



ACCESS TO S3 BUCKET FROM ANOTHER ACCOUNT

1. In this lab you have to use two accounts in order to access the S3 bucket and its objects.
2. Now you need to login with both of them in different browser.
3. You are going to command prompt, because this is how will access the buckets.
4. With that you need to create some policies to give access to your IAM user and the other account to connect with each other.
5. So, currently this is the policy which your IAM user has. But this version is now enough for you to give access.

Permissions defined in this policy [Info](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

[Copy](#) [Edit](#)

[Summary](#) [JSON](#)

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "VisualEditor0",  
6       "Effect": "Allow",  
7       "Action": "s3>ListAllMyBuckets",  
8       "Resource": "*"  
9     }  
10   ]  
11 }
```

6. Now click on policy versions then make another version as default which has more access over the buckets.

Permissions Entities attached Tags **Policy versions** Access Advisor

Versions of this policy [Info](#)

Each time you update a policy, you create a new version. You can have up to 5 versions of a customer managed policy.

[Set as default](#) [Delete](#)

<input type="checkbox"/>	Policy version	Creation time
<input type="checkbox"/>	Version 4	8 hours ago
<input type="checkbox"/>	Version 3	23 hours ago
<input checked="" type="checkbox"/>	Version 2 Default	23 hours ago
<input type="checkbox"/>	Version 1	23 hours ago

7. Then move to your other account then navigate to S3 and check whether it has buckets and some content in them.

Name	AWS Region	Access	Creation date
appbucket2000	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	August 17, 2023, 12:33:03 (UTC+04:00)
appbucket3000	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	August 17, 2023, 12:33:18 (UTC+04:00)
appbucket4000	Asia Pacific (Singapore) ap-southeast-1	Bucket and objects not public	August 17, 2023, 12:34:44 (UTC+04:00)
s3usrbucket	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	August 18, 2023, 18:44:38 (UTC+04:00)

8. Now go back to your root user this time and create a policy then attach it to the IAM user, this will give access to the user in the other account.
9. Now go to policies and click on create policies. Choose JSON and paste his code. This code will allow the user to get object and list object.
10. Then bucket name that you need to give should be from another account.
11. Then just give it a name and create your policy then attach it with the IAM user.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccountBucketAccess",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3>ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::appbucket4000",
        "arn:aws:s3:::appbucket4000/*"
      ]
    }
  ]
}
```

```
]  
}
```

12. Once your policy is attached, go to other account and select one of your buckets which name you have given while creating the policy.
13. Then in the bucket go to permissions.

The screenshot shows the AWS S3 console. In the top navigation bar, 'Amazon S3' is selected, followed by 'Buckets' and 'appbucket4000'. Below the navigation, the bucket name 'appbucket4000' is displayed with a blue 'Info' link. A horizontal menu bar contains six items: 'Objects', 'Properties', 'Permissions' (which is highlighted with a red border), 'Metrics', 'Management', and 'Access Points'. The 'Permissions' tab is currently active.

14. Then scroll down a little and click on edit bucket policy.

The screenshot shows the 'Bucket policy' editor. At the top, it says 'Bucket policy' and provides a brief description: '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.' Below this is a 'Learn more' link. There are two buttons at the top left: 'Edit' (which is highlighted with a red border) and 'Delete'. A cursor arrow points towards the 'Edit' button.

15. Now here you will add a JSON code. In this code you need to change the bucket name and ARN of the IAM user. Once you have done that you are good to go.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowobjectAccesssto3user",  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": "arn:aws:iam::213171387512:user/s3-usr01"  
            },  
            "Action": [  
                "s3:GetObject"  
            ],  
            "Resource": [  
                "arn:aws:s3:::appbucket4000/*"  
            ]  
    ]  
}
```

```

    },
    {
        "Sid": "AllowbucketAccesssto3User",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::213171387512:user/s3-usr01"
        },
        "Action": [
            "s3>ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::appbucket4000"
        ]
    }
]
}

```

16. After that you need to open command prompt and configure AWS.

```
C:\tmp>aws configure
AWS Access Key ID [*****5BGP]:
AWS Secret Access Key [*****NSvL]:
Default region name [ap-south-1]:
Default output format [None]:
```

17. Once you have configured now you need to try to access the bucket objects in your primary account and it should work properly.

```
C:\tmp>aws s3 ls s3://appbucket9000 --recursive
2023-08-20 18:07:31      253 01.sql
2023-08-20 18:07:31      477 02.sql
2023-08-21 12:16:05      290 03.sql
2023-08-20 18:07:46          0 scripts/
2023-08-20 18:07:57      290 scripts/03.sql
2023-08-20 18:07:58      385 scripts/04.sql
2023-08-20 18:07:59      567 scripts/05.sql
```

18. Now you need to try and access the bucket from other account. And you will see that it also works fine.

```
C:\tmp>aws s3 ls s3://appbucket4000 --recursive
2023-08-18 10:54:12      223 01.sql
2023-08-17 12:36:30          0 scripts/
2023-08-17 12:36:40      223 scripts/01.sql
2023-08-17 12:36:40      477 scripts/02.sql
2023-08-17 12:36:41      290 scripts/03.sql
2023-08-17 12:36:42      385 scripts/04.sql
2023-08-17 12:36:42      567 scripts/05.sql

C:\tmp>
```