**Steps to grant an Amazon EC2 instance in Account A access to create volume in another account (Account B).**

**From Account B, create an IAM role**

1.    Sign in to the AWS Management Console with **Account B**.

2.    Open the [AWS Identity and Access Management (IAM) console](https://console.aws.amazon.com/iam/).

3.    In the navigation pane, choose **Roles**.

4.    Choose **Create role**.

5.    For **Select type of trusted entity**, choose **Another AWS account**.

6.    For **Account ID**, enter the account ID of Account A.

7.    Choose **Next: Permissions**.

8.    Attach a policy/create inline policy to the role that delegates access to Elastic block store volume.

"Version": "2012-10-17",

"Statement": [

{

"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": [

"ec2:CreateVolume",

"ec2:CreateSnapshot",

"ec2:AttachVolume",

"ec2:DetachVolume",

"ec2:ModifyVolume",

"ec2:DescribeAvailabilityZones",

"ec2:DescribeInstances",

"ec2:DescribeSnapshots",

"ec2:DescribeTags",

"ec2:DescribeVolumes",

"ec2:DescribeVolumesModifications",

"ec2:DeleteVolume"

],

"Resource": "\*"

}

]

}

9.    For **Role name**, enter a name for the role.

10.    Choose **Create role**.

**From Account B, get the role's ARN**

1.    From the IAM console's navigation pane, choose **Roles**.

2.    Choose the IAM role that you created.

3.    Note the value that's listed for **Role ARN**.

**From Account A, create another role (instance profile) and attach it to the instance**

1.    Sign in to the AWS Management Console with **Account A**.

2.    Open the (IAM) console.

3.    From the navigation pane, choose **Roles**.

4.    Choose **Create role**.

5.    For **Select type of trusted entity**, choose **AWS service**.

6.    For **Choose the service that will use this role**, choose **EC2**.

7.    Choose **Next: Permissions**.

8.    For **Role name**, enter a name for the role.

9.    Choose **Create role**.

10.    From the list of roles, choose the role that you just created.

11.    Choose **Add inline policy**, and then choose the **JSON** view.

12.    Enter the following policy.

Replace **arn:aws:iam::111111111111:role/ROLENAME** with the Amazon Resource Name (ARN) of the IAM role that you created in Account B.

{

"Version": "2012-10-17",

"Statement": [{

"Effect": "Allow",

"Action": "sts:AssumeRole",

"Resource": "arn:aws:iam::111111111111:role/ROLENAME"

}]

}

15.    Choose **Review policy**.

16.    For **Name**, enter a name for the policy.

17.    Choose **Create policy**.

18.   Attach IAM role (instance profile) to the Amazon EC2 instance that you use to create the volume in Account B.

**From the Amazon EC2 instance, create a profile for the role in the CLI config file**

1. Connect to the Amazon EC2 instance.
2. After you connect to the instance, verify if the directory already has a folder named **~/.aws**.

To find the **~/.aws** folder, run the following **ls** command to list the directory:

**ls -l ~/.aws**

1. If you find the **~/.aws** folder, then proceed to the next step. If the directory doesn't have a **~/.aws** folder yet, then create the folder by running the **mkdir** command:

**mkdir ~/.aws/**

1. Within the **~/.aws** folder, create a file and Name the file **config**.
2. In the file, enter the following text. Replace **enterprofilename** with the name of your choice. Then, replace **arn:aws:iam::111111111111:role/ROLENAME** with the ARN of the role that you created in Account B.

**[profile enterprofilename]**

**role\_arn = arn:aws:iam::111111111111:role/ROLENAME**

**credential\_source = Ec2InstanceMetadata**

6.    Save the file.

Verify that the instance profile can assume the role

To verify that your instance's role (instance profile) can assume the role in Account B, run the following command while connected to the instance.

**$aws sts get-caller-identity --profile profilename**

The command returns a response similar to the following:

"Account": "11111111111",

"UserId": "AROAEXAMPLEID:sessionName",

"Arn": "arn:aws:sts::111111111111:assumed-role/ROLENAME/sessionName"

Confirm that the value for **"Arn"** matches the ARN of the role that you created in Account B.

**To Create EBS volume use the following command**

aws ec2 create-volume \

--volume-type gp2 \

--size 1 \

--availability-zone ap-south-1a \

--region ap-south-1

--profile profilename

