Home / AWS / Guided Lab / Check AWS Resources in Trusted Advisor

Check AWS Resources in Trusted Advisor

Level: **Fundamental**

Amazon S3 | Amazon VPC | Amazon Web Services | AWS Trusted Advisor

0h 43m 3s left

15 MIN

End Lab

Open Console

Validation

Lab Credentials

User Name

Whiz_User_80425.87712555

Password

a1f61102-479a-4832-a9ba-6913c757ea3e

Access Key

AKIA4G2Z5NDA6J5G6NXM

Secret Key

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

Lab Resources

No Lab Resources Found

Support Documents

No Support Documents Found

Need help?

How to use Hands on Lab

Troubleshooting Lab

FAQs

Submit Feedback Share

Lab Overview Lab Steps Lab Validation

Cloud Security Engineer, Cloud Administrator

Security, Management & Governance

Lab Steps

Task 1: Sign in to AWS Management Console

1. Click on the **Open Console** button, and you will get redirected to AWS Console in a new browser tab.
2. On the AWS sign-in page,
    - Leave the Account ID as default. Never edit/remove the 12 digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.
    - Now copy your **User Name** and **Password** in the Lab Console to the **IAM Username and Password** in AWS Console and click on the **Sign in** button.
3. Once Signed In to the AWS Management Console, Make the default AWS Region as **US East (N. Virginia) us-east-1.**

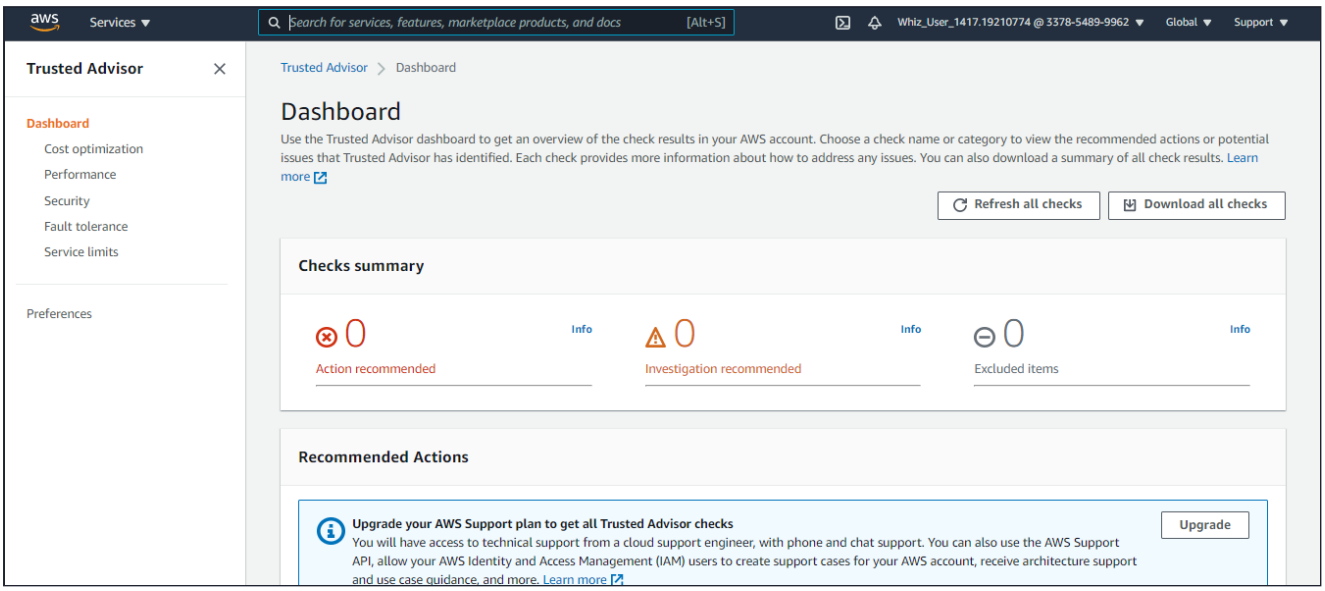
Task 2: Checking the initial status of the Trusted advisor dashboard

In this task, we will check the initial status of the Trusted advisor dashboard.

1. Make sure you are in **US East (N. Virginia) us-east-1** Region.

2. Navigate to **Trusted Advisor** by clicking on the **Services** menu at the top, then click on **Trusted Advisor** in the **Management & Governance** section.

3. On the home page of Trusted Advisor, we have the Dashboard. You can here check recommendations to optimize your services and resources.



4. By default, as you open the page all the recommendation actions will refresh automatically to fetch the latest results.

5. We will create 2 unrestricted security groups and 2 public S3 buckets to understand more about Trusted Advisor.

Task 3: Create a first unrestricted Security Group

In this task, we will create our first unrestriced security group by enabling the SSH rule.

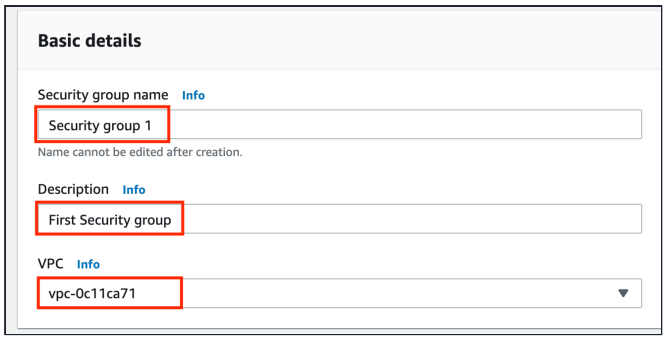
1. Navigate to **EC2** by clicking on the **Services** menu available under the **Compute** section.

2. On the left panel menu, Select the **Security groups** under the **Network & Security** section.

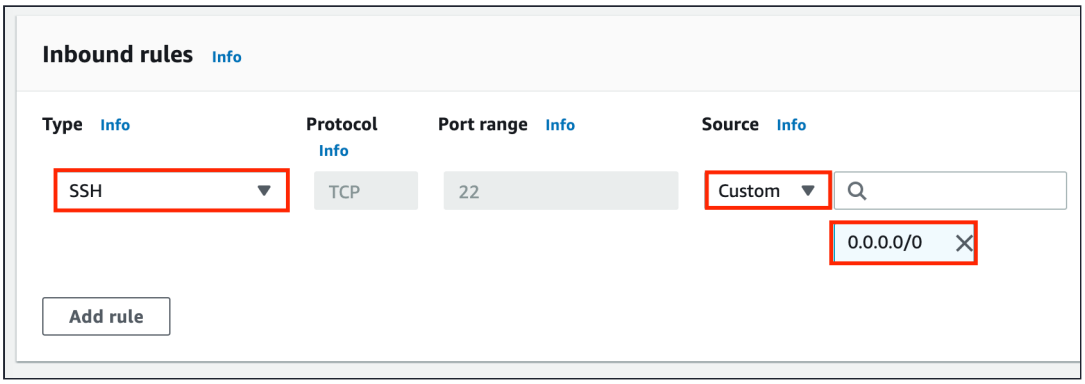
3. Click on the **Create security group** button.

4. We are going to create a Security group for the ECS cluster.

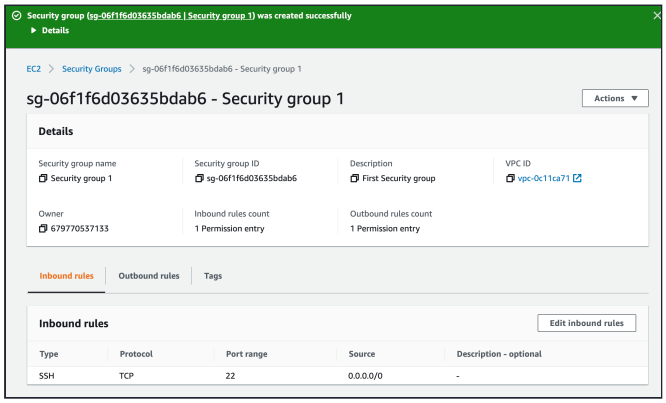
   - Security group name: Enter ***Security Group 1***
   - Description: Enter ***First Security group***
   - VPC: Select **Default VPC**



- Click on the **Add rule** button under **Inbound rules.**
  - Type : Select **SSH**
  - Source : Select **Custom**
  - In the textbox add **0.0.0.0/0**



5. Leave everything as default and click on the **Create security group** button.
6. Security group named **Security group 1** is now created.



Task 4: Create a second unrestricted Security Group

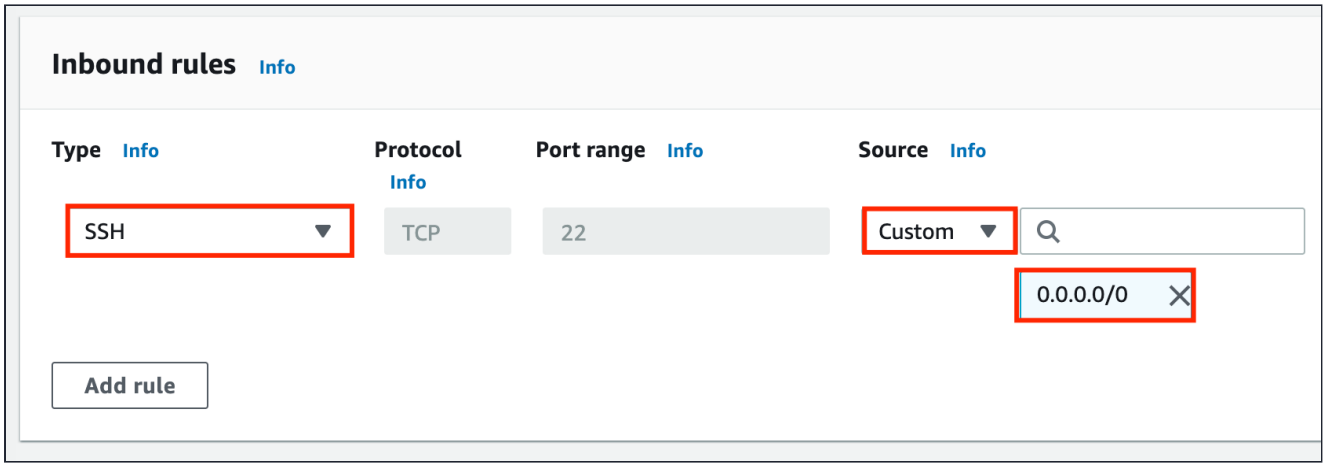
In this task, we will create our second unrestriced security group by enabling the SSH rule.

1. On the left panel menu, select the **Security groups** under the **Network & Security** section.
2. Click on the **Create security group** button again.

3. We are going to create a Security group for the ECS cluster.

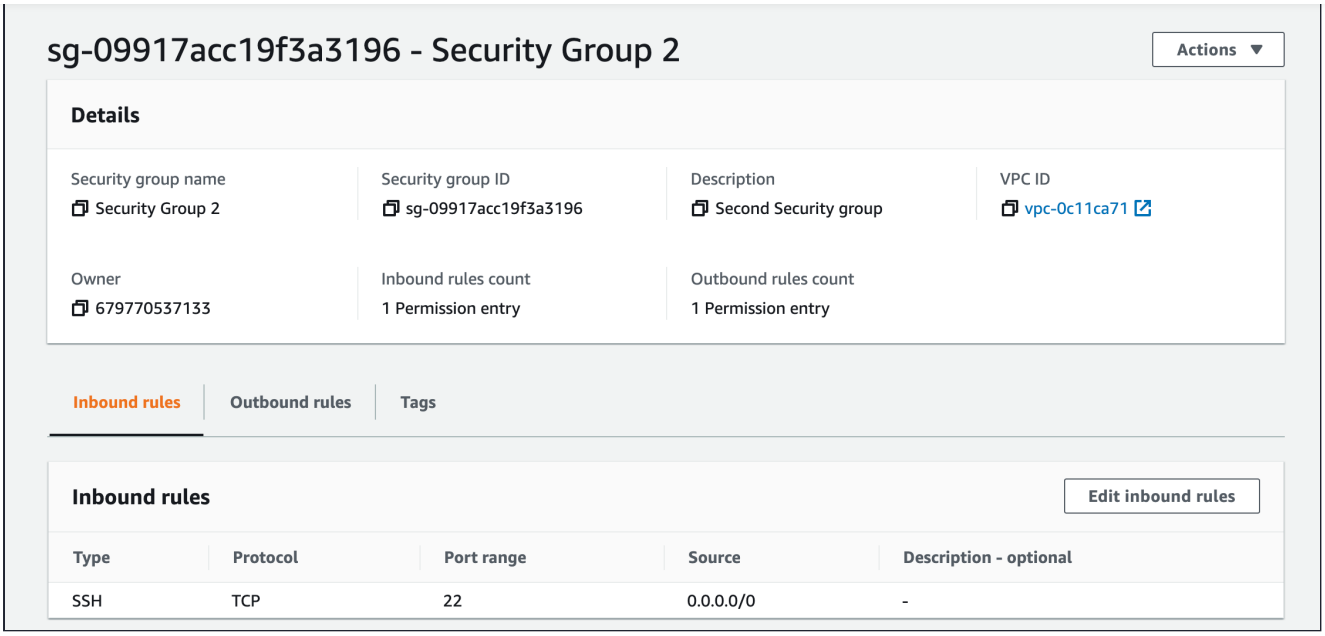
- Security group name: Enter ***Security Group 2***
- Description: Enter ***Second Security group***
- VPC: Select **Default VPC**

- Click on the **Add rule** button under **Inbound rules.**
  - Type : Select **SSH**
  - Source : Select **Custom**
  - In the textbox add **0.0.0.0/0**



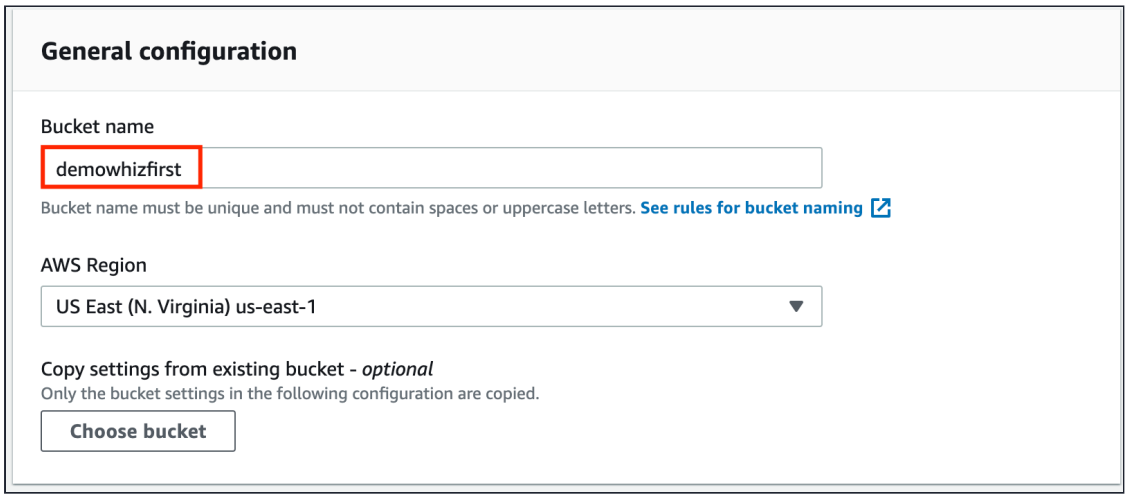
4. Leave everything as default and click on the **Create security group** button.

5. Security group named **Security group 2** is now created.



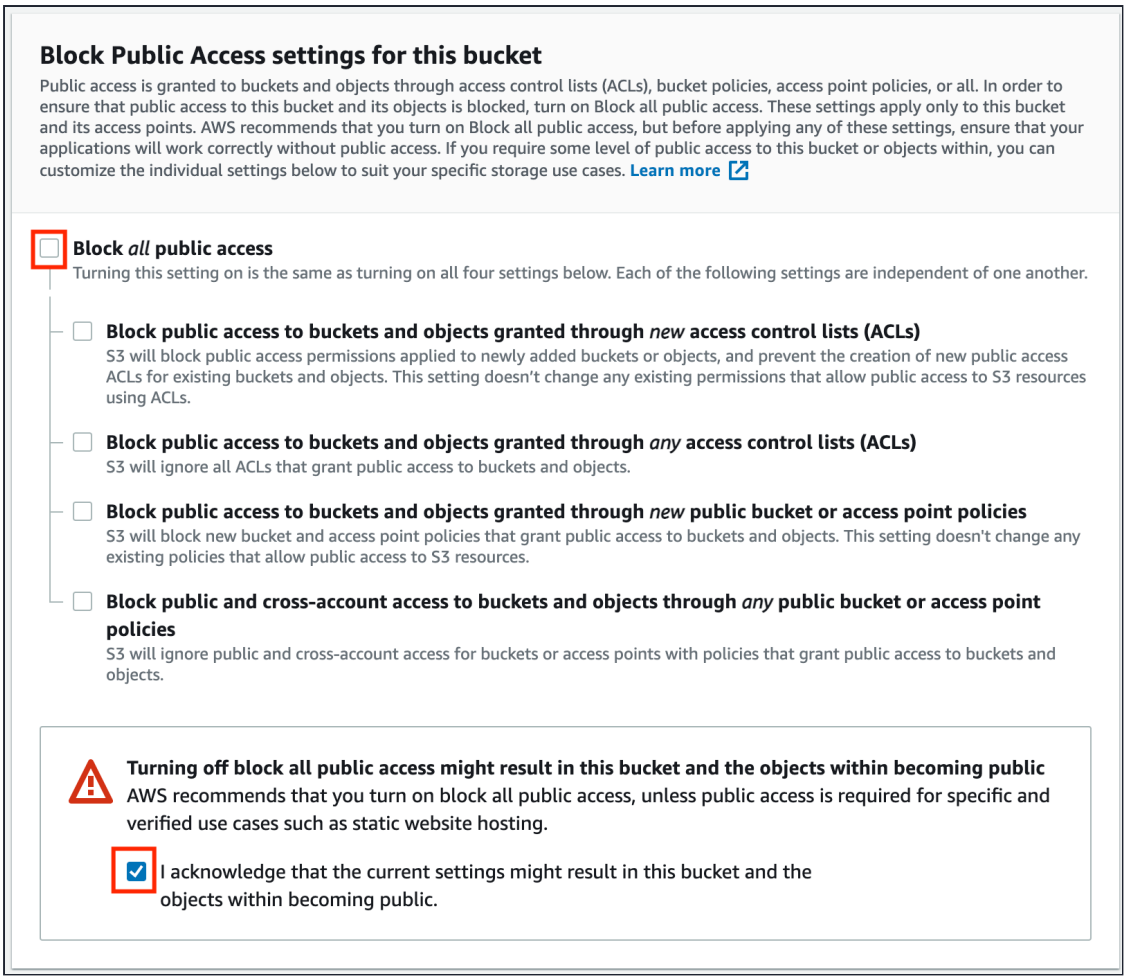
Task 5: Creating 2 Public S3 Buckets

1. Navigate to the **Services** menu at the top and click on **S3** in the **Storage** section.
2. In the left menu, click on **Create bucket** button and fill in the bucket details.
   - Bucket Name: Enter ***demowhizfirstXXXX (where XXXX could be numbers).***



(**Note:** The Bucket Name must be unique across all existing bucket names in Amazon S3)

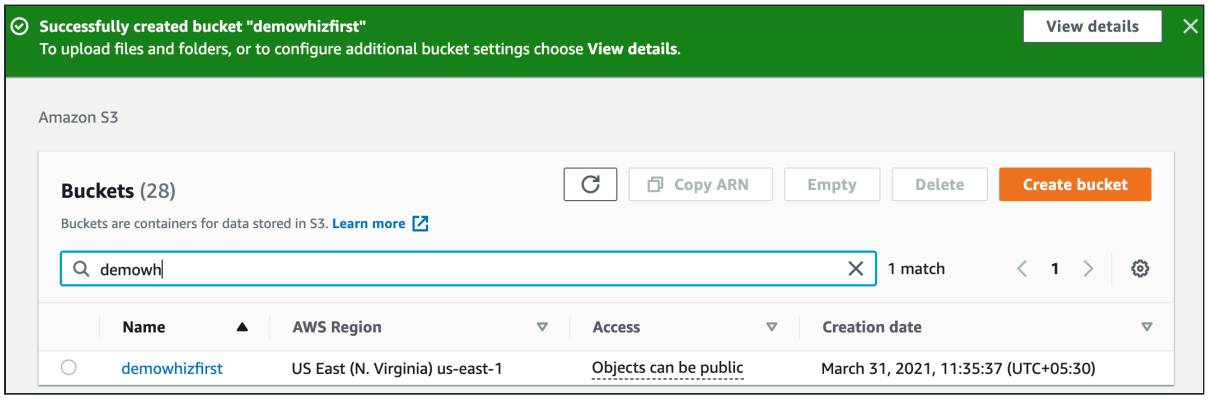
   - Region: Select **US East (N. Virginia) us-east-1**
   - Bucket settings for Block Public Access: **Uncheck** the option of **Block all public access** and **Select the check box option of Acknowledgment**.



Note: Making the bucket public is required for this lab.

- Leave other settings as default.
- Click on the **Create bucket** button.

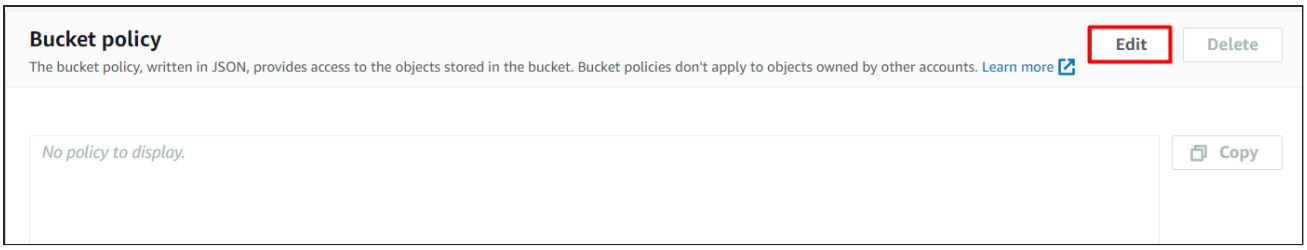
3. Your S3 Bucket is now created.



4. Click on the bucket name and make it public using **Bucket policy**

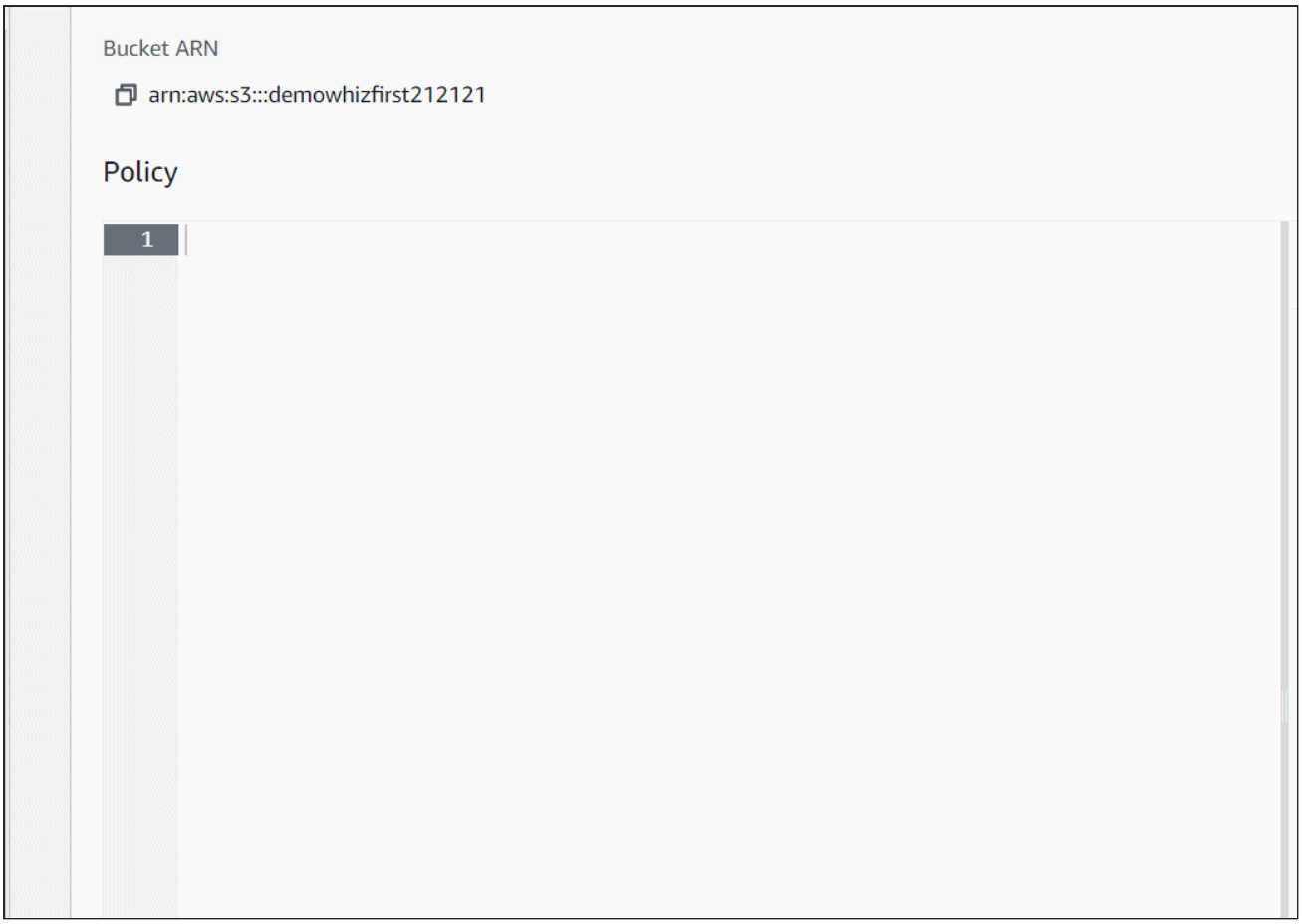
5. Click on the **Permissions** tab to configure your bucket.

- In the **Permissions** tab, Click on **Edit** button.



- You will be able to see a Blank policy editor.
- Before creating the policy, you will need to copy the ARN (Amazon Resource Name) of your bucket.
- Copy the **ARN** of your bucket to the clipboard. It is displayed at the top of the policy editor. it looks like **ARN:"arn:aws:s3:::your-bucket-name**".
- In the policy below, update the bucket ARN on the Resource key value and copy the policy code.

```
{
  "Id":"Policy1",
  "Version":"2012-10-17",
    "Statement":[
     {
      "Sid":"Stmt1",
      "Action":[
        "s3:GetObject"
         ],
          "Effect":"Allow",
          "Resource":"replace-this-string-with-your-bucket-
arn/*",
          "Principal":"*"
       }
   ]
}
```

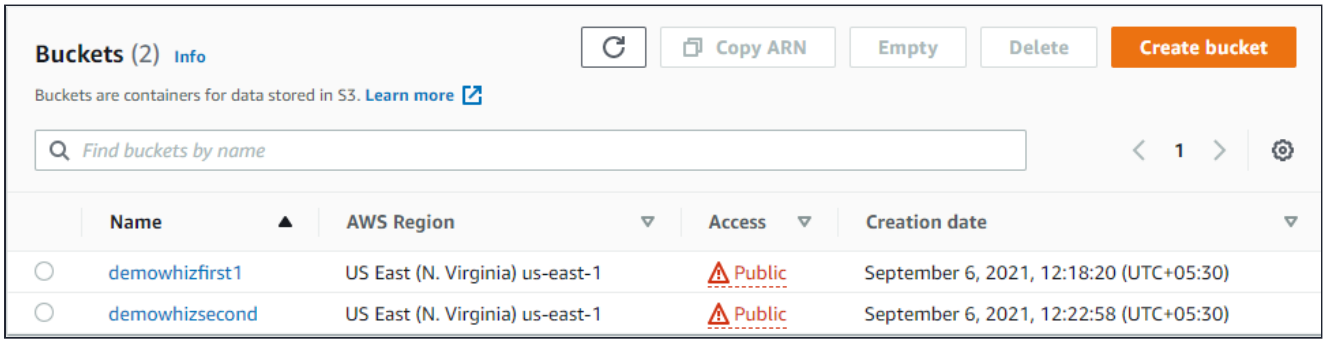


6. Click on **Save changes** button.

7. Create another S3 Bucket now, follow the same steps as above(including the code) and name the bucket as ***demowhizsecondXXXX (where XXXX could be numbers).***

8. Don't forget to **make them public**.

9. Both the required buckets are created now as we can see in the image given below.

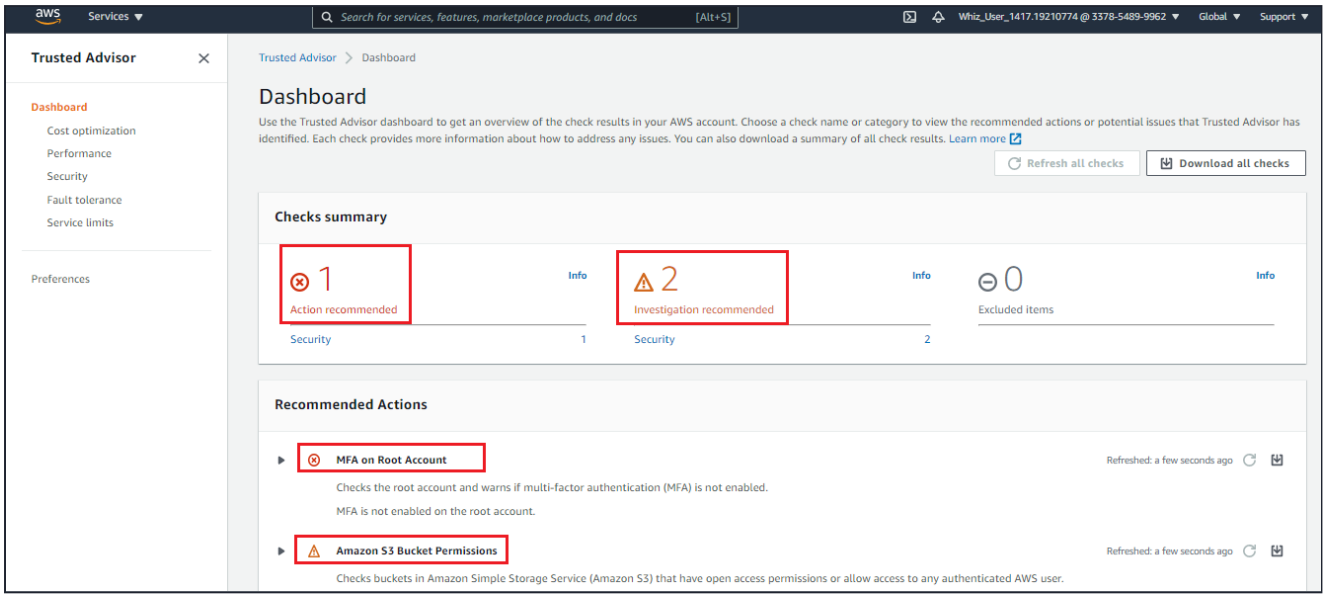


Task 6: Refresh the Trusted advisor dashboard

1. Navigate to **Trusted Advisor** by clicking on the **Services** menu at the top, then click on **Trusted Advisor** in the **Management & Governance** section.

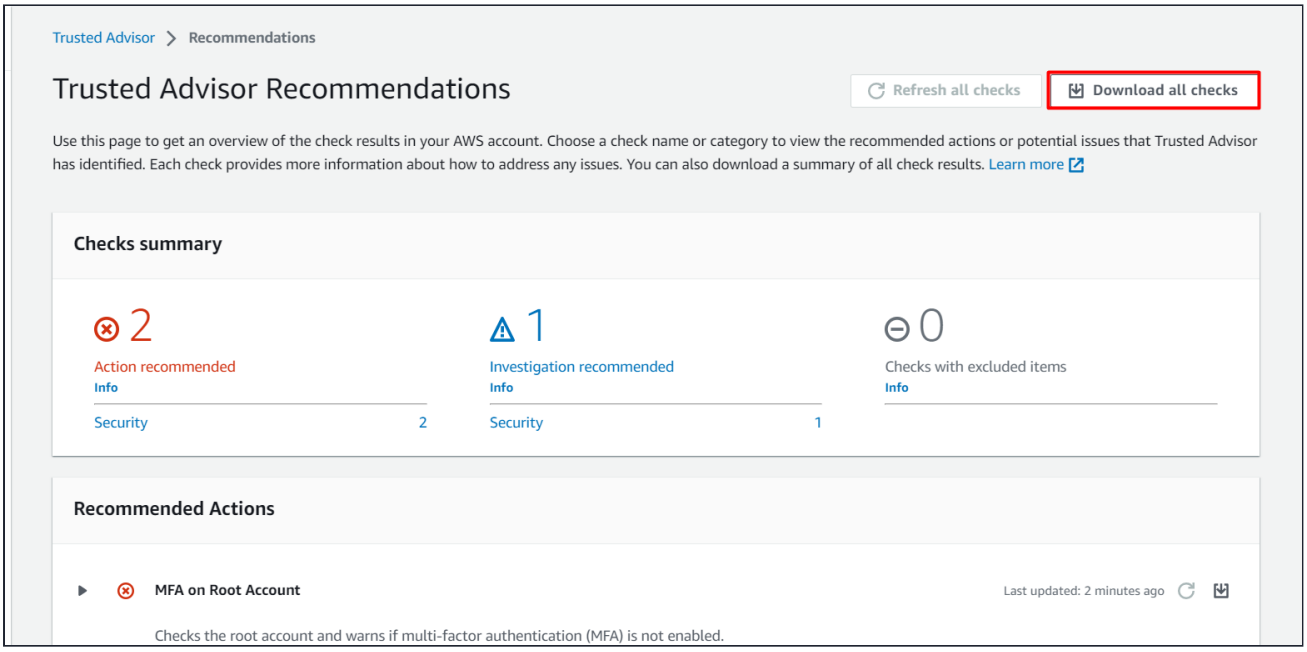
2. AWS has a default time cycle after it automatically refreshes all the checks.

3. Refresh will take up to 2 minutes, after that it will show all the flagged and unsecured resources. If it still doesn't show, hard refresh the tab once.



4. Optionally, you can click on the download report button to view the report in the excel file.

5. Unlike the refresh button, the download option is available with both dashboard and specific resource action.

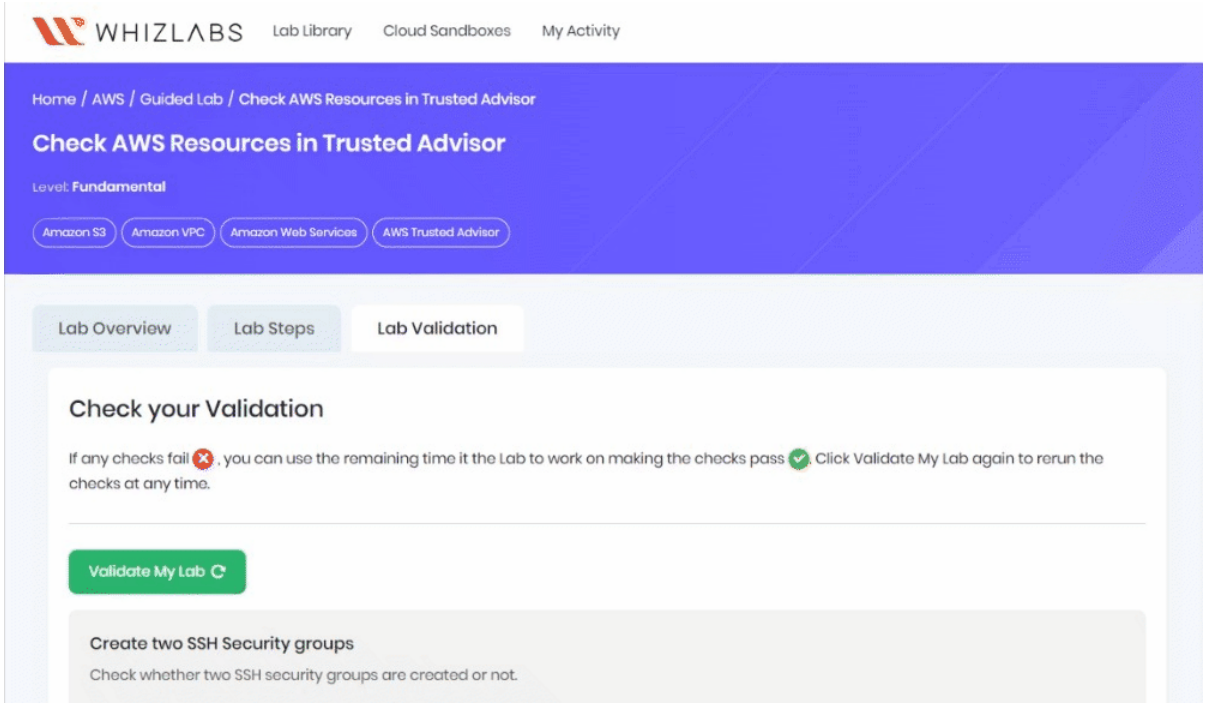


Do you know ?

AWS Trusted Advisor is available to AWS customers with an Enterprise-level support plan at no additional cost. This means that customers who have subscribed to AWS Enterprise Support can leverage the benefits of Trusted Advisor as part of their support package.

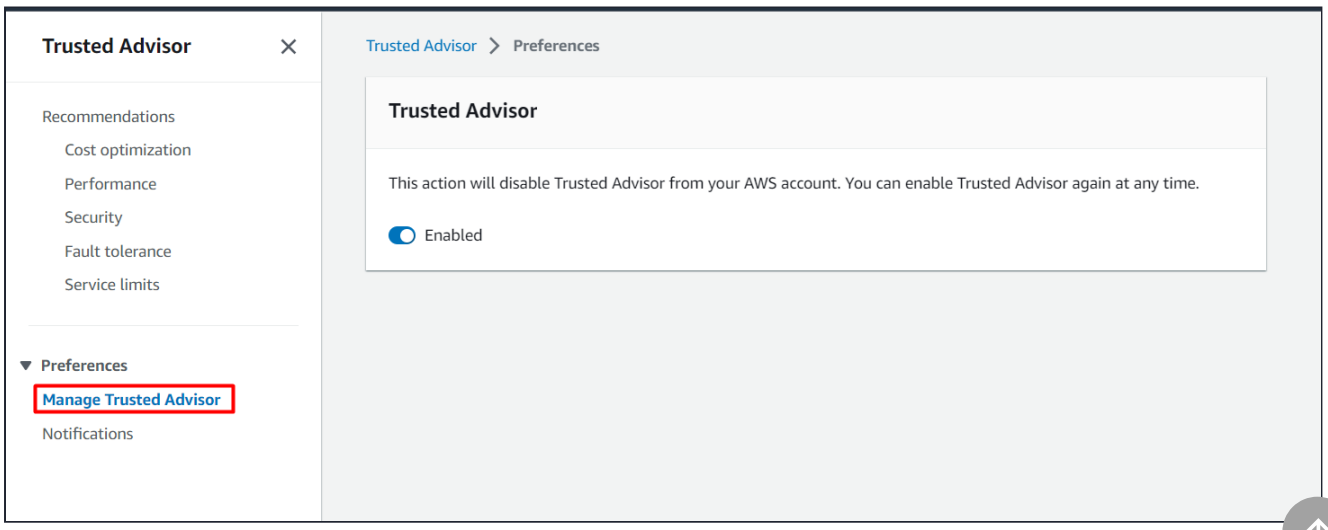
Task 7: Validation Test

1. Once the lab steps are completed, please click on the **Validation** button on the Right side panel and re-click **validate my lab** button.
2. This will validate the resources in the AWS account and displays whether you have completed this lab successfully or not.
3. Sample output :

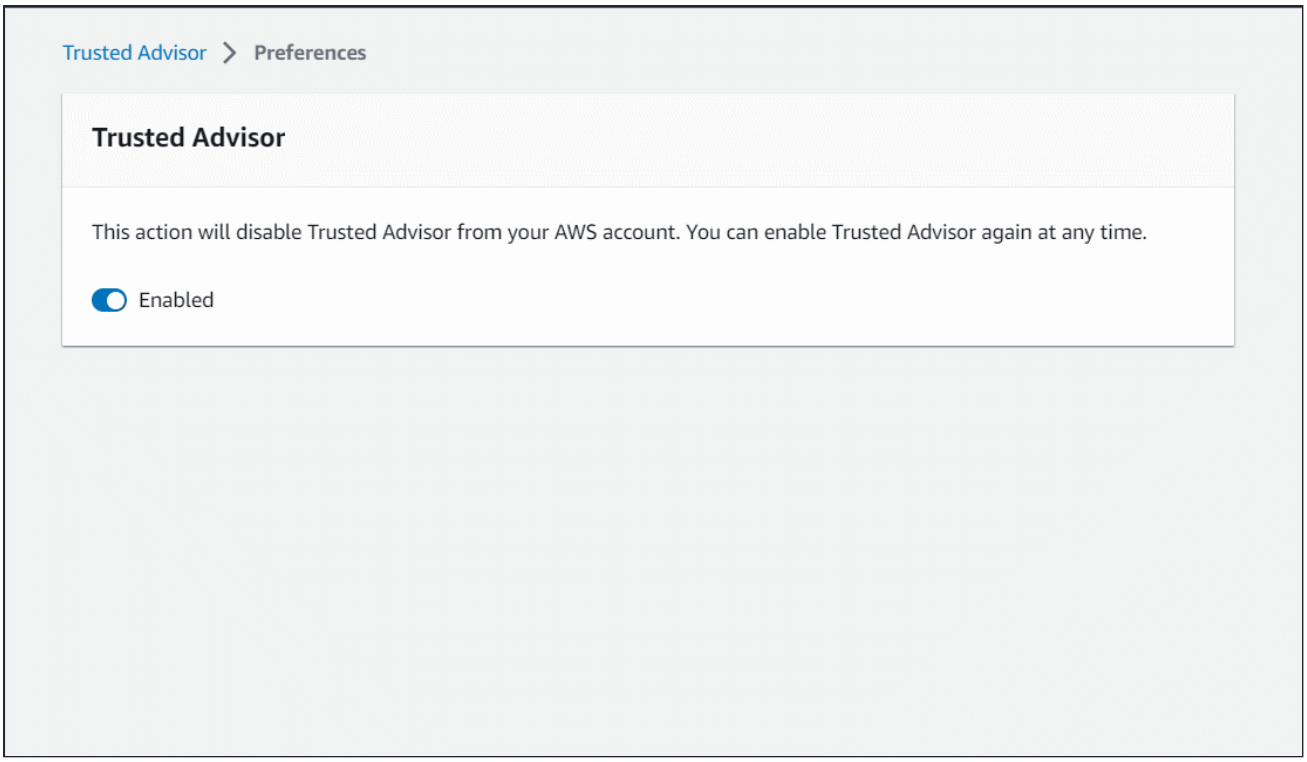


Task 8: Disable the Trusted Advisor

1. Go to **Manage Trused Advisor** under **Preferences**



2. Click on Enabled button and select **Disable.**



Completion and Conclusion

1. You have successfully created 2 unrestricted EC2 Security Group.
2. You have successfully created 2 public S3 buckets.
3. You have successfully checked resources in the Trusted adviser dashboard.
4. You have successfully validated the lab.
5. You have successfully disabled the Trusted Advisor.

End Lab

1. Sign out of AWS Account.
2. You have successfully completed the lab.
3. Once you have completed the steps, click on **End Lab** from your whizlabs lab console and wait till the process gets completed.