Home / AWS / Guided Lab / Creating IAM Policies

Creating IAM Policies

Level: **Fundamental**

Identity And Access Management Amazon Web Services

0h 28m 45s left

15 MIN

End Lab

Open Console

Validation

Lab Credentials

User Name

Whiz_User_80425.36691910

Password

66417b62-1221-4842-9ec5-b8d9a3fe686c

Access Key

AKIAWPK3VFXHM2HFFU6B

Secret Key

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

Lab Resources

No Lab Resources Found

Support Documents

1. FAQs and Troubleshooting

Need help?

How to use Hands on Lab

Troubleshooting Lab

FAQs

Submit Feedback | Share

Lab Overview | Lab Steps | Lab Validation

Cloud Administrator

Security

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.

WHIZLABS 0 K

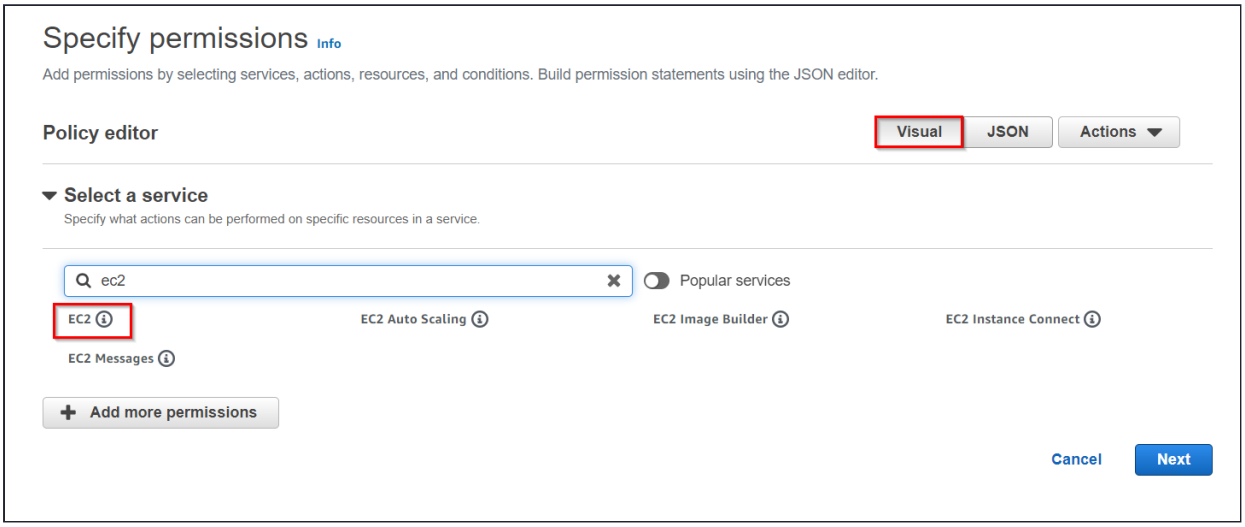
East (N. Virginia) us-east-1.

Note : If you face any issues, please go through **FAQs and Troubleshooting for Labs**.

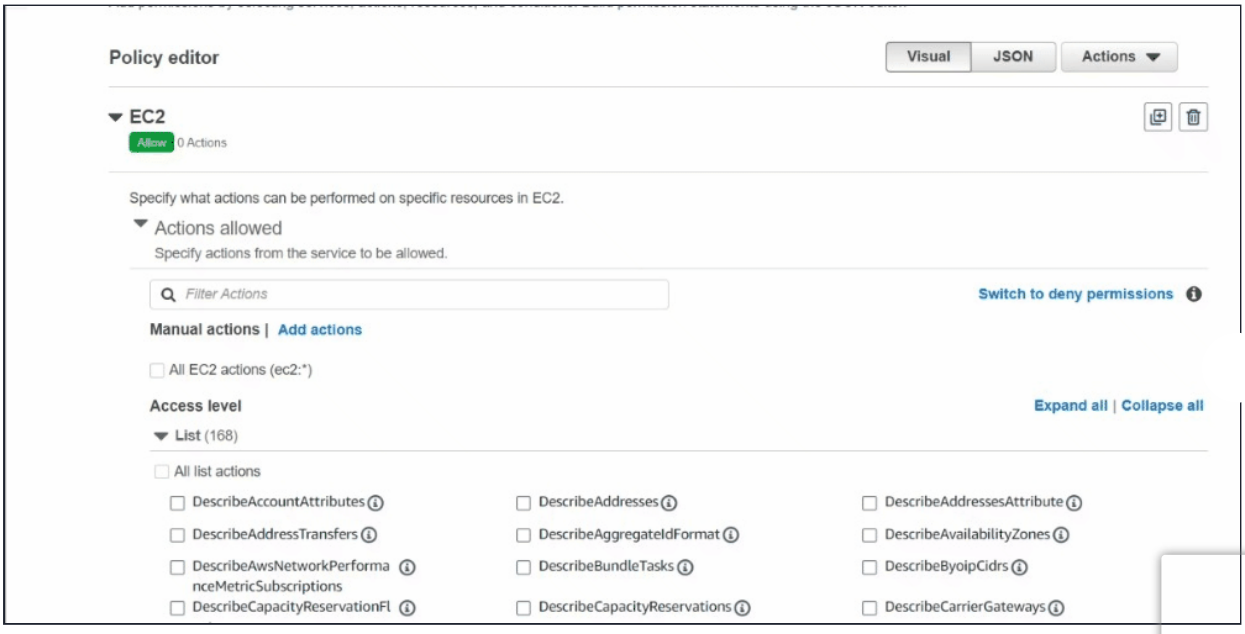
Task 2: Creating an IAM Policy for EC2

In this task, we are going to create an IAM policy specifically for the EC2 (Elastic Compute Cloud) service. EC2 is a core AWS service that provides virtual servers in the cloud. By creating an IAM policy for EC2, users can define the permissions and actions that are allowed or restricted for EC2 resources.

1. Navigate to the **Services** menu at the top, then click on **IAM** in the **Security, identity, & Compliance** section.
2. In the left menu, select **Policies**.
3. Click on **Create Policy** button.
4. Under **Visual**, Type **EC2** in the search box and select **EC2**.



5. In the **Actions**, specify the actions allowed in EC2. For this service, We'll choose **List.**
6. Click on **Resources,** scroll down and choose **All resources** so that there is no need to specify the resource ARN.

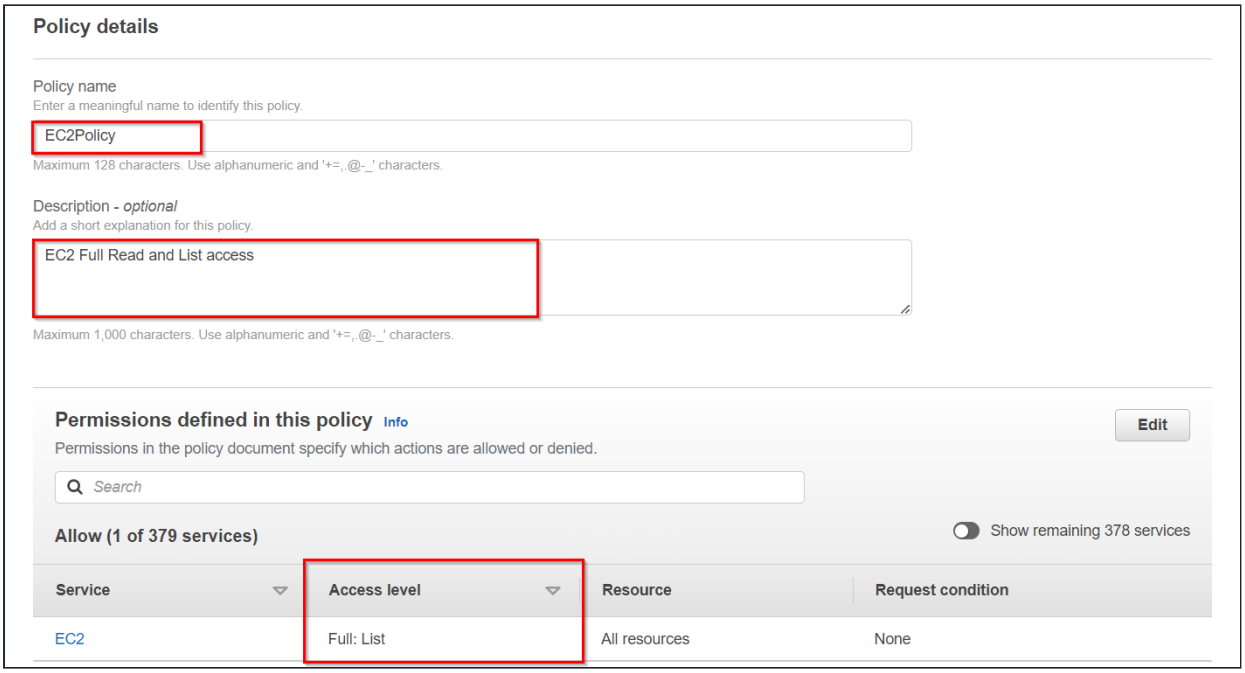


7. Now scroll up and If you click on the JSON, you can see the policy we created.

8. Click on **Next**

9. Review:

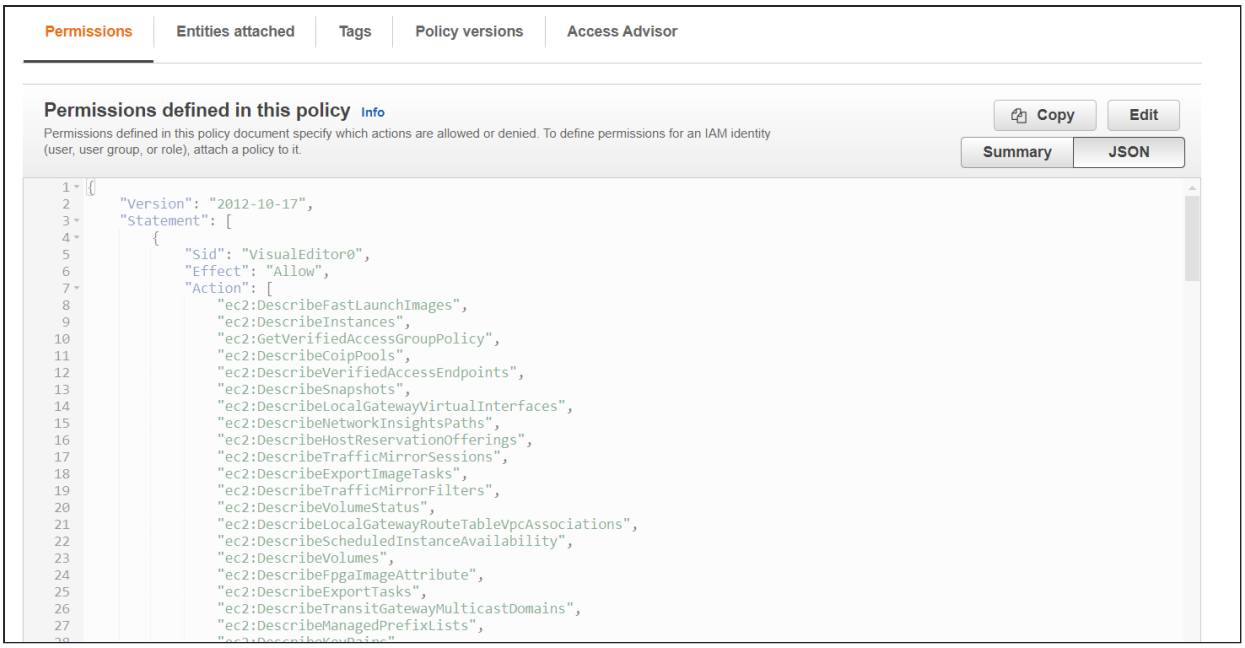
- Name : Enter **EC2Policy**
- Description : Enter **EC2 Full Read and List access**
- You can see the access level.
- Review the policy and then click on **Create policy**.



10. After creating, you will get a verification for the created Policy.

11. In the fiter policies, type your policy name and click on it.

12. In the Summary, (under the JSON) you can see the policy you created.



Task 3: Creating an IAM Policy for S3

In this task, we are going to create an IAM policy for the S3 (Simple Storage Service) service. S3 is a scalable storage service provided by AWS.

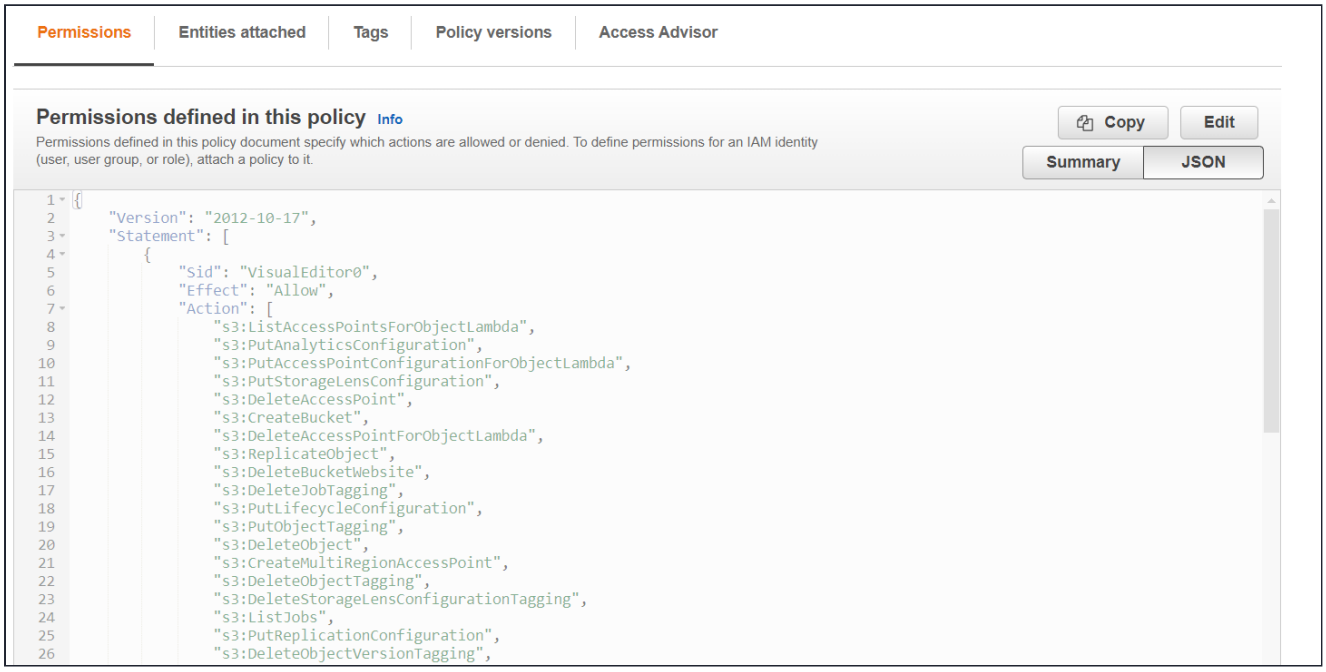
1. Click on **Create Policy** button again.
2. Under **Visual Editor**, type S3 in the search box and select **S3**.
3. In the **Actions**, specify the actions allowed in S3. For this service, we'll choose **List, Tagging** and **Write**.
4. Click on **Resources** and choose **All resources** so that there is no need to specify the resource ARN.

5. If you click on the JSON, you can see the policy we created.
6. Click on **Next** button.

7. Review:

    - Name : Enter **S3Policy**
    - For **Policy description**, type a description for the new policy.
    - In the Summary, you can see the Access level.
    - Review the policy and then click on **Create Policy**.

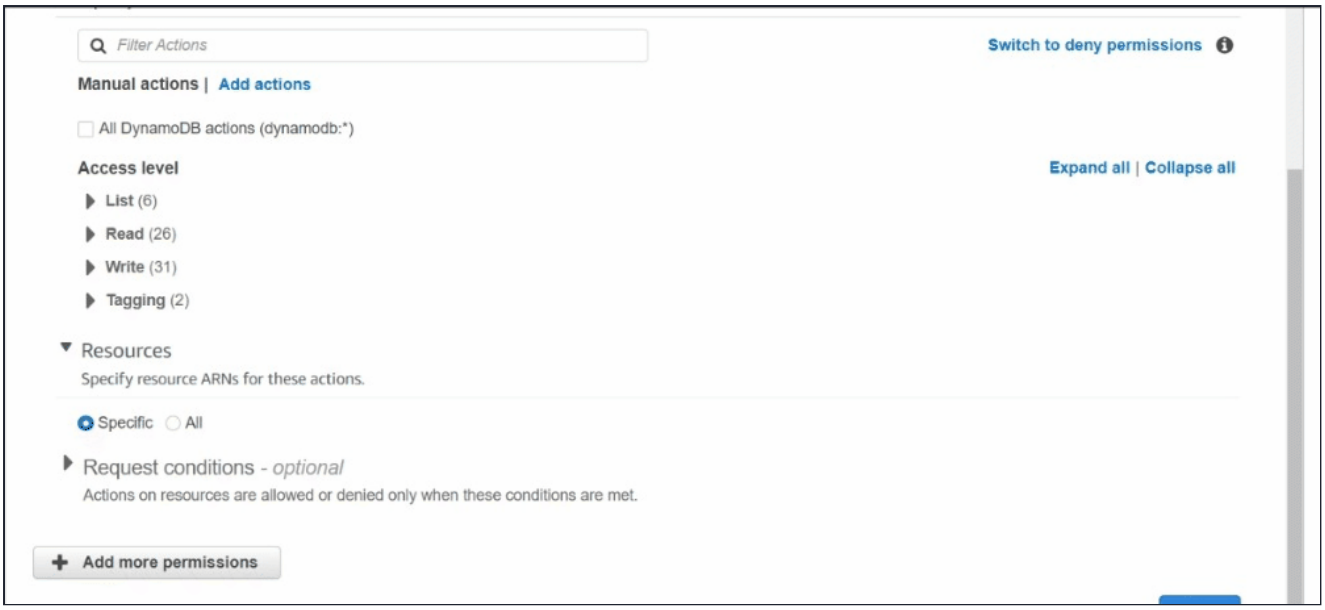
8. After creating, you will get a verification for the created policy
9. In the filter policies, type your policy name and click on it.
10. In the Summary, (under the JSON) you can see the policy you created.



Task 4: Creating an IAM Policy for DynamoDB

In this task, we are going to create an IAM policy for the DynamoDB service. DynamoDB is a fully managed NoSQL database service offered by AWS.

1. Click on **Create Policy** button again.
2. Under **Visual,** type **DynamoDB** in the search box and select **DynamoDB**.
3. In the **Actions**, specify the actions allowed in DynamoDB. For this service, we'll choose **All DynamoDB actions.**
4. Click on **Resources** and choose **All resources** so that there is no need to specify the resource ARN.



5. If you click on the **JSON** you can see the policy we created.
6. Click on **Next** button.
7. Review:
    - Name : Enter **DynamoDBPolicy**
    - For **Policy description**, type a description for the new policy.
    - In the Summary, you can see the Access level.
    - Review the policy and then click on **Create policy**.
8. After creating, you will get a verification for the created policy
9. In the filter policies, type your policy name and click on it.
10. In the Summary, (under the JSON) you can see the policy you created.

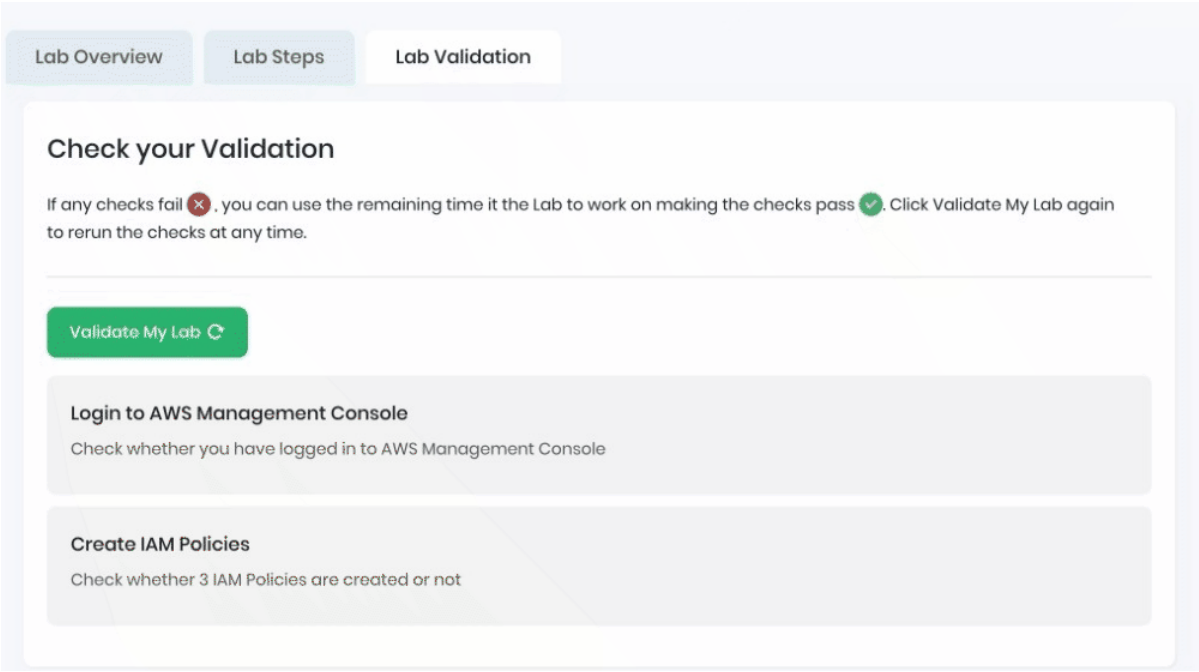
Do You know?

IAM policies are a powerful tool for managing access to AWS resources, and their default deny rule and support for conditions contribute to the robust security and access control capabilities of the AWS IAM system.

Task 5: Validation Test

1. Once the lab steps are completed, please click on the **Validation** button on the left side panel.

2. This will validate the resources in the AWS account and displays whether you have completed this lab successfully or not.
3. Sample output :



Completion and Conclusion

1. You have successfully created an IAM Policy for EC2 Service.
2. You have successfully created an IAM Policy for S3 Service.
3. You have successfully created an IAM Policy for DynamoDB service.

End Lab

1. Sign out of the AWS Account.
2. You have successfully completed the lab.
3. Once you have completed the steps, click on **End lab** from your whizlabs dashboard.