

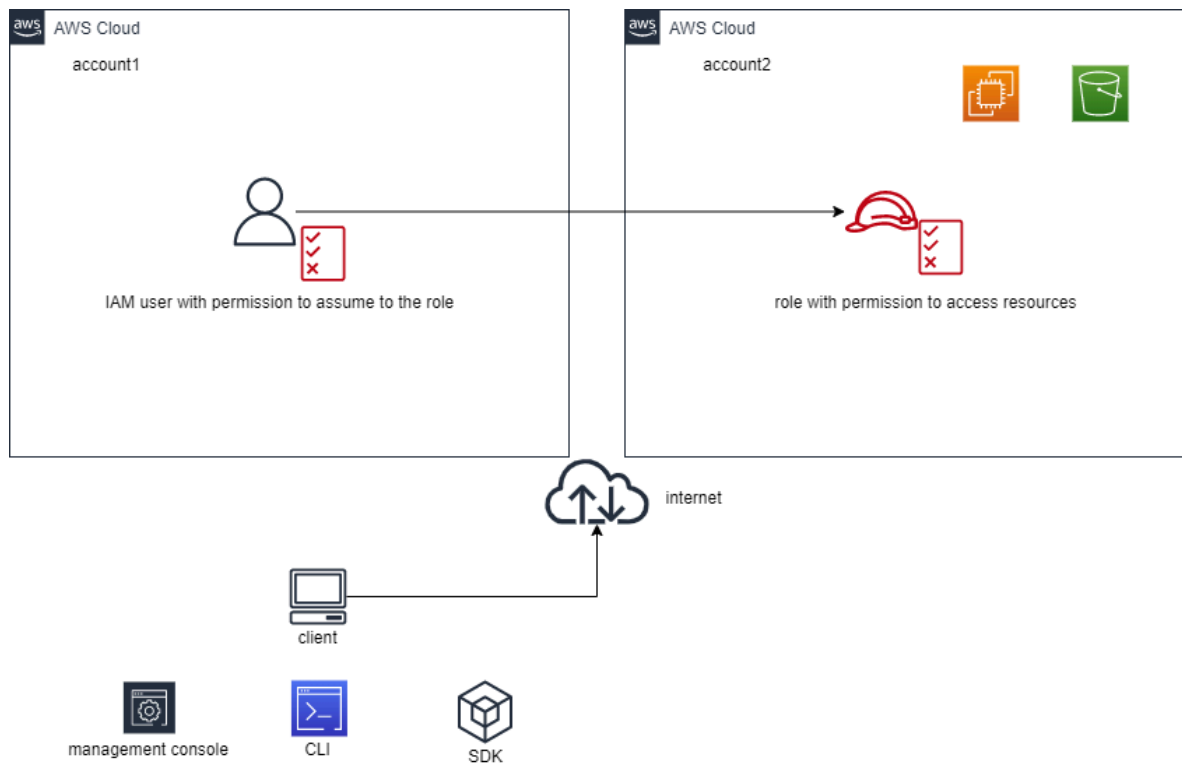
AWS Lab 37

Cross Account Access

Overview of the lab

In this lab you will learn how to access resource in one aws account from another aws account using switch role

Architecture



Step by Step Lab

(two aws account is needed for this lab)

Create a S3 bucket (config in account2)


1. In S3 click on [create bucket](#)
 - a. Bucket name - [jamesbond007](#) (should be unique name)
2. Click on [create bucket](#)

Create an IAM Role to access s3 (config in account2)

3. In IAM Click on [Roles](#) and [Create role](#)
 - a. Trusted entity type - [AWS account](#)
 - b. An AWS account - [Another AWS account](#)
 - i. Account ID - [123456789101](#) (account1 ID)
4. Click on [Next](#)
5. Permissions policies - Select - [AmazonS3FullAccess](#)
6. Click on [Next](#)
7. Role name - [account1-accessing-account2](#)
8. Click on [Create role](#)

Create an IAM user with Inline Permission to accessing resource in account2 (config in account1)

9. In IAM - Click on [Users](#) and [Create user](#)
-

- 
- a. User name - **developer1**
 - b. Select - **Provide user access to the AWS Management Console**
 - c. I want to create an IAM user
 - d. Console password - **Custom password**
 - e. Uncheck - **Users must create a new password at next sign-in**
10. Click on **Next**
 11. Click on **Next**
 12. Click on **Create user**
 13. Click **Return to users list** and **continue**
 14. Click on the username (**developer1**)
 15. In Permissions - **Add permissions** - Click on **Inline permission**
 16. Select **JSON** (remove the sample json / copy and paste the below policy and edit accordingly)

```
{  
  
  "Version": "2012-10-17",  
  
  "Statement": {  
  
    "Effect": "Allow",  
  
    "Action": "sts:AssumeRole",  
  
    "Resource": "arn:aws:iam::account-id:role/account1-accessing-account2*"  
  
  }  
  
}
```
-

17. Click on [Next](#)
18. Policy name - **cross-account-access**
19. Click on [Create policy](#)

Login as developer1 to switch role

20. Click on the username dropdown (right top)
21. Click on Switch role
 - a. Account ID - **098765432109** (account2 ID)
 - b. IAM role name - [account1-accessing-account2](#)
 - c. Display name - [cross-access](#)
 - d. Display color - [Yellow](#)
22. Click on [Switch role](#)

(now developer1 from account1 can access the s3 resource in account2)

Clean Up Step

(account1)

1. Delete the Role **account1-accessing-account2**
2. Delete the **S3 Bucket**

(account2)

3. Delete the **IAM user** and **Policy**
-