

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



➔ End Lab

⚙ Open Console

✓ Validation

Lab Credentials

User Name ⓘ
Whiz_User_80425.87712555

Password ⓘ
a1f61102-479a-4832-a9ba-6913c757ea3e

Access Key ⓘ
AKIA4G2Z5NDA6J5G6NXM

Secret Key ⓘ
GEvtA8bDXOWOdHUqCEstbfGYDuOgkS83BIR8H/jk




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**.

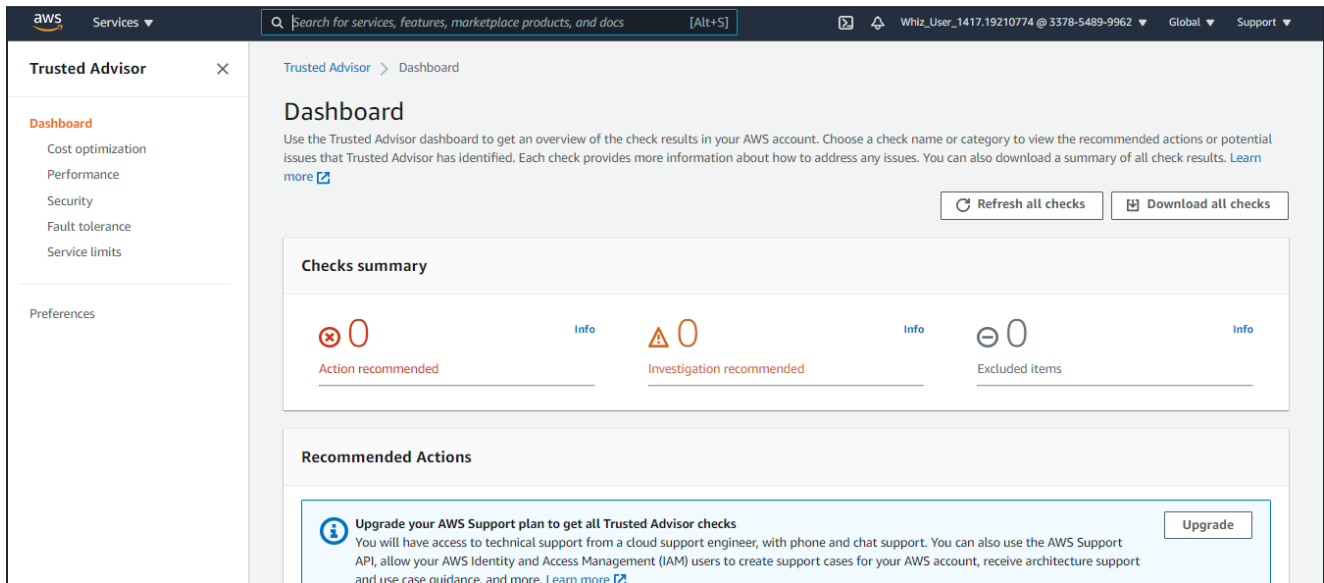


Task 2: Checking the initial status of the Trusted advisor dashboard

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 unrestricted 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**



Basic details

Security group name [Info](#)
 Security group 1
 Name cannot be edited after creation.

Description [Info](#)
 First Security group

VPC [Info](#)
 vpc-0c11ca71

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

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info
SSH	TCP	22	Custom 0.0.0.0/0

[Add rule](#)

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

6. Security group named **Security group 1** is now created.

Security group (sg-06f1f6d03635bdab6 | Security group 1) was created successfully

sg-06f1f6d03635bdab6 - Security group 1

Details

Security group name Security group 1	Security group ID sg-06f1f6d03635bdab6	Description First Security group	VPC ID vpc-0c11ca71
Owner 679770537133	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	0.0.0.0/0	-

Task 4: Create a second unrestricted Security Group

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

- On the left panel menu, select the **Security groups** under the **Network & Security** section.
- 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**



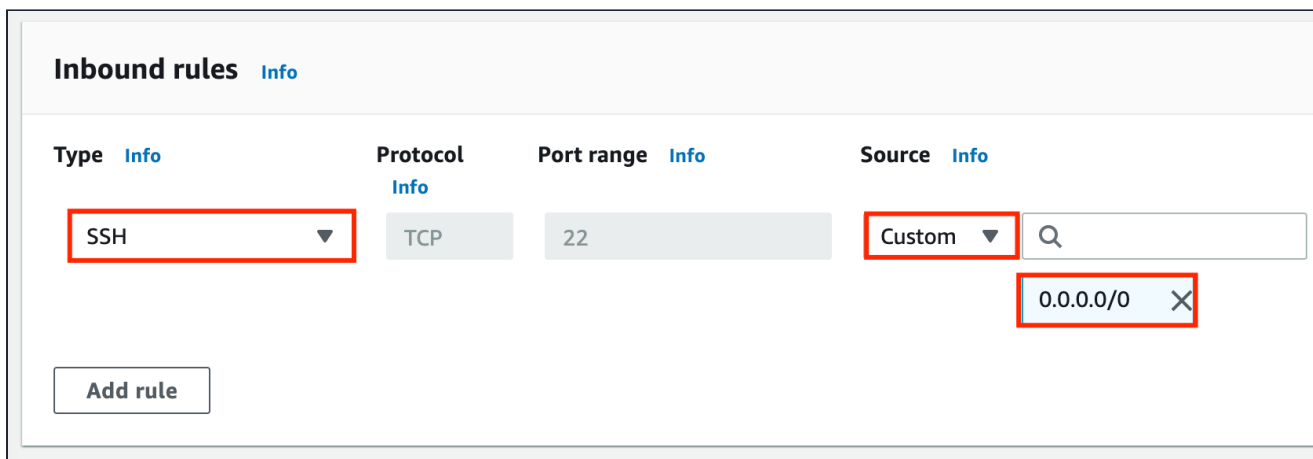
Basic details

Security group name [Info](#)
Security Group 2
Name cannot be edited after creation.

Description [Info](#)
Second Security group

VPC [Info](#)
vpc-0c11ca71

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



Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info
SSH	TCP	22	Custom 0.0.0.0/0

Add rule

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







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



sg-09917acc19f3a3196 - Security Group 2

[Actions ▼](#)

Details

Security group name  Security Group 2	Security group ID  sg-09917acc19f3a3196	Description  Second Security group	VPC ID  vpc-0c11ca71 
Owner  679770537133	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules

Outbound rules

Tags

Inbound rules

[Edit inbound rules](#)

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	0.0.0.0/0	-

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*).

General configuration

Bucket name

demowhizfirst

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#) 

AWS Region

US East (N. Virginia) us-east-1 ▼

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Choose bucket

(**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**.

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)



Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.



Block public access to buckets and objects granted through *new* access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.



Block public access to buckets and objects granted through *any* access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.



Block public access to buckets and objects granted through *new* public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.



Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.



I acknowledge that the current settings might result in this bucket and the objects within becoming public.

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.

Successfully created bucket "demowhizfirst"
View details

To upload files and folders, or to configure additional bucket settings choose [View details](#).

Amazon S3

Buckets (28) Refresh Copy ARN Empty Delete Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

Search: demowh 1 match

	Name	AWS Region	Access	Creation date
<input type="radio"/>	demowhizfirst	US East (N. Virginia) us-east-1	Objects can be public	March 31, 2021, 11:35:37 (UTC+05:30)

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.

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

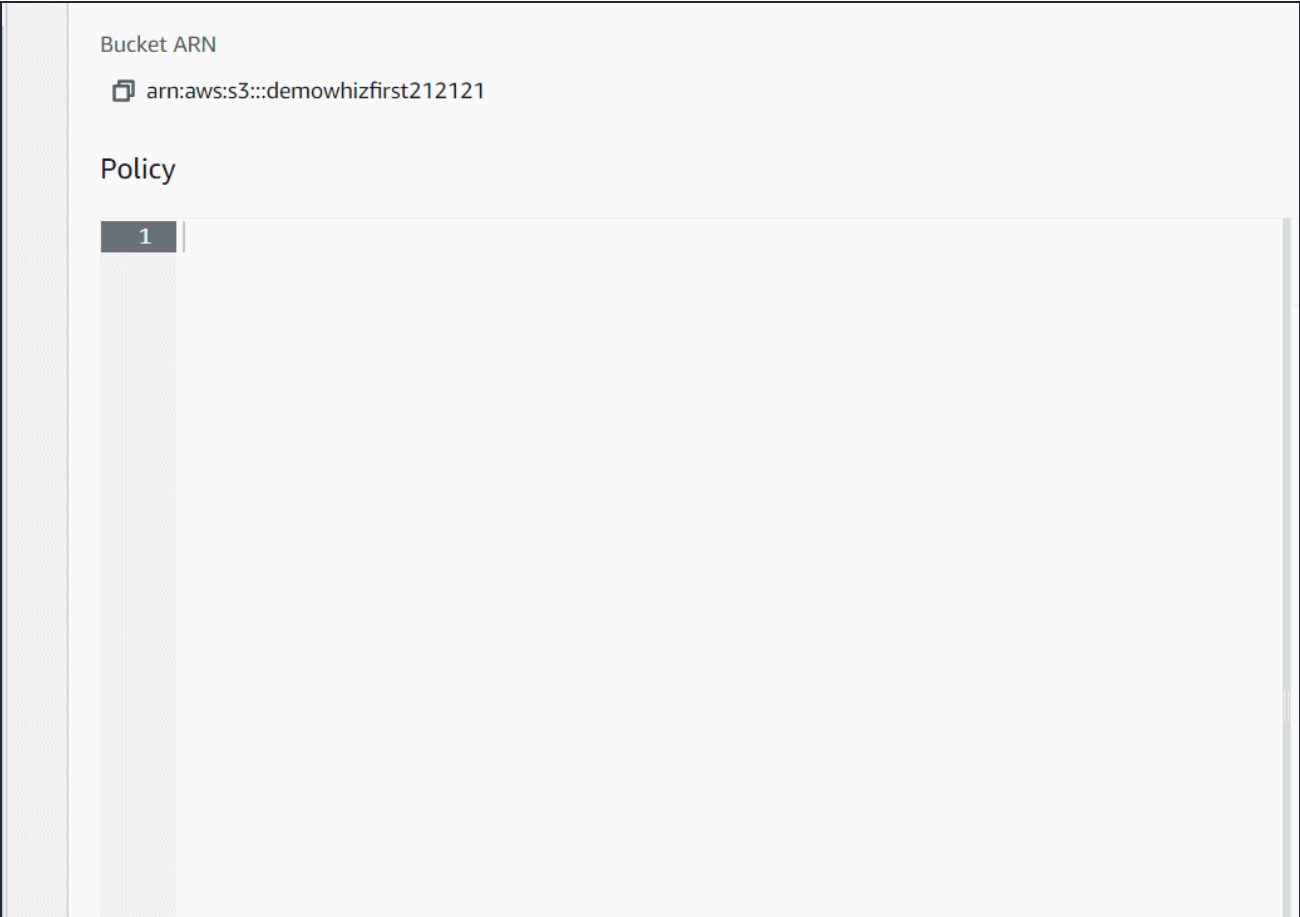
EditDelete

No policy to display.

Copy

- 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": "*"
    }
  ]
}
```

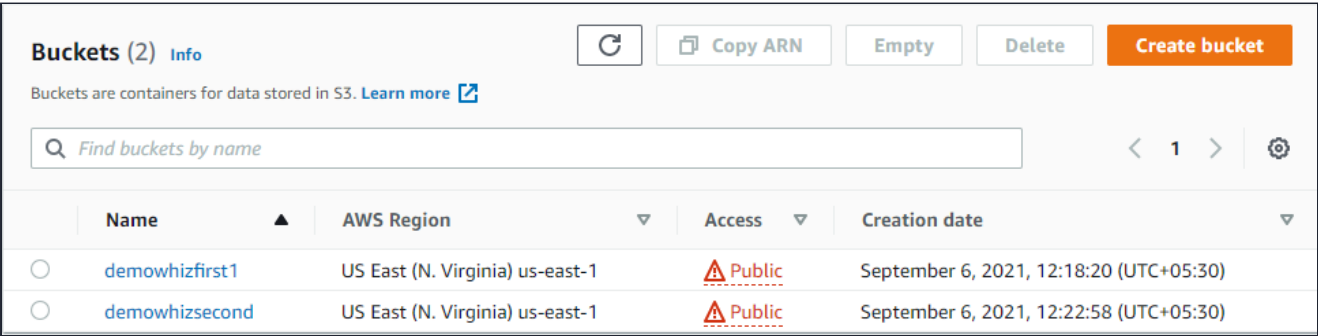



6. Click on **Save changes** button.

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**.

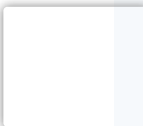
9. Both the required buckets are created now as we can see in the image given below.



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.

Trusted Advisor Dashboard

Use the Trusted Advisor dashboard to get an overview of the check results in your AWS account. Choose a check name or category to view the recommended actions or potential issues that Trusted Advisor has identified. Each check provides more information about how to address any issues. You can also download a summary of all check results. [Learn more](#)

[Refresh all checks](#) [Download all checks](#)

Checks summary

- Action recommended** (1) [Info](#)
- Investigation recommended** (2) [Info](#)
- Excluded items** (0) [Info](#)

Recommended Actions

- MFA on Root Account** (Refreshed: a few seconds ago)
 - Checks the root account and warns if multi-factor authentication (MFA) is not enabled.
 - MFA is not enabled on the root account.
- Amazon S3 Bucket Permissions** (Refreshed: a few seconds ago)
 - Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions or allow access to any authenticated AWS user.

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.

Trusted Advisor Recommendations

Use this page to get an overview of the check results in your AWS account. Choose a check name or category to view the recommended actions or potential issues that Trusted Advisor has identified. Each check provides more information about how to address any issues. You can also download a summary of all check results. [Learn more](#)

[Refresh all checks](#) [Download all checks](#)

Checks summary

- Action recommended** (2) [Info](#)
- Investigation recommended** (1) [Info](#)
- Checks with excluded items** (0) [Info](#)

Recommended Actions

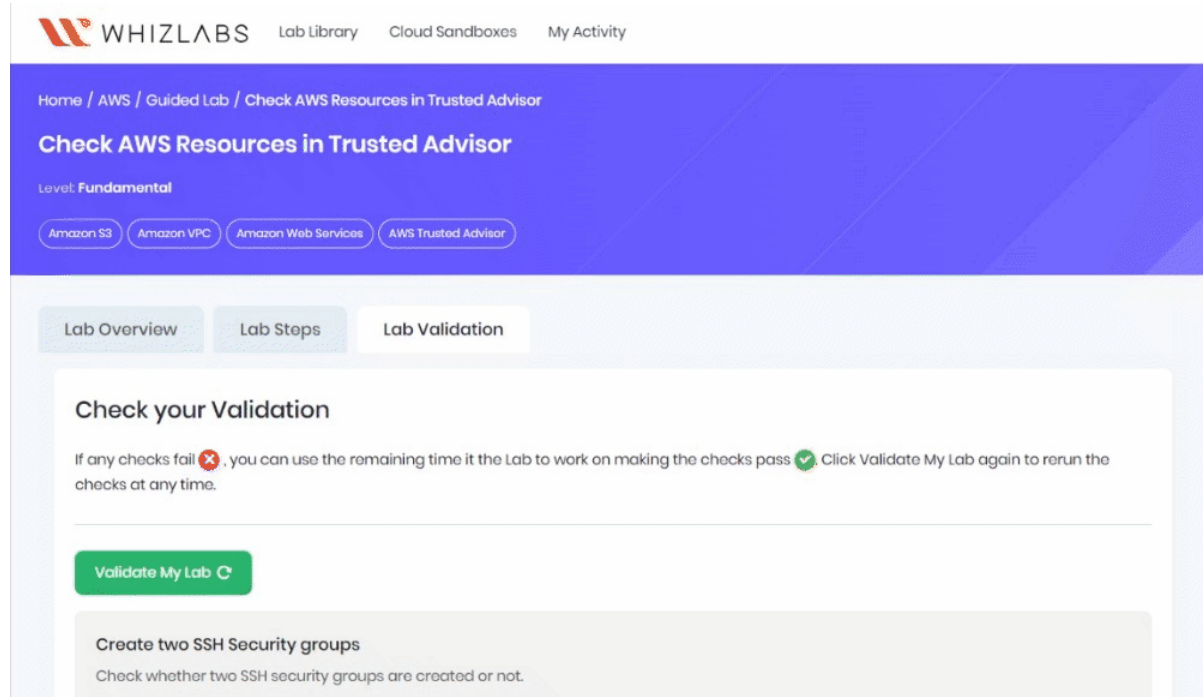
- MFA on Root Account** (Last updated: 2 minutes ago)
 - Checks the root account and warns if multi-factor authentication (MFA) is not enabled.

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.

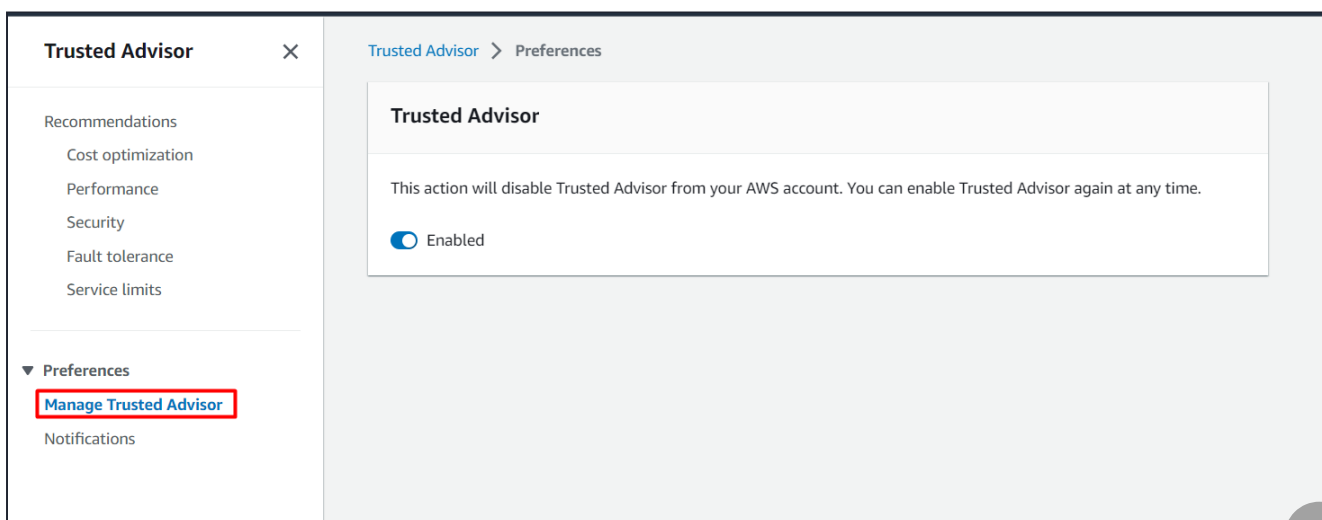
Task 7: Validation Test

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 Trusted Advisor** under **Preferences**



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

[Trusted Advisor](#) > Preferences

Trusted Advisor

This action will disable Trusted Advisor from your AWS account. You can enable Trusted Advisor again at any time.

☒ Enabled

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.



[About Us](#) [Subscription](#) [Instructions and Guidelines](#) [FAQ's](#) [Contact Us](#)



© 2024, Whizlabs Software Pvt. Ltd.

