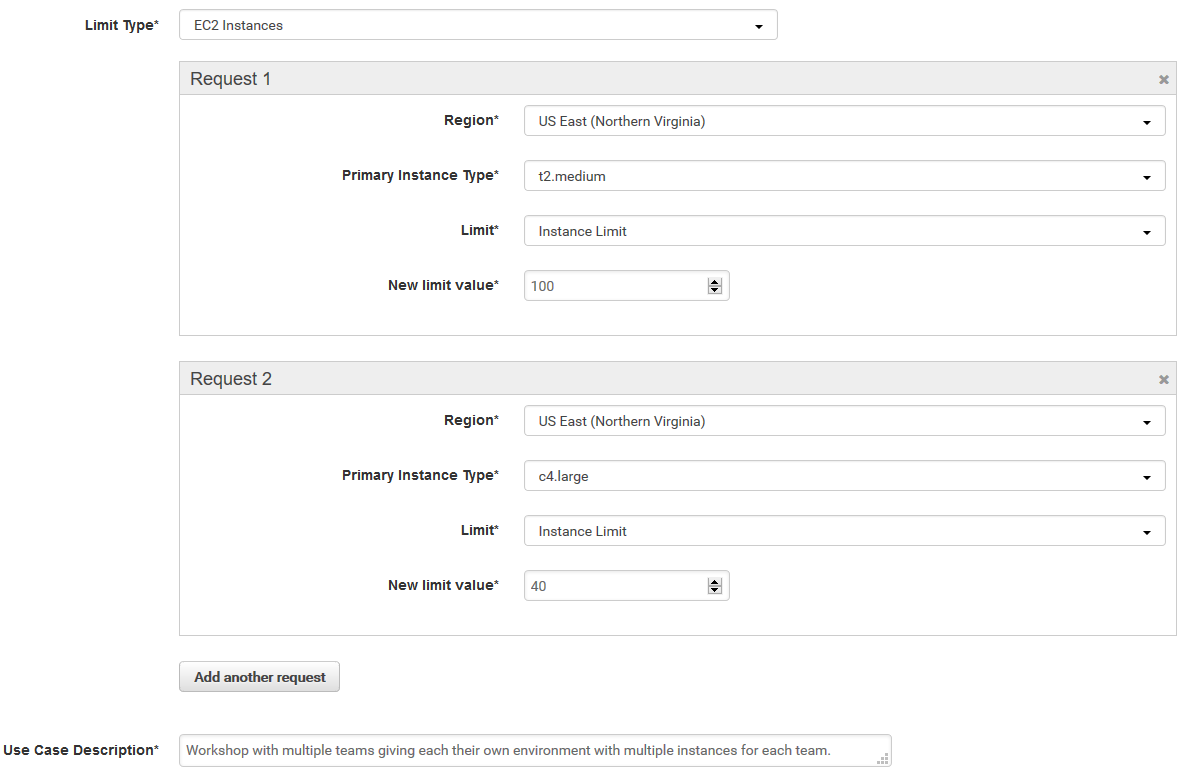


Click on “Submit” to send the request to increase the limit.

Now it is needed to increase the limit of EC2 machines. To do so, open the “Limits” window again and click on “Request limit increase” next to “Running On-Demand EC2 instances”:



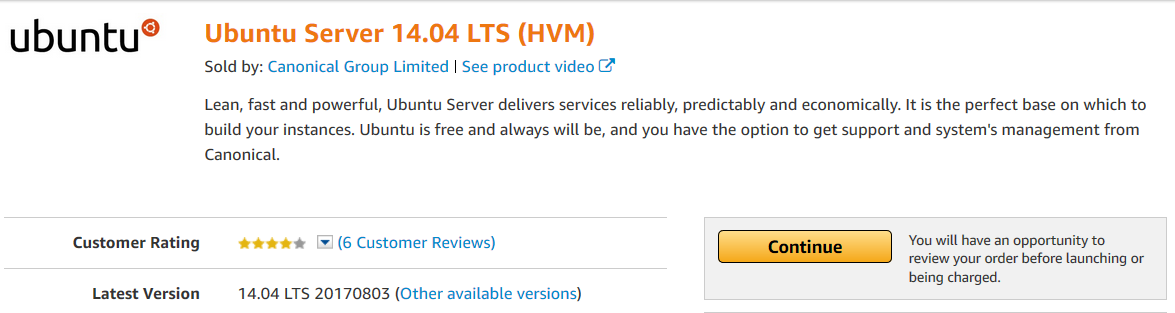
Fill the form as below:



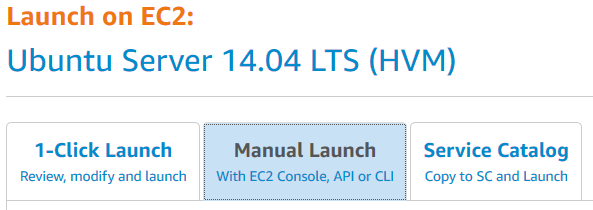
Click on “Submit” to send the request for limit increase. It could take up to 24 hours to both requests get processed and the limits increeseded.

# Ubuntu Instance

One key component of the CTF infrastructure is the Controller machine. Although the Controller will not be instantiated now, it is mandatory to authorize the AWS account to run Ubuntu machines. To do so, go to the following URL: <http://aws.amazon.com/marketplace/pp?sku=b3dl4415quatdndl4qa6kcu45>



Click on the yellow “Continue” button on the right and, in the following screen, click on the “Manual Launch” tab:



Click on “Accept Software Terms” on the right.

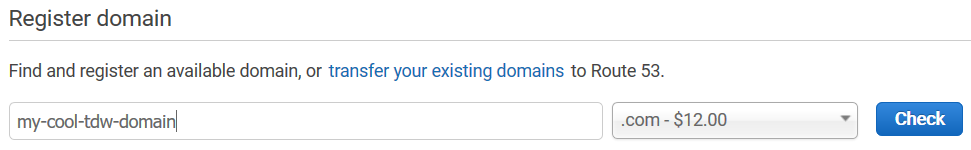
# Creating DNS on Route 53

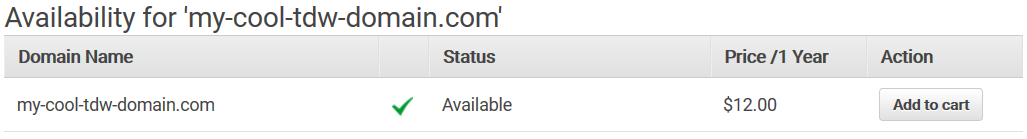
It is mandatory to have a DNS hosted on Route 53 to execute the TDW. It is possible to use a domain already hosted on Route 53, buy a new one straight from Route 53 or migrate an existing domain to Route 53 (not covered in this material).

If you already have a DNS in Route 53, you can skip this step.

## Buying a New Domain

Open the Route 53 service. On the middle panel, go to “Register domain” and enter the desired domain name, select the top level domain (.com, etc) and click on “Check”:



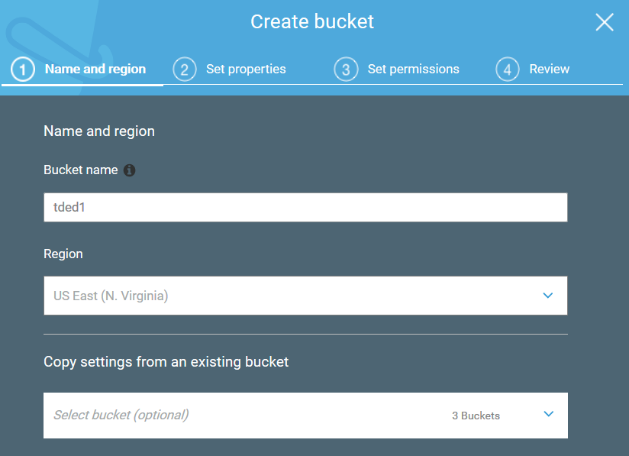
Click on “Add to cart” next to the desired domain name in the following screen: 

Click on “Continue” and fill all the forms with your data. It could take up to a couple of days to the domain appears as available to use to you.

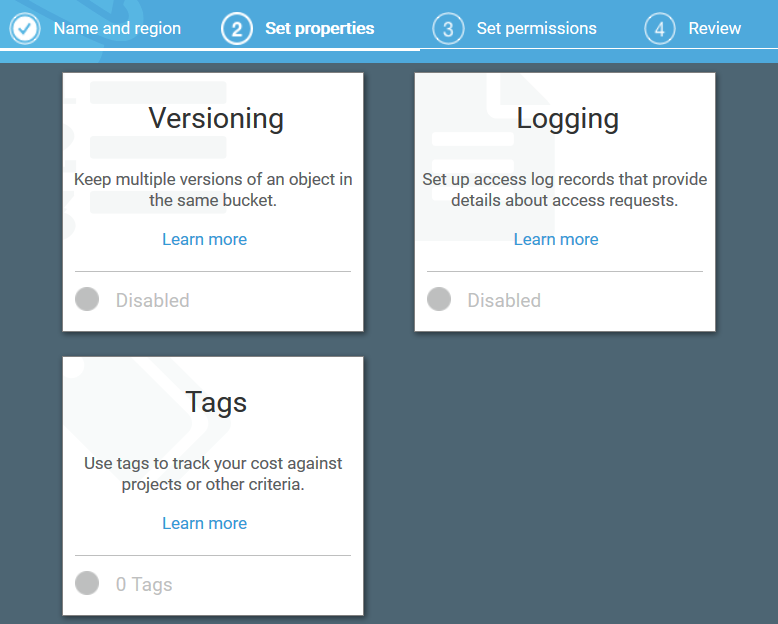
# S3 Bucket Creation

This step is **optional**, as one could use the already available and configured Trend Micro Brazil S3 bucket. If you decide to use your own S3 bucket, open the S3 service and click on “Create Bucket”.

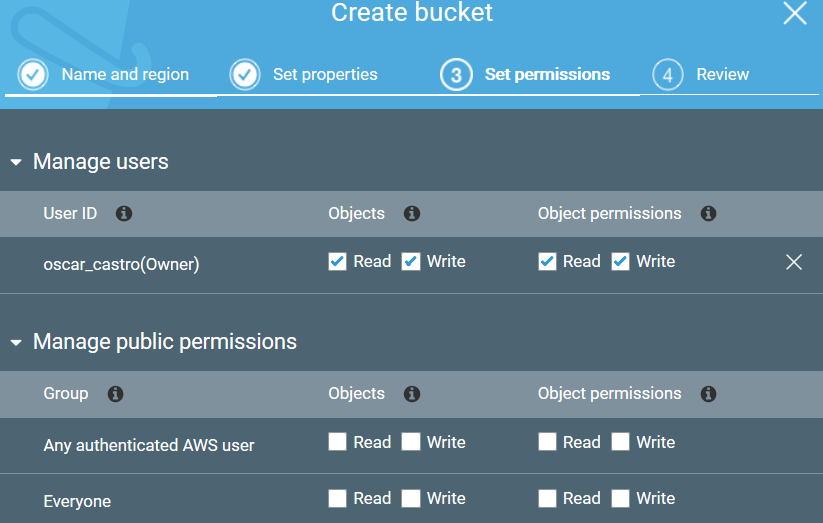
In the new window, select a name for the new bucket and make sure the region is “US East (N. Virginia):



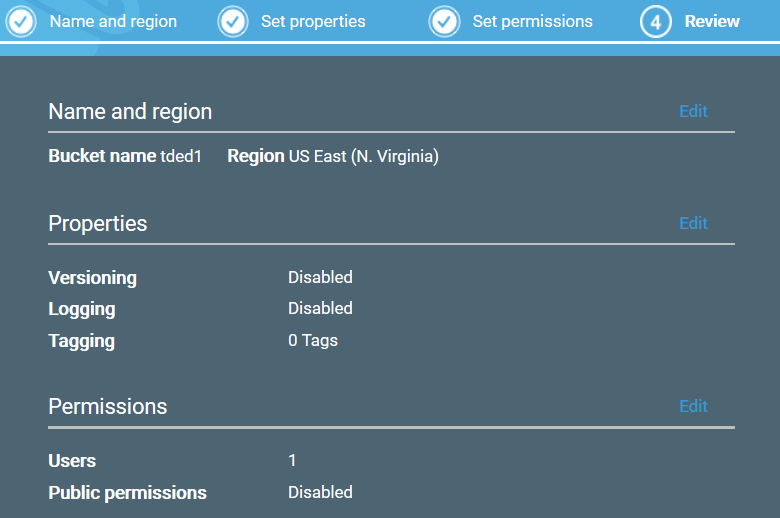
Do not select any option in the following screen:



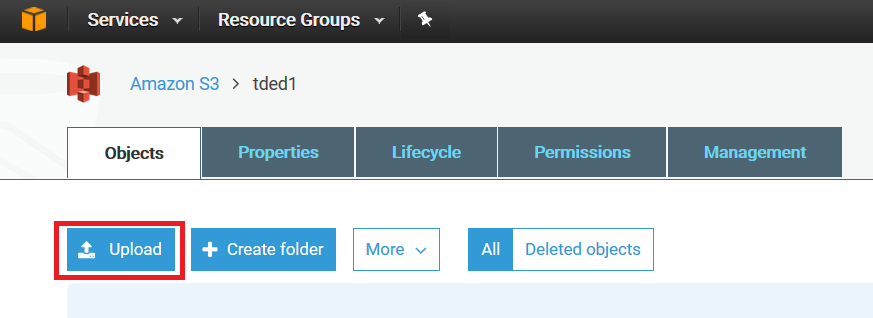
In addition, make sure the owner has Read and Write permissions just like below:



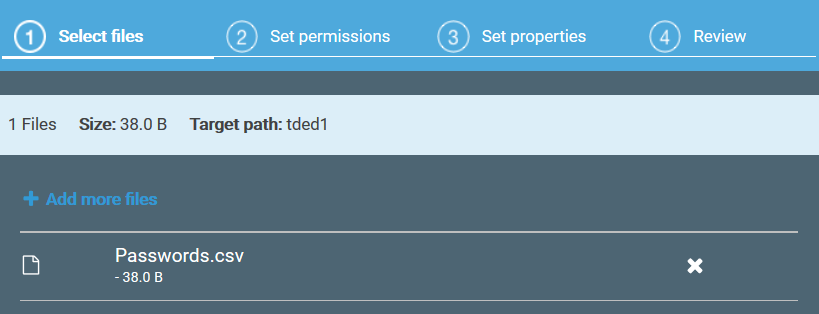
A summary just like below will show up. If everything seems to be ok, confirm:



In the bucket page, select “Upload”:

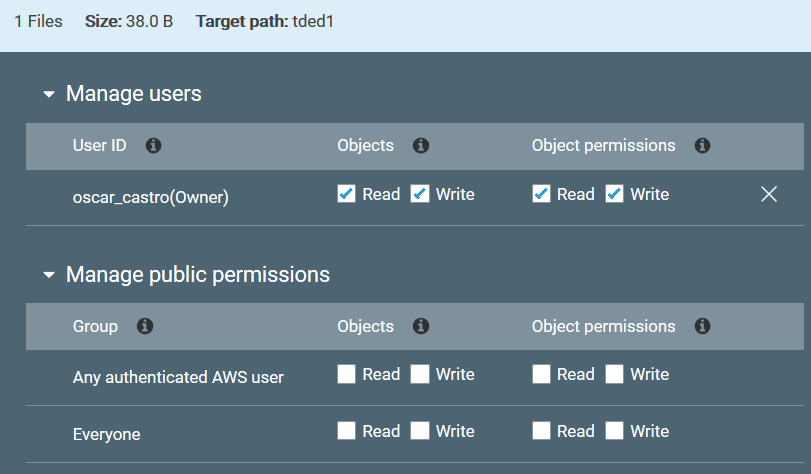


Select the “Passwords.csv” file in the “CTF Files” folder:

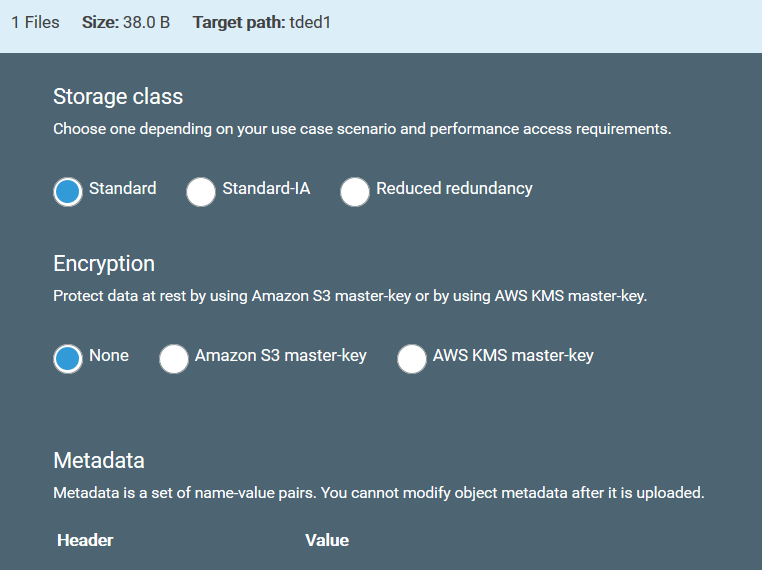


**Note:** This csv is the one used in Trend Micro Brazil S3 bucket. If you wish, change the file as desired to suit your needs before uploading it.

Set the permissions as below in the new window:



In the following screen, select “Standard-IA”:



Accept the upload in the last screen:

