Home / AWS / Guided Lab / Creating IAM Roles

Creating IAM Roles

Level: **Fundamental**

Identity And Access Management Amazon Web Services

WHIZLABS

0 K

0h 29m 46s left

15 MIN

End Lab

Open Console

Validation

Lab Credentials

User Name

Whiz_User_80425.48589750

Password

dffb78ef-70e5-40f3-9939-1f4f492987a3

Access Key

AKIA4IVQUK3QAC4WYCPY

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 | Lab FAQs

Cloud Administrator

Security

Lab Steps

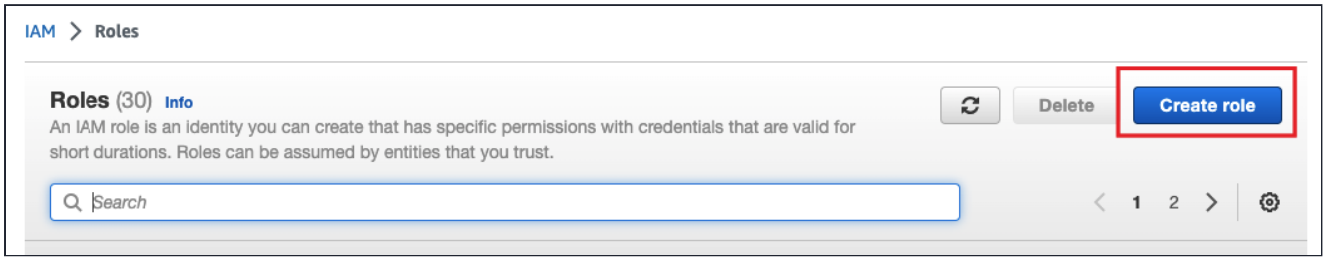
Task 1: Sign in to AWS Management Console

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.
    - 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.**

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

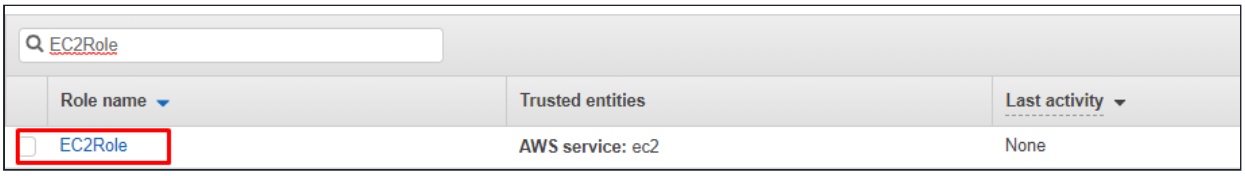
Task 2: Creating Role for an EC2 Service

1. Navigate to **IAM** by clicking on the **Services** menu at the top, then click on **IAM** in the **Security, identity, & Compliance** section.
2. In the left menu, select **Roles**.
3. Click on **Create Role** button.



1. **EC2** should be selected as the type of trusted entity under **Use Case**. Then click on **Next** button.
2. In Attach permissions policies, type **EC2** in the Filter Policies and select **AmazonEC2FullAccess**
3. **Note: Do not add other policies than the mentioned above. You will get an error while creating the Role.**
4. Then click on **Next** button
5. Review: Role name
6. Role Name : Enter ***EC2Role***
7. Review the role and then choose **Create role** button
8. After creating, you will get a verification for the created Role.

9. When searching for our role name, you will see the created role populate.

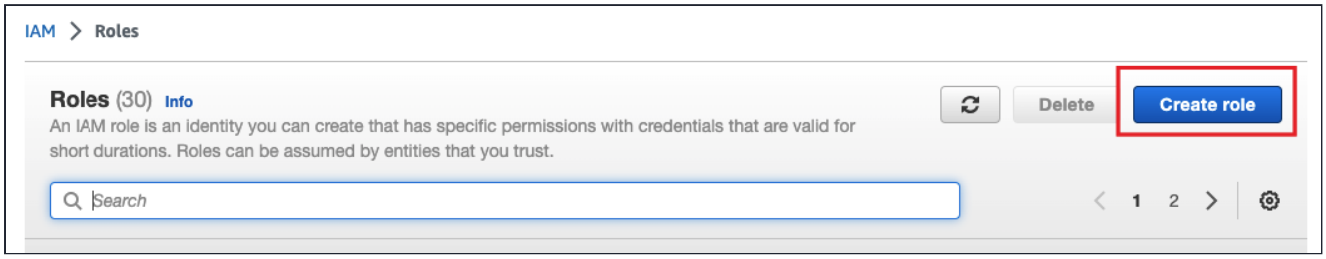


- When you set up an AWS service environment, you must define a role for the service to assume. You can attach this Role to the AWS services. This service role must include all the permissions required for the service to access the AWS resources that it needs.
- This allows EC2 to perform actions on our behalf.

Task 3: Creating Role for an AWS Service - DynamoDB

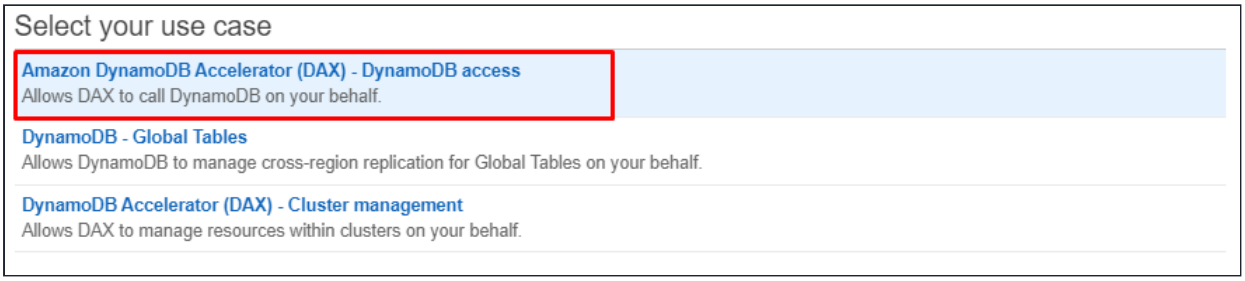
1. In the left menu, select **Roles.**

2. Click on **Create Role** button



3. For **DynamoDB** should be selected as the type of trusted entity under **Use Case.**

4. **Select the Use case as Amazon DynamoDB Accelerator (DAX) - DynamoDB access.**



5. Then click on **Next** button

6. In Attach permissions policies, you can see **AmazonDynamoDBFullAccess.**

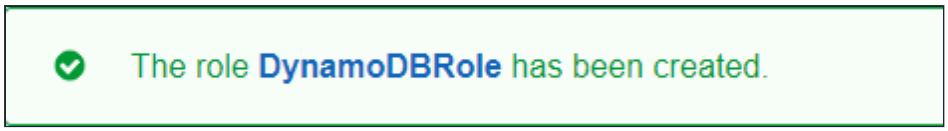
Note: Do not add other policies than the mentioned above. You will get an error while creating the Role.

7. Then click on **Next** button

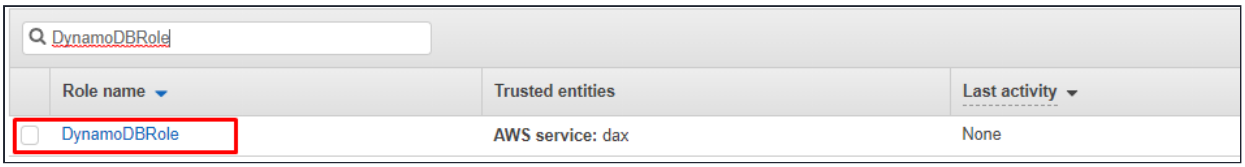
8. Review:

- Role Name : Enter ***DynamoDBRole***
- Review the role and then choose **Create role** button

9. After creating, you will get a verification for the created Role.



10. When searching for our role name, you will see the created role populate.



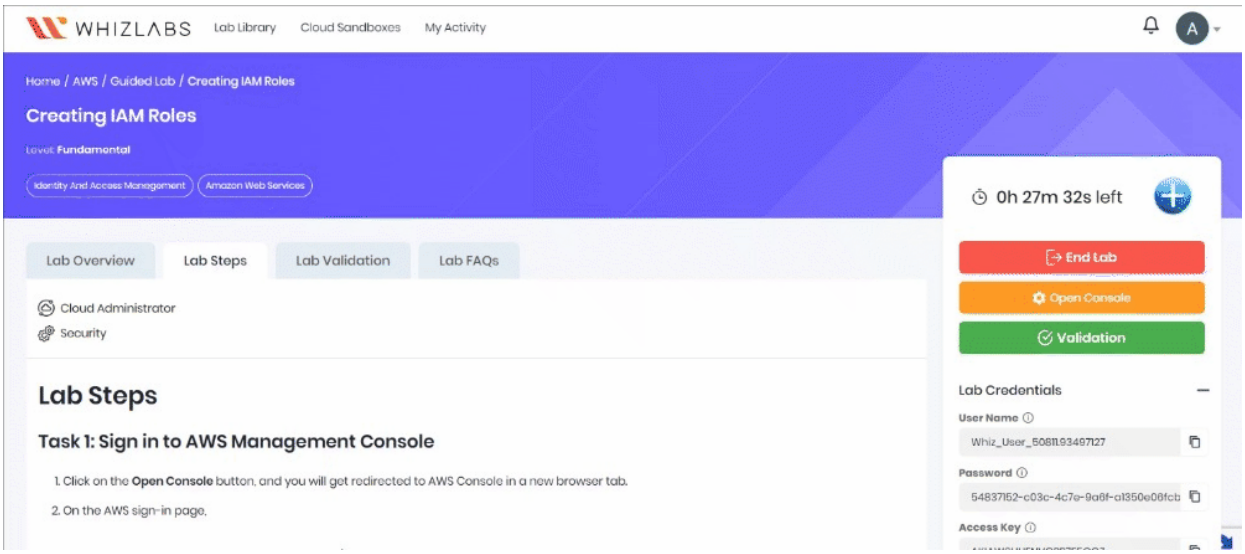
11. When you set up an AWS service environment, you must define a role for the service to assume.You can attach this Role to the AWS services. This service role must include all the permissions required for the service to access the AWS resources that it needs.
12. This allows DynamoDB to perform actions on our behalf.

Do you know ?

An IAM *role* is an IAM identity that you can create in your account that has specific permissions. An IAM role is similar to an IAM user, in that it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a role is intended to be assumable by anyone who needs it.

Task 4: Validation Test

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



Completion and Conclusion

1. You have successfully created an IAM Role for EC2 Service.
2. You have successfully created an IAM Role 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.