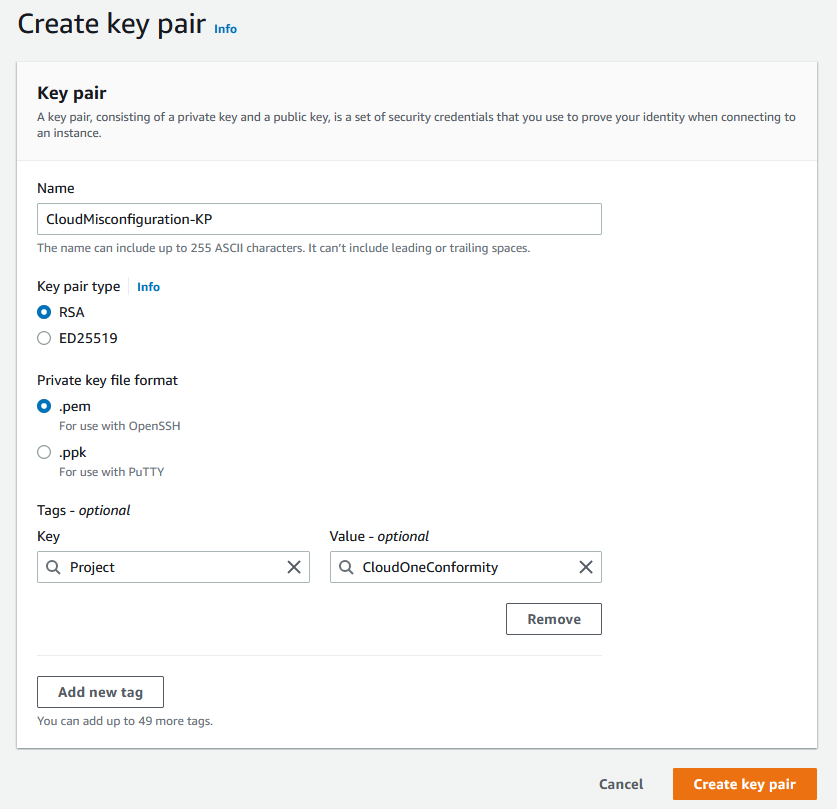
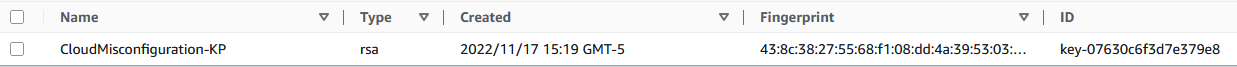
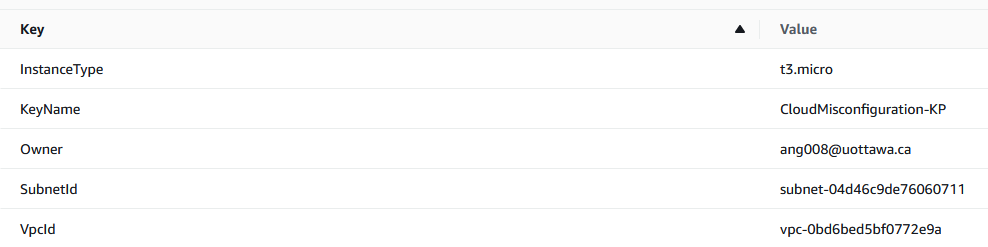
**CSPM Exercises**

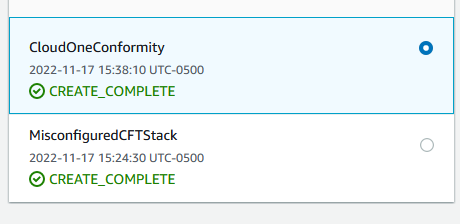




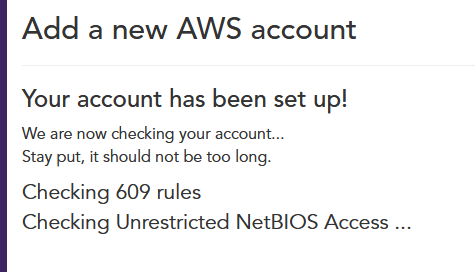
Created new key pair



Creating MisconfiguredStack

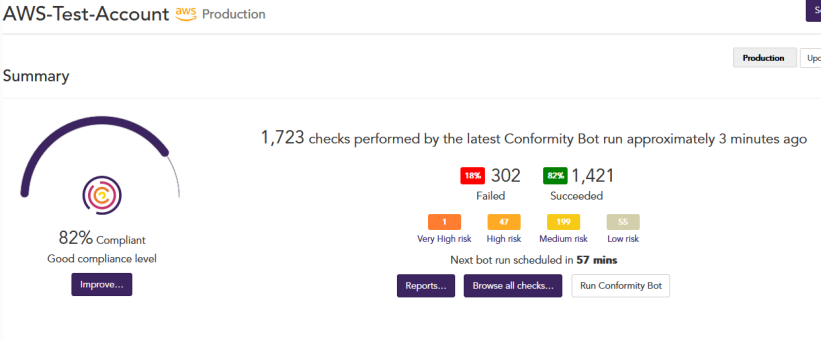


Created CloudOneConformity Stack

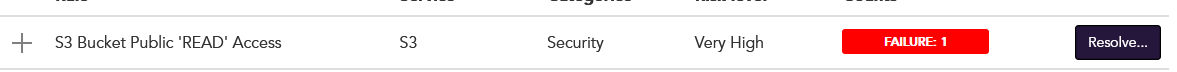


Added new AWS account to Trend Micro Cloud One

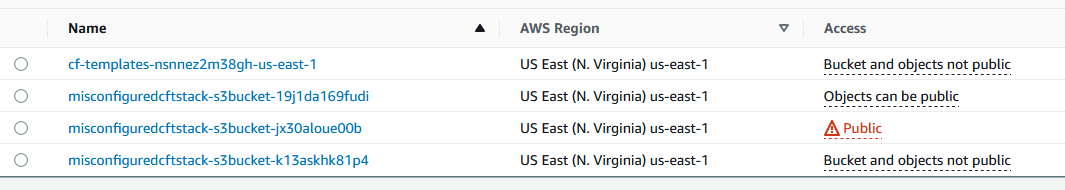
Exercise 4: Resolve “S3 Bucket Public 'READ' Access” Check Failure



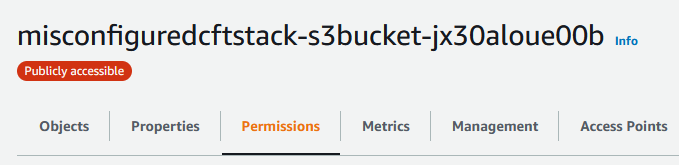
Current status of my account

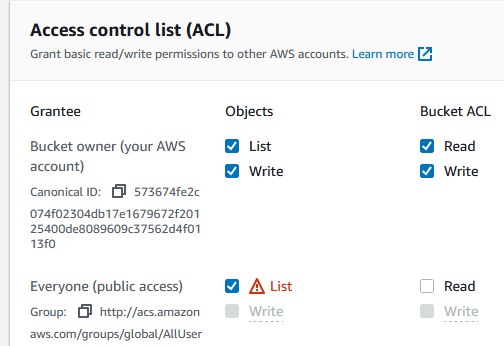


By applying filters S3 and Failure, I found the error in question. By clicking resolve, I’m lead to this page. <https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/S3/s3-bucket-public-read-access.html#> I attempted to resolve the issue using AWS console.



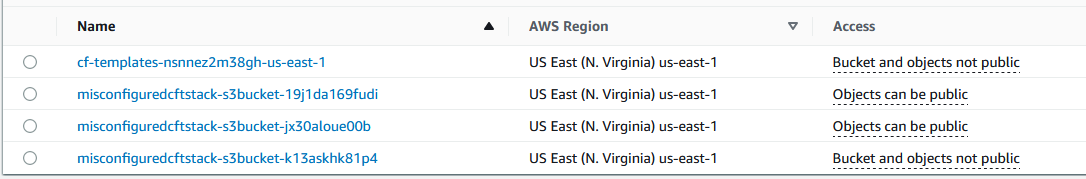
As shown, the 3rd bucket was public. This is the one that I’ve just created.







Navigated to permissions in the misconfigured stack. Went to ACL to disable public access.



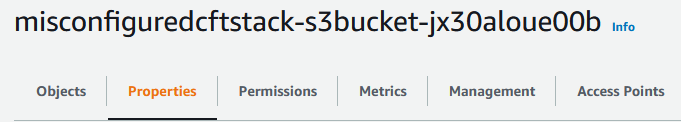
Issue resolved.

Exercise 5: Resolve “Server Side Encryption” Check Failure

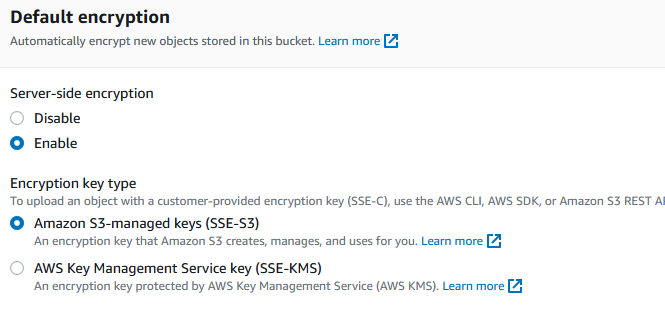


Applied filters S3 and found failure. Clicking resolve lead to

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/S3/server-side-encryption.html#863777181609>



Found the relevant stack and went to properties.

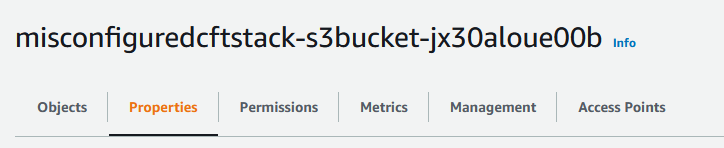


Enabled encryption for the bucket.

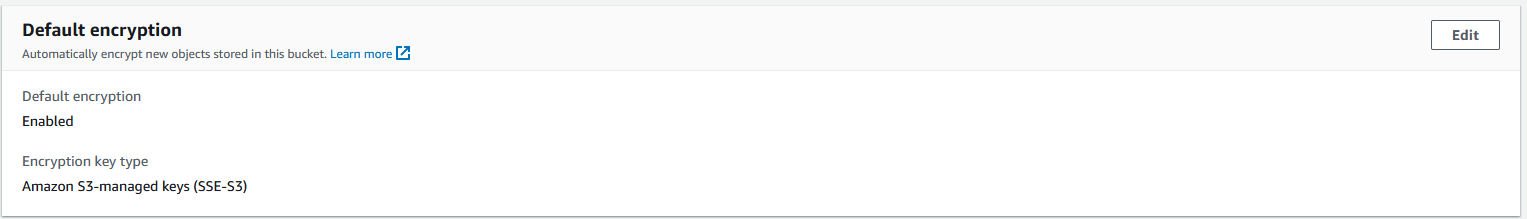
Exercise 6: Resolve “S3 Bucket Default Encryption” Check Failure

No failure was found on Trend Micro however, I still found a guide to fix the problem, should I ever have such failure occur.

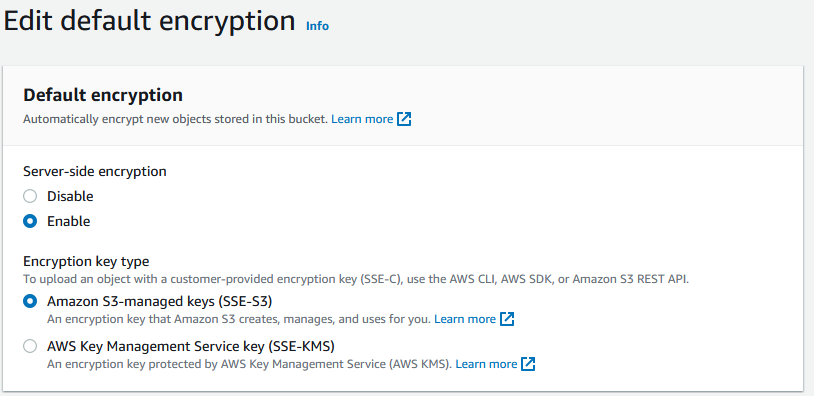
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/default-bucket-encryption.html>



Go to properties of misconfigured stack.



Find default encryption section.



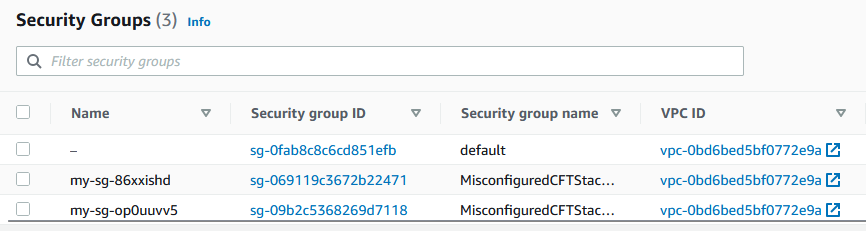
Enable or disable default encryption at your discretion.

Exercise 7: Resolve “Unrestricted SSH Access” Check Failure

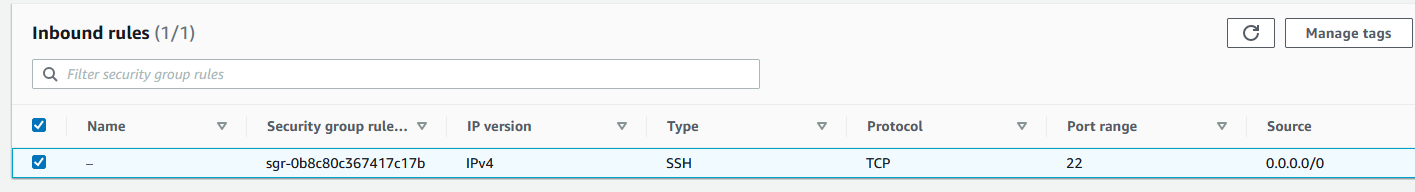


Applied filters EC2 and found failure. Clicking resolve lead to

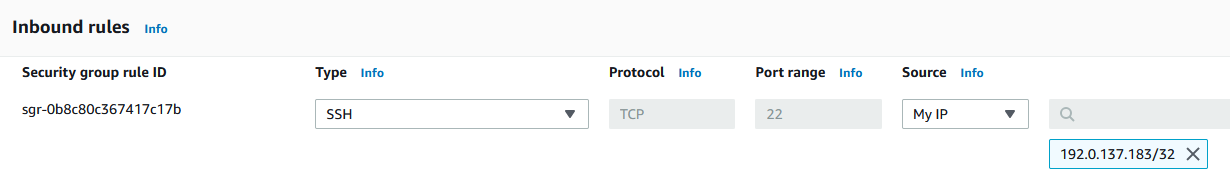
<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/EC2/unrestricted-ssh-access.html#863777181609>



Went to EC2 > NETWORK & SECURITY > Security Groups.



Discovered that one of these security groups had source set to 0.0.0.0/0. Meaning it allows unrestricted inbound traffic on port 22.



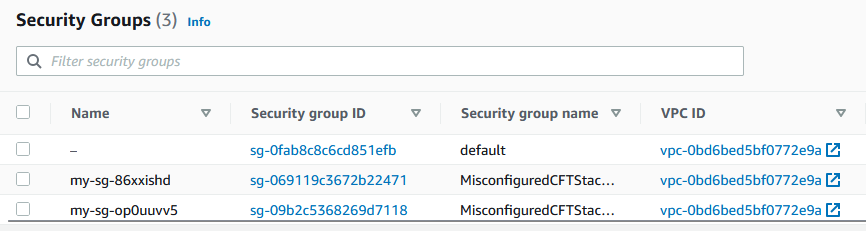
Edited rule to change source to “My IP”.

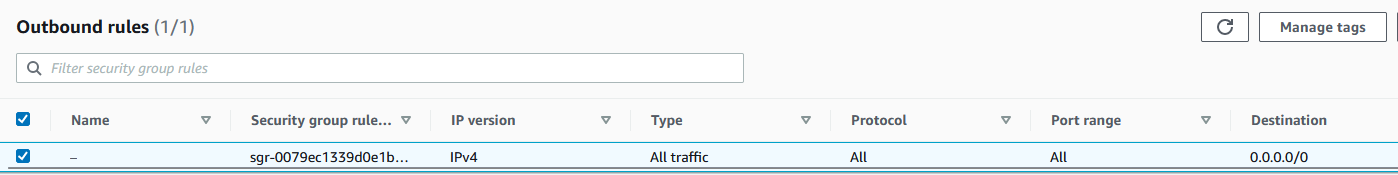
Exercise 8: Resolve “Unrestricted Security Group Egress” Check Failure



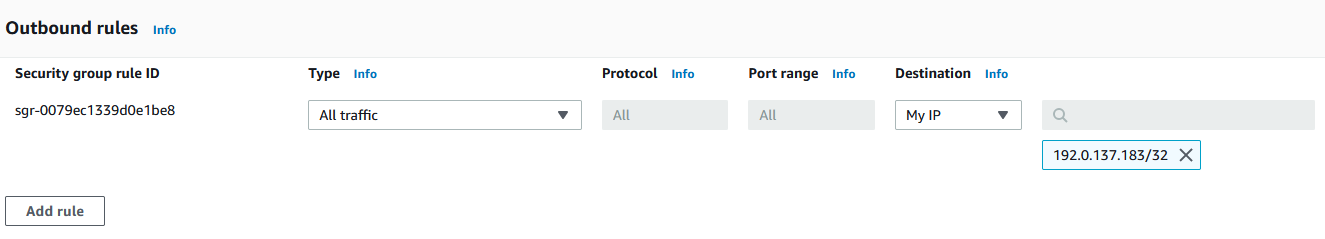
Applied filters EC2 and found failure. Clicking resolve lead to

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/EC2/security-group-egress-any.html#863777181609>

Went to EC2 > NETWORK & SECURITY > Security Groups.

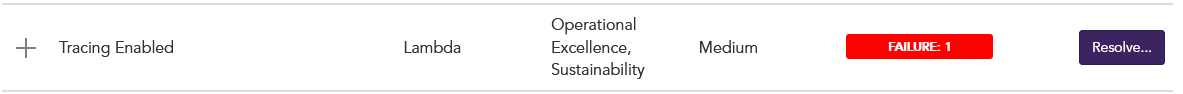


Discovered that one of these security groups had destination set to 0.0.0.0/0. Meaning it allows unrestricted outbound traffic on port 22.



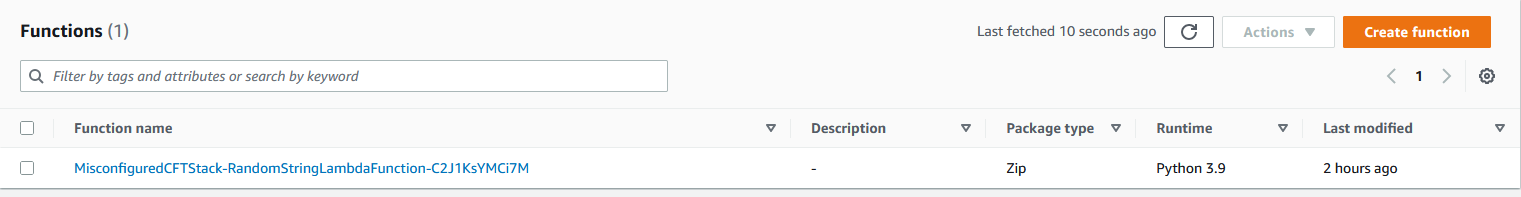
Edited rule to change destination to “My IP”.

Exercise 9: Resolve “Tracing Enabled” Check Failure

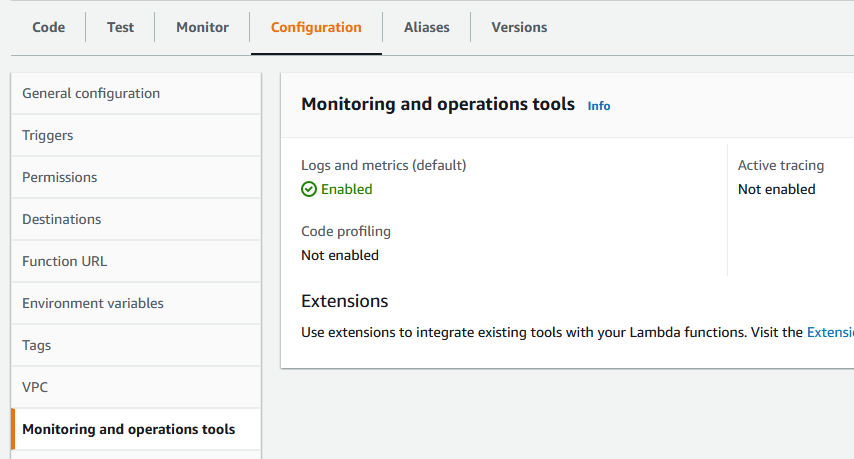


Applied filters Lambda and found failure. Clicking resolve lead to

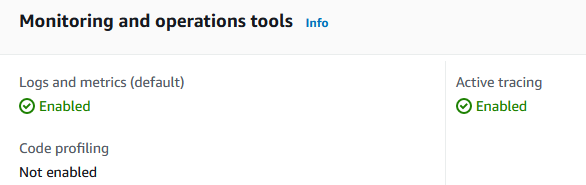
<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/Lambda/tracing.html#863777181609>



Navigated to AWS Lambda > Functions.



Under Configuration > Monitoring and operations tools, we discover that Active Tracing is not enabled.



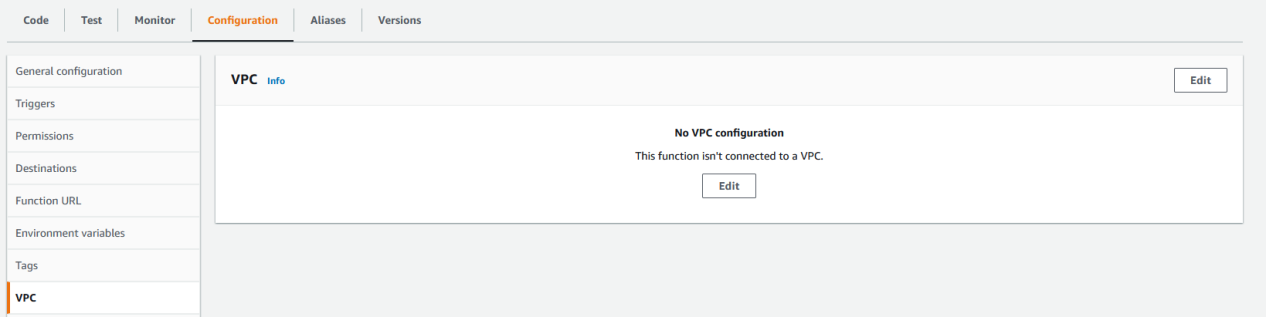
We enable it and save our settings.

Exercise 10: Resolve “VPC Access for AWS Lambda Functions” Check Failure

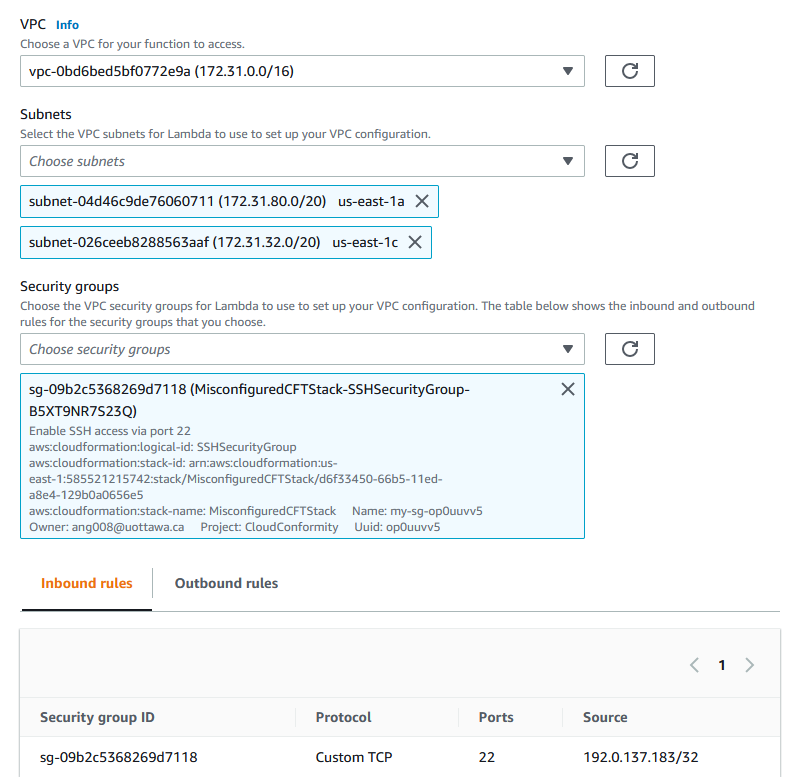


Applied filters Lambda and found failure. Clicking resolve lead to

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/Lambda/function-in-vpc.html#863777181609>



Navigate to AWS Lambda > Functions. Select the function in question. Then go to Configuration > VPC.



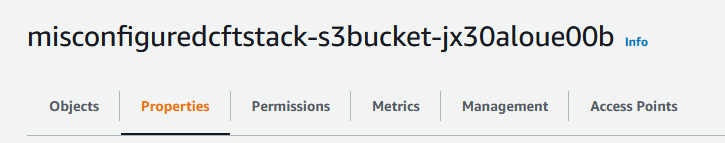
We configure this by choosing a VPC network, two subnets, and a security group for our function. Now we save our settings and exit.

Exercise 11: Resolve “S3 Bucket Logging Enabled” Check Failure

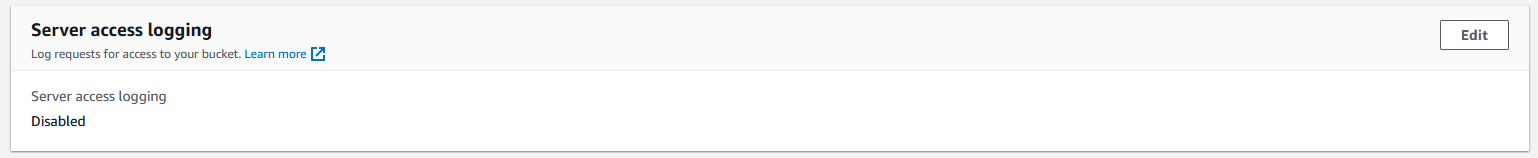


Applied filters S3 and found failure. Clicking resolve lead to

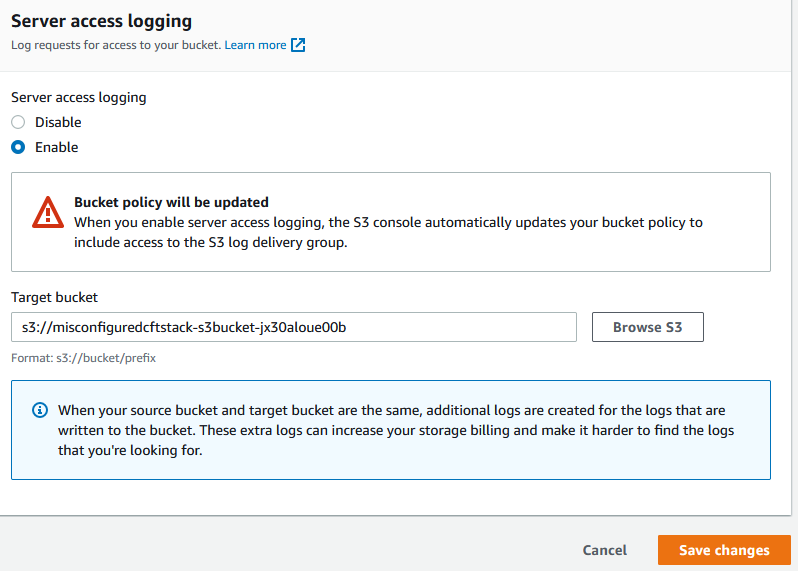
<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/S3/s3-bucket-logging-enabled.html#863777181609>



Navigate to the properties of the misconfigured stack.



Under server access logging, we can see it is disabled.



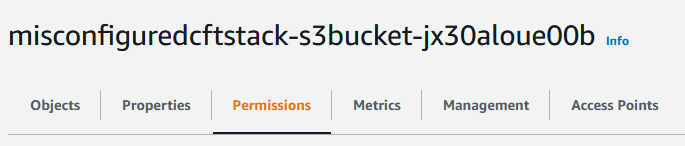
We will enable and set the target bucket to our bucket. Then save changes and exit.

Exercise 12: Resolve “Secure Transport” Check Failure

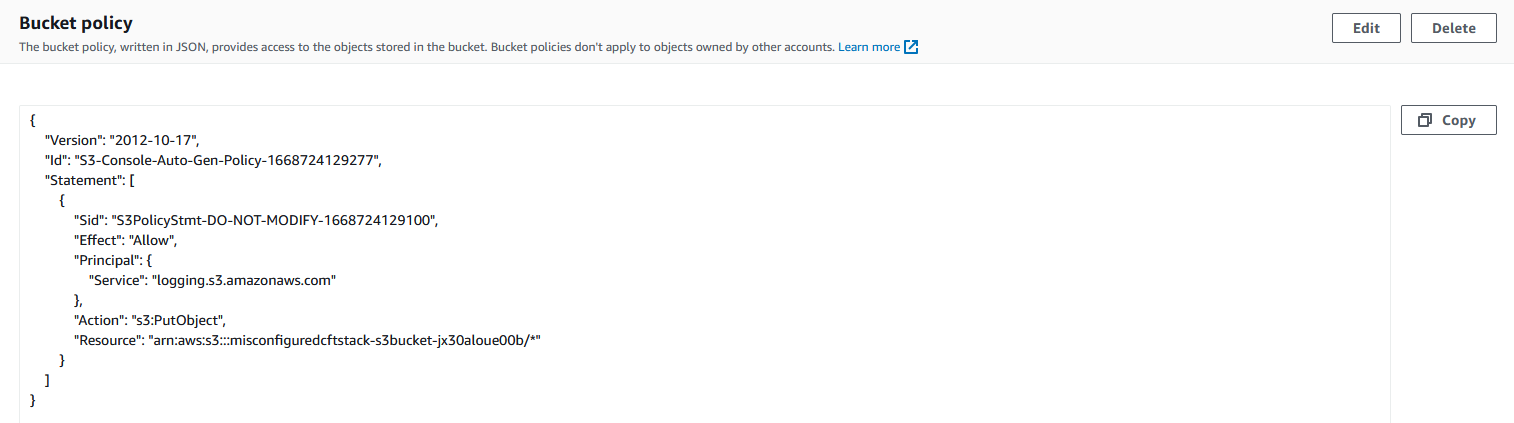


Applied filters S3 and found failure. Clicking resolve lead to

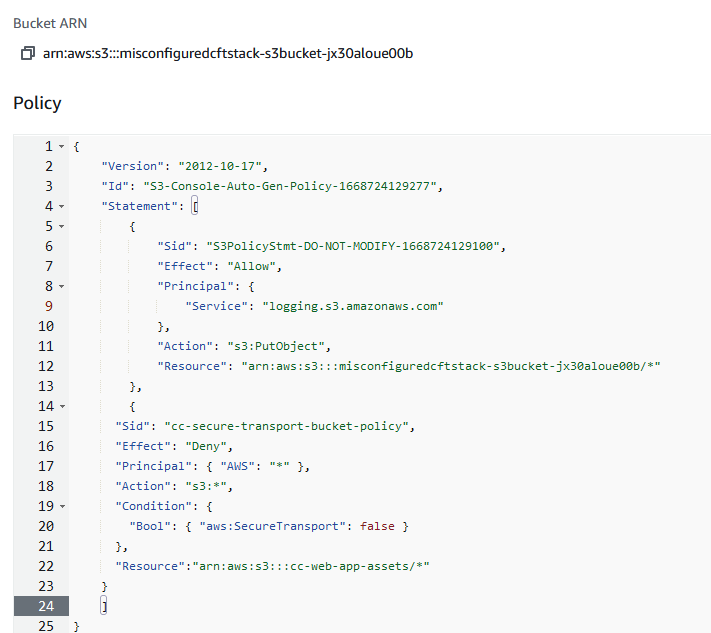
<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/S3/secure-transport.html#863777181609>



Navigate to the permissions under misconfigured stack.

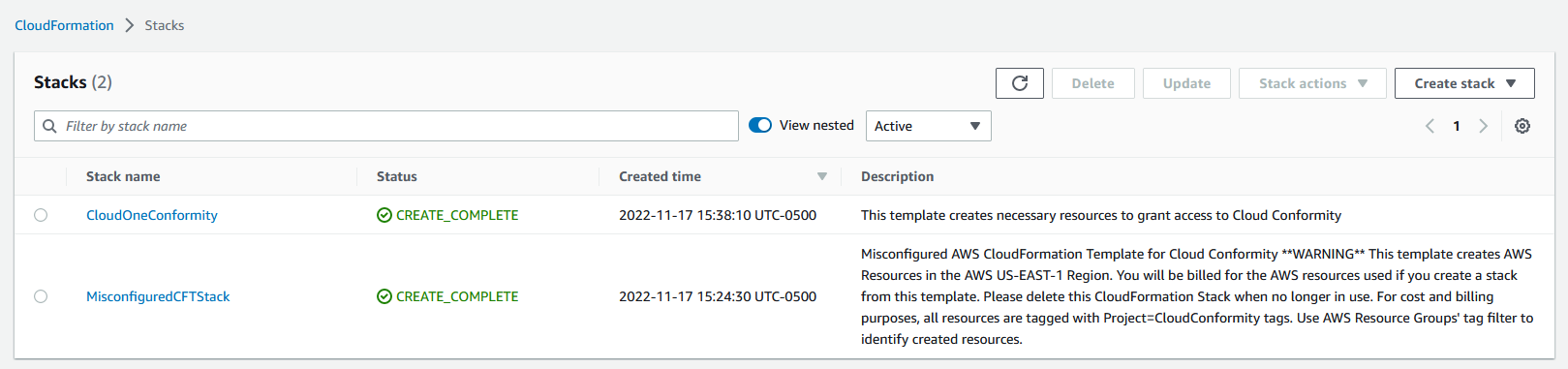


Navigate to the bucket policy section and edit it.



Since the bucket policy had some existing policy already, we append it with the following provided by Trend Micro. Now save settings and exit.

Exercise 13: Delete CloudFormation Template



Navigated to AWS Services > CloudFormation. Delete stacks used for this exercise.